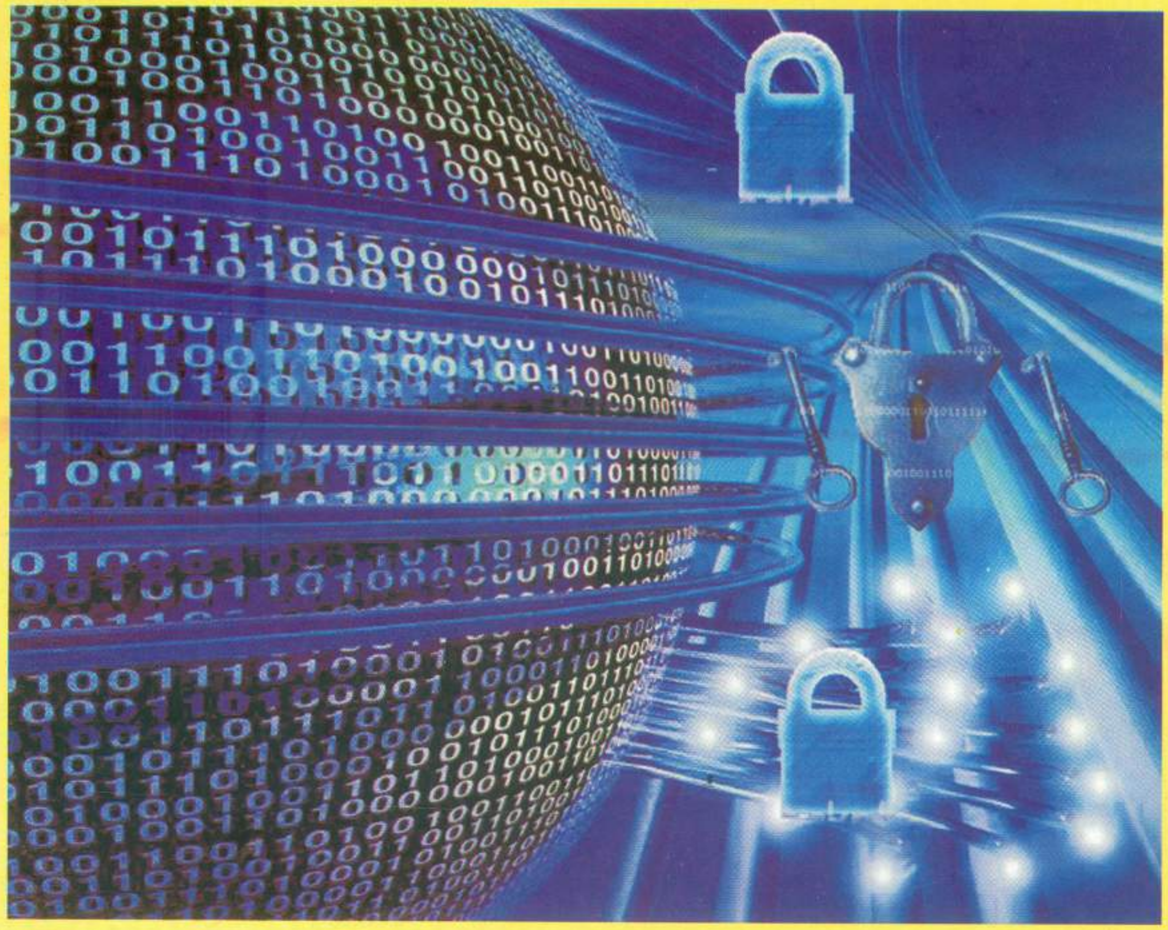
ignou
THE PEOPLE'S
UNIVERSITY

Indira Gandhi National Open University
School of Vocational Education and Training

MSEI-023
CYBER SECURITY



Information Gathering

1

"शिक्षा मानव को बन्धनों से मुक्त करती है और आज के युग में तो यह लोकतंत्रा की भावना का आधार भी है। जन्म तथा अन्य कारणों से उत्पन्न जाति एवं वर्गगत विषमताओं को दूर करते हुए मनुष्य को इन सबसे ऊपर उठाती है।"

- *इन्दिरा गाँधी*

"Education is a liberating force, and in our age it is also a democratising force, cutting across the barriers of caste and class, smoothing out inequalities imposed by birth and other circumstances."

- Indira Gandhi

ignou
THE PEOPLE'S
UNIVERSITY

Indira Gandhi National Open University
School of Vocational Education and Training

MSEI-023
Cyber Security

Block

1

INFORMATION GATHERING

Programme Expert/Design Committee of Post Graduate Diploma in Information Security (PGDIS)

Prof. K.R. Srivathsan
Pro Vice-Chancellor, IGNOU

Mr. B.J. Srinath, Sr. Director & Scientist 'G',CERT-In, Department of Information Technology, Ministry of Communication and Information Technology, Govt of India

Mr. A.S.A Krishnan, Director, Department of Information Technology, Cyber-Laws and E-Security Group, Ministry of Communication and Information Technology, Govt of India

Mr. S. Balasubramony, Dy. Superintendent of Police, CBI, Cyber Crime Investigation Cell Delhi.

Mr. B.V.C. Rao, Technical Director, National Informatics Centre, Ministry of Communication and Information Technology

Prof. M.N. Doja, Professor, Department of Computer Engineering, Jamia Milia Islamia New Delhi

Dr. D.K. Lobiyal, Associate Professor, School of Computer and Systems Sciences, JNU New Delhi

Mr. Omveer Singh, Scientist, CERT-In, Department of Information Technology, Cyber-Laws and E-Security Group, Ministry of Communication and Information Technology Govt of India

Dr. Vivek Mudgil, Director, Eninov Systems Noida

Mr. V.V.Subrahmanyam, Assistant Professor School of Computer and Information Science IGNOU

Mr. Anup Girdhar, CEO, Sedulity Solutions & Technologies, New Delhi

Prof. A.K. Saini, Professor, University School of Management Studies, Guru Gobind Singh Indraprastha University, Delhi

Mr. C.S. Rao, Technical Director in Cyber Security Division, National Informatics Centre Ministry of Communication and Information Technology

Prof. C.G Naidu, Director, School of Vocational Education & Training, IGNOU

Prof. Manohar Lal, Director, School of Computer and Information Science, IGNOU

Prof. K. Subramanian, Director, ACIIL, IGNOU Former Deputy Director General, National Informatics Centre, Ministry of Communication and Information Technology, Govt of India

Prof. K. Elumalai, Director, School of Law IGNOU

Dr. A. Murali M Rao, Joint Director, Computer Division, IGNOU

Mr. P.V. Suresh, Sr. Assistant Professor School of Computer and Information Science IGNOU

Ms. Mansi Sharma, Assistant professor, School of Law, IGNOU

Ms. Urshla Kant
Assistant Professor, School of Vocational Education & Training, IGNOU
Programme Coordinator

Block Preparation

Unit Writers

Mr. Anup Girdhar, CEO
Sedulity Solutions &
Technologies, New Delhi
(Unit 1, 2, 3 & 4)

Block Editor

Prof. K.R. Srivathsan
Pro Vice-Chancellor
IGNOU

Ms. Urshla Kant
Assistant Professor, School
of Vocational Education &
Training, IGNOU

Proof Reading

Ms. Urshla Kant
Assistant Professor
School of Vocational
Education & Training
IGNOU

Production

Mr. B. Natrajan
Dy. Registrar (Pub.)
MPDD, IGNOU, New Delhi

Mr. Jitender Sethi
Asstt. Registrar (Pub.)
MPDD, IGNOU, New Delhi

Mr. Hemant Parida
Proof Reader
MPDD, IGNOU, New Delhi

July, 2011

ISBN-978-81-266-5443-7

Further information about the School of Vocational Education and Training and the Indira Gandhi National Open University courses may be obtained from the University's office at Maidan Garhi, New Delhi-110068. or the website of IGNOU www.ignou.ac.in

Printed and published on behalf of the Indira Gandhi National Open University, New Delhi, by the Registrar, MPDD

Laser typeset by Mctronics Printographics, 27/3 Ward No. 1, Opp. Mother Dairy, Mehrauli, New Delhi-30

Printed by : A-One Offset Printers, 5/34, Kirti Nagar Indl. Area, New Delhi-110015

COURSE INTRODUCTION

This course of Cyber Security discusses in detail the concepts and terms of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In this age of technology and communication convergence, you can not help but be impacted by technologies and innovations that center on computers, cell phones and the Internet. But as we revolve our daily lives with these technologies, there are times that we set out to feel truly paranoid about our own safely.

This course helps to understand the process for protecting your personal information or any form of digital asset stored in your computer or in any digital memory device. The first thing that you'll have to realize is the forms of threats that you could encounter in cyber space. There are different forms of threats and each one has their own levels of seriousness which require their own levels of solutions. The higher degree the terror, the more advanced or complicated the approach to enforce safety measures to protect yourself.

This course concerns about the malware and spyware and define them properly for treating virus that can erase the whole contents of your computer and hackers that can access and use your personal data for their own personal gain. These are the dangers that are addressed in this course.

On the basis of these concepts and terminology relevant to cyber security, this course deals and highlight about these malevolent codes or malware which pass through your security system when you access a particular website or even when you open an email. These codes, exploit the loopholes in assorted applications and insert themselves within the computer system which enable them to copy and infect additional computers by attaching themselves to the emails that you send or through your local network. These malevolent codes are occasionally quite tricky. They claim to do something but instead they'll go on an altogether different path in infecting your system. These malevolent codes are not isolated to malware and spyware but as well refer to virus and worms which are deadlier and cause a lot of harm.

Even though those malicious codes are rather harmful, this course also explains another dangerous intruder which is none other than hackers or attackers. Regardless how you consider it, virus and worms can merely do what the original programmer has designated it to do. But hackers are people and they can get the information they want and utilize it for their own benefit. Sometimes hackers are just trying out their skills and intentionally invade your system not because they want your info for personal gain but because they're just plain curious or are just doing some mischief.

It is essential to know about cyber security in order to deal with such situations that you need to avoid and further to address the various threats. Students need to know how vulnerable computers are. This course is helpful to keep you ascertain in keeping check into firewall and virus protection software to see if your current system can prevent attacks. This course suggests students to continuously update software since new threats are being produced everyday and having an updated system could help protect computer from being attacked. Additional precautionary measures would be to make passwords. The passwords will serve as a deterrent and help you keep your entire system protected.

Further, with proper protection installed, you will be able to keep your files and data safe. It's very important that you keep in mind cyber security. Cyber security is all about keeping your data safe from those who wish to access them. It's an important facet of our lives and should never be dismissed above all in today's computer age.

This course includes the following blocks:

Block 1 - Information Gathering

Block 2 - Database Security

Block 3 - Web Technology

Block 4 - Internet technology

BLOCK INTRODUCTION

INFORMATION GATHERING is an Art of gathering the Information to determine the security posture of the target Profile of internet, remote access and intranet/ extranet, which is the first step of hacking. Information Gathering is being done in two major ways which are Foot Printing and Scanning. In Foot Printing and scanning, a cracker tries to gather the critical information of any enterprise/ organization like, Domain name, Network blocks, IP address reachable via internet, TCP and UDP services in each system, System architecture, Access control mechanisms, Intrusion detection systems, whois records, Location, contact names and email address , Security policies indicating the types of security mechanisms, Security configuration options for their firewall Comments in HTML source code, to identify the OS, TCP packets, Access Control Devices, to identify the versions of application and services, Port scanning etc. However, it should be noted that such kind of information could be gathered not only for the security purpose. In fact, it could also be gathered to make an external Cracking/Hacking attempts for misusing somebody's information using various techniques. This block comprises of four units and is designed in the following way;

The **Unit One** helps you by explaining the importance of Social Engineering in this Internet world. It states that along with the convenience and easy access to information, how does an attacker uses human interaction to obtain or compromise information about an organization or its computer systems. This unit continues by explaining with the countermeasures that will be benefitted for all the online users. It also, covered briefly about the Security Policies and Procedures for the organizations that should be implemented in order to fight against the social engineering attacks.

The **Unit two** covers that how the E-mail crimes are committed and what are the techniques to investigate whether a mail is a true or a fake mail. This unit will also explain the process of E-mail system i.e. how Email works and which protocols are responsible behind the E-Mail system. This unit explains that how could you trace a fake E-mail, its location and the IP as well. It will help you to understand the E-Mail header analysis and how the E-mail accounts could be secured from the external hacking attempts. By the end of this unit you'll learn major E-Mail related crimes and will be able to hands on various E-Mail tracing tools.

Reverse Engineering is a process where, a researcher gathers the technical data necessary for the documentation of the operation of a technology or component of a system. With the help of this research method researchers are able to examine the strength of the softwares, applications, systems etc. and identify their weaknesses in terms of performance, security, and interoperability. **Unit three** focuses on different types of stages Involved in the Reverse Engineering Process. It also explained the various tools & techniques that how Reverse Engineering could be implemented.

Unit four explains, about the various Cracking Methodologies and different techniques through which you could recover your passwords. This unit is meant to bring you closer to understand passwords in Windows operating system by addressing common password myths. This unit focuses the key elements of different password theft techniques and the process to recover Operating Systems and different application passwords in case if you forget or lost them due to any reason.

Hope you benefit from this block.

ACKNOWLEDGEMENT

The material we have used is purely for educational purposes. Every effort has been made to trace the copyright holders of material reproduced in this book. Should any infringement have occurred, the publishers and editors apologize and will be pleased to make the necessary corrections in future editions of this book.

UNIT 1 SOCIAL ENGINEERING

Structure

1.0 INTRODUCTION

Social Engineering

The Internet boom had its share of industrial engineering attacks during its initial phase, but now attacks generally focus on larger entities. In a social engineering, an attacker uses human interaction to obtain or compromise information about an organization or its computer systems.

An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network.

If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility. The basic goals of social engineering are the same as hacking in general: to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network. Typical targets include telephone companies and answering services, big-name corporations and financial institutions, military and government agencies, and hospitals.

In this Unit we'll understand the key elements that comprise a successful Social engineering and eventually apply these concepts to their own efforts.

Hacker utilizes social engineering many times because the human weakness factor is much easier to penetrate than the network weaknesses. Most of the times hackers "win" when it comes to the battle because they are not limited by time or lack of motivation. An IT Director/ or CTO of every organization works during the official working hours, however the hacker works 24 hours a day to accomplish his/her targets. As they spent the time and due attentiveness to research every aspect of the target, Hackers can launch every possible type of attack which also includes the Social Engineering. Obtaining personal information, password, remote user accounts etc. an attacker generally use such confidential information to launch technical attacks on the target.

1.1 OBJECTIVES

After going through this Unit, you should be able to:

- Types of Social Engineering;
- Behaviours vulnerable to attacks;
- Social Engineering: Threats and Defences;
- Countermeasures for Social engineering;
- Policies and Procedures;
- Impersonating Orkut, Facebook, MySpace & Identity Theft; and
- Countermeasures for Identity theft.

1.2 WHAT IS SOCIAL ENGINEERING?

Social Engineering is the act of manipulating a person to accomplish goals that may or may not be in the "target's" best interest. This may include obtaining information, gaining access, or getting the target to take certain action. Social engineering is generally a hacker's clever manipulation of the natural human tendency to trust. The hacker's goal is to obtain information that will allow him/ her to gain unauthorizePd access to a valued system and the information that resides on that system.

Security is all about trust. The weakest link in the security chain is, the natural human willingness to accept someone at his or her word leaves many of us vulnerable to attack. The Internet is a fertile ground for all social engineers looking to harvest passwords. The primary weakness is that many users often repeat the use of one simple password on every account like Yahoo, Gmail, rediff, Facebook, and even for their corporate Ids.

So once the hacker has got one password, he or she can probably get into multiple accounts. One way through which hackers have been known to obtain this kind of password is through an on-line form which they can send and ask the user to put in their User name, password & other important details. These forms can be sent through E-mail and seems to be the legitimate from the genuine source.

Every time you try to get someone to do something in your interest, you are engaging in social engineering. From children trying to get a toy from their parents to adults trying to land a job or score the big promotion, all of it is a form of social engineering in a way. Social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves deceiving other people to break normal security procedures. A person using social engineering to break into a computer network would try to gain the confidence of someone who is authorized to access the network in order to get them to reveal information that compromises the network's security. They might call the authorized employee with some kind of urgent problem; social engineers often rely on the natural helpfulness of people as well as on their weaknesses.

Another aspect of social engineering relies on people's inability to keep up with a culture that relies heavily on information technology. Social engineers rely on the fact that people are not aware of the value of the information they possess and are careless about protecting it. Frequently, social engineers search dumpsters for valuable information, memorize access codes by looking over someone's shoulder (shoulder surfing), or take advantage of people's natural inclination to choose passwords that are meaningful to them but can be easily guessed. Security experts propose that as our culture becomes more dependent on information, social engineering will remain the greatest threat, to any security system.

The goal of a Social Engineer is to trick someone into giving them what they want. The Social Engineer targets on qualities of human nature, such as:

- **The desire to be helpful:** Most of the employees are desirous to be helpful to others and this can lead to giving away too much information which could be very unsafe to the company.
- **A tendency to trust people:** Human nature is to actually trust others until they prove that they are not trustworthy. If someone tells something to a certain person, we usually accept that statement which might be incorrect and could lead towards a situation where, we might get stuck, or have to bear loss.
- **The fear of getting into trouble:** Most of us have seen negative situations in our life and want to get rid of such kind of situations. This is very common entry point of the Social Engineers to say something which might take you towards negative and troublesome situation and on the basis of that they try to fetch out the details.
- **The careless nature:** Sometimes we get lazy or careless and post the passwords on the screen in front of others or leave important material lying out, which ultimately help the Social Engineer to access the information.

The Art of Human Persuasion

Social engineering depends on an understanding of human behaviour, and on the ability to motivate others to release information or perform actions on the attacker's behalf. The hackers themselves teach social engineering from a psychological point-of-view, emphasizing how to create the perfect psychological environment for the attack. Basic methods of persuasion include: impersonation, ingratiation, conformity, diffusion of responsibility, and plain old friendliness. Regardless of the method used, the main objective is to convince the person disclosing the information that the social engineer is in fact a person that they can trust with that sensitive information. The other important key is to never ask for too much information at a time, but to ask for a little from each person in order to maintain the appearance of a comfortable relationship.

Studies show that humans have certain behavioural tendencies that are exploitable via careful manipulation. Some individuals possess a natural ability to manipulate, while others develop the skill through practice using positive (and negative) reinforcement. Social engineering attackers play on these tendencies and motivators to elicit certain responses in the target. For example:

- Fear of job loss or personal embarrassment may cause an individual to release proprietary information if he or she thinks it will prevent the unwanted result.
- Desire for prestige can be stimulated to induce bragging, often resulting in information release.
- Overworked and tired employees tend to make mistakes, and it's often possible to predict when people are more likely to be susceptible to manipulation (e.g., end of month, end of quarter or lunch hour).

1.3 BEHAVIOURS VULNERABLE TO SOCIAL ENGINEERING ATTACKS

All the security measures that the organization adopts go in vain when employees get "social engineered" by strangers. Some examples of social engineering include unwittingly answering the questions of strangers, replying to spam email, and bragging to co-workers.

Most often, people are not even aware of a security lapse on their part. Chances are that they divulge information to a potential hacker inadvertently. Attackers take special interest in developing social engineering skills, and can be so proficient that their victims might not even realize that they have been scammed. Despite having security policies in place, organization can be compromised because social engineering attacks target on the human tendency to be helpful.

Attackers are always looking for new ways to gather information, they ensure that they know the perimeter and the people on the perimeter-security guards, receptionists, and help desk workers-in order to exploit human oversight. People have been conditioned not to be overly suspicious; they associate certain behaviour and appearances with known entities.

For instance, upon seeing a man dressed in a uniform and carrying a stack packages for delivery, any individual would take him to be a delivery person. Companies list their employee IDs, names and email addresses on their official websites. Alternatively, a corporation may put advertisements in the paper for high-tech workers who trained on Oracle databases or UNIX servers. These bits of information help attackers know what kind of system they're tackling. This overlaps with the reconnaissance phase.

1.3.1 Targets

The basic goals of social engineering are same as hacking in general to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network. Typical targets include telephone companies and answering services, big-name corporations and financial institutions, military and government agencies, and hospitals.

Anything that stores or accesses information is vulnerable to a social engineering attack, and no person at any level of the enterprise is safe. While an old invoice or phone list may not seem dangerous in itself however, the attacker can use this information to develop a relationship by showing "inside" knowledge as a way of gaining short-term trust. Electronic systems are subject to direct attack or probing. Learning a system name or IP number may allow an attacker to present himself or herself as a network technician, and a large amount of information on your enterprise or personnel is probably available on the Internet in public or private databases. Social engineering attackers can often gain at least limited access to enterprise systems, even if it's just by looking over someone's shoulder during an on-site visit.

Every little scrap of information is valuable to an attacker. It's important to remember that social engineering attacks are cyclical, with attackers slowly gaining information with each cycle until they reach their target. Information can be public or private, sensitive or non-sensitive, secure or non-secure. Unfortunately, there are large amounts of information that are public, sensitive and non-secure, such as financial data, personal data (e.g., Social Security number, mother's maiden name and driver's license number), platform details for systems and networks, and leaked secret documents.

1.3.2 The Social Engineering Attack Cycle

While social engineering attacks are as varied as any criminal act, a common pattern has emerged that is often recognizable and preventable. This figure will help you to understand the Social Engineering Attack Cycle as follows:

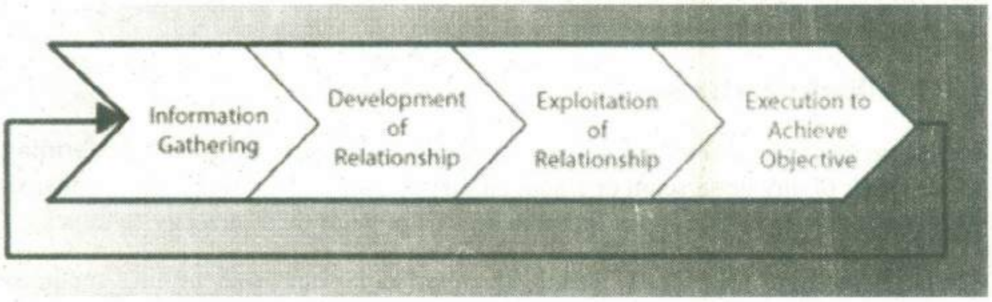

Information Gathering
Development of Relationship
Exploitation of Relationship
Execution to Achieve Objective

Fig. 1

1) **Information Gathering:** It is a technique by which we can gather the required information of a Target's system. Attackers use a variety of techniques to gather information about their targets. For example; if you want to hack www.anupgirdhar.net, then you must have an IP address or DNS to approach to this site. Once we get the IP address then we have to search the location for the target. Once you get the IP Address or DNS then we have to search the way to enter website or any destination. And so on... Few of the Techniques & tools which are generally used by the attackers are;

   - Ping Command
   - Email Bouncing Techniques
   - Netstat
   - Whois
   - Neo Trace Pro
   - http://visualroute.visualware.com
   - Nmap
   - Port Scan
   - Shadow Scan etc.

- Domain name lookup
- NSlookup

2) **Development of Relationship:** It's human nature to be somewhat trusting. Attackers exploit this tendency to develop a rapport with their targets. In some cases, this takes place in a single phone call; in others, it can span weeks or longer. By developing a relationship, attackers place themselves in a position of trust, which can then be exploited.

3) **Exploitation of Relationship:** The attacker exploits the target into revealing information (e.g., passwords, credit card numbers or vacation schedules) or performing an action (e.g., creating an account or reversing telephone charges) that would not normally occur. This information or action can be the end objective or can be used to stage the next attack/ phase of attack.

4) **Execution to Achieve Objective:** The attacker executes the cycle to achieve the end objective. Often an attack can include a number of these cycles, combined with traditional cracking methods and some physical information gathering, to achieve the end-to-end objective.

A series of small, apparently unrelated successes can form the base of a more-serious attack. As in our example, if hacking a website is a target, then all the information that you gather will be useful to make a solid attack in order to hack the website.

The gathered information can then be used to explore deeper into the enterprise, until finally attackers convince their targets to release the information they need to compromise the enterprise's security.

1.3.3 Adaptive Attacks

Social engineering attacks are as numerous and varied as the people performing them. Think of any good scam or fraud, and try to analyse, the root cause is always social engineering which helps the attackers to prepare their strategy to attack.

Although we can't list every possibility, there are some overarching methods commonly employed:

- **Playing the authority:** With some knowledge, attackers can impersonate authority figures and pressure or trick human targets.
- **Playing someone in need:** Humaηs have a tendency to help others in need, such as users having difficulty accessing their accounts. With a little research, attackers can learn enough information about a real user (e.g., employee number or manager) to fool the help desk into revealing a password.
- **Identity theft:** This is a rising problem for individuals and enterprises. Much of the information we use to identify ourselves to the world is easily available. It's not uncommon these days for criminals to obtain enough information about you to "steal" your identity, creating new bank or credit card accounts and accessing existing accounts.
- **Maintenance and support:** One of the easiest ways to gain access to an enterprise is to work there. While a new professional-level employee is noticeable, few enterprises pay attention to the cleaning staff, temporary workers, phone repairmen or maintenance employees who have full access to the premises.
- **Malicious software:** Many of the most-prolific viruses are actually social engineering attacks, such as "Melissa" or ILOVEU. These viruses only work

if users execute them on their system. Users are fooled into doing so by the compelling content of the e-mail, the subject line or because the assumed origin of the message is known and trusted.

- **Reverse social engineering:** This method involves attackers creating a reason for targets to contact them and reveal information, as shown in our opening example. Another common example is the many fraudulent E-mails on the Internet requesting credit card information for non-existent charities.

- **Research:** In the information age, there's very little about ourselves or who we work for that a good researcher can't find out. Everything from personal driving and credit history to corporate financial reports, and even network topography, are at risk.

Check Your Progress 1

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

What is Social Engineering? Describe any 3 tools of Information Gathering?

....

....

....

....

....

....

....

....

....

....

1.4 TYPES OF SOCIAL ENGINEERING

Social Engineering can be broadly divided into 2 different categories which are mentioned as below;

1) Human-based Social Engineering,

2) Computer-based Social Engineering.

Human-based social engineering involves human interaction in one manner or another, whereas computer-based social engineering depends on computers and Internet systems to carry out the targeted action.

1.4.1 Human-based Social Engineering

- **Posturing as an Authentic End User**

An attacker might use the technique of impersonating an employee, and then resorting to unusual methods to gain access to privileged data. He may give a fake identity and ask for sensitive information. Another example of this is that a "friend" of an employee might ask to retrieve information that a bedridden employee supposedly needs. There is a well-recognized rule in social interaction that a favour brings a favour, even if the original "favour" is offered without a request from the recipient. This is known as reciprocation, where corporate environments deal with reciprocation on a daily basis.

Employees help one another, expecting a favour in return. Social engineers try to take advantage of this social trait via impersonation.

For Example:

"Hi! This is Anup, from HR Department. I have forgotten my password. Can I get it please?"

- **Posing as an Important User**

Impersonation is taken to a higher level by assuming the identity of an important employee in order to add an element of extortion. The reciprocation factor also plays a role in this scenario where lower-level employees might go out of their way to help a higher-level employee, so that their favour gets the positive attention needed to help them in the corporate environment. Another behavioural tendency that aids a social engineer is people's inclination not to question authority.

Frequently people will do something outside their routine for someone they perceive to be in authority. An attacker posing as an important individual such as a Director or Vice-President, can often manipulate an unprepared employee. This technique assumes greater significance when considering that the attacker may consider it a challenge to get away with impersonating an authority figure.

For example, a help desk employee is less likely to turn down a request from a vice president who says he/she is pressed for time and needs to get some important information needed for a meeting. Social engineer may use authority to intimidate or may even threaten to report employees to their supervisor if they do not provide the requested information.

Example:

"Hi! This is Anup, CFO Secretary. I'm working on an urgent project, and lost the system password. Can you help me out - it's very urgent?"

- **Posing as Technical Support**

Another technique involves an attacker masked as a technical support person, particularly when the victim is not proficient in technical areas. The attacker may pose as a hardware vendor, a technician, or a computer-accessories supplier when approaching the victim. The unsuspecting user, especially who is not Tech savvy will probably not even ask questions or watch while the computer is taken over by the so called "Technical Support Person".

- **In person**

Attackers might try to visit a target site and physically survey the organization for information. A great deal of information can be gleaned from the tops of desks, the trash, or even phone directories and nameplates. Hackers may disguise themselves as a courier or delivery person, a custodian, or they may hang out as a visitor in the lobby. Hackers can pose as a businessperson, client, or technician. Once inside, attackers can look for passwords on terminals, important papers lying on desks, or they may even try to overhear confidential conversations.

Social engineering in person includes survey of a target company to collect information of:

- Current technologies implemented in the company
- Contact information of employees etc.

- **Third-party Authorization**

Another popular technique for attackers is to represent themselves as agents authorized by some authority figures to obtain information on their behalf. For instance, knowing who is responsible to grant access to desired information, an attacker might keep tabs on him/her and use the individual's absence to leverage access to the needed data. The attacker might approach the help desk or other personnel claiming he/she has approval to access this information. This can be particularly effective if the person is on vacation or out of town, and verification is not instantly possible.

Even though there might be a hint of suspicion on the authenticity of the request, people tend to stumble on the side of being helpful in the workplace. People tend to believe that others are expressing their true attitudes when they make a statement.

Refer to an important person in the organization to try to collect data

"Mr. Anup, our Finance Manager, asked that I pick up the audit reports he needs for his report. Will you please provide them to me?"

- **Tailgating**
  - An unauthorized person, wearing a fake ID badge, enters a secured area by closely following an authorized person through a door requiring key access.
  - An authorized person may not be aware of having provided an unauthorized person access to a secured area.

- **Piggybacking**

"I forgot my ID badge at home. Please help me..."

An authorized person provides access to an unauthorized person by keeping the secured door open.

- **Reverse Social Engineering**

In reverse social engineering, a perpetrator assumes the role of a person in authority and has employees asking him/ her for information. The attacker usually manipulates the types of questions asked to get required information. The social engineer will first create a problem, and then present himself/herself as the expert of such problem through general conversation, encouraging employees to ask for solutions. For example, an employee may ask about how this problem has affected particular files, servers, or equipment. This provides relevant information to the social engineer. Many different skills and experiences are required to carry out this tactic successfully.

- **Sabotage**

Once the attacker gains access, the workstation will be corrupted or will appear to be corrupted. Under such circumstances, users seek help as they face problems.

- **Marketing**

In order to ensure that the user calls the attacker, the attacker must advertise. The attacker can do this by either leaving his/her business cards around the target's office and/or by placing his/her contact number on the error message itself.

- **Support**

Although the attacker has already acquired needed information, he or she may continue to provide assistance to users so that they remain ignorant about the hacker's identity.

- **Service Desk**

The service desk or Help Desk is one of the support defences against hackers, but it is, conversely, a target for social engineering hackers. Although support staff is often aware of the threat of hacking, they also train to help and support callers, offering them advice and solving their problems. Sometimes the enthusiasm demonstrated by technical support staff in providing a solution overrides their commitment to adherence to security procedures and presents service desk staff with a dilemma: If they enforce strict security standards, asking for proofs that validate that the request or question comes from an authorized user, they may appear unhelpful or even disruptive. Production or sales and marketing staffs who feel that the IT department is not providing the immediate service that they require are apt to complain, and senior managers asked to prove their identities are often less than sympathetic to the support staff's thoroughness.

- **Waste Management Threats**

Business paper waste can contain information that is of immediate benefit to a hacker, such as discarded account numbers and user IDs, or can serve as background information, for example telephone lists and organization charts. This latter type of information is invaluable to a social engineering hacker, because it makes him or her appear credible when launching an attack. For example, if the hacker appears to have a good working knowledge of the staff in a company department, he or she will probably be more successful when making an approach; most staff will assume that someone who knows a lot about the company must be a valid employee.

Electronic media can be even more useful. If companies do not have waste management rules that include disposal of redundant media, it is possible to find all sorts of information on discarded hard disk drives, CDs, and DVDs. The robust nature of fixed and removable media means that those responsible for IT security must stipulate media management policies that include wiping or destruction instructions.

- **Personal Approaches**

The simplest and cheapest way for a hacker to get information is for them to ask for it directly. This approach may seem crude and obvious, but it has been the bedrock of confidence tricks since time began. Four main approaches prove successful for social engineers:

  - **Intimidation:** This approach may involve the impersonation of an authority figure to coerce a target to comply with a request.
  - **Persuasion:** The most common forms of persuasion include flattery or name dropping.
  - **Ingratiation:** This approach is usually a more long term ploy, in which a subordinate or peer co-worker builds a relationship to gain trust and, eventually, information from a target.
  - **Assistance:** In this approach, the hacker offers to help the target. The assistance will ultimately require the target to divulge personal information that will enable the hacker to steal the target's identity.

Most people assume that anyone who talks to them are being truthful, which is interesting because it is a fact that most people admit that they will tell lies themselves.

- **Virtual Approaches**

Social engineering hackers need to make contact with their targets to make their attacks. Most commonly, this will take place through some electronic medium, such as an e-mail message or a pop-up window. The volume of junk and spam mail that arrives in most personal mailboxes has made this method of attack less successful, as users become more skeptical of chain mail and conspiratorial requests to take part in "legal" and lucrative financial transactions. Despite this, the volume of such mail and the use of Trojan horse mail engines mean that it remains attractive, with only a minimal success rate, to some hackers. Most of these attacks are personal and aim to discover information about the target's identity. However, for businesses, the widespread abuse of business systems, such as computers and Internet access, for personal use means that hackers can enter the corporate network.

Telephones offer a more personal, lower-volume method of approach. The limited risk of arrest means that some hackers use the telephone as a means of approach, but this approach is primarily for PBX and service desk attacks; most users would be dubious about a call requesting information from someone that they did not know personally.

- **Insider Attack**

60% of attacks in organization are done by insiders. Insiders are employees of a company or person who has some trusted relation with that company. In this kind of attack the attacker uses some other person to implement the attack.

For eg:

A competitor can inflict damages to an organization by stealing sensitive data, and may eventually bring down an organization by gaining access to a company through a job opening by sending a malicious person as a candidate to be interviewed, and—with luck—hired. Other attacks may come from unhappy employees or contract workers. It takes just one disgruntled person to take revenge on a company by compromising its computer system.

1.4.2 Computer-based Social Engineering

Computer based social engineering is implemented by using software or programming applications like E-Mails, Virus, Trojan, Chatting, etc.

- **Pop-up Windows**

In this type of social engineering, a window appears on the screen informing the user that he/ she has lost his/her network connection and needs to re-enter his/ her username and password. A program that the intruder had previously installed will then email the information to a remote site. This type of attack is mainly done by using virus and trojans. The spyware can also perform this type of attack. The spyware will pretend to be an antivirus and will pop up a message to user that his/ her machine contains virus & in order to remove them, it needs username & password etc. When user enters that information it will then give a fake reply like virus removed and in backend it will send information to attacker.

- **Spam & E-Mail Attachments**

In this attack the user sends an email to victim in order to get information. for eg: The mail will declare that you have won a lottery of 20,000$ and then it will ask you to go to some link, where then it will ask you about your confidential information like bank account details so that delivery can be made. Attacker can also send an attachment along with email & that attachment can be Virus or Trojan. For eg: "Anna Kournikova" worm. Social engineers try to hide the file extension by giving the attachment a long file name. In this case, the attachment is named AnnaKournikova.jpg.vbs. If the name is truncated, it will look like a jpeg file and the user may not notice the .vbs extension.

- **Chatting/Instant Messaging**

Now a day, Chatting is quite popular medium of communication. People of almost all ages chat online. Usually it is very popular among the teenagers. Performing social engineering via chatting is quite easy.

Attacker just needs to chat with someone and then try to elicit the information. As chatting is informal way of communication which means attacker is not directly communicating with the person. Now due to this attacker can even tell lie to other person about his/ her identity etc., because victim can't see attacker without using webcam.

For instance: Usually what attacker does is, he/she chats with boys by behaving as a girl & vice-versa. By using fascinating picture during chatting attacker can lure any one. Display picture usually works like bait. Then slowly attacker will ask certain questions by which he/she can elicit information about the victim. This method is very dangerous because you would not even know when you got victim to social engineer.

- **Malicious Websites**

This involves a trick to get an unwitting user to disclose potentially sensitive data, such as the password used at work. Some methods include using advertisements that promote and display messages offering free gifts and holiday trips, and then asking for a respondent's contact email address, as well as asking the person to create a password. This password may be one that is similar, if not the same, as the one that the target user utilizes at work. Many employees enter the same password that they use at work, so the social engineer now has a valid username and password to enter into an organization's network.

Now a days many websites ask you to use your E-mail ID as Username while registering a new account. Then it asks to create a new password. Many times some peoples (newbies) get fooled they enter the same password that they are using with that email account..!! Beware about this; some attacker can fool you by Phishing.

- **Private Branch Exchange**

There are three major goals for a hacker who attacks a PBX:

- Request information, usually through the imitation of a legitimate user, either to access the telephone system itself or to gain remote access to computer systems.
- Gain access to "free" telephone usage.
- Gain access to communications network.

Each of these goals is a variation on a theme, with the hacker calling the company and attempting to get telephone numbers that provide access directly to a PBX or through a PBX to the public telephone network. The hacker term for this is phreaking. The most common approach is for the hacker to pretend to be a telephone engineer, requesting either an outside line or a password to analyze and resolve the problems reported on the internal telephone system.

Requests for information or access over the telephone are a relatively risk-free form of attack. If the target becomes suspicious or refuses to comply with a request, the hacker can simply hang up. But realize that such attacks are more sophisticated than a hacker simply calling a company and asking for a user ID and password. The hacker usually presents a scenario, asking for or offering help, before the request for personal or business information happens, almost as an afterthought.

1.5 DESIGNING DEFENCES AGAINST SOCIAL ENGINEERING THREATS

Prevention includes educating people about the value of information, training them to protect it, and increasing people's awareness, of how social engineers operate. After understanding the wide range of threats that exists, three steps are necessary to design a defence against social engineering threats against the staff within your company. An effective defence is a function of planning. Often defences are reactive—you discover a successful attack and erect a barrier to ensure that the problem cannot reoccur. Although this approach demonstrates a level of awareness, the solution comes too late if the problem is a major or expensive one. To pre-empt this scenario, you must take the following three steps:

- **Develop a security management framework.** You must define a set of social engineering security goals and staff members who are responsible for the delivery of these goals.
- **Undertake risk management assessments.** Similar threats do not present the same level of risk to different companies. You must review each of the social engineering threats and rationalize the danger that each presents to your organization.
- **Implement social engineering defences within your security policy.** Develop a written set of policies and procedures that stipulate how your staff should manage situations that may be social engineering attacks. This step assumes the existence of a security policy, outside the threat presented by social engineering. If you do not currently have a security policy, then you need to develop one. The elements identified by your social engineering risk assessment will get you started, but you will need to look at other potential threats.

1.5.1 Developing a Security Management Framework

A security management framework defines an overall view of the possible threats to your organization from social engineering and allocates named job roles responsible for the development of policies and procedures that mitigate these threats. This approach does not mean that you have to employ a staff whose only function is to ensure the security of business assets. Although such an approach may be an option within large organizations, it is seldom viable or desirable to have such roles within mid-sized organizations.

The requirement is to make sure that a group of people take on the key responsibilities of the following security roles:

- **Security sponsor.** A senior manager, probably board-level, who can provide the necessary authority to ensure that all staff take the business of security seriously.
- **Security manager.** A management-level employee who has responsibility for arranging the development and upkeep of a security policy.
- **IT security officer.** A technical staff member who has responsibility for developing the IT infrastructure and operational security policies and procedures.
- **Facilities security officer.** A member of the facilities team who is responsible for developing site and operational security policies and procedures.
- **Security awareness officer.** A management-level member of staff-often from within the human resources or personnel development department-who is responsible for the development and execution of security awareness campaigns.

Attack vector	Describe company usage	Comments
Online		
E-mail	All users have Microsoft Outlook® on desktop computers.	
Internet	Mobile users have Outlook Web Access (OWA) in addition to Outlook client access.	There is currently no technological barrier implemented against pop-ups.
Pop-up applications		
Instant Messaging	The company allows unmanaged use of a variety of IM products.	
Telephone		
PBX		
Service Desk	Currently the "Service Desk" is a casual support function provided by the IT department.	We need to extend support provisions beyond the IT area.
Waste management		
Internal	All departments manage their own waste disposal.	
External	Dumpsters are placed outside the company site. Garbage collection is on Thursday.	We do not currently have any space for dumpsters within the site.
Personal approaches		
Physical Security		
Office security	All offices remain unlocked throughout the day.	25 percent of staff works from home. We have no written standards for home worker security.
Home workers	We have no protocols of home worker onsite maintenance.	
Other/Company-specific		
In-house franchisees	All catering is managed through a franchise.	We do not know anything about these staff, and there is no security policy for them.

When the Security Steering Committee has a good understanding of the vulnerabilities, it can develop a Company Social Engineering Attack Vector Vulnerabilities table (shown in the previous example). The table outlines the company's protocols in potentially vulnerable areas. Knowledge of the vulnerabilities enables the committee to develop a blueprint for the potential policy requirements.

The Security Steering Committee needs to first identify areas that may pose a risk to the company. This process should include all of the attack vectors identified within this paper and company-specific elements, such as use of public terminals or office management procedures.

1.5.2 Risk Assessment

All security requires you to assess the level of risk that an attack presents to your company. Although risk assessment needs to be thorough, it does not have to be time-consuming. Based on the work done in identifying the core elements of a security management framework by the Security Steering Committee, you can categorize and prioritize the risks.

The risk categories include:

- Confidential information
- Business credibility
- Business availability
- Resources
- Money

You set priorities by identification of the risk and calculation of the cost of mitigating the risk-if mitigating the risk is more expensive than the occurrence of the risk, it may not be justifiable. This risk assessment phase can be very useful in the final development of the security policy. For a company that expects no more than 10-15 visitors in an hour, there is no need to consider having anything more sophisticated than one receptionist, a sign-in book, and some numbered visitor badges.

But for a company that expects more than 100 visitors per hour, more reception staff or self-service registration terminals are necessary. Although the smaller company could not justify the costs of self-service registration terminals, the large one could not justify the cost of lost business due to lengthy delays.

Alternatively, a company that never has visitors or contract staff may feel that there is a minimal risk in leaving printed output in a central location while it awaits collection. However, a company with a large number of non-employee staff may feel that it can only circumvent the business risk presented by potentially confidential information lying in a printer by installing local print facilities at every desk. The company can obviate this risk by stipulating that a member of staff accompanies a visitor throughout their visit. This solution is far less expensive, except, possibly, in terms of staff time.

This group-the Security Steering Committee-represents the facilitators within the company. As the selected champions for security, the Security St^ering Committee needs to establish the core goals of the security management framework. Without a set of definable goals, it is difficult to encourage participation of other staff or to measure the success of the project. The initial task of the Security Steering Committee is to identify what social engineering vulnerabilities exist within the company. A simple table like the following one quickly enables you to develop a picture of these attack vectors.

1.5.3 Social Engineering in the Security Policy

A company's management and IT personnel must develop and help implement an effective security policy within the organization. Sometimes, the focus of a security policy is technological controls that will help protect against technological threats, such as viruses and worms. Technological controls help defend technologies, such as data files, program files, and operating systems. Social engineering defences must help anticipate generic social engineering assaults against staff members.

The Security Steering Committee has the core security areas and risk assessment for which it must delegate the development of procedure, process, and business documentation. The following table shows how the Security Steering Committee, with the assistance of interest groups, may define the documentation required to support the security policy.

Policy requirement	Procedure/document requirement
Written set of social engineering security policies	None
Changes to make policy compliance part of the standard employee contract	Wording for new contract requirements (Legal) New format for contractor contracts
Changes to make policy compliance part of the standard contractor contract	Wording for new contract requirements (Legal) New format for contractor contracts
Policy for visitor management	Procedure for visitor sign in and sign out Procedure for visitor accompaniment
Dumpster management guidelines	Procedure for waste paper disposal (see Data) Procedure for electronic media disposal (see Data)
Policy for the provision of data access	
Policy for waste paper management	
Policy for the management of electronic media waste materials	
Policy for Internet usage, with specific focus on what to do with unexpected dialog boxes	
Policy for user ID and password management - no writing passwords on a sticky note and attaching it to a screen, etc.	
Policy for the use of mobile computers outside the company	
Policy for managing issues when connecting to partner applications (banking, financial, buying, stock management)	

Check Your Progress 2

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

How attackers take the advantage of reverse social engineering?

....

....

....

....

....

....

....

....

....

....

1.6 IMPLEMENTING DEFENSES AGAINST SOCIAL ENGINEERING THREATS

Any social engineer may simply walk in and behave like an employee in an organization. Many companies do not require anyone to wear photo identification or only require visitors to wear a visitor's badge. To become an employee, a visitor simply has to remove the paper badge. The first step in social engineering defense is to ensure that only authorized persons should get the access granted to be in the facility. All visitors need to be escorted when they are inside the lobby area.

Employee identification is not just a security measure, however; it is a process to protect the employees in the work place. By ensuring that only authorized personnel are permitted access, the employees should have a safe work environment. Since there is neither hardware nor software available to protect an enterprise against social engineering, it is essential that good practices should be implemented. Some of those practices might include:

- Require somebody to perform service to show proper identification. Make certain that the reception area has been trained to verify all service personnel and there are procedures in place for the receptionist to summon assistance quickly. It should be impossible to gain entry to a company building or site without the proper authorization. Reception staff must be polite but firm when they deal with staff, contractors, and visitors. A few simple conditions within the company security policy will make it nearly impossible for a physical social engineering attack within the building.
- Establish a standard that passwords are never to be spoken over the phone. The telephone offers a unique attack vector for social engineering hackers. It is a familiar medium, but it is also impersonal, because the target cannot see the hacker. The most common approach is for the hacker to pretend to be an engineer, requesting password to analyze and resolve the problems reported on the internal system. When contacting the help desk to have a password reset, the organization should establish a set of phrases or words which should

be known only by the user. The help desk should then reset the password to one of those words. If the organizations strict security standards, asking for proofs over the phone that validate whether the request or question comes from an authorized user or not, the hackers may appear unhelpful or even obstructive.

- Implement a standard that prevents passwords from being left. Now a days most of the employees have around 8-10 access accounts and passwords on an average due to which, it is no longer possible to forbid the writing down of accounts and passwords. The new requirement should place the emphasis on the classification of passwords and confidential information and require the employees to treat them accordingly.

- Implement caller ID technology for the Help Desk and other support functions. Many facilities have different ring tones based on inter-office phone calls as opposed to calls that originate from outside. Employees need to be trained to not forward outside calls. Take down the name and number of the call and forward the message on to the proper person. The service desk needs to balance security with business efficiency, and as such security policies and procedures must support them. Proof of identification, such as providing an employee number, department, and manager name, will not be too much for a service desk analyst to request, as everyone knows these. But this proof may not be completely secure, because a hacker may have stolen this information.

- Invest in shredders and have one on every floor: Your staff must fully understand the implications of throwing waste paper or electronic media in a bin. After this waste moves outside your building, its ownership can become a matter of legal obscurity. Dumpster diving may not be deemed illegal in all circumstances, so you must ensure that you advise staff how to deal with waste materials. Always shred paper waste and wipe or destroy magnetic media. If any waste is too large or tough to put in a shredder, such as a telephone directory, or it is technically beyond the ability of a user to destroy it, you must develop specific protocol for disposal. You should also place trash dumpsters in a secure area that is inaccessible to the public.Every work area should have shredder in order to destroy all the papers completely. The size of the shredder should be based on how much confidential information is present in the office area. Eliminate confidential information collection bins.

1.6.1 Employee Education is the Key

To be effective, policies, procedures and standards must be taught and reinforced to the employees. This process must be ongoing and must not exceed 6 months between reinforcement times. It is not enough to just publish policies and expect them to read, understand and implement what is required. They need to be taught to emphasize what is important and how it will help them do their job. This training should begin at new employee orientation and continue through employment. When a person becomes an ex-employee, a final time of reinforcement should be done during the exit interview process.

Another method to keep employees informed and educated is to have a web page dedicated to security. It should be updated regularly and should contain new social engineering ploys. It could contain a "security tip of the day" and remind employees to look for typical social engineering signs. These signs might include such behaviors as:

- Refusal to give contact information

- Rushing the process

- Name-dropping

- Intimidation
- Small mistakes
- Requesting forbidden information or accesses

As part of this training or education process, reinforce a good catch. When an employee does the right thing, make sure they receive proper recognition. Train the employees on who to call if they suspect they are being social engineered. Apply technology where you can. Consider implementing trace calls if possible or at least caller ID where available. Control overseas long distance services to most phones. Ensure that physical security for the building and sensitive areas are effective.

1.6.2 Defense-in-Depth Layered Model

The defense-in-depth layered model categorizes the security solutions against attack routes—areas of weakness—that hackers may use to threaten your computer environment. Defense-in-depth model helps you to visualize the areas of your business that are under threat. The model is not specific to social engineering threats, but each of the layers should have social engineering defenses.

The overarching defenses in the model are security policies, procedures, and awareness. These defenses target staff within an organization, explaining what to do, when, why, and by whom. The remaining layers may fine-tune your defenses, but the essential protection comes from having a well-structured and well-known set of rules that protect your IT environment.

These security Solutions are as follows:

- **Policies, procedures, and awareness.** The written rules that you develop to manage all areas of security, and the education program that you put in place to help ensure that staff members know, understand, and implement these rules. An effective defense is a function of planning. Often defenses are considered to be re-active however, you discover a successful attack and erect a barrier to ensure that the problem cannot reoccur. Although this approach demonstrates a level of awareness, the solution comes too late if the problem is a major or expensive one. To prevent this scenario, a strong planning is required which could be implemented in case of any attack.
- **Physical security.** The barriers that manage access to your premises and resources. It is important to remember this latter element; if you place waste containers outside the company, for example, then they are outside the physical security of the company.
- **Data.** Your business information, account details, mail, and so on. When you consider social engineering threats, you must include both hard and soft copy materials in your data security planning.
- **Application.** The programs run by your users. You must address how social engineering hackers may subvert applications, such as e-mail or instant messaging.
- **Host.** The servers and client computers used within your organization. Help ensure that you protect users against direct attacks on these computers by defining strict guidelines on what software to use on business computers and how to manage security devices, such as user IDs and passwords.
- **Internal network.** The network through which your computer system communicates. It may be a local, wireless, or wide area network (WAN). The internal network has become less "internal" over the last few years, with home

and mobile working gaining in popularity. So, you must make sure that users understand what they must do to work securely in all networked environments.

- **Perimeter.** The contact point between your internal networks and external networks, such as the Internet or networks that belong to your business partners, perhaps as part of an extranet. Social engineering attacks often attempt to breach the perimeter to launch attacks on your data, applications, and hosts through your internal network.

Check Your Progress 3

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of this Unit.

What are the practices that could be implemented to protect an enterprise against social engineering?

....

....

....

....

....

....

....

....

....

....

1.7 COUNTERMEASURES

1.7.1 Training

Periodic training sessions must be conducted to increase awareness on social engineering. An effective training program must include security policies and techniques for improving awareness.

1.7.2 Password Policies

- Passwords must be changed frequently so that they would not be guessed easily by anyone.
- Passwords that are easy to guess should be avoided. Passwords can be guessed from.
- answers to social engineering questions such as, "Where were you born?" "What is your favourite movie?" or "What is the name of your pet?"
- User accounts must be blocked if a user makes a number of failed attempts to guess passwords.
- Length and Complexity of passwords is important.
- Many policies typically require a minimum a password length of 6 or 8 characters.

- It is helpful to also require the use of special characters and numbers, e.g. ar1f23#$g.
- Passwords must not be disclosed to any other person.

Password policies often include advice on proper password management such as:

- Never sharing a computer account.
- Never using the same password for more than one account.
- Never telling a password to anyone, including people who claim to be from customer service or security.
- Never writing down a password.
- Never communicate a password over telephone, email or instant messaging.
- Exercising caution while logging off or before leaving a computer unattended.
- Changing passwords whenever there is suspicion of they been compromised.

1.7.3 Operational Guidelines

Confidential information must always be protected from misuse. Measures must be taken to protect the misuse of sensitive data. Unauthorized users must not be given access to these resources.

1.7.4 Physical Security Policies

- Employees of a particular organization must be issued identification cards (ID cards), and perhaps uniforms, along with other access control measures.
- Visitors to an organization must be escorted into visitor rooms or lounges by office security or personnel.
- Certain areas of an organization must be restricted in order to prevent unauthorized users from accessing them.
- Old documents that might still contain some valuable information must be disposed off by using equipment such as paper shredders and burn bins. This can prevent dangers posed by such hacker techniques as dumpster diving
- Security personnel must be employed in an organization to protect people and property.
- Trained security personnel can be assisted by alarm systems, surveillance cameras, etc.

1.7.5 Classification of Information

Information has to be categorized on a priority basis as top secret, proprietary, for internal use only, for public use, etc.

Access privileges

Access privileges must be created for groups such as administrators, users and guests with proper authorization required. Access privileges are provided with respect to reading, writing, accessing files, directories, computers and peripheral devices.

Background checks of employees and proper termination process

Before hiring new employees, check their background for criminal activity. Follow a process for terminated employees, since they may pose a future threat to the security of an organization

Proper Incidence Response System

There should be proper guidelines to react in case of a social engineering attempt.

1.8 POLICIES AND PROCEDURES

No software or hardware security solutions can truly secure a corporate computing environment unless there is a sound security policy. Things such as acceptable Internet use policies should be clearly articulated to users. The security policy sets the standard for the level of security a corporate network will have. It also gives the network a security posture that can serve as a benchmark. This is even more critical when the security policy is formulated keeping in mind the threat a network might face from social engineering attempts. The security policy can provide guidelines to users who are in a quandary when they confront an attacker's con. The policy can spell out what information can and cannot be released. This should be well defined in advance by people who have seriously contemplated the value of such information.

Increasing employee awareness by laying down clear policies decreases the chance of an attacker wielding undue influence over an employee. Security policies should address such processes as access information control, account setup, approval access, changing passwords, and any other areas that might be susceptible to social engineering attempts. Additional areas to consider include methods for dealing with locks, IDs, the shredding of paper, etc.

The policy must have discipline built-in and, above all, it must be enforced. The policies must have a balancing effect so that the user approached will not go out of his/her way to assist the attacker or assume a different role when interacting with the attacker in person or on the phone. Users must be able to recognize what kind of information a social engineer can use and what kinds of conversations should be considered suspicious. Users must be able to identify confidential information and understand their responsibility towards protecting it. They also need to know when and how to refuse to divulge information from an inquirer with the assurance that management will support them.

1.8.1 Security Policies – Checklist

- **Account Setup:** There should be an appropriate security policy that new employees can familiarize themselves with regarding their responsibilities when using the computing infrastructure.

- **Password Change Policy:** The password policy should explicitly state that employees are required to use strong passwords and are encouraged to change them frequently.

  They should be made aware of the security implications, in case their password is compromised due to their negligence.

- **Help Desk Procedures:** There must be a standard procedure for employee verification before the help desk is allowed to give out passwords. A caller ID system on the phone is a good start so the help desk can identify where the call originates. The procedure could also require that the help desk call the employee back to verify his/her location. Another method would be to maintain an item of information that the employee would be required to know before the password was given out. Some organizations do not allow any passwords to be given out over the phone. The help desk must also know whom to contact in case of security emergencies.

- **Access Privileges:** There should be a specific procedure in place for how access is granted to various parts of the network. The procedure should state who is authorized to approve access and who can approve any exceptions.
- **Violations:** There should be a procedure for employees to report any violations to policy. They should be encouraged to report any suspicious activity and be assured that they will be supported for reporting a violation.
- **Employee Identification:** Employees should be required to wear picture ID badges. Any guest should be required to register and wear a temporary ID badge while in the building. Employees should be encouraged to challenge anyone without a badge.
- **Privacy Policy:** Company information should be protected. A policy should be in place stating that no one is to give out any more information than is necessary. A good policy would be to refer all surveys to a designated person. The policy should also contain procedures for escalating the request if someone is asking for more information than the employee is authorized to provide.
- **Paper Documents:** All confidential documents should be shredded or burned.
- **Physical Access Restriction:** Sensitive areas should be physically protected with limited access. Doors should be locked and access only granted to employees with a business purpose.
- **Virus Control:** Established procedures should be in place to take action and prevent the spread of viruses.

1.8.2 Prevention Techniques for Personal Defence

Following are the prevention techniques for personal defence:

1) We have to be suspicious of any e-mail with urgent requests for personal financial information or threats of termination of online accounts.

2) Unless the e-mail is digitally signed, you can't be sure it wasn't forged or "spoofed." because any one can mail it by any name hence when it is stating some important better to check for the full headers.

3) Phishers typically ask for information such as usernames, passwords, credit card numbers, social security numbers, etc. and such information normally won't be asked by the genuine organization online.

4) Phisher e-mails are typically not personalized, while valid messages from your bank or ecommerce company generally are.

   "Phisher e-mails start something like "Dear customer" but there are some attacks which are customized or more advance which uses your personal information and if the attack is specifically for you then it will be customize like our case study.

5) When contacting your financial institution, use only channels that you know from independent sources. (e.g., information on your bank card, hard-copy correspondence, or monthly account statement), and don't rely on links contained in e-mails, even if the sites looks genuine.

6) Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser. Check in the address bar URL must start with https:// instead of http://

7) Regularly log into your online accounts and change password frequently.

8) Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate.

9) Don't assume that you can correctly identify a website as legitimate just by looking at its general appearance.

10) Avoid filling out forms in e-mail messages or pop-up windows that ask for personal financial information because it might be used by spammers as well as phisher for future attack.

1.8.3 Counter Measures for the Organizations

Over the years much has been written about how users are the weakest link in security, and there are surely not many people who would disagree. Despite this, companies often under value the importance of educating personnel about the important security issues of the day. It is easy to see what the reasons might be; companies have spent considerable time and money deploying firewalls and other technical controls. This makes sense to IT staff and it is often what people expect IT to spend their time on.

1) **Well defined and documented security policy:** Documented and enforced security policies and security-awareness programs are the most critical component in any information-security program. Good policies and procedures aren't effective if they aren't taught and reinforced to employees. The policies need to be communicated to employees to emphasize their importance and then enforced by management. After receiving security-awareness training, employees will be committed to supporting the security policies of the organization.

2) **Acceptable usage Policy:** The corporate security policy should address how and when accounts are set-up and terminated, how often passwords are changes, who can access, what information and how violations or the policies are to be handled. Also, the help desk procedures for the previous tasks as well as identifying employees. For example using an employee number or other information to validate a password change. The destruction of paper documents and physical access restrictions are additional areas the security policy should address. Lastly, the policy should address technical areas such as use of modems and virus control.

3) **Personnel security:** A screening of prospective employees, contractor to ensure that they do not pose a security threat to the organization. One of the advantages of a strong security policy is that it removes the responsibility of employees to make judgment calls regarding a hacker's request. If the requested action is prohibited by the policy, the employee has guidelines for denying it.

4) **Information Access Control:** To prevent social engineering attacks, a company/organisation must know how to keep all it's information securely, and to prevent social engineering attacks, all the factors that lead to a successful social engineering attack must be countered like Password usage and guidelines for generating password, access authorization and accounting procedure, installation procedure etc.

   Automated password reset and synchronization tools can lift the responsibility of managing password from tech support and help desk without placing an undo burden on end user.

5) **Protection from Malware:** It is also one of the most important part of security which has to be provided by the technical team in their infrastructure like Spyware, virus, adware, Trojan etc using software systems. It is always recommended to implement strong security policies with the help of firewalls, antispyware and anti-virus software with regular updating of patches so that the data would not be stolen or misused by any anonymous person.

6) **Awareness and Education:** Giving education to the user about the common techniques employed and used by the social engineer is an important part of security system. For example, a knowledgeable user can be advised that he/she should never give out any information without the appropriate authorization and that he/she should report any suspicious behaviour. A good training and awareness program focusing on the type of behaviour required will undoubtedly pay for itself. By providing real incident example, social engineering can be implemented effectively in the system.

7) **Audits and compliance:** Policy gets effective only when it gets implemented and everyone conforms to the policy. Hence auditing the security policy usage and to make sure that everyone compliance to the rules as well.

8) **Security Incident Management:** When a social engineering attacks occurs make sure service desk staff knows how to manage such attack. As each attack is different, system will get new data and hence its need to be manages for future use. Hence reporting and storage of such incident should be done properly

Check Your Progress 4

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of this Unit.

Why password security is an important issue? Why the security policies should have the balancing effect?

....

....

....

....

....

....

....

....

....

....

1.9 IMPERSONATION

Impersonation is committed when an individual impersonates another and does an act in such assumed character with intent to obtain a benefit or to injure or defraud another. Impersonation is a part of a criminal act such as identity theft. This is usually happened where the criminal is trying to assume the identity of another, in order to commit fraud, such as accessing confidential information, or to gain property not belonging to them. It is also known as social engineering and impostors.

1.9.1 Impersonating on Orkut

Impersonation can be described as imitating or copying the behaviour or actions of other people. Orkut is a famous social networking site, and since it is open for all, anyone can use it as a social engineering tool to steal personal and corporate information and create the account on other's name. There are two common methods to hack a person's Orkut accounts:

- **Cookie Stealing:** Cookie stealing is done by using a simple JavaScript code with the support of a PHP program in the background. This script is sent to the victim through scraps and when the victim runs this code, his/her cookie is immediately sent to the attacker, using which attacker can get into the victim's account.
- **Phishing (Fake Page):** Fake Pages look like pages of Orkut; when user name and password is inserted into relevant fields, they are transferred to the email ID of the hacker.
- **MW.Orc worm:** The MW.Orc worm propagates through Orkut account and steals important information such as banking details, usernames, and passwords. After entering into the victim's machine, the worm launches an executable file. When the user clicks on this file, it installs two more files, i.e. winlogon_.jpg and wzip32.exe on the user's computer. Banking details and passwords are transmitted via e-mail to the worm creator when the victim user clicks on "My Computer" icon.

Apart from stealing victim's personal information, the malware enables the hacker to remotely control the victim's PC and make it a part of the infected PCs network. This network uses bandwidth to distribute large pirated movie files and thus brings down the connection speed. The victim is added to an XDCC Botnet that helps in file sharing and then the infected link is also sent to other users on Orkut network.

MW.Orc worm starts distributing itself automatically to other user's Orkut Scrapbook (guest book) for further infection where users can post comments that are visible to the user's page. The message has different links and can divert them to other sites and these users can also lose their critical data.

1.9.2 Impersonating on Facebook

Facebook is also a well-known social networking site that connects people around the globe. It is used to communicate with friends, share and upload unlimited images, links and videos. To impersonate, Facebook bloggers use nicknames instead of using their real names. Bloggers use fake accounts, which are a violation of Terms of Use. Facebook accounts need users to give their valid first and last names to avoid impersonation. The impostor tries and keeps on adding friends and uses other's profile to get critical and valuable information.

1.9.3 Impersonating on MySpace

On MySpace users can create a private community where they can share their photos, articles, likes and dislikes, and interests with friends. MySpace has also become an effective marketing tool where people post their details to:

- Talk online.
- Meet other singles.
- Connect their friends with other friends.
- Keep in touch, with your family.
- Meet business people and co-workers interested in networking.

Many people post their profiles on MySpace to gain exposure. Most of the profiles posted on MySpace are not genuine.

1.9.4 What is "Identity Theft"?

Identity theft is also known as ID theft, which is an online/ Cyber-Crime; in which a criminal obtains key pieces of personal information in order to pose as someone else. Identity theft is a serious problem that many online users face today. It happened because of Social Engineering, lost or stolen wallets, pilfered mail, a data breach, computer virus, phishing, a scam, or paper documents thrown out by an individual or a business.

Identity theft has become an epidemic in US, while in India the cases of identity theft are relatively low given the less number of online transactions and use of internet. While in India there is no reliable statistics available on the extent of identity theft, however it would be safe to assume a rapid escalation in identity theft cases with increase in the number of online banking and ecommerce transactions like online share transactions and owing to the fact that the customers are not technically adept with virtual world.

Examples of Identity Theft:

Few of the most common Identity Theft incidents; which have come into the picture are mentioned as below;

Online Fraudulent transactions of Shares & Commodities

Now a days, if you are associated with the stock market and make some transactions for buying and selling of shares then you must be aware of the online Shares & Commodity transactions, where you get a unique User Name & Password from your broker and you make the transactions online.

There are lot cases/ complainant registered where it has been found that their online share/commodity account has been compromised and fraudulent transactions has been executed by unknown fraudster which resulted in huge loss. The fraudster who are generally software experts or the executives (core dealers) at the broker office try to acquire the Client ID's from the broker office itself, and try hit & trial methods or social engineering for accessing the accounts. After acquiring the client Id & password, the fraudster makes unauthorized access to the client account and also accesses their own account in which the profits are to be transferred from the victim client account. The fraudster executes the transactions into the client accounts at unrealistic prices and match these transactions into their own account simultaneously. In this way, he shifts the profit to his own account and losses to the account of the unsuspecting clients.

Bank Phishing scams

Phishing is the biggest identity theft scam and is widely prevalent in India now a days. In some recent cases of phishing it has been found that, a fake Bank Web site was created and the bank customers received an E-mail asking them to renew certain services and claiming that failure to do so, would result in the suspension or deletion of their Net banking accounts/ services. The E-Mail contains a link to a phished website, in an illegal attempt to collect personal and account information

Nigerian 419 Scam or Advance Fee Fraud

There has been number of Cyber-Crime cases reported where the perpetrators of the fraud send E-Mail or a letter to the victim E-mail id or address requesting the help of the victim for retrieving huge blocked funds due to some problems and offer a healthy percentage of these funds as commission. The victim believing the fraudster in lure of receiving huge funds and pass on his credit card information, bank account details to fraudster which results in financial loss.

Defamation or posting of porn or obscene material on social networking sites

There are many cases registered, in which the victim have reported that their profile and personal information has been stolen and a fake & vulgar profile in his or her name containing pornography & obscene material along with the victims contact details like phone numbers & address has been posted on the social networking site like ORKUT.

Legal measures

Though in India Identity Theft has still not been made a standalone crime unlike USA, however there are various legal measures which has been taken by the India which are well defined in IPS and IT Act 200 as well. The offence of identity theft is committed by a series of act which attracts many penal provisions of present IPC & IT Act, 2000 which are as follows;

Section 419 IPC : When the fraudster by stolen identifying information impersonates the victim to commit fraud or cheating.

Section 420 IPC : When the fraudster deceive people into disclosing valuable personal data in the nature of identifiable information which is used later to swindle money from victim account.

Section 468 IPC : When the fraudster commits forgery of website which is in the nature of electronic record to lure the victims to pass their identifiable information in order to cheat them.

Section 471 IPC : When fraudster fraudulently or dishonestly uses as genuine, the aforesaid fake website in the nature of electronic record.

Section 66C IT Act : Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person. Penalty under this act is 3 years and 1 lakh.

Section 66D IT Act : Whoever, by means of any communication device or computer resource cheats by personation. Penalty under this act is 3 years and 1 lakh.

Section 66E IT Act : Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person. Penalty under this act is 3 years and 2 lakh.

Section 67 IT Act : Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it. Penalty under this act; **First Conviction** – 3years and 5 lakhs and **2nd or Subsequent Conviction** – 5 years or 10 lakhs.

Check Your Progress 5

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of this Unit.

What is impersonation? Describe it by giving an example.

....

....

....

....

....

....

....

....

....

....

1.10 LET US SUM UP

This unit deals with the "Social Engineering" the act of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques. However, an attacker, by asking questions, may be able to piece together enough information to infiltrate an organization's network.

Obtaining personal information, password, remote user accounts etc. an attacker generally use such confidential information to launch technical attacks on the target. The section recapitulates the bits of information help attackers know what kind of system they're tackling. Different types of social engineering and main approaches to prove successful for social engineers. It also deals with policy and procedures that give the network a security posture that can serve as a benchmark.

1.11 CHECK YOUR PROGRESS: THE KEY

1) Social Engineering is the act of manipulating a person to accomplish goals that may or may not be in the "target's" best interest. This may include obtaining information, gaining access, or getting the target to take certain action. Social engineering is generally a hacker's clever manipulation of the natural human tendency to trust. 3 tools of Information Gathering are 1.Netstat 2.Whois 3. Nmap

2) In reverse social engineering, a perpetrator assumes the role of a person in authority and has employees asking him/ her for information. The attacker usually manipulates the types of questions asked to get required information. The social engineer will first create a problem, and then present himself/ herself as the expert of such problem through general conversation, encouraging employees to ask for solutions.

   For example, an employee may ask about how this problem has affected particular files, servers, or equipment. This provides relevant information to the social engineer. Many different skills and experiences are required to carry out this tactic successfully

3) - Require somebody to verify the identification of all the visitors: Make certain that the reception area team has been trained properly to verify all

internal/external service personnel and there should be thorough procedures in place for the front desk team to call for assistance quickly.

- Establish a standard that passwords are never to be spoken over the phone.
- Implement a standard that forbids passwords from being left lying about. Because employees now average around eight access accounts and passwords, it is no longer possible to forbid the writing down of accounts and passwords.
- Implement caller ID technology for the Help Desk and other support functions. Many facilities have different ring tones based on inter-office phone calls as opposed to calls that originate from outside. Employees need to be trained to not forward outside calls. Take down the name and number of the call and forward the message on to the proper person.
- Invest in shredders and have one on every floor. Every work area needs a shredder. Eliminate confidential information collection bins. Require shredding, not storing.

4) Password Policy is a countermeasure.

- Passwords must be changed frequently so that they are not easy to guess.
- Passwords that are easy to guess should be avoided.
- User accounts must be blocked if a user makes a number of failed attempts to guess passwords.
- Length and Complexity of passwords is important.
- Passwords must not be disclosed to any other person.

The policies must have a balancing effect so that the user approached will not go out of his/her way to assist the attacker or assume a different role when interacting with the attacker in person or on the phone.

5) Impersonation can be described as imitating or copying the behaviour or actions of other people. Orkut is a famous social networking site, and since it is open for all, anyone can use it as a social engineering tool to steal personal and corporate information and create the account on other's name. There are two common methods to hack a person's Orkut accounts:

- **Cookie Stealing:** Cookie stealing is done by using a simple JavaScript code with the support of a PHP program in the background. This script is sent to the victim through scraps and when the victim runs this code, his/her cookie is immediately sent to the attacker, using which attacker can get into the victim's account.
- **Phishing (Fake Page):** Fake Pages look like pages of Orkut; when user name and password is inserted into relevant fields, they are transferred to the email ID of the hacker.

UNIT 2 E-MAIL CRIME & INVESTIGATION

Structure

2.0 INTRODUCTION

In today's electronic world, E-Mail is critical to any business being competitive. In most cases it now forms the backbone of most organisations' day-to-day activities, and its use will continue to grow. E-Mails have enabled an efficient means of communication, without the limitations of time zones, speed or cost, usually associated with many of the other forms of communication. Though it has lot of advantages, however; E-Mails can easily be used for the negative purposes as well, making SPAM and virus E-Mails a problem especially by the hackers. In this Unit, we'll understand the key elements that comprise a successful E-Mail Crime & its Investigation and eventually work out on securing the E-Mails.

E-Mail is now considered to be most important in the area of information technology. Hackers come with various sophisticated tools and techniques to invade computers and stealing personal details of users from their E-Mail accounts. There are various traditional security measures available, but in most of the cases it is useless to fight against the latest attacks. So, to protect E-Mails every user/ company should adopt the right security software on computer. The Internet has opened up new doors of opportunities for both private individuals and companies. However,

Email Crime Investigation

there are different types of viruses, malware and other harmful items that may cause your computer.

Now-a-days, most of the companies implement online transactions and not only the companies but an individual also reap the benefits of the internet. They shop online and also carry out other financial transactions online and somehow keep their personal, financial, and credit card information, Bank Statements etc. in their E-Mail. So, the risk of hacking has also gone up significantly. Due to this reason sufficient assurance for a network, software, and PC are no longer enough. In order to protect the information and data, it has become the need of the hour to adopt new methods, techniques and various tools to implement the optimum level of security. This unit will provide all of measures to be taken for the E-Mail investigation and how to trace the fake E-Mails.

2.1 OBJECTIVES

After going through this Unit, you should be able to understand:

- What is E-Mail;
- How E-Mail Works?;
- Structure of E-Mail;
- E-Mail Crimes;
- E-Mail Header Analysis;
- E-Mail Investigation;
- Tracking an E-Mail;
- Tracing IP Address; and
- Securing E-Mail Account.

2.2 WHAT IS ELECTRONIC MAIL?

Electronic mail, which is commonly known as E-Mail is a method of exchanging digital messages across the Internet or other computer networks. E-Mail systems are based on a store-and-forward model in which E-Mail server computer systems accept, forward, deliver and store messages on behalf of users, who only need to connect to the E-Mail infrastructure. Typically an E-Mail server, with a network-enabled device for the duration of message submission or retrieval. Originally, E-Mail was transmitted directly from one user's device to another user's computer, which required both computers to be connected online at the same time.

An electronic mail message consists of two components, the message header, and the message body, which is the E-Mail's content. The message header contains control information, including, minimally, an originator's E-Mail address and one or more recipient addresses. Usually additional information is added, such as a subject header field.

Originally a text-only communications medium, E-Mail was extended to carry multi-media content attachments, which was standardized in RFC 2045 through RFC 2049, collectively called, Multipurpose Internet Mail Extensions (MIME).

The foundation for today's global Internet E-Mail services reaches back to the early ARPANET and standards for encoding of messages were proposed as early as 1973 (RFC 561). An E-Mail sent in the early 1970s looked very similar to one sent on the Internet today. Conversion from the ARPANET to the Internet in the early 1980s produced the core of the current services.

Network-based E-Mail was initially exchanged on the ARPANET in extensions to the File Transfer Protocol (FTP), but is today carried by the Simple Mail Transfer Protocol (SMTP), first published as Internet standard 10 (RFC 821) in 1982. In the process of transporting E-Mail messages between systems, SMTP communicates delivery parameters using a message envelope separately from the message (header and body) itself.

2.3 HOW E-MAIL WORKS?

2.3.1 Operations

E-Mail is based around the use of electronic mailboxes. When an E-Mail is sent, the message is routed from server to server, all the way to the recipient's E-Mail server. More precisely, the message is sent to the mail server tasked with transporting E-Mails (called the MTA, for *Mail Transport Agent*) to the recipient's MTA. On the Internet, MTAs communicate with one another using the protocol SMTP, and so are logically called **SMTP** servers (or sometimes outgoing mail servers).

The recipient's MTA then delivers the E-Mail to the incoming mail server (called the MDA, for *Mail Delivery Agent*), which stores the E-Mail as it waits for the user to accept it. There are two main protocols used for retrieving E-Mail on an MDA:

- **POP3** (*Post Office Protocol*), the older of the two, which is used for retrieving E-Mail and, in certain cases, leaving a copy of it on the server.
- **IMAP** (*Internet Message Access Protocol*), which is used for coordinating the status of E-Mails (read, deleted, moved) across multiple E-Mail clients. With IMAP, a copy of every message is saved on the server, so that this synchronization task can be completed.

For this reason, incoming mail servers are called POP servers or IMAP servers, depending on which protocol is used.

To use a real-world analogy, MTA act as the post office (the sorting area and mail carrier, which handle message transportation), while MDA act as mail boxes, which store messages (as much as their volume will allow) until the recipients check the box. This means that it is not necessary for recipients to be connected in order, for them to be sent E-Mail.

To keep everyone from checking other users' E-Mails, MDA is protected by a user name called a login and by a password.

Retrieving mail is done using a software program called an **MUA** (*Mail User Agent*). When it is a web interface used for interacting with the incoming mail server, it is called **webmail**.

The MUA is the application, which an originating sender uses to compose, and read E-Mail, such as Outlook, Thunderbird, Eudora etc.

The sender's MUA transfers the E-Mail to a Mail Delivery Agent (MDA). Frequently, the sender's MTA also handles the responsibilities of an MDA. Several of the most common MTA's do this, including sendmail, postfix, exim, qmail etc. The MDA/MTA accepts the E-Mail, then routes it to local mailboxes or forwards it if it isn't locally addressed.

An E-Mail can encounter a network cloud within a large company or ISP, or the largest network cloud in existence: the Internet. The network cloud may encompass a mass of mail servers, DNS servers, routers, and other devices and services too numerous to mention. These are likely to be slow when processing an unusually

In figure 1.0, MDA forwards the email to an MTA and it enters the first of a series of "network clouds,"

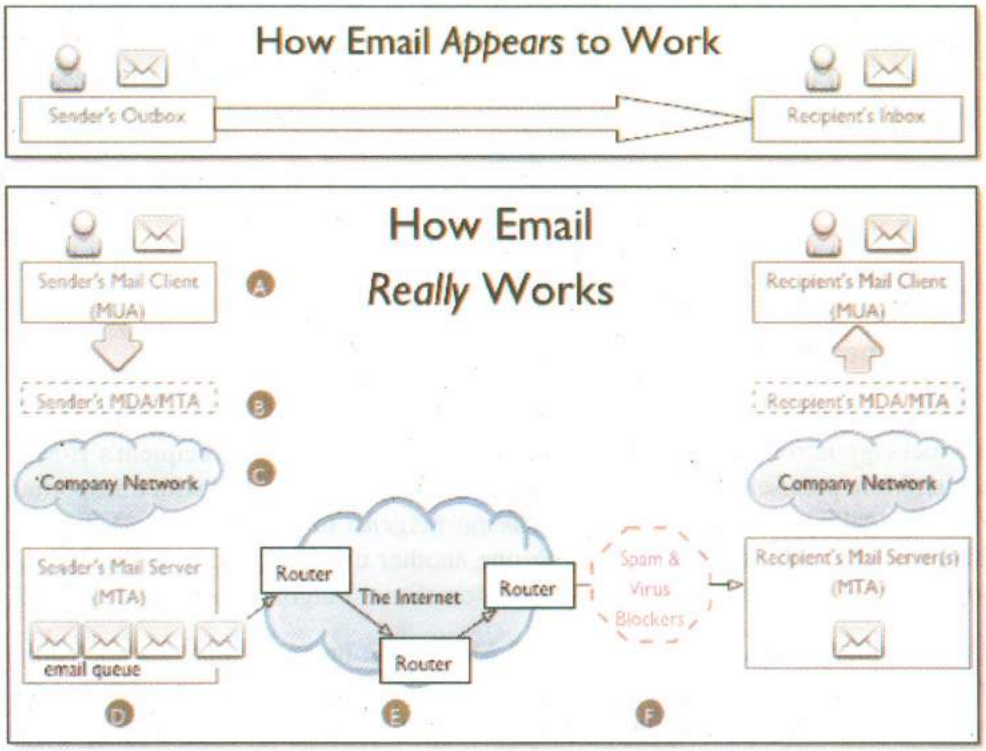


Fig. 1

heavy load, temporarily unable to receive an E-Mail when taken down for maintenance, and sometimes may not have identified themselves properly to the Internet through the Domain Name System (DNS) so that other MTAs in the network cloud are unable to deliver mail as addressed. These devices may be protected by firewalls, spam filters and malware detection software that may bounce or even delete an E-Mail. When an E-Mail is deleted by this kind of software, it tends to fail silently, so the sender is given no information about where or when the delivery failure has occurred.

The E-Mail in the figure 1 is addressed to someone at another company, so it enters an E-Mail queue with other outgoing E-Mail messages. If there is a high volume of mail in the queue, either because there are many messages or the messages are unusually large, or both then the message will be delayed in the queue until the MTA processes the messages ahead of it.

When transferring an E-Mail, the sending MTA handles all aspects of mail delivery until the message has been either accepted or rejected by the receiving MTA. As the E-Mail clears the queue, it enters the Internet network cloud, where it is routed along with a host-to-host chain of servers. Each MTA in the Internet network cloud needs to "stop and ask directions" from the Domain Name System (DNS) in order to identify the next MTA in the delivery chain. The exact route depends partly on server availability and mostly on which MTA can be found to accept E-Mail for the domain specified in the address. Most E-Mail takes a path that is dependent on server availability, so a pair of messages originating from the same host and addressed to the same receiving host could take different paths. These days, it's mostly spammers that specify any part of the path, deliberately routing their message through a series of relay servers in an attempt to obscure the true origin of the message.

To find the recipient's IP address and mailbox, the MTA must drill down through the Domain Name System (DNS), which consists of a set of servers distributed across the Internet. Beginning with the root name servers at the top-level domain (.tld), then domain name servers that handle requests for domains within that .tld, and eventually to name servers that know about the local domain. The MTA contacts the MX servers on the MX record in order of priority until it finds the designated host for that address domain. The sending MTA asks if the host accepts messages for the recipient's username at that domain (i.e., username@domain.tld) and transfers the message.

An E-Mail may be transferred to more than one MTA within a network cloud and is likely to be passed to at least one firewall before it reaches it's destination. An E-Mail encountering a firewall may be tested by spam and virus filters before it is allowed to pass inside the firewall. These filters test to see if the message qualifies as spam or malware. If the message contains malware, the file is usually quarantined and the sender is notified. If the message is identified as spam, it will probably be deleted without notifying the sender.

Spam is difficult to detect because it can assume so many different forms, so spam filters test on a broad set of criteria and tend to misclassify a significant number of messages as spam, particularly messages from mailing lists. When an E-Mail from a list or other automated source seems to have vanished somewhere in the network cloud, the culprit is usually a spam filter at the receiver's ISP or company.

In the figure, the E-Mail makes it past the hazards of the spam trap...er...filter, and is accepted for delivery by the receiver's MTA. The MTA calls a local MDA to deliver the mail to the correct mailbox, where it will sit until it is retrieved by the recipient's MUA.

2.3.2 Sending E-Mail

Create an E-Mail message

Applies to: Microsoft Outlook 2010

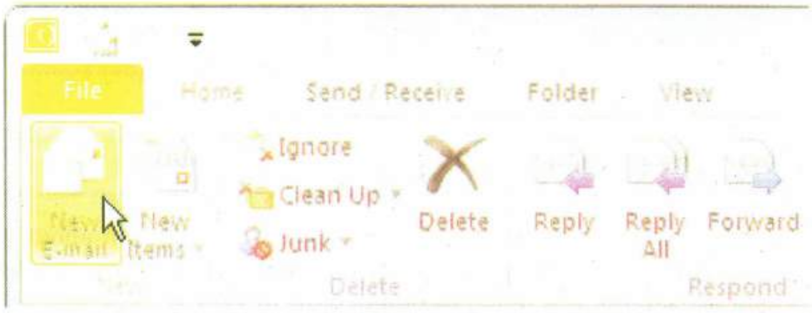


Fig. 2

1) On the Home tab, in the new group, click New E-Mail.

   Keyboard shortcut to create an E-Mail message; press CTRL+SHIFT+M.

2) In the Subject box, type the subject of the message.

3) Enter the recipients' E-Mail addresses or names in the To, Cc, or Bcc box (To, Cc, and Bcc boxes: A message is sent to the recipients in the To box. Recipients in the Cc (carbon copy) and Bcc (blind carbon copy) boxes also get the message; however, the names of the recipients in the Bcc box aren't visible to other recipients.). Separate multiple recipients with a semicolon.

   To select recipients' names from a list in the Address Book, click To, Cc, or Bcc and then click the names you want.

   Show I don't see the Bcc box. How do I turn it on?

   To display the Bcc box for this and all future messages, on the Options tab, in the Show Fields group, click Bcc.

4) After you have composed the message, click Send.

Anup Girdhar ✕ : Automatic reply: " I am out of the office until 12.

Fig. 3

Check Your Progress 1

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

What are the components of E-Mail? What is the use of Mail transfer agent?

....

....

....

....

....

....

....

....

....

2.4 STRUCTURE OF E-MAIL

A mail message consists of a header, which contains information about who the message was sent from, the recipient(s) and the route. Many of the header fields are not shown by default, but most programs used to read E-Mail will allow full headers to be displayed. This is then followed by the body of the message which contains whatever the sender wishes.

The message header should include at least the following fields:

- **From:** The E-Mail address, and optionally the name of the author(s). In many E-Mail clients not changeable except through changing account settings.
- **To:** The E-Mail address/addresses and optionally name(s) of the message's recipient(s). Indicates primary recipients (multiple allowed).
- **Cc:** Carbon copy; many E-Mail clients will mark E-Mail in your inbox differently depending on whether you are in the To: or Cc: list.
- **Bcc:** Blind Carbon Copy; addresses added to the SMTP delivery list but not (usually) listed in the message data, remaining invisible to other recipients.
- **Subject:** A brief summary of the topic of the message. Certain abbreviations are commonly used in the subject, including "RE:" and "FW:".
- **Message-ID:** Also an automatically generated field; used to prevent multiple delivery and for reference in In-Reply-To.

If the mail message is a formal one, it is customary although not obligatory to finish with your name, return address and other useful information as a signature. For example:

```
From owner-is-all-compcont@sedulitygroups.com Fri Aug 18 15:10:01 2010
Received: from sedulitygroups.com by anup@ sedulitygroups.com (8.8.8/
1.1.8.2/14Aug95-0452PM)
id PAA0000016479; Fri, 18 Aug 2000 15:10:00 +0100 (IST)
Received: from contact by sedulitygroups.com with local (Exim 3.16 #3)
id 13PmpO-0000XU-00
for IS-ALL-COMPCONT-outgoing@ sedulitygroups.com; Fri, 18 Aug 2010
15:08:58 +0530
Received: from contact by sedulitygroups.com with local (Exim 3.16 #3)
id 13PmpN-0000XK-00
for all-compcont-outgoing@ sedulitygroups.com; Fri, 18 Aug 2010 15:08:57
+0530
Received: from contact.sedulitygroups.com ([122.160.175.70] helo=clientid.
sedulitygroups.com)
by sedulitygroups.com with esmtp (Exim 3.16 #3)
id 13PmpM-0000XA-00; Fri, 18 Aug 2000 15:08:56 +0100
Received: by clientid.sedulitygroups.com (8.8.8/1.1.8.2/14Aug2010-0452PM)
id PAA0000009231; Fri, 18 Aug 2010 15:09:56 +0530 (IST)
Message-Id: <200008181409.PAA0000009231@clientid.sedulitygroups.com >
Subject: Netscape vulnerability fix
To: all-compcont@sedulitygroups.com
Date: Fri, 18 Aug 2010 15:09:56 +0530 (IST)
From: Team Sedulity <contact@ sedulitygroups.com >
Reply-To: contact@sedulitygroups.com
X-Mailer: ELM [version 2.4 PL25]
MIME-Version: 1.0
Content-Type: text/plain; charset=US-ASCII
Content-Transfer-Encoding: 7bit
Sender: owner-is-all-compcont@sedulitygroups.com
Precedence: bulk
Status: RO

Congratulations.

Sedulity Solutions & Technologies has recently launched its 64 bit operating
system.


Team Sedulity
Sedulity Solutions & Technologies
```

The header consists of lines beginning with a keyword followed by a colon (:), followed by information on each line. A brief explanation of each field of the header is given below. This header contains most of the common fields.

- **Received:** These lines indicate the route that the E-Mail has taken and which systems have handled it and the times that it was handled.
- **Date:** The date and time at which the message was sent including time zone.
- **From:** The sender. The part in angle brackets is a real electronic mail address. This field may be user settable, so may not reflect the true sender. In this case, it shows the original sender of the message.
- **Sender:** The sender. This is inserted by some systems if the actual sender is different from the text in the From: field. This makes E-Mail more difficult to forge, although this too can be set by the sender. There are other uses for a sender field. In the example above, the sender is set to the list owner by the mailing list system. This allows error messages to be returned to the list owner rather than the original sender of the message
- **To:** Who the mail is sent to. This may be a list or an individual. However it may bear no relation to the person that the E-Mail is delivered to. Mail systems used a different mechanism for determining the recipient of a message.
- **Cc:** Addresses of recipients who will also receive copies.
- **Subject:** Subject of the message as specified by the sender.
- **Message-id:** A unique system generated id. This can sometimes be useful in fault tracing if multiple copies of a message have been received.
- **Reply-to:** Where any reply should be sent to (in preference to any electronic mail address in the From: field if present). This may be inserted by the sender, usually when they want replies to go to a central address rather than the address of the system they are using. It is also inserted automatically by some systems
- **X-Mailer:** Any field beginning with X can be inserted by a mail system for any purpose.

When using a reply facility it is important to check where the reply is going by looking at the header of the outgoing message displayed on your screen. If the message has been forwarded to you, the reply will often go to the original sender and not the person who sent it to you.

2.5 E-MAIL CRIMES

Some of the major E-Mail related crimes are:

1) E-Mail spoofing

2) Sending malicious codes through E-Mail

3) E-Mail bombing

4) Sending threatening E-Mails

5) Defamatory E-Mails

6) E-Mail frauds

E-Mail spoofing

A spoofed E-Mail is the one that appears to originate from one source however, has emerged from another source in reality. In other words, E-Mail spoofing is the forgery of an E-Mail header so that the message appears to have originated from someone or somewhere other than the actual source. To send spoofed E-Mail, senders insert commands in headers that will alter message information. It is possible to send a message that appears to be from anyone, anywhere, saying whatever the sender wants it to say. Thus, someone could send spoofed E-Mail that appears to be from you with a message that you didn't write.

Although most spoofed E-Mail falls into the "nuisance" category and requires little action other than deletion, the more malicious varieties can cause serious problems and security risks. For example, spoofed E-Mail may import to be from someone in a position of authority, asking for sensitive data, such as passwords, credit card numbers, or other personal information -- any of which can be used for a variety of criminal purposes. One type of E-Mail spoofing, self-sending spam, involves messages that appear to be both to and from the recipient. E-Mail spoofing is surely possible because, Simple Mail Transfer Protocol (SMTP), is the main protocol used in sending E-Mail, does not include an authentication mechanism.

In order to send a spoofed E-Mail, the sender has to enter the following information mentioned below:

- E-Mail address of the receiver of the E-Mail
- E-Mail address(es) of the person(s) who will receive a copy of the E-Mail (referred to as CC for carbon copy)
- E-Mail address(es) of the person(s) who will receive a copy of the E-Mail (referred to as CC for carbon copy, but whose identities will not be known to the other recipients of the E-Mail (known as BCC for blind carbon copy)
- Subject of the message (a short title / description of the message)
- Message

There are certain web-based E-Mail services like, www.SendFakE-Mail.com, www.anonymailer.net which offers a facility, wherein in addition to the above, a sender can also enter the E-Mail address of the supposed sender of the E-Mail.

For example, Mr. XYZ whose E-Mail address is xyz@hotmail.com. His friend ABC's E-Mail address is abc@yahoo.com. Using anonymailer.net, XYZ can send E-Mails which are supposed to be sent from ABC's E-Mail account. All he has to do is enter abc@yahoo.com in the space provided for sender's E-Mail address. ABC's friends would trust such E-Mails, as they would assume that they have come from ABC (whom they trust). XYZ can use this misplaced trust to send viruses, Trojans, worms etc. to ABC's friends, who would unwittingly download them.

Spreading Trojans, viruses and worms

E-Mails are often the fastest and easiest ways to propagate malicious code over the Internet. The Love Bug virus, for instance, reached millions of computers within 36 hours of its release from the Philippines thanks to E-Mail. Hackers often bind Trojans, viruses, worms and other computer contaminants with E-greeting cards and then E-Mail them to unsuspecting persons. Such contaminants can also be bound with software that appears to be an anti-virus patch. E.g. a person receives an E-Mail from Compose From To CC BCC Subject

Message

information@mcaffee.com (this is a spoofed E-Mail but the victim does not know this). The E-Mail informs him that the attachment contained with the E-Mail is a security patch that must be downloaded to detect a certain new virus. Most unsuspecting users would submit to such an E-Mail (if they are using a registered copy of the McAffee anti-virus software) and would download the attachment, which could be a Trojan or a virus itself!

E-Mail bombing

E-Mail bombing refers to sending a large amount of E-Mails to the victim resulting in the victim's E-Mail account (in case of an individual) or servers (in case of a company or an E-Mail service provider) crashing. A simple way of achieving this would be to subscribe the victim's E-Mail address to a large number of mailing lists. Mailing lists are special interest groups that share and exchange information on a common topic of interest with one another via E-Mail. Mailing lists are very popular and can generate a lot of daily E-Mail traffic - depending upon the mailing list. Some generate only a few messages per day others generate hundreds. If a person has been unknowingly subscribed to hundreds of mailing lists, his incoming E-Mail traffic will be too large and his service provider will probably delete his account. The simplest E-Mail bomb is an ordinary E-Mail account. All that one has to do is compose a message, enter the E-Mail address of the victim multiple times in the "To" field, and press the "Send" button many times.

Writing the E-Mail address 25 times and pressing the "Send" button just 50 times (it will take less than a minute) will send 1250 E-Mail messages to the victim! If a group of 10 people do this for an hour, the result would be 750,000 E-Mails!

There are several hacking tools available to automate the process of E-Mail bombing. These tools send multiple E-Mails from many different E-Mail servers, which make it very difficult, for the victim to protect himself.

Threatening E-Mails

This is another type of E-Mail crime, where an E-Mail is send to a person for the purpose of threatening. It is a useful tool for technology savvy criminals as it becomes fairly easy for anyone with even a basic knowledge of computers to become a blackmailer by threatening someone via E-Mail.

Defamatory E-Mails

Defamation is defined as communication to third parties of false statements about a person that injure the reputation of or deter others from associating with that person. Defamation can take one of two forms: slander or libel. Slander covers oral defamatory statements while libel addresses the written version. Defamation is an abusive attack on a person's character or good name. If a person is harmed in any way by any statement(s), a person sending defamatory E-Mail can be held accountable in a court of law.

Check Your Progress 2

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

Explain the structure of an E-Mail. What are the major E-Mail related crimes?

....

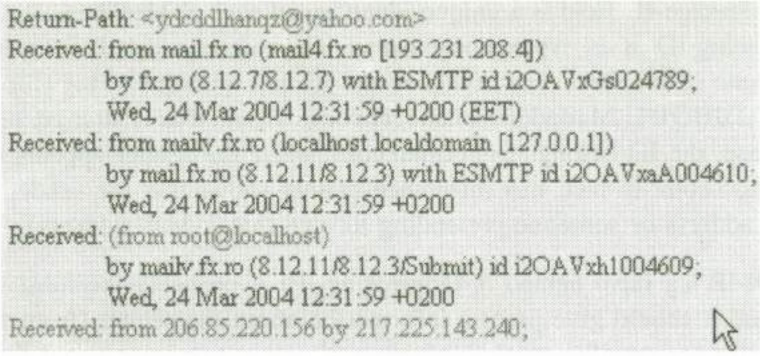
....

....

....

2.6 E-MAIL HEADER ANALYSIS

Here is the starting part of the header of a junk E-Mail (spam), which includes information about the transfer of the E-Mail between the sender and the receiver:



```
Return-Path: <ydcddlhanqz@yahoo.com>
Received: from mail.fx.ro (mail4.fx.ro [193.231.208.4])
          by fx.ro (8.12.7/8.12.7) with ESMTP id i2OAVxGs024789;
          Wed, 24 Mar 2004 12:31:59 +0200 (EET)
Received: from mailv.fx.ro (localhost.localdomain [127.0.0.1])
          by mail.fx.ro (8.12.11/8.12.3) with ESMTP id i2OAVxaA004610;
          Wed, 24 Mar 2004 12:31:59 +0200
Received: (from root@localhost)
          by mailv.fx.ro (8.12.11/8.12.3/Submit) id i2OAVxh1004609;
          Wed, 24 Mar 2004 12:31:59 +0200
Received: from 206.85.220.156 by 217.225.143.240;
```

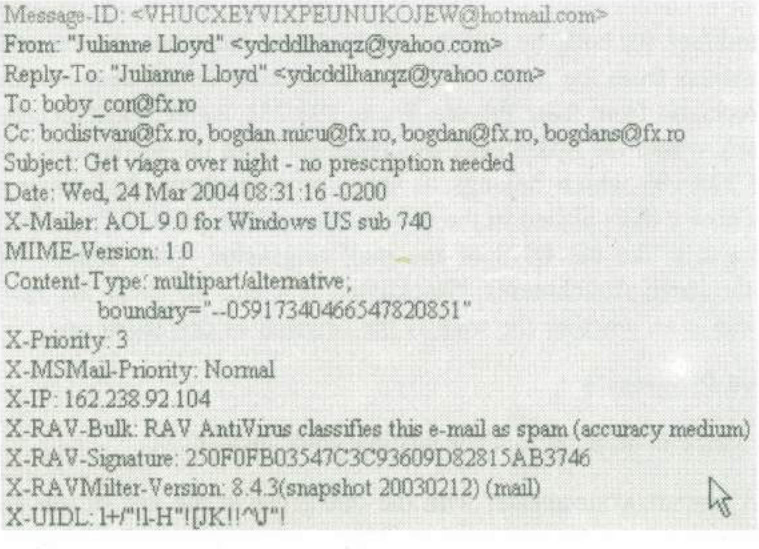
- **Return-path:** the header tells that if you reply to this E-Mail message, the reply will be sent to ydcdd...@yahoo.com. Would you use such an E-Mail address for real?

- **Received tags:** As on web blogs, read them from the bottom to top. The header says the E-Mail was originally sent from 206.85... and it was sent to 217.225... (which is the name/IP of the first mail server that got involved into transporting this message). Then suddenly, the next Received tag says the message was received from root@localhost, by mailv.fx.ro. You can also notice that so far, the Received tags do not contain any information about how the E-Mail was transmitted (the "with" tag is missing: this tag tells the protocol used to send the E-Mail).

In reality, this is the common case of a spammer pretending to be the root user of mailv.fx.ro and sending the E-Mail from 206.85..., through 217.225... and telling 217.225... to act as the root user of mailv.fx.ro, in order to use the SMTP server of mailv.fx.ro to send the E-Mail. Since more and more mail servers are not allowing open-relay connections, the spammer can only use the mail server of the receiver, in order to send the message. If the spammer will try to send the E-Mail to support@E-Mailaddressmanager.com, through exactly the same route as above, it wouldn't work, because support@E-Mailaddressmanager.com is not a network user of mailv.fx.ro. This is the reason why you may have received spam E-Mails appearing to be sent through an E-Mail address of your own ISP.

Going deeper with the analysis, you can use an IP tracing tool, like Visual Route, in order to see to whom the IP belongs to. As in most of the spamming cases, the starting IP (206.85...) is unreachable, which means that the spammer could have routed the real IP or he could have used a dynamic IP (a normal case for dial-up users). However, by tracing 217.225..., you will get to the ISP used by the spammer, a German provider. The ISP has nothing to do with the spam itself, but it was simply used by the spammer to connect to the Internet.

Let's look further into the E-Mail header:



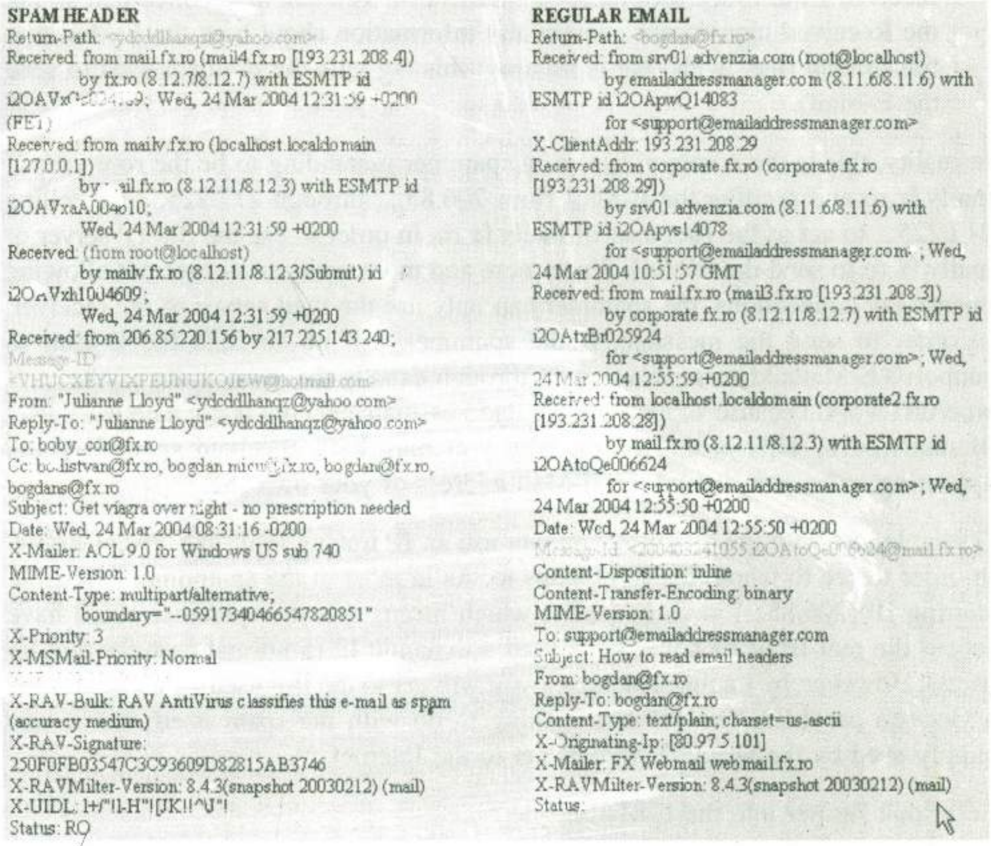
```
Message-ID: <VHUCXEYVIXPEUNUKOJEW@hotmail.com>
From: "Julianne Lloyd" <ydcddlhanqz@yahoo.com>
Reply-To: "Julianne Lloyd" <ydcddlhanqz@yahoo.com>
To: boby_con@fx.ro
Cc: bodistvan@fx.ro, bogdan.micu@fx.ro, bogdan@fx.ro, bogdans@fx.ro
Subject: Get viagra over night - no prescription needed
Date: Wed, 24 Mar 2004 08:31:16 -0200
X-Mailer: AOL 9.0 for Windows US sub 740
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="--05917340466547820851"
X-Priority: 3
X-MSMail-Priority: Normal
X-IP: 162.238.92.104
X-RAV-Bulk: RAV AntiVirus classifies this e-mail as spam (accuracy medium)
X-RAV-Signature: 250F0FB03547C3C93609D82815AB3746
X-RAVMilter-Version: 8.4.3(snapshot 20030212) (mail)
X-UIDL: 1+/"!l-H"![JK!!^V"!
```

- The Message-IL field is a unique identifier of each E-Mail message. It is like the tracing ID of an express postal mail. The rule says the ID is composed by the name of the server that assigned the ID and a unique string (for example, QESADJHO@E-Mailaddressmanager.com). Hmm, this is strange, because on our case, the ID belongs to hotmail.com, while the sender appears to belong to yahoo.com. In fact, this difference mainly shows that the sender is forged (fake address or someone pretending to own that E-Mail address).

- The X-IP tag (also named X-Originating-IP) is probably the most important one and it should give precise information about the sender (from where the E-Mail was actually sent). Unfortunately, this tag is optional for E-Mail protocols, so some spam messages will not include it. As you can see, the originating IP is not even close to the sender's IP, from the Received tags.

- The X-UIDL tag is another unique ID, but this one is used by the POP3 protocol when your E-Mail client is receiving the E-Mail. This is an optional E-Mail tag, but the rule of thumb says spammers love to include it.

Spam E-Mail Header vs Regular E-Mail Header.



SPAM HEADER

```
Return-Path: <ydcddlhanqz@yahoo.com>
Received: from mail.fx.ro (mail4.fx.ro [193.231.208.4])
        by fx.ro (8.12.7/8.12.7) with ESMTP id
i2OAVx[illegible]; Wed, 24 Mar 2004 12:31:59 +0200
(FET)
Received: from mailv.fx.ro (localhost.localdomain
[127.0.0.1])
        by [illegible]ail.fx.ro (8.12.11/8.12.3) with ESMTP id
i2OAVxaA004o10;
        Wed, 24 Mar 2004 12:31:59 +0200
Received: (from root@localhost)
        by mailv.fx.ro (8.12.11/8.12.3/Submit) id
i2OAVxh10U4609;
        Wed, 24 Mar 2004 12:31:59 +0200
Received: from 206.85.220.156 by 217.225.143.240;
Message-ID
<VHUCXEYVIXPEUNUKOJEW@hotmail.com>
From: "Julianne Lloyd" <ydcddlhanqz@yahoo.com>
Reply-To: "Julianne Lloyd" <ydcddlhanqz@yahoo.com>
To: boby_con@fx.ro
Cc: bo.listvan@fx.ro, bogdan.micu@fx.ro, bogdan@fx.ro,
bogdans@fx.ro
Subject: Get viagra over night - no prescription needed
Date: Wed, 24 Mar 2004 08:31:16 -0200
X-Mailer: AOL 9.0 for Windows US sub 740
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="--05917340466547820851"
X-Priority: 3
X-MSMail-Priority: Normal

X-RAV-Bulk: RAV AntiVirus classifies this e-mail as spam
(accuracy medium)
X-RAV-Signature:
250F0FB03547C3C93609D82815AB3746
X-RAVMilter-Version: 8.4.3(snapshot 20030212) (mail)
X-UIDL: l+/"!l-H"![JK!!^\J"!
Status: RO
```

REGULAR EMAIL

```
Return-Path: <bogdan@fx.ro>
Received: from srv01.advenzia.com (root@localhost)
        by emailaddressmanager.com (8.11.6/8.11.6) with
ESMTP id i2OApwQ14083
        for <support@emailaddressmanager.com>
X-ClientAddr: 193.231.208.29
Received: from corporate.fx.ro (corporate.fx.ro
[193.231.208.29])
        by srv01.advenzia.com (8.11.6/8.11.6) with
ESMTP id i2OApvs14078
        for <support@emailaddressmanager.com> ; Wed,
24 Mar 2004 10:51:57 GMT
Received: from mail.fx.ro (mail3.fx.ro [193.231.208.3])
        by corporate.fx.ro (8.12.11/8.12.7) with ESMTP id
i2OAtxBr025924
        for <support@emailaddressmanager.com>; Wed,
24 Mar 2004 12:55:59 +0200
Received: from localhost.localdomain (corporate2.fx.ro
[193.231.208.28])
        by mail.fx.ro (8.12.11/8.12.3) with ESMTP id
i2OAtoQe006624
        for <support@emailaddressmanager.com>; Wed,
24 Mar 2004 12:55:50 +0200
Date: Wed, 24 Mar 2004 12:55:50 +0200
Message-Id: <200403241055.i2OAtoQe006624@mail.fx.ro>
Content-Disposition: inline
Content-Transfer-Encoding: binary
MIME-Version: 1.0
To: support@emailaddressmanager.com
Subject: How to read email headers
From: bogdan@fx.ro
Reply-To: bogdan@fx.ro
Content-Type: text/plain; charset=us-ascii
X-Originating-Ip: [80.97.5.101]
X-Mailer: FX Webmail webmail.fx.ro
X-RAVMilter-Version: 8.4.3(snapshot 20030212) (mail)
Status:
```

The look and feel for both the mail header is almost same but, the major difference is the IP address from the mail which was originated, In the above case, Regular mail was received from their Private IP i.e. 193.231….(localhost.localdomain) of the Company where the Spam mail was received from the Anonymous IP address i.e. 206.85.220.156 which belongs to some other country. And there are many validations now a days placed in the new release of the good MTA's which detects the SPAM mails like the DNS of the mail originator, Time frame, Key words placed in the mail, Attachments, Blacklisted IP's etc. So these are the ways by which we can scan whether the mail is the original or the Spam one.

Check Your Progress 3

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of this Unit.

Explain the function of received tags? What is message ID?

....

....

....

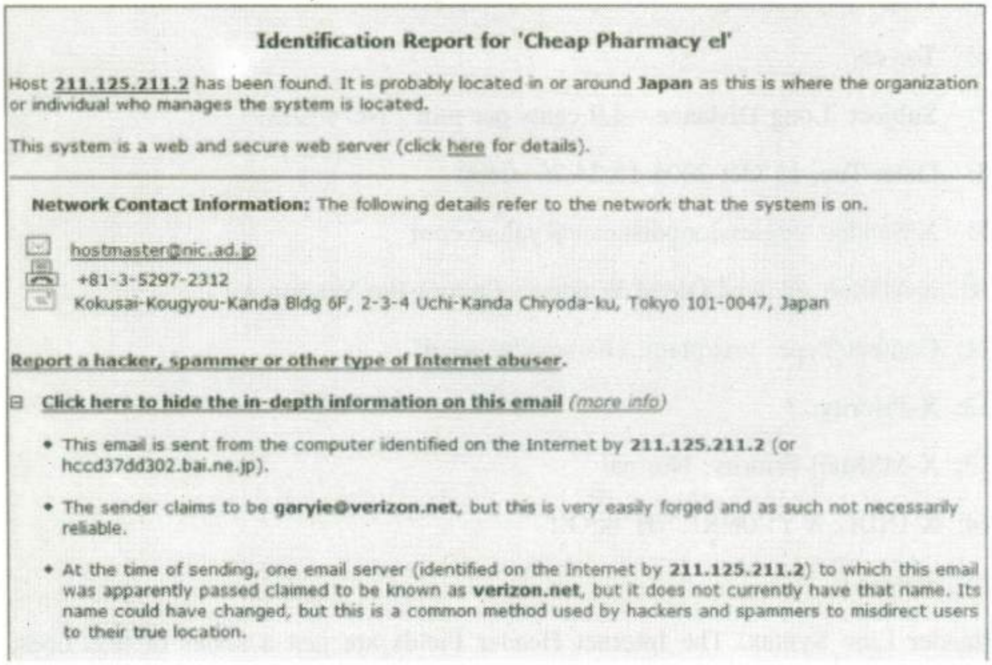
....

....

2.7 RECEIVED E-MAIL TRACING TOOLS

2.7.1 E-Mail Track Pro

E-MailTrackerPro will automatically analyse an E-Mail and its headers and provide a report similar as shown below:



Identification Report for 'Cheap Pharmacy el'

Host **211.125.211.2** has been found. It is probably located in or around **Japan** as this is where the organization or individual who manages the system is located.

This system is a web and secure web server (click here for details).

Network Contact Information: The following details refer to the network that the system is on.

hostmaster@nic.ad.jp
+81-3-5297-2312
Kokusai-Kougyou-Kanda Bldg 6F, 2-3-4 Uchi-Kanda Chiyoda-ku, Tokyo 101-0047, Japan

Report a hacker, spammer or other type of Internet abuser.

⊟ **Click here to hide the in-depth information on this email** *(more info)*

- This email is sent from the computer identified on the Internet by **211.125.211.2** (or hccd37dd302.bai.ne.jp).
- The sender claims to be **garyie@verizon.net**, but this is very easily forged and as such not necessarily reliable.
- At the time of sending, one email server (identified on the Internet by **211.125.211.2**) to which this email was apparently passed claimed to be known as **verizon.net**, but it does not currently have that name. Its name could have changed, but this is a common method used by hackers and spammers to misdirect users to their true location.

Tracing an E-Mail address: If you do not have an actual E-Mail message, but only have an E-Mail address, you can trace the address through its E-Mail server. However, it should be noted that E-Mail addresses can be easily forged, the results from tracing an E-Mail address may not be related to the true sender.

In most cases, using an E-Mail tracking tool like E-MailTrackerPro to trace an E-Mail message you have received is your best option. To trace an E-Mail message received by someone else, have them forward the message to you as an attachment (just forwarding the message itself will show them as the sender). You can then open the attached message and copy the E-Mail header, start E-MailTrackerPro and paste the header for analysis.

E-Mail Internet Headers

Every received E-Mail has Internet Headers. Using Microsoft Outlook as an example (other mail programs are very similar), just follow these steps to view the headers:

1) Right-click on the mail message that is still in your Outlook Inbox

2) Select 'Options...' from the resulting popup menu

3) Examine the 'Internet Headers' in the resulting 'Message Options' dialog

Right-click in the 'Internet Headers' field and click on 'Select All' in the popup menu (or type ctrl-A). Then right-click again and click on 'Copy' in the popup menu (or type ctrl-C). Finally, paste all the Internet Headers into your favourite text editor for full examination (such as 'Notepad', included with Windows).

Example: What you see will be very similar to the following (with 'line numbers' added for clarity and discussion in following sections):

1: Received: from tes1a623.OnE-Mail.com.sg ([203.127.89.129]) by visualroute.com (8.11.6) id f9CIVSk24480; Tue, 12 Oct 2004 12:31:29 -0600 (MDT)

2: Message-Id: <200110121831.f9CIVSk24480@s2.domain.com>

3: Received: from drb.com (IIM1608 [203.127.89.138]) by tes1a623.OnE-Mail.com.sg with SMTP (Microsoft Exchange Internet Mail Service Version 5.5.2448.0)

4: id 4XNK9ATR; Wed, 13 Oct 2004 01:19:10 +0800

5: From: paylesslongdistance@somedomain.com

6: To: <>

7: Subject: Long Distance - 4.9 cents per min - NO FEES!

8: Date: Tue, 12 Oct 2004 13:24:26 -0400

9: X-Sender: paylesslongdistance@yahoo.com

10: X-Mailer: QUALCOMM Windows Eudora Pro Version 4.1

11: Content-Type: text/plain; charset="us-ascii"

12: X-Priority: 3

13: X-MSMail-Priority: Normal

14: X-UIDL: 8`Y!!0GR!!"?H"!k:O!!

15: Status: U

Header Line Syntax: The Internet Header Fields are just a series of text lines, where each line looks like:

Header-Name: Header-Value

And if a line starts with a tab or spaces, like line 4 above, that line is a continuation of the previous Header-Value line. So, the Header-Name Received in line 3 has a Header-Value that spans lines 3 and 4.

'Received' Headers

The most important header field for tracking purposes is the Received header field, which usually has syntax similar to:

Received: from ? by ? via ? with ? id ? for ? ; date-time

Where from, by, via, with, id, and for are all tokens with values within a single Header-Value, which may span multiple lines. Note: Some mail servers may not include all of these tokens -- or additional tokens/values may be added to this field, but now you are prepared to break it apart and understand it.

Every time an E-Mail moves through a new mail server, a new Received header line (and possibly other header lines, like line 2 above) is added to the beginning of the headers list. This is similar to FedEx package tracking, when your package enters a new sorting facility and is 'swiped' through a tracking machine.

This means that as you read the Received headers from top to bottom, that you are gradually moving closer to the computer/person that sent you the E-Mail.

But please note that as you read through the Received header fields and get closer to the computer/person that sent you the E-Mail, you need to consider the possibility that the sender added one or more false Received header lines to the list (at the time, the senders beginning of the list) in an attempt to redirect you to another location and prevent you from finding the true sender. But, now that you know false header lines are possible, just stay alert.

You will probably find it very useful to break a single Received line into multiple lines, with one token per line. Namely, the header line:

Received: from tes1a623.OnE-Mail.com.sg ([203.127.89.129]) by visualroute.com (8.11.6) id f9CIVSk24480; Tue, 12 Oct 2004 12:31:29 -0600 (MDT)

is much easier to read and understand when formatted so that each token is on a new line, as in:

```
Received:

from tes1a623.OnE-Mail.com.sg ([203.127.89.129])

by   visualroute.com (8.11.6)

id   f9CIVSk24480

;    Tue, 12 Oct 2004 12:31:29 -0600 (MDT)
```

The Sender's IP Address

For tracking purposes, we are most interested in the from and by tokens in the Received header field. In general, you are looking for a pattern similar to:

```
Received: from BBB (dns-name [ip-address]) by AAA ...

Received: from CCC (dns-name [ip-address]) by BBB ...

Received: from DDD (dns-name [ip-address]) by CCC ...
```

In other words, mail server AAA received the E-Mail from BBB and provides as much information about BBB, including the IP Address BBB used to connect to AAA. This patterns repeats itself on each Received line. The syntax of the from token most times looks like:

```
name (dns-name [ip-address])
```

Where: name is the name the computer has named itself. Most of the time we never look at this name because it can be intentionally misnamed in an attempt to foil your tracking (but it may leak the windows computer name). dns-name is the reverse dns lookup on the ip-address. ip-address is the ip-address of the computer used to connect to the mail server that generated this Received header line. So, the ip-address is gold to us for tracking purposes.

The by token syntax just provides us with the name that the mail server gives itself. But since the last mail server could be under the control of a spammer, we should not trust this name.

So, what is crucial for tracking, is to pay attention to the trail of ip-address in the from tokens and not necessarily the host name provided to us in the by tokens. Hopefully an example will make the reason why very clear:

1: Received: from **tes1a623.OnE-Mail.com.sg** ([203.127.89.129]) by visualroute.com (8.11.6) id f9CIVSk24480; Tue, 12 Oct 2004 12:31:29 -0600 (MDT)

3: Received: from drb.com (IIM1608 [203.127.89.138]) by **tes1a623.OnE-Mail.com.sg** with SMTP (Microsoft Exchange Internet Mail Service Version 5.5.2448.0)

If you ignore line 1, you would conclude from line 3 that mail server tes1a623.OnE-Mail.com.sg sent you an E-Mail, but this would be wrong. When you trace to the host name tes1a623.OnE-Mail.com.sg, you are actually tracing to the IP Address lookup on that host name, which is 192.9.200.230. But as you can see from line 1, the IP Address used was really 203.127.89.129. Do not be fooled by this attempted misdirection by spammers and fraudsters.

Determine the IP Address of the Sender: Using the example E-Mail headers above and analyzing the Received header lines we can conclude:

- A Visualware employee received an E-Mail
- which came from visualroute.com (line 1)
- which came from tes1a623.OnE-Mail.com.sg (line 1; line 3 confirms)
- but whose ip-address used was 203.127.89.129 (line 1)
- which came from drb.com/IIM1608 (line 3)
- but whose ip-address used was 203.127.89.138 (line 3)

So, we have just tracked this E-Mail to the source -- IP Address **203.127.89.138.**

Leaked Sender Information

The Internet Headers for an E-Mail message may contain some really interesting information about the sender.

A) **Windows Computer Name:** It appears that the Windows computer name is sometimes leaked. Consider the following partial header information from an actual E-Mail:

Received: from **hanksdell** (11-22-33-44.xyz.net [11.22.33.44]) by visualroute.com (8.8.5) id SAA26331; Mon, 11 Oct 2004 18:46:53-0600 (MDT)

Where we can clearly see the IP'Address of the sender, but we can also see the computer name of hanksdell. While the computer name can be named anything, in this case, I might assume that the person is named Hank and uses a Dell computer.

This computer name may be intentionally misleadingly named or not be meaningful but it can become very useful confirming information if law enforcement can confirm that the name of the suspect's computer matches the name in the E-Mail header.

B) **Timezone Information:** Consider lines 3 and 4 from the Internet Header discussion above:

3: Received: from drb.com (IIM1608 [203.127.89.138]) by tes1a623.OnE-Mail.com.sg with SMTP (Microsoft Exchange Internet Mail Service Version 5.5.2448.0)

4: id 4XNK9ATR; Wed, 13 Oct 2004 01:19:10 **+0800**

Notice that in the Internet Headers, when a time is displayed, many times it is followed with a plus/minus and four digits, which represent HHMM (hour and minutes) from GMT (Greenwich Mean Time), or London, UK time. Plus means east of GMT. Minus means west of GMT.

So, according to +0800, the server is 8 hours east of GMT. TIP: Go into the Windows Control panel and enter into the Date/Time dialog, where there is a Time Zone list. This time zone appears to be in Singapore. Then, the .sg in tes1a623.OnE-Mail.com.sg means Singapore, which is one more confirmation of this information. A final confirmation comes from performing a VisualRoute trace 203.127.89.129 (the IP Address for tes1a623.OnE-Mail.com.sg). TIP: Trace to the IP Address, not the host name.

C) **X-Mailer:** This will usually tell you the mailer software used by the sender of the E-Mail. Consider:

10: X-Mailer: QUALCOMM Windows Eudora Pro Version 4.1

This may or may not be immediately useful, but it can be very useful if there is a follow-up investigation by authorities.

D) X-Originating-IP: If you are attempting to track down an E-Mail received from a Hotmail E-Mail account, look for the X-Originating-IP header field, which will tell you the IP Address of the computer that sent the E-Mail. Consider:

1: Received: from hotmail.com (f105.pav1.hotmail.com [64.4.31.105]) by s2.xyz.com (8.11.6) id f9BIvve34655; Mon, 11 Oct 2004 12:58:00 -0600 (MDT)

2: Received: from mail pickup service by hotmail.com with Microsoft SMTPSVC;

3: Mon, 11 Oct 2001 11:57:51 -0700

4: Received: from **202.156.2.147** by pv1fd.pav1.hotmail.msn.com with HTTP;

5: Mon, 11 Oct 2004 18:57:51 GMT

6: **X-Originating-IP: [202.156.2.147]**

However, notice that we could have obtained the same IP Address information by examining the Received header fields. But it is nice to have this extra confirmation.

2.8 E-MAIL LOCATION TRACKING TOOL

2.8.1 ReadNotify

Re@dNotify

ReadNotify is the most powerful and reliable E-Mail tracking service that exists today. In short - ReadNotify tells you "when" the E-Mail you sent gets read / re-opened / forwarded and so much more. The Salient features are: Certified email with delivery Receipts, Silent Tracking, Proof of Opening History, Security and Timestamps etc.

How do you send a tracked E-Mail?

There are two ways you can send tracked E-Mails:

1) Simply add: .readnotify.com to the end of your recipients E-Mail address (they won't see this)

OR

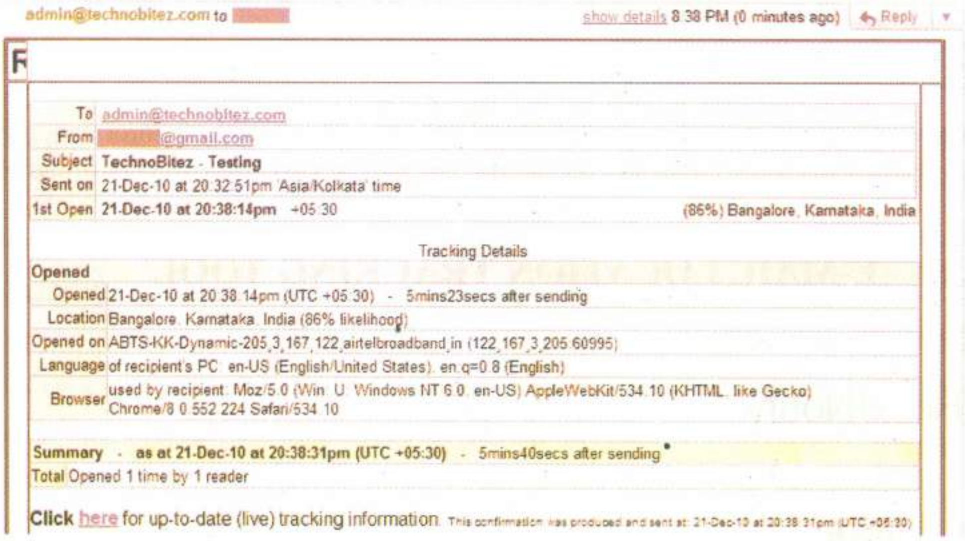
2) Install our ActiveTracker plugin to add the tracking for you.

Testing? If you send tracked E-Mails to yourself, your anti-spam filters may block them (people don't usually write to themselves) – so we recommend you test by sending to other people.

What will you tell me about the tracked E-Mails I send?

ReadNotify will endeavour to provide the following in your tracking reports:

- Date and time opened
- Location of recipient (per their ISP city /town)
- Map of location (available on paid subscriptions)
- Recipients IP address
- Apparent E-Mail address of opening (if available)
- Referrer details (i.e.; if accessed via web mail etc)
- URL clicks
- How long the E-Mail was read for
- How many times your E-Mail was opened
- If your E-Mail was forwarded, or opened on a different computer



admin@technobitez.com to [redacted] 8 38 PM (0 minutes ago)

R

To	admin@technobitez.com
From	[redacted]@gmail.com
Subject	TechnoBitez - Testing
Sent on	21-Dec-10 at 20 32 51pm 'Asia/Kolkata' time
1st Open	21-Dec-10 at 20:38:14pm +05 30 (86%) Bangalore, Karnataka, India

Tracking Details

Opened

Opened	21-Dec-10 at 20 38 14pm (UTC +05 30) - 5mins23secs after sending
Location	Bangalore Karnataka India (86% likelihood)
Opened on	ABTS-KK-Dynamic-205,3,167,122,airtelbroadband,in (122,167,3,205 60995)
Language	of recipient's PC en-US (English/United States). en q=0 8 (English)
Browser	used by recipient Moz/5.0 (Win U Windows NT 6 0 en-US) AppleWebKit/534 10 (KHTML like Gecko) Chrome/8 0 552 224 Safari/534 10

Summary - as at 21-Dec-10 at 20:38:31pm (UTC +05:30) - 5mins40secs after sending

Total Opened 1 time by 1 reader

Click here for up-to-date (live) tracking information. This confirmation was produced and sent at: 21-Dec-10 at 20:38 31pm (UTC +05:30)

All messages sent via ReadNotify benefit from our SPF compliant and Sender-ID compliant mail servers. This confirms safe transmission of your messages, and also enables us to report delivery status to you (including: bounce-backs, delays and success notifications). Delivery information is listed in your Personal Tracking Page.

Try hovering your mouse over the sections in our Live Sample Receipt for more information.

Note: ReadNotify.com does not use or contain any Spyware, Malware, nor viruses, it is not illegal to use, and does not breach any privacy regulations in any countries.

What else does ReadNotify do?

There are lots of great features available to you – these include the following sending options:

- Certified E-Mail
- Ensured-Receipts and retractable E-Mails
- Invisible tracking
- Self-Destructing E-Mails
- Block printing
- Adobe Acrobat PDF Document Tracking
- Track MS Word or Excel documents

You can also choose how to receive your receipts:

- In your Personal Tracking Page (when you log in)
- E-Mail ReadNotifications
- Legal Proof-of-Opening receipts
- Delivery Service Notifications (DSN's)
- SMS alert on your cell-phone or pager
- Instant Messenger

These options are available to you from "My Account" in Member Utilities.

Check Your Progress 4

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of this Unit.

How ip address is gold for the tracking purposes?

....

....

....

....

....

....

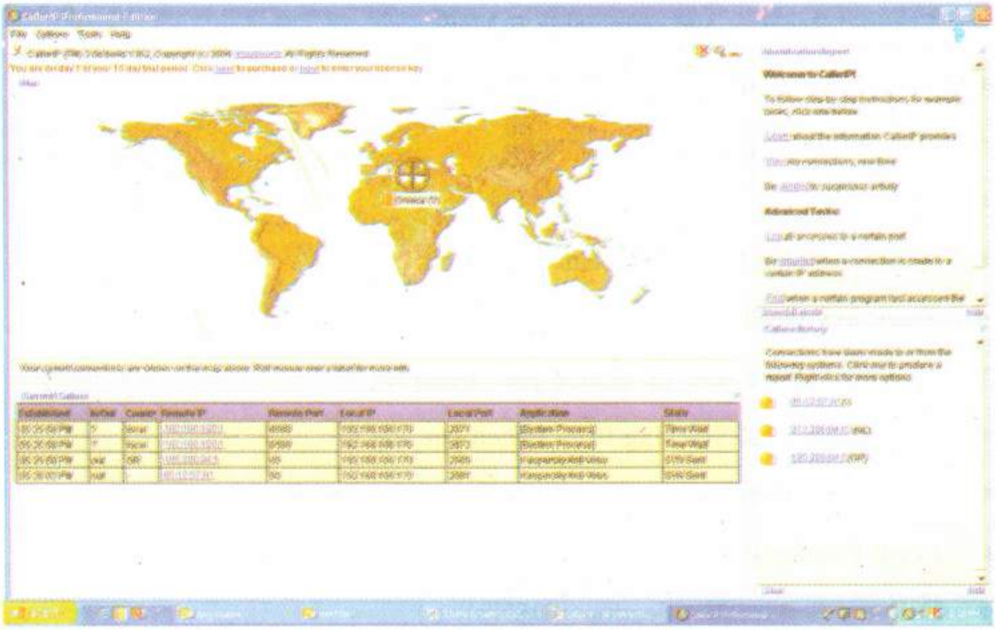
....

2.9 HOW TO TRACE IP ADDRESS

2.9.1 CallerIP

CallerIP Standard Edition allows real time monitoring of any machine that it is installed on. This allows you to detect suspicious activity such as spyware and see where in the world they are connecting from. Worldwide whois reports and network provider reports are also available for any connection!

Advanced CallerIP Advanced Edition (inc. all Standard features) allows you to run it as a server! This allows you to monitor the connections made to and from your machines from a remote location! Automated Alerts are also available to you are notified the moment something suspicious attempts a connection to your server(s).



- **Plot all connections**

  This feature enables you to have CallerIP plot all the connections on the world map. This in turn allows for easy and quick analysis of where connections made to/from your machine reside.

- **New look table**

  The new look table includes gradient fills. This means the colour of the row in the table depends on the threat of the connection. If the connection being made to your machine is harmless then the gradient will be green. It is another quick and easy way to identify the threat of a connection.

- **Condensed CallerIP**

  CallerIP now allows you to minimize it to a very small and detailed dialog box. The small window gives you everything you need to know but stays in the background.

- **Real-time monitoring instantly identifies suspect activity and spyware**

  CallerIP monitors all connections to and from your system and actively scans ports for possible back doors that allow unauthorized access.

- **Identifies the country of origin for all connections**

  A connection to/from a high-risk country is a key indicator of suspect activity and could likely be someone looking to steal your confidential information or compromise your system. CallerIP shows you the country location of connections so you can identify suspect activity and protect your information.

- **Network Provider reporting with abuse reporting information**

  See the contact and abuse reporting information for the company providing internet access for an IP address or website, so you can easily report hackers or Internet abuse.

- **Worldwide Whois reports**

  Caller IP Pro queries worldwide databases to report the up-to-date registration information for the 'owner' of an IP address or domain. Information includes name, address, phone and E-Mail contact information.

- **Detailed log of connection history with search options**

  Each connection or attempted connection is automatically logged, with search capabilities for quick lookups of past connection activity.

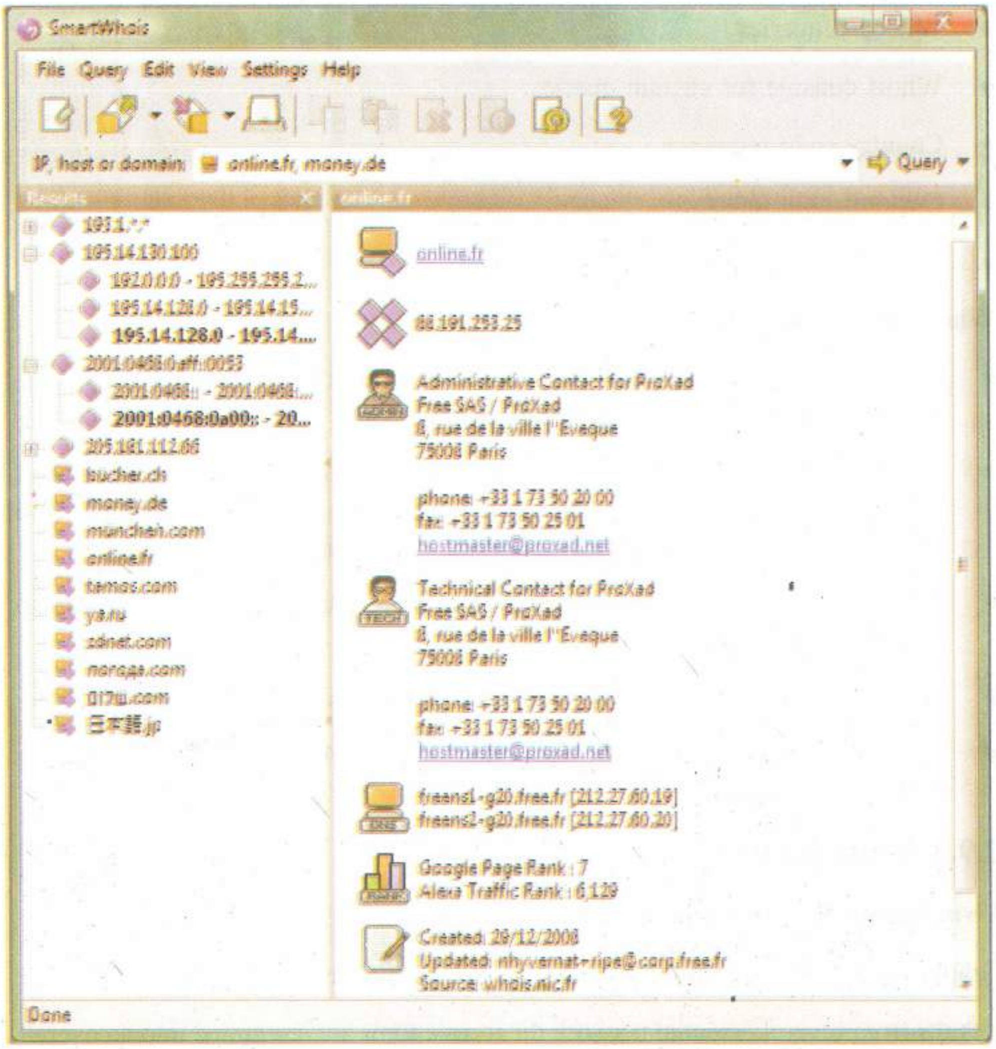
2.9.2 SmartWhois

SmartWhois is a useful network information utility that allows you to look up all the available information about an IP address, hostname or domain, including country, state or province, city, name of the network provider, administrator and technical support contact information. It helps you find answers to these important questions:

Who is the owner of the domain?

When was the domain registered and what is the owner's contact information?

Who is the owner of the IP address block?



IP, host or domain: online.fr, money.de

```
195.1.*.*
195.14.130.100
    192.0.0.0 - 195.255.255.2...
    195.14.128.0 - 195.14.15...
    195.14.128.0 - 195.14....
2001:0468:0:aff::0053
    2001:0468:: - 2001:0468:...
    2001:0468:0a00:: - 20...
205.161.112.66
bucher.ch
money.de
munchen.com
online.fr
temos.com
ya.ru
zdnet.com
noroga.com
017lu.com
日本語.jp
```

```
online.fr

88.191.253.25

Administrative Contact for ProXad
Free SAS / ProXad
8, rue de la ville l'Eveque
75008 Paris

phone: +33 1 73 50 20 00
fax: +33 1 73 50 25 01
hostmaster@proxad.net

Technical Contact for ProXad
Free SAS / ProXad
8, rue de la ville l'Eveque
75008 Paris

phone: +33 1 73 50 20 00
fax: +33 1 73 50 25 01
hostmaster@proxad.net

freens1-g20.free.fr [212.27.60.19]
freens2-g20.free.fr [212.27.60.20]

Google Page Rank : 7
Alexa Traffic Rank : 6,129

Created: 26/12/2008
Updated: nhyvernat-ripe@corp.free.fr
Source: whois.nic.fr
```

With SmartWhois you can focus on your work; the program will unmistakably choose the right database from over 100 whois databases all over the world and fetch the most complete results within a few seconds. SmartWhois supports Internationalized Domain Names (IDNs), so you can query domain names that use non-English characters, like German umlauts, French accent grave, or fully consist of the letters from Chinese, Hebrew, Russian, and other alphabets. It also fully supports IPv6 addresses.

Features:

- Smart operation: The program always looks up whois data in the right database; you don't have to waste your time trying them all.
- Integration with Microsoft Internet Explorer and Microsoft Outlook. Look up domain owners and IP addresses in E-Mail headers instantly!
- Saving results into an archive: you can build your own database that can be viewed offline.
- Batch processing of IP addresses or domain lists.
- Caching of obtained results.
- Hostname resolution and DNS caching.
- Integration with CommView Network Monitor: Can be accessed from CommView for quick, easy lookup.
- Calling SmartWhois directly from your application. See SmartWhois FAQ.
- Wildcard queries.
- Whois console for custom queries.
- Country code reference.
- Customizable interface.
- SOCKS5 firewall support.

Who needs SmartWhois

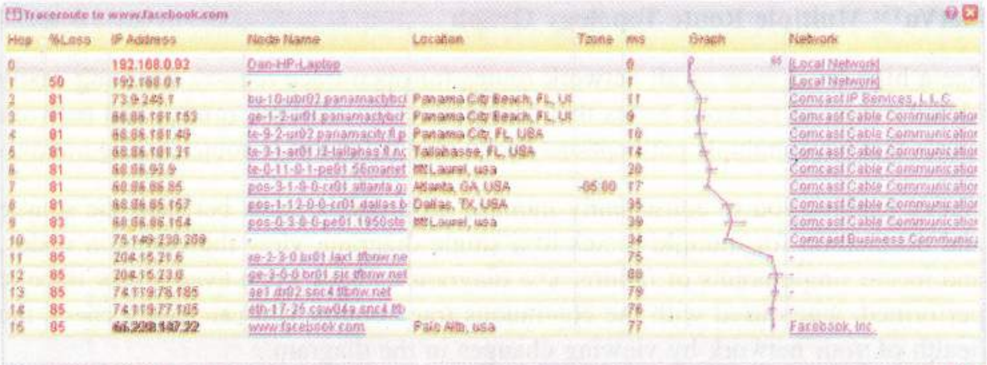
- Everyone who uses standard Whois utilities: SmartWhois saves a lot of time and does things standard Whois utilities can't do.
- People who hate spam or want to identify the origin of suspicious E-Mail messages: check the message header and locate the real sender! You can also send E-Mail to the network administrator with a mouse click.
- Webmasters who want to study the logs more carefully and are unable to identify many IP addresses.
- Online vendors who want to learn exactly where an order comes from.
- People who want to identify the origin of suspicious E-Mail messages by studying the headers.

2.9.3 VisualRoute

VisualRoute Features and Benefits

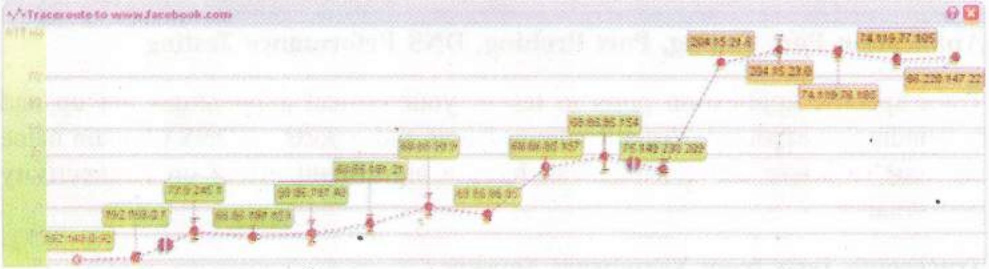
Graphical View of Traceroute provides key data in an easily digestible way.

Results from several essential network diagnostic tools are integrated into an overall connectivity report, providing a graphical view of connection performance report including packet loss and latency for each network hop. Drill-down detail is easily visible with a mouse over any network hop.



Traceroute to www.facebook.com

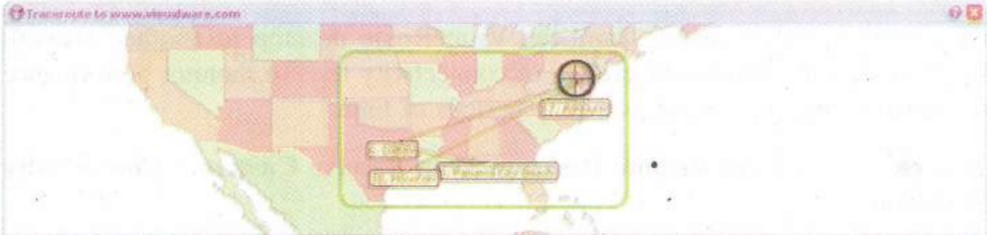
Hop	%Loss	IP Address	Node Name	Location	Tzone	ms	Graph	Network
0		192.168.0.92	Dan-HP-Laptop			0	65	Local Network
1	50	192.168.0.1	*			1		Local Network
2	81	73.9.245.1	bu-10-ubr02.panamactybc	Panama City Beach, FL, US		11		Comcast IP Services, L.L.C.
3	81	68.86.181.153	ge-1-2-ur01.panamactybc	Panama City Beach, FL, US		9		Comcast Cable Communicatior
4	81	68.86.181.49	te-9-2-ur02.panamacity.fl.p	Panama City, FL, USA		10		Comcast Cable Communicatior
5	81	68.86.181.21	te-3-1-ar01.l2-tallahas.fl.n	Tallahasse, FL, USA		14		Comcast Cable Communicatior
6	81	68.86.93.9	te-0-11-0-1-pe01.56manet	Mt Laurel, usa		20		Comcast Cable Communicatior
7	81	68.86.86.85	pos-3-1-0-0-cr01.atlanta.g	Atlanta, GA, USA	-05:00	17		Comcast Cable Communicatior
8	81	68.86.85.157	pos-1-12-0-0-cr01.dallas.b	Dallas, TX, USA		35		Comcast Cable Communicatior
9	83	68.86.86.164	pos-0-3-0-0-pe01.1950ste	Mt Laurel, usa		39		Comcast Cable Communicatior
10	83	75.149.230.209	*			34		Comcast Business Communic
11	85	204.15.21.6	ge-2-3-0.br01.lax1.tfbnw.ne			75		*
12	85	204.15.23.0	ge-3-0-0.br01.sjc.tfbnw.net			80		*
13	85	74.119.76.185	ae1.dr02.snc4.tfbnw.net			79		*
14	85	74.119.77.105	eth-17-26.csw04a.snc4.tfb			76		*
15	85	66.220.147.22	www.facebook.com	Palo Alto, usa		77		Facebook, Inc.



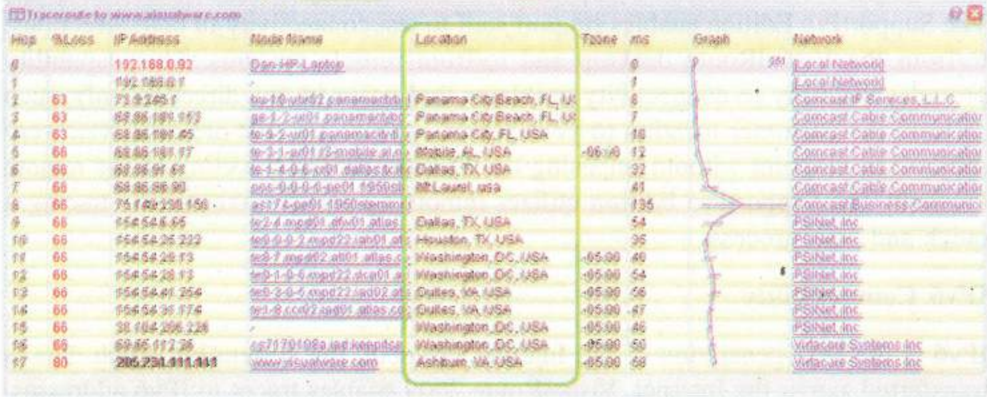
Traceroute to www.facebook.com

IP Location Reporting

The physical geographical locations of network servers and routers is key information for understanding routing problems, viewing the actual route path on global map provides an instant of picture of routing efficiency and distances. Try an IP trace online.



Traceroute to www.visualware.com



Traceroute to www.visualware.com

Hop	%Loss	IP Address	Node Name	Location	Tzone	ms	Graph	Network
0		192.168.0.92	Dan-HP-Laptop			0	581	Local Network
1		192.168.0.1	*			1		Local Network
2	63	73.9.245.1	bu-10-ubr02.panamactybc	Panama City Beach, FL, US		6		Comcast IP Services, L.L.C.
3	63	68.86.181.153	ge-1-2-ur01.panamactybc	Panama City Beach, FL, US		7		Comcast Cable Communicatior
4	63	68.86.181.45	te-9-2-ur01.panamacity.fl	Panama City, FL, USA		16		Comcast Cable Communicatior
5	66	68.86.181.17	te-3-1-ar01.l3-mobile.al.c	Mobile, AL, USA	-06:00	12		Comcast Cable Communicatior
6	66	68.86.91.68	te-1-4-0-6-cr01.dallas.tx.ib	Dallas, TX, USA		32		Comcast Cable Communicatior
7	66	68.86.86.90	pos-0-0-0-0-pe01.1950st	Mt Laurel, usa		41		Comcast Cable Communicatior
8	66	75.149.230.150	as174-pe01.1950stemmon			135		Comcast Business Communic
9	66	154.54.6.65	te2-4.mpd01.dfw01.atlas	Dallas, TX, USA		54		PSINet, inc
10	66	154.54.26.222	te9-0-0-2.mpd22.iah01.at	Houston, TX, USA		36		PSINet, inc
11	66	154.54.28.13	te8-7.mpd02.at01.atlas.c	Washington, DC, USA	-05:00	40		PSINet, inc
12	66	154.54.28.13	te0-1-0-6.mpd22.dca01.a	Washington, DC, USA	-05:00	54		PSINet, inc
13	66	154.54.41.254	te0-2-0-6.mpd22.iad02.at	Dulles, VA, USA	-05:00	56		PSINet, inc
14	66	154.54.35.174	te1-8.ccr02.iad01.atlas.co	Dulles, VA, USA	-05:00	47		PSINet, inc
15	66	38.104.206.226	*	Washington, DC, USA	-05:00	46		PSINet, inc
16	66	69.65.112.26	cs7170198a.iad.kenpdsa	Washington, DC, USA	-05:00	50		Vidacare Systems inc
17	80	205.234.111.111	www.visualware.com	Ashburn, VA, USA	-05:00	68		Vidacare Systems inc

Whois Lookups, Network Provider Reporting

Get instant lookups of domain information from worldwide databases, so you can see the registered 'owner' of an IP address or domain. See the contact information for the company providing Internet access for each hop of a network route, so you can easily report network problems.

OmniPath™ Multiple Path Discovery

Get real-time views of all possible routes to a destination and easily compare the performance of different routes. The common use of load-balancers creates multiple paths that data packets may travel between the source and destination. OmniPath discovers the various paths, enables you to easily see which routes are the fastest/slowest, have the highest/lowest packet loss, or have the highest probability. More info.

NetVu™ Multiple Route Topology Graph

See a high-level view of all network routes for open trace reports, enabling easily identification of network nodes that are common to multiple routes, and network routes that have multiple path options due to load balancers or router configurations.

NetVu enables you to consistently monitor all possible paths between the source and destination for mutiple routes in a single diagram, view the common nodes, and locate single points of failure. The diagram updates when even a new trace is performed, when used with the continuous trace option you can easily check the health of your network by viewing changes in the diagram.

Application Port Testing, Port Probing, DNS Peformance Testing

Trace specific application ports to test if your critical applications are up and responding as expected. VisualRoute measures and reports on DNS (domain name service) response time, which can have a significant effect on connectivity performance.

Traceroute Tests from Visualware Servers

Test from Visualware servers in Washington and London to test connectivity to your servers or network devices. This capability provides additional testing points to help identify network routes and network providers causing poor performance. Try a traceroute test now.

Continuous Connection Testing with Report History

Continuous network testing from the VisualRoute desktop to another network location supports automated cycling of connectivity tests to monitor performance degradation that may occur over long periods of time.

Reverse Traces from Remote Desktops Help Resolve Customer Connectivity Problems

The SupportPro Edition enables support staff to test connectivity in both directions: to/from the VisualRoute desktop and to/from remote systems. This capability provides visibility to connectivity problems that occur in one direction only, such as from the customer location to your server -- problems that are otherwise very difficult to pinpoint without imposing on the customer or traveling to the remote location. The SupportPro Edition utilizes remote agents to make reverse tracing a quick and easy process.

IPv6 Compatibility

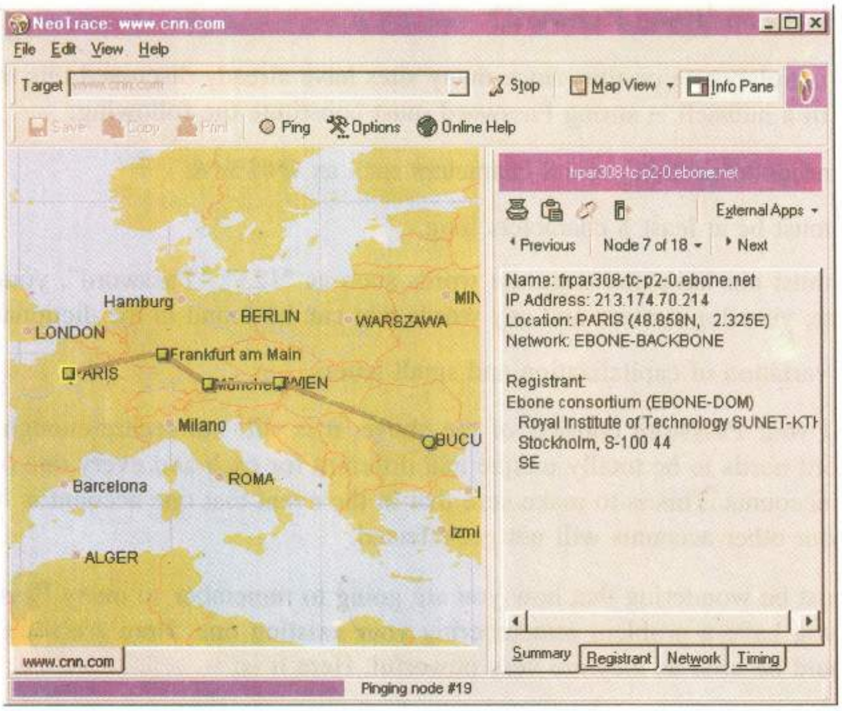
IPv6 is the next generation of the Internet Protocol, the system by which data is transferred across the Internet. VisualRoute 2009 enables traces to IPv6 addresses, including IPv6 domain and network provider lookups.

2.9.4 McAfee NeoTrace Professional

McAfee NeoTrace Pro delivers a powerful tool for checking information on internet locations.

You can trace any computer on the internet simply by entering an E-Mail, IP address or URL. The display shows you the route between you and the remote site including all intermediate nodes and their registrant information.

McAfee NeoTrace is the world's most popular Internet tracer, used by law enforcement, ISPs, and network professionals, yet easy enough for the home user. Explore the powerful new features designed to make our most popular product even easier to use!



Name: frpar308-tc-p2-0.ebone.net
IP Address: 213.174.70.214
Location: PARIS (48.858N, 2.325E)
Network: EBONE-BACKBONE

Registrant:
Ebone consortium (EBONE-DOM)
Royal Institute of Technology SUNET-KTH
Stockholm, S-100 44
SE

Features:

- Internet Explorer Integration Website tracing is just a click away with our IE browser integrated Trace Button.
- Variety of Graphical Information The Node View complements improvements in our existing Map and List Views, offering users a wide range of graphical data for precision tracing.
- Detailed Map View Map View shows most detailed available map for current view using expanded regional information.
- Streamlined List View Node data is simple to understand with an integrated graph and an array of user-configurable data columns.
- Expanded Geographical Data Improves accuracy of node placement with increased server based lookups for all traces.
- HackerWatch.org Event Reporting when using McAfee NeoTrace in conjunction with a firewall it is simple to submit event reports to HackerWatch right from McAfee NeoTrace.
- Mail Server Tracing E-Mail address entry allows McAfee NeoTrace to locate the mail server for that address.
- Many Save Formats Allows trace data, maps or both to be saved in formats such as JPG, PNG, BMP, HTML, RTF, and plain text

2.10 SECURING E-MAIL ACCOUNTS

To secure the E-Mail Account from the Crackers/ Hackers is one of the major challenges for all of us now a days. However, we can still try our level best to making it secure by using the following ways mentioned below:

2.10.1 Creating Strong Passwords

Creating strong Passwords for all your online accounts is not a thing you should do. It is one of the most important thing you must do. In case you are still thinking that your Password is strong and safe, maybe it's time to wake up.

What makes a strong Password?

I shall not elaborate on this, since many sites have already discussed this in great detail. In a nutshell, a strong Password must constitute the following:

- It needs to contain special characters such as @#$%^&
- It must be at least 8 characters long.
- It must not have any common words such as "123", "Password", your birth date, your login name and any words that can be found in the dictionary.
- A variation of capitalization and small letters.

Even if your Password consists of the above, it is still not secure enough. Your Password needs to be totally unique and different for each and every one of your online accounts. This is to make sure that in the event that one account is hacked into, your other accounts will not get affected.

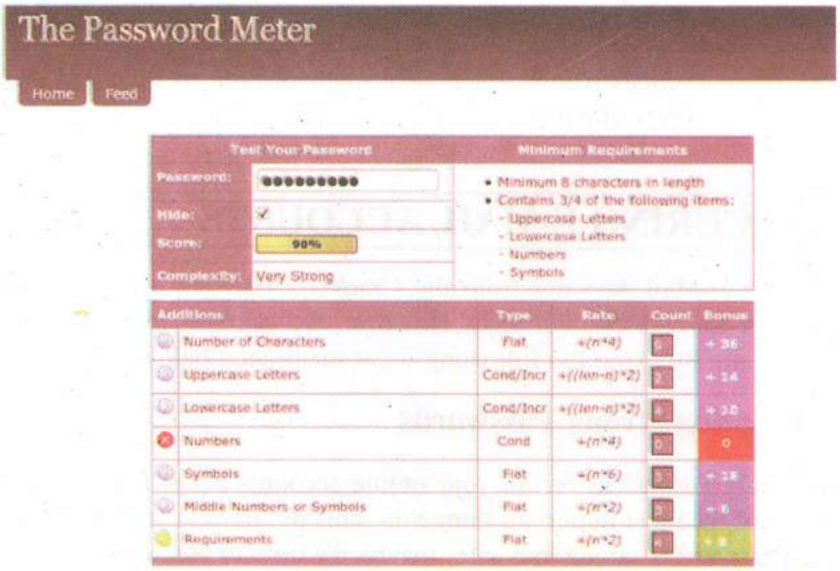
You must be wondering that how you are going to remember so many Passwords when you have a problem remembering your existing one. Here are some steps that could be used as they are very powerful. Here it is;

1) First, think of a thing, date, phrase, event, place or anything that is unique only to you. It must be of at least 8 characters long. For demonstration purpose, a name "Damien Oh" will be used as the term throughout this topic. Note that the capital letters and the space in between the name are part of this term. For your own account, please select a term that is difficult for others to guess.

2) Use the following rules to replace the regular characters with special characters. You could even form your own rules.

   - Replace all the 'a' with @
   - Replace all the 's' with $
   - Replace any space with %
   - Replace any 'o' with 0
   - Replace any 'i' with !
   - In this case, the simple term Damien Oh becomes D@m!en%Oh.

3) Now go to Password Meter (see "MakeUseOf" review here) and test the strength of your term. This is the result of the above term. If your term is not strong enough, you will see a list of items that you can improve on.



Test Your Password		Minimum Requirements
Password:	●●●●●●●●●●	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	✓	
Score:	90%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	9	+ 36
Uppercase Letters	Cond/Incr	+((len-n)*2)	2	+ 14
Lowercase Letters	Cond/Incr	+((len-n)*2)	4	+ 10
✗ Numbers	Cond	+(n*4)	0	0
Symbols	Flat	+(n*6)	3	+ 18
Middle Numbers or Symbols	Flat	+(n*2)	3	+ 6
Requirements	Flat	+(n*2)	4	+ 8

4) Once you are happy with your term and are sure that only you can decipher it, go to any of your online accounts now. To set a Password for that account, append the name of the site, or the URL of the site to the end of your term.

For example, for a MakeUseOf account, you may use D@m!en%OhM@keU$e0f as your Password and use D@m!en%OhG00glem@!l for Gmail account. If you do this for each and every one of your sites, you will be surprised to find that you have just created tens, hundreds, or even thousands of different Passwords that you can be remembered easily. Instead of the site name or the URL, you can also put a variation of the site names or any other names that are related to the site.

Is that enough?

That is just the beginning. To really make it secure and hard for others to guess, you must change your Passwords on frequent basis. Some of you may find it an assignment to come up with new Passwords every month. Here is what you can do:

Instead of appending the site name to the end, you can now append it to the front, in the middle or even split the site name out into few parts. For example:

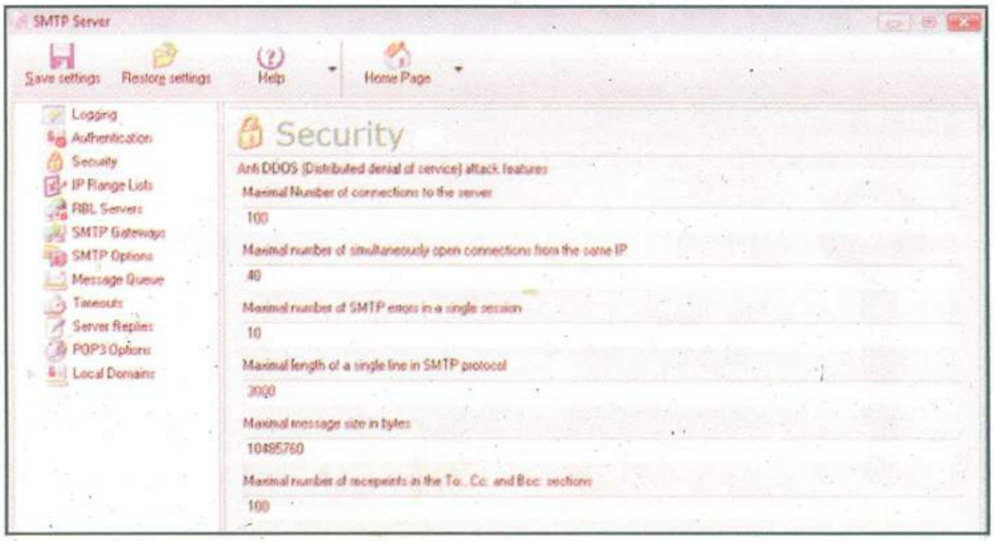
- M@keD@m!enU$e0h0f
- M@keU$eD@m!en%0h

You can also change the replacement characters such as @ for ~ and whatsoever. You can also do a complete changeover of your term to come up with a totally different Password.

Some important points to be noted

- Always check the strength of the Password provided to you on Password strength meter.
- At the time of creating a new mail account provide verification question so that it can be used to recover the forgotten Password for that particular E-Mail id.
- Always try to provide the secondary E-Mail id so that new Password could be mailed or Password change instructions could be mailed to you on that particular mail id.
- Never click on "Keep me sign in" check box, if you have selected this option and if Attacker gains access of your computer then he can sign in your account as well as he can recover your Password.

2.10.2 E-Mail Protector



Anti DDOS (Distributed denial of service) attack features

Maximal Number of connections to the server
100

Maximal number of simultaneously open connections from the same IP
40

Maximal number of SMTP errors in a single session
10

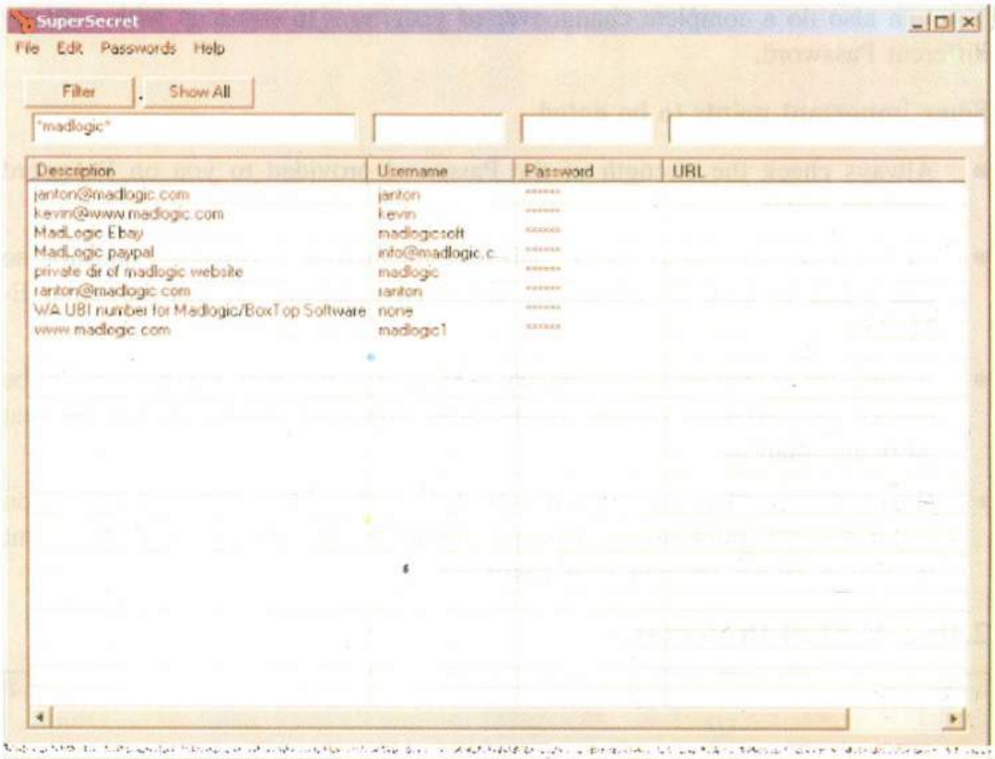
Maximal length of a single line in SMTP protocol
3000

Maximal message size in bytes
10485760

Maximal number of recepeints in the To:, Cc: and Bcc: sections
100

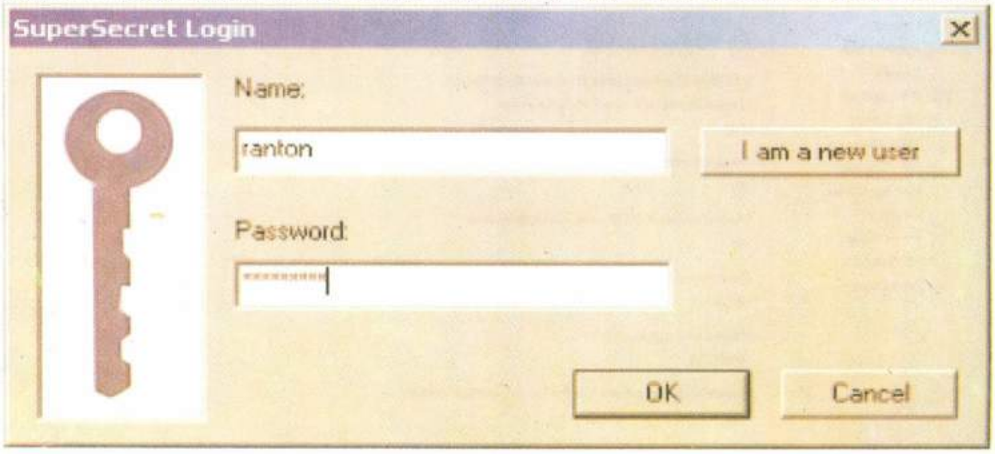
Do you know that when you send your E-Mail messages, they do not go directly to recipient mailboxes? Do you know that your Internet Service Provider (ISP) stores copies of all your E-Mail messages on its mail servers before it tries to deliver them? Do you know that someday all the information kept on the servers can be easily used against you? E-Mail Security is a system-tray local SMTP server program for Windows that lets you send E-Mail messages directly from your PC to recipient mailboxes ensuring your E-Mail security and privacy by means of bypassing your ISP's mail servers where your relevant information can be stored and viewed. Do you also know that when you send an E-Mail message to a list of E-Mail addresses, the respondents can see each other in the E-Mail message header? You think it is secure? While sending, E-Mail Security always breaks E-Mail messages addressed to a group of people to individual messages to ensure your security and security of your respondents. Also, E-Mail Security does not leave any traces on your PC because it just gets your E-Mail messages from your E-Mail client and puts them in the recipient mailboxes at the same time without making any temporary files on your PC. E-Mail Security supports all E-Mail programs like Outlook Express, Outlook, Eudora, etc. The E-Mail program you already use for sending and receiving messages can be connected to E-Mail Security in a very easy way – just by using the word "localhost" instead of your current SMTP host. Having done so, you can send messages in a usual manner. Install E-Mail Security on your PC before it is too late!

2.10.3 SuperSecret



"madlogic"

Description	Username	Password	URL
janton@madlogic.com	janton	******	
kevin@www.madlogic.com	kevin	******	
MadLogic Ebay	madlogicsoft	******	
MadLogic paypal	info@madlogic.c...	******	
private dir of madlogic website	madlogic	******	
ranton@madlogic.com	ranton	******	
WA UBI number for Madlogic/BoxTop Software	none	******	
www.madlogic.com	madlogic1	******	



Name: ranton

Password: *********

SuperSecret provides secure storage for all of your logins and Passwords so that you only have one Password to remember from now on. SuperSecret supports multiple users on the same computer using different SuperSecret login names so that you can keep your Passwords private, even if you share a computer with others at work or home. Now with version 2 SuperSecret supports filtering Passwords by the login name, Password, or the entry description so that you can quickly find the Password you need. You can also store a URL for each entry so you never forget where you need to go to access your online accounts. SuperSecret can generate secure, random Passwords for you.

Only one Password is required to use SuperSecret. All of your other account and Password information is stored securely in an encrypted format on your computer and can be accessed only with your one and only Password. SuperSecret allows each family member or co-worker to have his/her own storage area for Passwords. Your confidential information is safe even if prying intruders are sitting at your computer, because SuperSecret's data can only be accessed by your one secret Password.

Use SuperSecret to remember all of your Passwords. Remember your Password to your personal E-Mail address, business E-Mail address, online banking login and Password. Store any kind of secret with SuperSecret. Keep track of the PIN number to that ATM/debit card you never use. Others will not be able to access your private information. And SuperSecret is quick and easy to use. Simply double click on an empty entry to add a new login and Password or double click on an existing entry to edit it.

Select the entry you need the Password for and the Password will be displayed; deselect the entry and the Password will be hidden again to protect you from anyone who may look over your shoulder.

You can keep SuperSecret open to save time by minimizing it to the taskbar for easy access. SuperSecret runs on Windows 95, Windows 98, Windows ME, Windows NT, Windows 2000, and Windows XP.

Check Your Progress 5

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of this Unit.

What are the different ways of tracing ip address? Expalin any one. Highlights the points of securing E-Mail accounts?

....

....

....

....

....

....

....

....

....

....

....

2.11 LET US SUM UP

This unit throws light on "E-MAIL CRIME AND INVESTIGATION". E-Mail, as simple as it is to use, relies on a more complicated set of operating procedures than that of the Web. For most users, its operation is transparent, which means that it is not necessary to understand how email works in order to be able to use it.

This unit help users to understand its basic principles, give them an idea of how to best configure their email clients and inform them about the underlying mechanisms of spam. This unit also provides useful background information on E-Mail security issues. It will help you to examine the security threats facing by your corporate E-Mail system and determine what kind of E-Mail security solution your company needs. A variety of different elements weaken your corporate email system and while some are widely known – such as email viruses – others tend to be ignored. Emails carrying offensive messages or confidential corporate information can create immense inconvenience and expense for a company that has not equipped its mail server with the appropriate tools. The same goes for spammers who use the email system at work to send thousands of unsolicited email messages.

2.12 CHECK YOUR PROGRESS: THE KEY

1) An electronic mail message consists of two components, the message header, and the message body, which is the E-Mail's content. etwork routes and network providrol information, including, minimally, an originator's E-Mail address and one or more recipient addresses. Usually additional information is added, such as a subject header field.

   Originally a text-only communications medium, E-Mail was extended to carry multi-media content attachments, which was standardized in RFC 2045 through RFC 2049, collectively called, Multipurpose Internet Mail Extensions (MIME).

   The user Mail User Agent formats the message in E-Mail format and uses the Simple Mail Transfer Protocol (SMTP) to send the message to the local mail transfer agent (MTA), in this case smtp.a.org, run by user's internet service provider (ISP).

   The MTA looks at the destination address provided in the SMTP protocol (not from the message header), in this case bob@b.org. An Internet E-Mail address is a string of the form localpart@exampledomain. The part before the @ sign is the local part of the address, often the username of the recipient, and the part after the @ sign is a domain name or a fully qualified domain name. The MTA resolves a domain name to determine the fully qualified domain name of the mail exchange server in the Domain Name System (DNS).

2) A mail message consists of a header, which contains information about who the message was sent from, the recipient(s) and the route. Many of the header fields are not shown by default, but most programs used to read E-Mail will allow full headers to be displayed. This is then followed by the body of the message which contains whatever the sender wishes.

   The message header should include at least the following fields:

   - **From:** The E-Mail address, and optionally the name of the author(s). In many E-Mail clients not changeable except through changing account settings.

   - **To:** The E-Mail address/addresses and optionally name(s) of the message's recipient(s). Indicates primary recipients (multiple allowed).

- **Cc:** Carbon copy; many E-Mail clients will mark E-Mail in your inbox differently depending on whether you are in the To: or Cc: list.
- **Bcc:** Blind Carbon Copy; addresses added to the SMTP delivery list but not (usually) listed in the message data, remaining invisible to other recipients.
- **Subject:** A brief summary of the topic of the message. Certain abbreviations are commonly used in the subject, including "RE:" and "FW:".
- **Message-ID:** Also an automatically generated field; used to prevent multiple delivery and for reference in In-Reply-To.

The header consists of lines beginning with a keyword followed by a colon (:), followed by information on each line. A brief explanation of each field of the header is given below. This header contains most of the common fields.

- **Received:** These lines indicate the route that the E-Mail has taken and which systems have handled it and the times that it was handled.
- **Date:** The date and time at which the message was sent including time zone.
- **From:** The sender. The part in angle brackets is a real electronic mail address. This field may be user settable, so may not reflect the true sender. In this case, it shows the original sender of the message.
- **Sender:** The sender. This is inserted by some systems if the actual sender is different from the text in the From: field. This makes E-Mail more difficult to forge, although this too can be set by the sender. There are other uses for a sender field. In the example above, the sender is set to the list owner by the mailing list system. This allows error messages to be returned to the list owner rather than the original sender of the message
- **To:** Who the mail is sent to. This may be a list or an individual. However it may bear no relation to the person that the E-Mail is delivered to. Mail systems used a different mechanism for determining the recipient of a message.
- **Cc:** Addresses of recipients who will also receive copies.
- **Subject:** Subject of the message as specified by the sender.
- **Message-id:** A unique system generated id. This can sometimes be useful in fault tracing if multiple copies of a message have been received.
- **Reply-to:** Where any reply should be sent to (in preference to any electronic mail address in the From: field if present). This may be inserted by the sender, usually when they want replies to go to a central address rather than the address of the system they are using. It is also inserted automatically by some systems
- **X-Mailer:** Any field beginning with X can be inserted by a mail system for any purpose.

The major E-Mail related crimes are:

i) E-Mail spoofing

ii) Sending malicious codes through E-Mail

iii) E-Mail bombing

iv) Sending threatening E-Mails

v) Defamatory E-Mails

vi) E-Mail frauds

3) **Received tags:** as on web blogs, reading from the bottom to top. The header says the E-Mail was originally sent from 206.85... and it was sent to 217.225... (which is the name/IP of the first mail server that got involved into transporting this message). Then suddenly, the next Received tag says the message was received from root@localhost, by mailv.fx.ro. One can also notice that so far, the Received tags do not contain any information about how the E-Maïl was transmitted (the "with" tag is missing: this tag tells the protocol used to send the E-Mail).

The Message-ID field is a unique identifier of each E-Mail message. It is like the tracing ID of an express postal mail. The rule says the ID is composed by the name of the server that assigned the ID and a unique string (for example, QESADJHO@E-Mailaddressmanager.com).

4) For tracking purposes, the user is most interested in the from and by tokens in the Received header field. The pattern similar to:

Received: from BBB (dns-name [ip-address]) by AAA ...

Received: from CCC (dns-name [ip-address]) by BBB ...

Received: from DDD (dns-name [ip-address]) by CCC ...

In other words, mail server AAA received the E-Mail from BBB and provides as much information about BBB, including the IP Address BBB used to connect to AAA. This pattern repeats itself on each Received line. The syntax of the from token most times looks like: name (dns-name [ip-address])

Where: name is the name the computer has named itself. Most of the time user never look at this name because it can be intentionally misnamed in an attempt to foil your tracking (but it may leak the windows computer name). dns-name is the reverse dns lookup on the ip-address. ip-address is the ip-address of the computer used to connect to the mail server that generated this Received header line. So, the ip-address is gold to us for tracking purposes.

The by token syntax just provides us with the name that the mail server gives itself. But since the last mail server could be under the control of a spammer, one should not trust this name.

So, what is crucial for tracking, is to pay attention to the trail of ip-address in the from tokens and not necessarily the host name provided to us in the by tokens. For Example;

1: Received: from **tes1a623.OnE-Mail.com.sg** ([203.127.89.129]) by visualroute.com (8.11.6) id f9CIVSk24480; Tue, 12 Oct 2004 12:31:29 -0600 (MDT)

3: Received: from drb.com (IIM1608 [203.127.89.138]) by **tes1a623.OnE-Mail.com.sg** with SMTP (Microsoft Exchange Internet Mail Service Version 5.5.2448.0)

If one ignores line 1, one would conclude from line 3 that mail server tes1a623.OnE-Mail.com.sg sent you an E-Mail, but this would be wrong. When one trace to the host name tes1a623.OnE-Mail.com.sg, you are actually tracing to the IP Address lookup on that host name, which is 192.9.200.230. But as one can see from line 1, the IP Address used was really 203.127.89.129. Do not be fooled by this attempted misdirection by spammers and fraudsters.

Determine the IP Address of the Sender: Using the example E-Mail headers above and analyzing the Received header lines we can conclude:

- A Visualware employee received an E-Mail
- which came from visualroute.com (line 1)
- which came from tes1a623.OnE-Mail.com.sg (line 1; line 3 confirms)
- but whose ip-address used was 203.127.89.129 (line 1)
- which came from drb.com/IIM1608 (line 3)
- but whose ip-address used was 203.127.89.138 (line 3)

So, we have just tracked this E-Mail to the source — IP Address **203.127.89.138.**

The different ways of tracing IP addresses are:

i) CallerIP

ii) SmartWhois

iii) VisualRoute

iv) McAfee NeoTrace Professional

CallerIP Standard Edition allows real time monitoring of any machine that it is installed on. This allows you to detect suspicious activity such as spyware and see where in the world they are connecting from. Worldwide whois reports and network provider reports are also available for any connection!

Advanced CallerIP Advanced Edition (inc. all Standard features) allows you to run it as a server! This allows you to monitor the connections made to and from your machines from a remote location! Automated Alerts are also available to you are notified the moment something suspicious attempts a connection to your server(s).

- **Plot all connections**

  This feature enables you to have CallerIP plot all the connections on the world map. This in turn allows for easy and quick analysis of where connections made to/from your machine reside.

- **New look table**

  The new look table includes gradient fills. This means the colour of the row in the table depends on the threat of the connection. If the connection being made to your machine is harmless then the gradient will be green. Another quick an easy way to identify the threat of a connection.

- **Condensed CallerIP**

  CallerIP now allows you to minimize it to a very small and detailed dialog box. The small window gives you everything you need to know but stays in the background.

- **Real-time monitoring instantly identifies suspect activity and spyware**

  CallerIP monitors all connections to and from your system and actively scans ports for possible back doors that allow unauthorized access.

- **Identifies the country of origin for all connections**

  A connection to/from a high-risk country is a key indicator of suspect activity and could likely be someone looking to steal your confidential information or compromise your system. CallerIP shows you the country location of connections so you can identify suspect activity and protect your information.

- **Network Provider reporting with abuse reporting information**

  See the contact and abuse reporting information for the company providing internet access for an IP address or website, so you can easily report hackers or Internet abuse.

- **Worldwide Whois reports**

  Caller IP Pro queries worldwide databases to report the up-to-date registration information for the 'owner' of an IP address or domain. Information includes name, address, phone and E-Mail contact information.

- **Detailed log of connection history with search options**

  Each connection or attempted connection is automatically logged, with search capabilities for quick lookups of past connection activity.

For securing E-Mail accounts:

a) The user should Create Strong Passwords

b) E-Mail Protector

c) SuperSecret

UNIT 3 REVERSE ENGINEERING

Structure

3.0 INTRODUCTION

Reverse engineering is the general process of analyzing a technology specifically to ascertain, how it was designed or how it operates. This kind of inquiry engages individuals in a constructive learning process about the operation of systems and products. Reverse engineering as a method, is not confined to any particular purpose, However it is often an important part of the scientific method and technological development. The process of taking something apart and revealing the way in which it works is often an effective way to learn how to build a technology or make improvements to it. In this unit, you'll establish a thorough knowledge about the various aspects of reverse engineering and how is it useful in the today E-World.

In day to day work, whether it's rebuilding a vehicle engine or rearrenging a sentence, people can learn about many things simply by taking them apart and putting them back together again. The concept behind everything is reverse-engineering, which means breaking something down in order to understand it, build a copy or improve it.

In this Unit we'll understand the key elements that comprise a successful reverse engineering program and eventually apply those concepts for better productivity. Reverse-engineering is used for many purposes: as a learning tool; as a way to make new, compatible products that are cheaper than what's currently on the market; for making software interoperate more effectively or to bridge data between different operating systems or databases; and to uncover the undocumented features of commercial products.

3.1 OBJECTIVES

After going through this Unit, you should be able to:

- Understand the importance of Reverse Engineering;
- Need of Reverse Engineering;
- Stages involved in the Reverse Engineering Process;
- What is a Disassembler?;
- How Software Protection could be cracked; and
- Make hands on various tools which are very important in reverse Engineering.

3.2 WHAT IS REVERSE ENGINEERING?

Reverse Engineering is a process where, a researcher gathers the technical data necessary for the documentation of the operation of a technology or component of a system. With the help of this research method researchers are able to examine the strength of the softwares, applications, systems etc. and identify their weaknesses in terms of performance, security, and interoperability. The reverse engineering process allows researchers to understand both how a program works and also what aspects of the program contribute to its not working. Independent manufacturers can participate in a competitive market that rewards the improvements made on dominant products. For example, there are lot of vendors who does the security audits like 'Sedulity Solutions & Technologies', which allow users of software to better protect their systems and networks by revealing security flaws, which ultimately require reverse engineering. The creation of better designs and the interoperability of existing products often begin with Reverse Engineering.

Reverse engineering is taking apart an object to see how it works in order to duplicate or enhance the object. The practice, taken from older industries, is now frequently used on computer hardware and software. Software reverse engineering involves reversing a program's machine code (the string of 0s and 1s that are sent to the logic processor) back into the source code that it was written in, using program language statements.

Reverse engineering can be viewed as the process of analysing a system to:

1) Identify the system's components and their interrelationships
2) Create representations of the system in another form or a higher level of abstraction
3) Create the physical representation of that system

There are two types of Reverse Engineering, which are mentioned as below:

- Software Reverse Engineering,
- Hardware Reverse Engineering.

3.2.1 Software Reverse Engineering

Software reverse engineering is the process to retrieve the source code of a program. It is a process of reading the software's binary code to find what the software can make the computer do. It is the code that the computer reads and obeys, not the source code. Though binary code is not easily read by humans, a representation in assembly-language mnemonics, as shown in a debugger, is exactly equivalent (on all but some very obscure theoretical points) to what the computer reads. Indeed, reverse engineering is essentially debugging in advance of having a bug to debug. The process is implemented in few of the scenarios like;

- If the source code is lost,
- To study how the program performs certain operations,
- To improve the *performance* of a program,
- To *fix a bug* (correct an error in the program when the source code is not available),
- To identify malicious content in a program such as a virus or to adapt a program written for use with one microprocessor for use with another.

Reverse engineering for the purpose of copying or duplicating programs may constitute a copyright violation. In fact, in some cases, the licensed use of software specifically prohibits reverse engineering.

Any researcher who is doing reverse engineering on software may use several tools to disassemble a program which are mentioned as below;

- **Hexadecimal dumper:** It prints or displays the binary numbers of a program in hexadecimal format (which is easier to read than a binary format). By knowing the bit patterns that represent the processor instructions as well as the instruction lengths, the reverse engineer can identify certain portions of a program to see how they work.
- **Disassembler.** This is another important tool which helps to reads the binary code and then displays each executable instruction in text form. A disassembler cannot tell the difference between an executable instruction and the data used by the program so a debugger is used, which allows the disassembler to avoid disassembling the data portions of a program. These tools might be used by a cracker to modify code and gain entry to a computer system or cause other harm.

3.2.2 Hardware Reverse Engineering

Hardware reverse engineering involves taking apart a device to see how it works. Reverse engineering at the hardware level involves taking the allegedly infringing product apart, determining what components are used in the product, and determining how the components are interconnected. For example, if a processor manufacturer wants to see how a competitor's processor works, he can purchase a competitor's processor, disassemble it, and then make a processor similar to it along with some modifications or by adding some new features. However, this process is illegal in many countries. In general, hardware reverse engineering requires a great deal of expertise and is quite expensive.

It is often not sufficient to reverse engineer a product to the component level in order to determine infringement. Many products incorporate microprocessors or microcontrollers in their design. A microprocessor or microcontroller operates in accordance with programming instructions programmed into a ROM, RAM, EPROM, or FLASH memory. To determine how the microcontroller or microprocessor operates it is necessary to reverse engineer the software or firmware within the memory.

This is not as easy as one might think. First, the program embodied by the firmware is simply a collection of binary digits (1's and 0's). In order to decipher this machine specific program code it is necessary not only to convert the binary data into a readable form, but to assign meaning to the data. Thus, reverse engineering of microcontroller software or firmware requires program disassembly via a disassembler or decompiler.

Reverse engineering enables the duplication of an existing part by capturing the component's physical dim^nsions, features, and material properties. Before attempting reverse engineering, a well-planned life-cycle analysis and cost/benefit analysis should be conducted to justify the reverse engineering projects. Reverse engineering is typically cost effective only if the items to be reverse engineered reflect a high investment or will be reproduced in large quantities. Reverse engineering of a part may be attempted even if it is not cost effective, if the part is absolutely required and is mission-critical to a system.

Any researcher who is doing reverse engineering on hardware may use several tools to disassemble a product which are mentioned as below;

- **REFAB (Reverse Engineering - Feature Based):** This tool uses a laser digitizer to scan the part, and the analysis software then analyses the shape of the part, using features which are based on typical machining operations, to generate a computerized manufacturing description which can be displayed, used to copy the product, or produce new products using the design.
- **PRINTED CIRCUIT BOARDS (PCBS):** Computer vision has been widely used to scan PCBs for quality control and inspection purposes, and based on this, there are a number of machine vision for analysing and reverse engineering PCBs.
- **INTEGRATED CIRCUIT (IC) COMPONENTS:** The first step is to get through the encapsulating material into the product itself, by chemical etching or grinding. Once at the chip surface, each layer of components is photographed, then ground away to reveal the layer below. This process reveals the structure of the chip. Although these processes can reveal the structure of the chip, they do not indicate the voltages at each point. However, if the chip is undamaged, voltage contrast electron microscopy can be used to scan the chip in use, and watch the voltage level change over time. These processes are generally referred to as "stripping" or "peeling" the chip.

3.3 NEED OF REVERSE ENGINEERING

Reverse engineering is very common in such diverse fields as software engineering, entertainment, automotive, consumer products, microchips, chemicals, electronics, and mechanical designs. For example, when a new machine comes to market, competing manufacturers may buy one machine and disassemble it to learn how it was built and how it works. A chemical company may use reverse engineering to defeat a patent on a competitor's manufacturing process. In civil engineering, bridge and building designs are copied from past successes so there will be less chance of catastrophic failure. In software engineering, good source code is often a variation of other good source code.

Another reason for reverse engineering is to compress product development times. In the intensely competitive global market, manufacturers are constantly seeking new ways to shorten lead-times to market a new product. Rapid product development (RPD) refers to recently developed technologies and techniques that assist manufacturers and designers in meeting the demands of reduced product development time. For example, injection-moulding companies must drastically reduce the tool and die development times. By using reverse engineering, a three-dimensional product or model can be quickly captured in digital form, re-modelled, and exported for rapid prototyping/tooling or rapid manufacturing.

Software developers often use reverse engineering techniques to better understand systems with which their software will interact. In addition, developers use reverse engineering to learn the ideas behind other developers' successful techniques. Most commercial software packages are distributed to customers in machine language. Therefore, humans must disassemble programs, translating them from machine language to assembly language, in order to better understand the ideas on which they are based.

It is not possible to reconstruct the original sequence of a program or the programmers' comments and annotations which are usually a part of high-level language programs, but through disassembly, programmers can gain insight into the way a program functions and how it can interface with other software and hardware.

There are various important factors which influence the Reverse Engineering which are mentioned as below:

- Interoperability: Interoperability is a property of a product or system, whose interfaces are completely understood, to work with other products or systems, present or future, without any restricted access or implementation. Generally, interoperability allows technologies to work together when they use the same inputs and create the same outputs. For computers, interoperability is the ability of programs and systems running on various kinds of software and hardware to communicate with each other.

  Standards foster interoperability by ensuring that all groups implementing the standard interpret it the same way, so that the technology produces consistent performance regardless of the individual brand or model. By contrast, a lack of standards means that parties must reverse engineer the technology to achieve interoperability. Moreover, owners of proprietary, non-standardized technologies retain control over upgrades and developments to those technologies, and may change them at will, disrupting the interoperability with other technologies.

- **Lost documentation:** Reverse engineering often is done because the documentation of a particular device has been lost or was never written, and the person who built it is no longer available. Integrated circuits often seem to have been designed on obsolete, proprietary systems, which means that the only way to incorporate the functionality into new technology is to reverse-engineer the existing chip and then re-design it.

- **Product analysis:** To examine how a product works, what components it consists of, estimate costs, and identify potential patent infringement.

- **Digital update/ correction:** To update the digital version (e.g. 3D/CAD model) of an object to match an "as-built" condition.

- **Security Auditing:** To determine whether vulnerabilities exist in a product or not.

- **Learning:** learn from others' mistakes. Do not make the same mistakes that others have already made and subsequently corrected.

- Acquiring sensitive data by disassembling and analysing the design of a system component.

- Military or commercial espionage. Learning about an enemy's or competitor's latest research by stealing or capturing a prototype and dismantling it.

- Removal of copy protection, circumvention of access restrictions or creation of unlicensed/unapproved duplicates.

- Determining whether an application contains any undocumented functionality.

Another reason for reverse engineering is to compress product development times. In the intensely competitive global market, manufacturers are constantly seeking new ways to shorten lead-times to market a new product. Rapid product development (RPD) refers to recently developed technologies and techniques that assist manufacturers and designers in meeting the demands of reduced product development time. For example, injection-molding companies must drastically reduce the tool and die development times. By using reverse engineering, a three-dimensional product or model can be quickly captured in digital form, re-modelled, and exported for rapid prototyping/tooling or rapid manufacturing.

Reverse engineering enables the duplication of an existing part by capturing the component's physical dimensions, features, and material properties. Before attempting reverse engineering, a well-planned life-cycle analysis and cost/benefit analysis should be conducted to justify the reverse engineering projects. Reverse engineering is typically cost effective only if the items to be reverse engineered reflect a high investment or will be reproduced in large quantities. Reverse engineering of a part may be attempted even if it is not cost effective, if the part is absolutely required and is mission-critical to a system.

Check Your Progress 1

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

What is the importance of reverse engineering? What is the need of it?

....

....

....

....

....

....

....

....

....

....

3.4 STAGES INVOLVED IN THE REVERSE ENGINEERING PROCESS

Since the Reverse Engineering process can be time-consuming and expensive, reverse Engineers generally consider whether the financial risk of such an endeavour is preferable to purchasing or licensing the information from the original manufacturer, if possible.

In order to Reverse Engineer, a product or component of a system, engineers and researchers generally follow the following four-stage process:

1) Identifying the product or component which will be reverse engineered.

2) Observing or disassembling the information documenting how the original product works.

3) Implementing the technical data generated by reverse engineering in a replica or modified version of the original.

4) Creating a new product (and, perhaps, introducing it into the market).

In the first stage, the process, sometimes called "pre-screening," Reverse Engineers determine the candidate product for their project. Potential candidates for such a project include singular items, parts, components, units, subassemblies, some of which may contain many smaller parts sold as a single entity. The second stage, disassembly or decompilation of the original product, is the most time-consuming aspect of the project. In this stage, Reverse Engineers attempt to construct a characterization of the system by accumulating all of the technical data and instructions of how the product works. In the third stage of Reverse Engineering, Reverse Engineers try to verify that the data generated by disassembly or decompilation is an accurate reconstruction of the original system. Engineers verify the accuracy and validity of their designs by testing the system, creating prototypes, and experimenting with the results.

The final stage of the Reverse Engineering process is the introduction of a new product into the marketplace. These new products are often innovations of the original product with competitive designs, features, or capabilities. These products may also be adaptations of the original product for use with other integrated systems, such as different platforms of computer operating systems. Often different groups of engineers perform each step separately, using only documents to exchange the information learned at each step. This is to prevent duplication of the original technology, which may violate copyright. By contrast, Reverse Engineering creates a different implementation with the same functionality.

3.5 DISASSEMBLY OR DECOMPILATION

In the development of software, the source code in which programmers originally write is translated into object (binary) code. The translation is done with a computer program called an "assembler" or "compiler," depending on the source code's language, such as Java, C++, or assembly. A great deal of the original programmer's instructions, including commentary, notations, and specifications, are not included in the translation from source to object code (the assembly or compilation). Disassembly or decompilation reverses this process by reading the object code of the program and translating them into source code. By presenting the information in a computer language that a software programmer can understand, the reverse engineer can analyze the structure of the program and identify how it operates.

The data generated in the disassembly of a typical computer program is one to many files with thousands of lines of computer code. Because much of the original programmer's commentary, notations, and specifications are not retained in the object code, the reverse engineered code constitutes only a part of the program information included in the original source code. Engineers must interpret the resulting source code using knowledge and expertise to recreate the data structures of the original program and understand the overall design rationale of the system. Not all reverse engineering efforts require "decompilation" of software. Some "black box" reverse engineering is done by characterizing software through observation of its interaction with system components, other software, and other (external) systems through networks.

Source Code and Object Code

Source code is the category of computer language instructions that is most frequently written and read by software programmers. A computer cannot generally run a program in source code form though. The source code is translated, with the use of an assembler or compiler, into a language form that contains instructions to the computer known as object code.

Object code consists of numeric codes specifying each of the computer instructions that must be executed, as well as the locations in memory of the data on which the instructions are to operate. While source code and object code are commonly referred to as different classes of computer language, these terms actually describe the series of transformations a program goes through when being converted from a higher level language more easily comprehensible to humans to the lower level language of computer operations.

Check Your Progress 2

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

Which stage is the most time-consuming aspect of the project in the reverse engineering? Explain.

....

....

....

....

....

....

....

....

....

....

3.6 CRACKING SOFTWARE PROTECTION

The most common software crack is the modification of an application's binary to cause or prevent a specific key branch in the program's execution. This is accomplished by reverse engineering the compiled program code using a debugger until the software cracker reaches the subroutine that contains the primary method of protecting the software or by disassembling an executable file. The binary is then modified using the debugger or a hex editor in a manner that replaces a prior branching opcode with its complement or a NOP opcode so the key branch will either always execute a specific subroutine or skip over it. Almost all common software cracks are a variation of this type. Proprietary software developers are constantly developing techniques such as code obfuscation, encryption, and self-modifying code to make this modification increasingly difficult. Even with these measures being taken, developers struggle to combat software cracking. This is because it's very common for a professional to publicly release a simple cracked EXE or Retrium Installer for public download, eliminating the need for inexperienced users to crack the software themselves.

A specific example of this technique is a crack that removes the expiration period from a time-limited trial of an application. These cracks are usually programs that patch the program executable and sometimes the .dll or .so linked to the application. Similar cracks are available for software that requires a hardware dongle. A company can also break the copy protection of programs that they have legally purchased but that are licensed to particular hardware, so that there is no risk of downtime due to hardware failure (and, of course, no need to restrict oneself to running the software on bought hardware only).

Another method is the use of special software such as CloneCD to scan for the use of a commercial copy protection application. After discovering the software used to protect the application, another tool may be used to remove the copy protection from the software on the CD or DVD. This may enable another program such as Alcohol 120%, CloneDVD, Game Jackal, or Daemon Tools to copy the protected software to a user's hard disk. Popular commercial copy protection applications which may be scanned for include SafeDisc and StarForce.

Check Your Progress 3

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of this Unit.

How the developers struggle to combat software cracking?

....

....

....

....

....

....

....

....

....

....

....

3.7 TOOLS

3.7.1 Resource Hacker

Resource Hacker is a utility to view, modify, add, rename and delete resources in Windows executable and resource files. Furthermore, Resource Hacker also includes an integrated resource compiler and decompiler. Here are some key features of "Resource Hacker":

- It helps to view resources in Win32 executable files (*.exe, *.dll, *.cpl, *.ocx) and in Win32 resource files (*.res) in both their compiled and decompiled formats.

- It helps to extract (save) resources to file in: *.res format; as a binary; or as decompiled resource scripts or images.

- Icons, bitmaps, cursors, menus, dialogs, string tables, message tables, accelerators, Borland forms and version info resources can be fully decompiled into their respective formats, whether as image files or *.rc text files.
- It helps to Modify (rename or replace) resources in executable files. Image resources (icons, cursors and bitmaps) can be replaced with an image from a corresponding image file (*.ico, *.cur, *.bmp), · a *.res file or even another *.exe file.
- Dialogs, menus, string tables, accelerators and message table resource scripts (and also Borland forms) can be edited and recompiled using the internal resource script editor.
- Resources can also be replaced with resources from a *.res file as long as the replacement resource is of the same type and has the same name.
- Add new resources to executable files. It enables a program to support multiple languages, or add a custom icon or bitmap (company logo etc) to a program's dialog.
- Delete resources. Most compilers add resources into applications which are never used by the application. Removing these unused resources can reduce an application's size.
- 32bit Resource Files (*.res) can now also be viewed and edited.
- Added support for the following Dialog extended style flags:

  WS_EX_LAYERED,WS_EX_NOINHERITLAYOUT,WS_EX_ LAYOUTRTL and WS_EX_NOACTIVATE.
- All resource language ids (except those for cursors and icons) can now be easily changed.
- Bug Fix:

  LBS_NOINTEGRALHEIGHT and LBS_MULTICOLUMN listbox style flags in dialogs previously could not be combined.

3.7.2 Hex Workshop

The Hex Workshop Hex Editor by BreakPoint Software is a complete set of hexadecimal development tools for Microsoft Windows 2000 and later. Hex Workshop integrates advanced,binary editing and data interpretation and visualization with the ease and flexibility of a modern word processor. With the Hex Workshop, you can edit, cut, copy, paste, insert, fill and delete binary data. You can also work with data in its native structure and data types using our integrated structure viewer and smart bookmarks. Data editing is quick and easy with our extensive features that allow you to: jump to file or sector location, find or replace data, perform arithmetic, bitwise, and logical operations, binary compare files, generate checksums and digests, view character distributions and export data to RTF or HTML for publishing.

Hex Workshop includes a Sector Editor with disk imaging tools, a Base Converter for converting between hex, decimal and binary data types, a Hex Calculator supporting arithmetic and bitwise operations, an expression calculator supporting variables, conditionals, iteration and arithmetic and bitwise operations, and a data visualizer designed to help you visually identify patterns and interesting data from rendered images. Also included is our Data Inspector that allows you to quickly edit and view data in decimal, floating point or time and date representations.

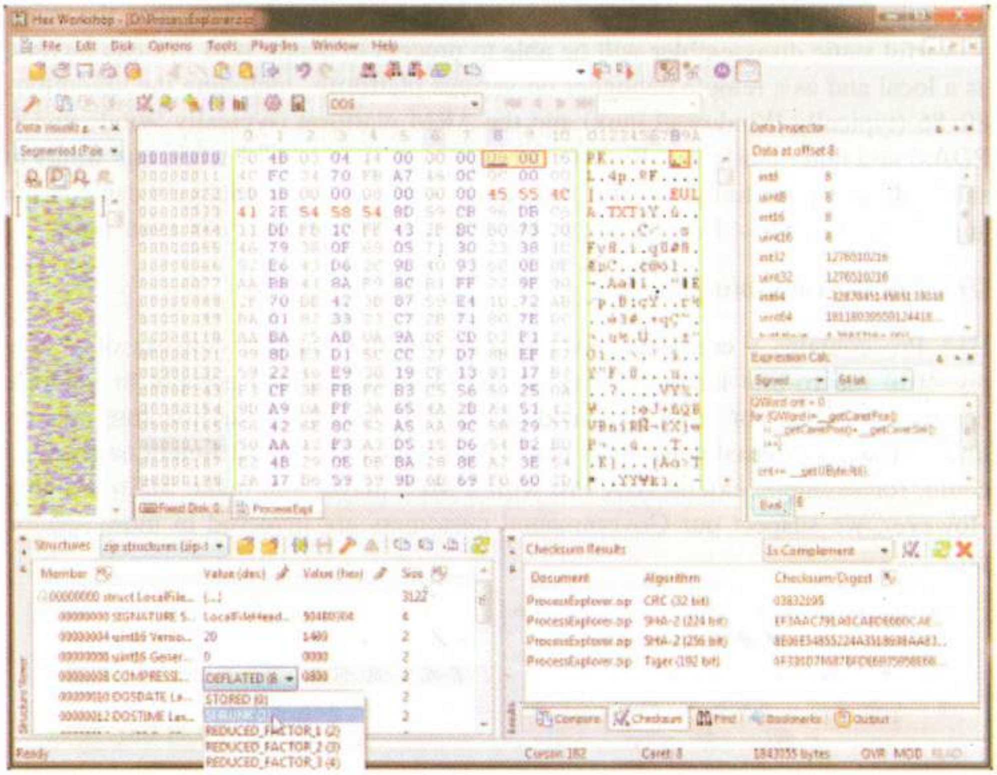


Fig. 1

Key Features:

Rich Feature Set

Highly Customizable User Interface

Data Interpretation and Parsing

Integrated Binary Comparison

3.7.3 IDA Pro

IDA Pro combines an interactive, programmable, multi-processor disassembler coupled to a local and remote debugger and augmented by a complete plug-in programming environment.

IDA Pro is a disassembler

As a disassembler, IDA Pro explores binary programs, for which source code isn't always available, to create maps of their execution. The real interest of a disassembler is that it shows the instructions that are actually executed by the processor in a symbolic representation called assembly language. If the friendly screen saver you have just installed is spying on your E-Banking session or logging your E-Mails, a disassembler can reveal it. However, assembly language is hard to make sense of. That's why advanced techniques have been implemented into IDA Pro to make that code more readable, in some cases, quite close to the original source code that produced the binary program. The map of the program's code then is post-processed for further investigations. Some people have used it as the root of a genomic classification of Viruses.

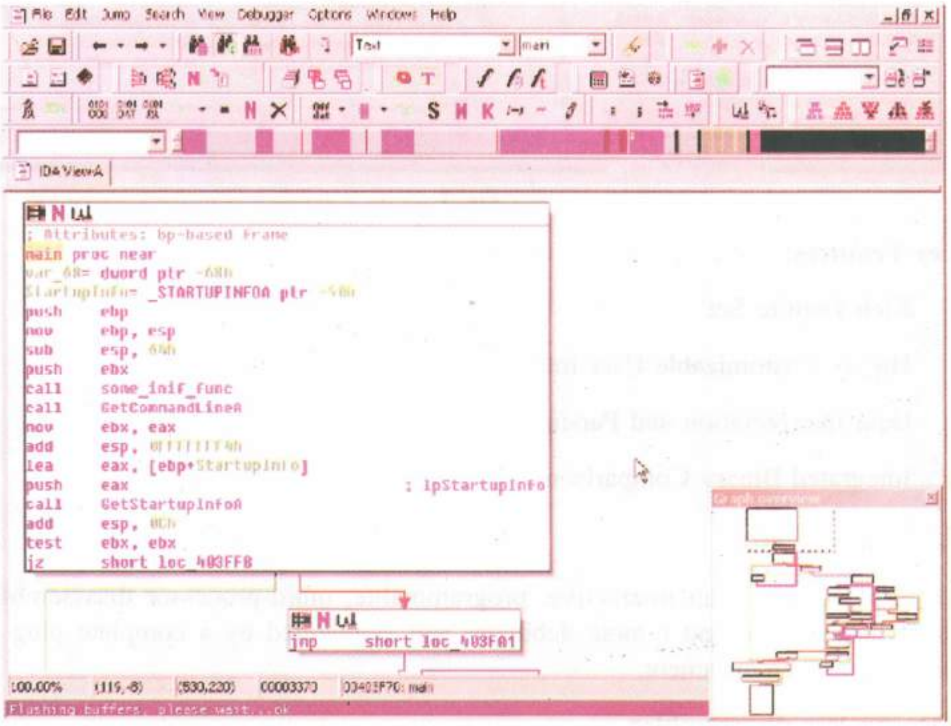
IDA Pro is a debugger

But, in real life, things aren't always simple. Hostile code usually does not co-operate with the analyst. Viruses, Worms and Trojans are often armoured and obfuscated. More powerful tools are required.

The debugger in IDA Pro complements the static analysis capabilities of the disassembler: by allowing singling step through the code being investigated, the debugger often bypasses the obfuscation and helps obtain data that the more powerful static disassembler will be able to process in depth. IDA Pro can be used as a local and as a remote debugger on various platforms, including the ubiquitous 80x86 (typically Windows/Linux) and the ARM platform (typically Windows CE PDAs) and other platforms. Remote debuggers are very useful when one wants to safely dissect potentially harmful programs. Some of IDA debuggers can run the application in a virtual environment: this makes Malware analysis even safer.

IDA Pro is programmable

IDA Pro contains a complete development environment that consists of a very powerful macro-like language that can be used to automate simple to medium complexity tasks. For more advanced tasks, our open plugin Architecture puts no limits on what external developers can do to enhance IDA Pro's functionality. One could, for example, extend IDA Pro with a MP3 player and make Malware sing. However, we suspect our Governmental customers are involved in more serious projects.



```
; Attributes: bp-based frame
main proc near
var_68= dword ptr -68h
StartupInfo= _STARTUPINFOA ptr -58h
push    ebp
mov     ebp, esp
sub     esp, 68h
push    ebx
call    some_init_func
call    GetCommandLineA
mov     ebx, eax
add     esp, 0FFFFFFF4h
lea     eax, [ebp+StartupInfo]
push    eax                              ; lpStartupInfo
call    GetStartupInfoA
add     esp, 0Ch
test    ebx, ebx
jz      short loc_403FF8

jmp     short loc_403FA1
```

```
100.00%   (119,-8)   (530,220)   00003373   00403F70: main
Flushing buffers, please wait...ok
```

Fig. 2

3.7.4 PE Explorer

PE Explorer is the most feature-packed program for inspecting the inner workings of your own software, and more importantly, third party Windows applications and libraries for which you do not have source code. PE Explorer lets you open, view and edit a variety of different 32-bit Windows executable file types (also called PE files) ranging from the common, such as EXE, DLL and ActiveX Controls, to the less familiar types, such as SCR (Screensavers), CPL (Control Panel Applets), SYS, MSSTYLES, BPL, DPL and more (including executable files that run on MS Windows Mobile platform).

PE Explorer gives you the power to look inside these PE binary files, perform static analysis, reveal a lot of information about the function of the executable, and collect as much information about the executable file as possible, without executing it. PE Explorer leaves you with only minimal work to do in order to get an analysis of a piece of software. Once you have selected the file you wish to examine, PE Explorer will analyze the file and display a summary of the PE header information, and all of the resources contained in the PE file. From here, the tool allows you to explore the specific elements within an executable file.

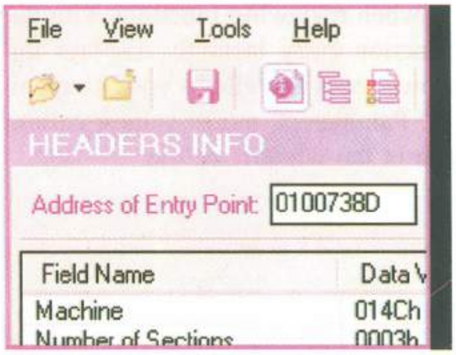
Besides being an effective Resource Editor, PE Explorer also provides several tools that elevate it to Power Coder status: an API Function Syntax Lookup, Dependency Scanner, Section Editor, UPX Unpacker, and a powerful yet easy-to-use Disassembler. With PE Explorer you can view and inspect unknown binaries, examine and edit the properties of EXE and DLL files, and correct and repair the internal structures of any PE (portable executable) files with the click of a button. PE Explorer is intended to be used in various scenarios such as software development, Forensics practice, Reverse Engineering extensive binary security analysis and binary auditing processes.

With PE Explorer You Can

- See what's inside an executable and what it does
- Change and customize the GUI elements of your Windows programs
- Track down what a program accesses and which DLLs are called
- Understand the way a program works, behaves, and interacts with others
- Verify the publisher and the integrity of the signed executable files
- Say good bye to digging through bloated help files just to hash out an API reference
- Open UPX-, Upack- and NsPack-compressed files seamlessly in PE Explorer, without long workarounds
- Special support for Delphi applications

Viewing and Editing Portable Executable (PE) Files

Working with 32-bit PE files such as .EXE, .DLL, Device Drivers (.SYS, .ACM), ActiveX Controls (.OCX), Borland Libraries (.DPL and .BPL), XP Visual Styles (.MSSTYLES), Control Panel Extensions (.CPL), Screen Savers (.SCR) and any other win32 executables.



Address of Entry Point 0100738D

Field Name	Data V
Machine	014Ch
Number of Sections	0003h

Fig. 3

- Working with damaged files: PE Explorer opens broken or packed files in Safe mode.
- PE files integrity verification.
- Checksum computing and modification.
- Entry Point value modification.
- Modification of EXE and DLL file properties.
- UPX Unpacker.
- UPack Unpacker.
- NSPack Unpacker.

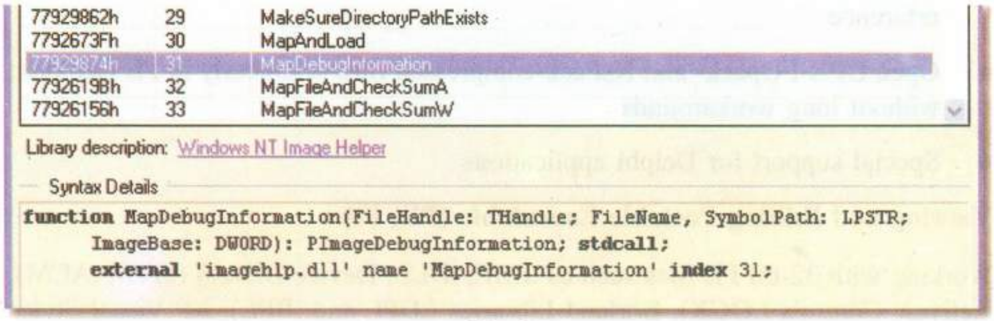
Support for custom plug-ins to perform any startup processing.

PE Header Viewer

PE Explorer makes it easy to analyze PE file structure, correct errors, fix compilation bugs, repair damaged resources or modify the internal arrangements of PE files. With PE Explorer file headers, data directories, section headers and export tables are ready and waiting for your command. Use it for serious development projects, for restoring lost information, for keeping damaged files intact, to reverse engineer projects with missing source code, or to view the imports/exports of the standard DLL's.

Viewers

- Headers Info Viewer displays the EXE header information contained in the PE file header.
- Data Directories Viewer to view and edit Data Directories.
- Sections Header Viewer to view, extract, recalculate or delete sections from the program body.
- Export, Import and Delay Import Viewers.
- Function Syntax Viewer displays the calling syntax for functions.
- Digital Signature Viewer to validate the digital signature of a PE file.
- Dependency Scanner traces the dependency chain for the program's libraries.
- Relocation Viewer to view contents of the base relocation table.
- Debug Information Viewer displays the debug information contained in the file.
- Resource Viewer to browse, deletes, or extracts nearly every type of resources.



77929862h	29	MakeSureDirectoryPathExists
7792673Fh	30	MapAndLoad
77929874h	31	MapDebugInformation
7792619Bh	32	MapFileAndCheckSumA
77926156h	33	MapFileAndCheckSumW

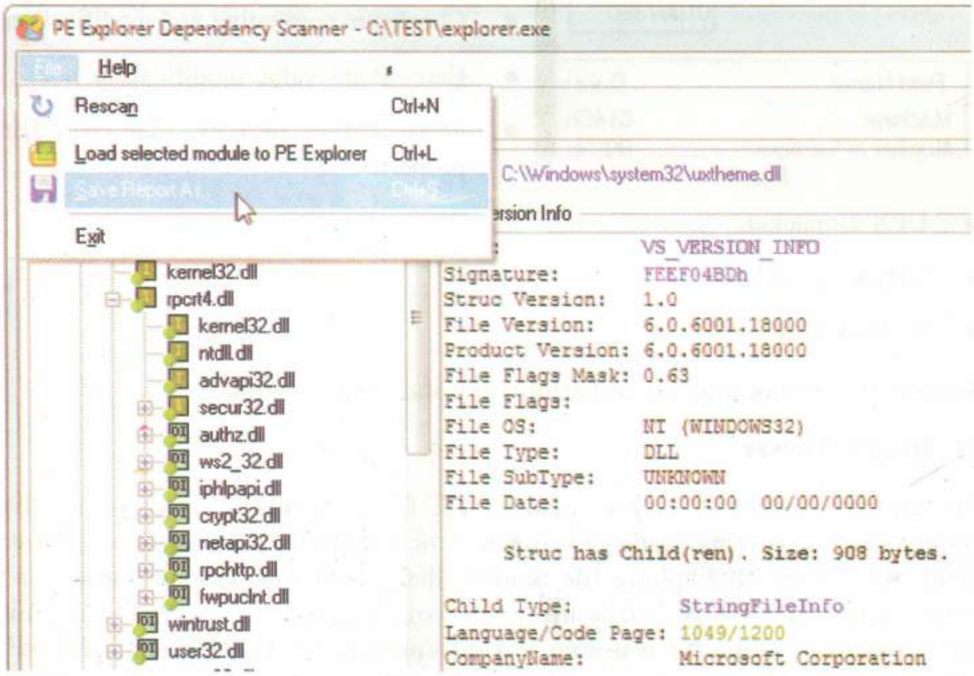
Library description: Windows NT Image Helper

Syntax Details

```
function MapDebugInformation(FileHandle: THandle; FileName, SymbolPath: LPSTR;
      ImageBase: DWORD): PImageDebugInformation; stdcall;
      external 'imagehlp.dll' name 'MapDebugInformation' index 31;
```

Fig. 4

PE Explorer provides important information about entry points, numbers, names and calling syntax of exported functions. Now, when reviewing functions with the Import and Export Viewers, by clicking a function entry instantly displays the calling syntax for that function PE Explorer knows about and allows you to expand the syntax database with your own definitions. Parameters, return values, calling conventions are conveniently displayed for you in the window below.


PE Explorer Dependency Scanner - C:\TEST\explorer.exe
File
Help
Rescan Ctrl+N
Load selected module to PE Explorer Ctrl+L
Save Report As... Ctrl+S
Exit
ersion Info

C:\Windows\system32\uxtheme.dll

kernel32.dll
rpcrt4.dll
kernel32.dll
ntdll.dll
advapi32.dll
secur32.dll
authz.dll
ws2_32.dll
iphlpapi.dll
crypt32.dll
netapi32.dll
rpchttp.dll
fwpuclnt.dll
wintrust.dll
user32.dll

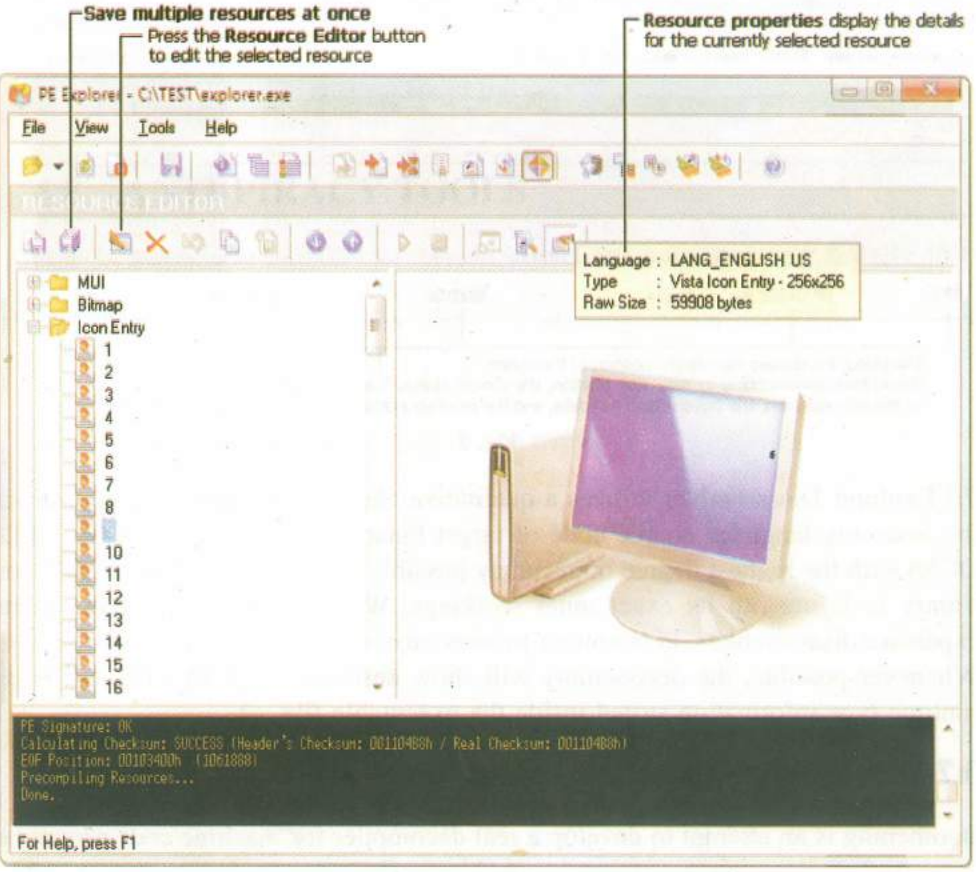
```
                 VS_VERSION_INFO
Signature:       FEEF04BDh
Struc Version:   1.0
File Version:    6.0.6001.18000
Product Version: 6.0.6001.18000
File Flags Mask: 0.63
File Flags:
File OS:         NT (WINDOWS32)
File Type:       DLL
File SubType:    UNKNOWN
File Date:       00:00:00  00/00/0000

     Struc has Child(ren). Size: 908 bytes.

Child Type:          StringFileInfo
Language/Code Page:  1049/1200
CompanyName:         Microsoft Corporation
```

Fig. 5

The Dependency Scanner tool allows you to recursively scan all modules linked to by a particular PE file. Use the Dependency Scanner to make it crystal clear which libraries an application depends on, so you know exactly which files you need to package into your application's installation program. Or which files to copy when moving a 3rd party application from one computer to another. Dependency Scanner also detects delay-load dependencies.

Editors

- Resource Editor to edit or replace nearly every type of resources.
- Application Manifest Wizard for adding the manifest resource into existing applications and marking applications with a requested execution level to tell Vista to run the applications elevated.
- Characteristics Editor to view or set flag bits in the PE file header Characteristics field.
- Section Editor to change all the fields in the section header, or repair and restore the damaged section headers settings.
- Syntax Description Editor for adding custom comments, altering values or creating new library descriptions.
- Debug Information and Relocations Removal Tools
- Time Date Stamp Adjuster to modify all the timestamps in the PE file header to one uniform value.


Save multiple resources at once
Press the Resource Editor button to edit the selected resource
Resource properties display the detals for the currently selected resource
PE Explorer - C:\TEST\explorer.exe
File
View
Tools
Help
RESOURCES EDITOR
MUI
Bitmap
Icon Entry
1
2
3
4
5
6
7
8
10
11
12
13
14
15
16
For Help, press F1

Language : LANG_ENGLISH US
Type : Vista Icon Entry - 256x256
Raw Size : 59908 bytes

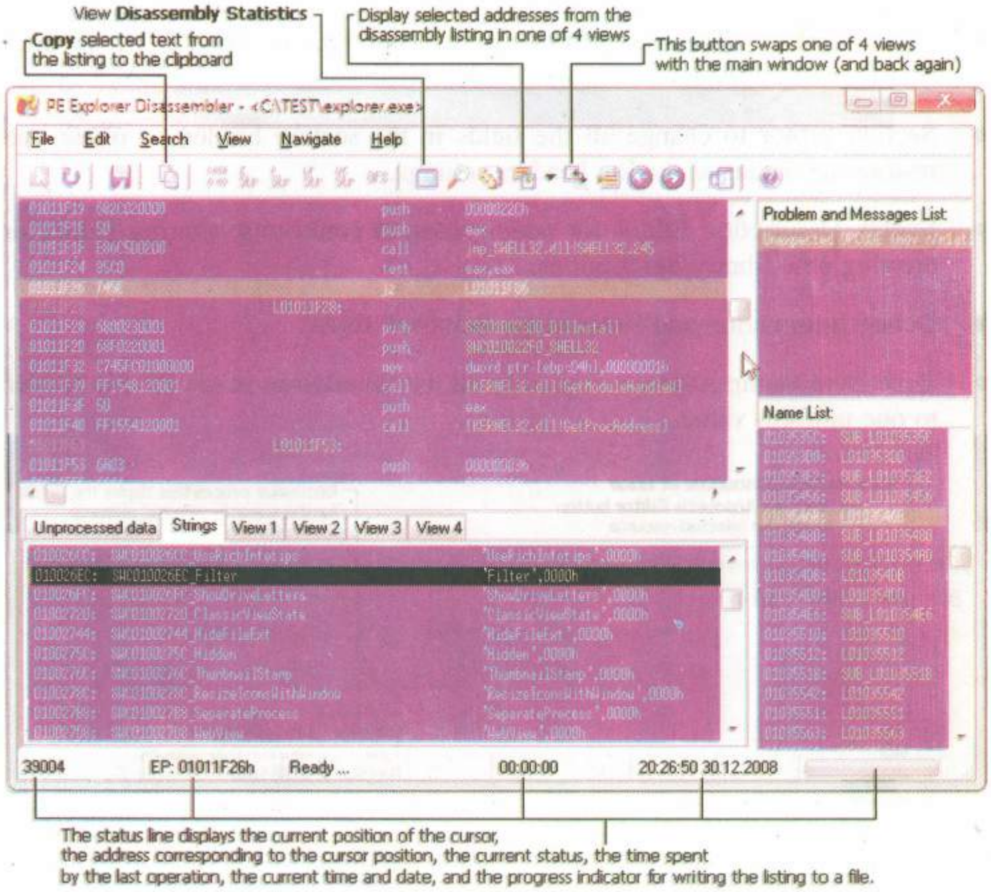
```
PE Signature: OK
Calculating Checksum: SUCCESS (Header's Checksum: 001104B8h / Real Checksum: 001104B8h)
EOF Position: 00103400h  (1061888)
Precompiling Resources...
Done.
```

Fig. 6

PE Explorer offers one of the most convenient and easy-to-use resource editors available for Windows. Visual editing features let you quickly browse and modify executable file resources from within the file. Dialog boxes, menus, string tables, icons, bitmaps, manifests and more are right at your fingertips.

Disassembler

- It Supports the Intel 80x86, Pentium family, and other compatible processors.
- IT has X86 instruction sets and extensions (MMX, SSE, SSE2 and SSE3), AMD K6-2 3D-Now! extensions.
- It provides easy browsing using Found Data panes, search options and address/ offset jumps history.
- It pulls ASCII text strings and VCL Objects out the data portion of the file.
- It saves and loads the disassembly listing and all the changes made to continue on later.



View **Disassembly Statistics**
Copy selected text from the listing to the clipboard
Display selected addresses from the disassembly listing in one of 4 views
This button swaps one of 4 views with the main window (and back again)
PE Explorer Disassembler - <C:\TEST\explorer.exe>
File
Edit
Search
View
Navigate
Help
Problem and Messages List
Name List
Unprocessed data
Strings
View 1
View 2
View 3
View 4

```
01011F19  682C020000            push   0000022Ch
01011F1E  50                    push   eax
01011F1F  E86C500200            call   jmp_SHELL32.dll!SHELL32.245
01011F24  85C0                  test   eax,eax
01011F26  7456                  jz     L01011F96
                     L01011F28:
01011F28  6800230001            push   SSZ01002300_DllInstall
01011F2D  68F0220001            push   SHC010022F0_SHELL32
01011F32  C745FC01000000        mov    dword ptr [ebp-04h],00000001h
01011F39  FF1548120001          call   [KERNEL32.dll!GetModuleHandleW]
01011F3F  50                    push   eax
01011F40  FF1554120001          call   [KERNEL32.dll!GetProcAddress]
                     L01011F53:
01011F53  6A03                  push   00000003h
```

```
010026CC:  SHC010026CC_UseRichInfotips      'UseRichInfotips',0000h
010026EC:  SHC010026EC_Filter               'Filter',0000h
010026FC:  SHC010026FC_ShowDriveLetters     'ShowDriveLetters',0000h
01002720:  SHC01002720_ClassicViewState     'ClassicViewState',0000h
01002744:  SHC01002744_HideFileExt          'HideFileExt',0000h
0100275C:  SHC0100275C_Hidden               'Hidden',0000h
0100276C:  SHC0100276C_ThumbnailStamp       'ThumbnailStamp',0000h
0100278C:  SHC0100278C_ResizeIconsWithWindow 'ResizeIconsWithWindow',0000h
010027B8:  SHC010027B8_SeparateProcess      'SeparateProcess',0000h
010027D8:  SHC010027D8_WebView              'WebView',0000h
```

```
0103535C:  SUB_L0103535C
010353D0:  L010353D0
010353E2:  SUB_L010353E2
01035456:  SUB_L01035456
01035468:  L01035468
01035480:  SUB_L01035480
010354A0:  SUB_L010354A0
010354D8:  L010354D8
010354DD:  L010354DD
010354E6:  SUB_L010354E6
01035510:  L01035510
01035512:  L01035512
01035518:  SUB_L01035518
01035542:  L01035542
01035551:  L01035551
01035563:  L01035563
```

39004   EP: 01011F26h   Ready ...   00:00:00   20:26:50 30.12.2008

The status line displays the current position of the cursor, the address corresponding to the cursor position, the current status, the time spent by the last operation, the current time and date, and the progress indicator for writing the listing to a file.

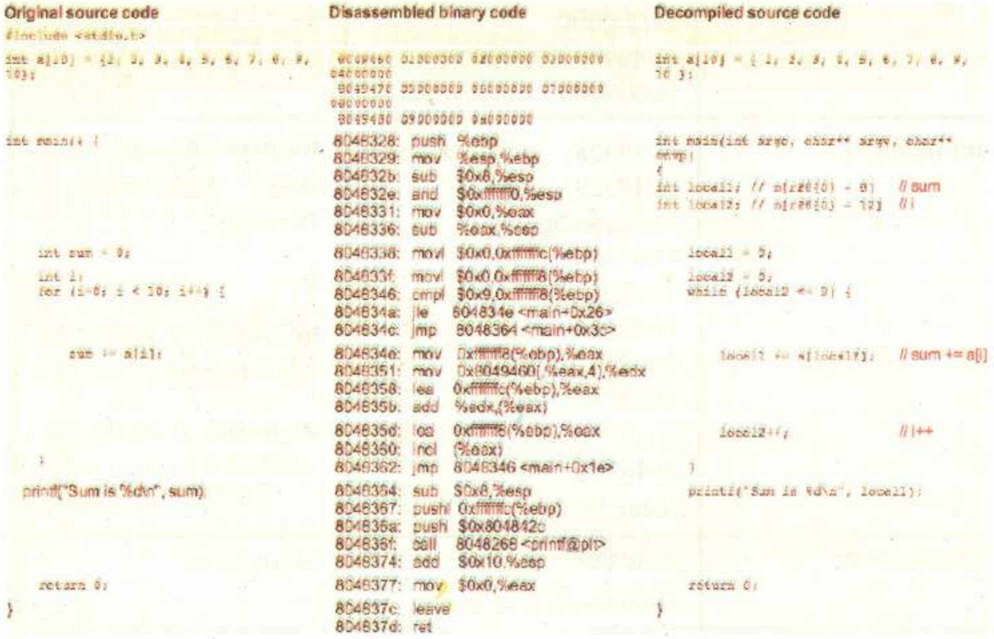
Fig. 7

PE Explorer Disassembler utilizes a qualitative algorithm designed to reconstruct the assembly language source code of target binary win32 PE files (EXE, DLL, OCX) with the highest degree of accuracy possible. Disassemble an application or library to figure out its exact inner workings. While as powerful as the more expensive disassemblers, PE Explorer focuses on ease of use, clarity and navigation. Whenever possible, the disassembly will show descriptive names extracted from runtime type information stored inside the executable file.

3.7.5 Boomerang (Machine Decompiler)

Boomerang is an attempt to develop a real decompiler for machine code programs through the open source community. A decompiler takes as input an executable file, and attempts to create a high level, compliable, possibly even maintainable source file that does the same thing. It is therefore the opposite of a compiler, which takes a source file and makes an executable. However, a general decompiler does not attempt to reverse every action of the decompiler; rather it transforms the input program repeatedly until the result is high level source code. It therefore won't recreate the original source file; probably nothing like it. It does not matter if the executable file has symbols or not, or was compiled from any particular language.

The intent is to create a re-targetable decompiler (i.e. one that can decompile different types of machine code files with modest effort, e.g. X86-windows, sparc-solaris, etc). It was also intended to be highly modular, so that different parts of the decompiler can be replaced with experimental modules. It was intended to eventually become interactive, because some things (not just variable names and comments, though these are obviously very important) require expert intervention. Whether the interactivity belongs in the decompiler or in a separate tool remains unclear.



Original source code

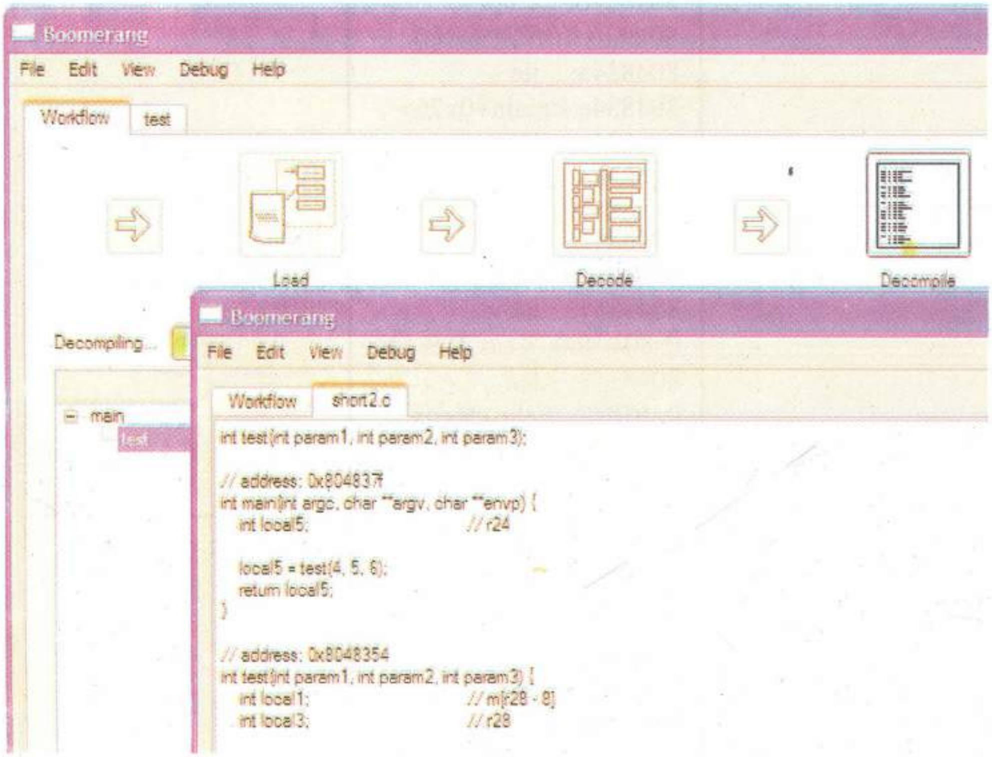
```
#include <stdio.h>

int a[10] = {1, 2, 3, 4, 5, 6, 7, 8, 9,
10};

int main() {

    int sum = 0;

    int i;
    for (i=0; i < 10; i++) {

        sum += a[i];

    }
  printf("Sum is %d\n", sum);

    return 0;
}
```

Disassembled binary code

```
 8049460 01000000 02000000 03000000
04000000
 8049470 05000000 06000000 07000000
08000000
 8049480 09000000 0a000000
8048328: push  %ebp
8048329: mov   %esp,%ebp
804832b: sub   $0x8,%esp
804832e: and   $0xfffffff0,%esp
8048331: mov   $0x0,%eax
8048336: sub   %eax,%esp
8048338: movl  $0x0,0xfffffffc(%ebp)
804833f: movl  $0x0,0xfffffff8(%ebp)
8048346: cmpl  $0x9,0xfffffff8(%ebp)
804834a: jle   804834e <main+0x26>
804834c: jmp   8048364 <main+0x3c>
804834e: mov   0xfffffff8(%ebp),%eax
8048351: mov   0x8049460(,%eax,4),%edx
8048358: lea   0xfffffffc(%ebp),%eax
804835b: add   %edx,(%eax)
804835d: lea   0xfffffff8(%ebp),%eax
8048360: incl  (%eax)
8048362: jmp   8048346 <main+0x1e>
8048364: sub   $0x8,%esp
8048367: pushl 0xfffffffc(%ebp)
804836a: push  $0x804842c
804836f: call  8048268 <printf@plt>
8048374: add   $0x10,%esp
8048377: mov   $0x0,%eax
804837c: leave
804837d: ret
```

Decompiled source code

```
int a[10] = { 1, 2, 3, 4, 5, 6, 7, 8, 9,
10 };

int main(int argc, char** argv, char**
envp)
{
int local1; // m[r28{0} - 8]   // sum
int local2; // m[r28{0} - 12]  // i

    local1 = 0;

    local2 = 0;
    while (local2 <= 9) {

        local1 += a[local2];    // sum += a[i]

        local2++;               // i++

    }
    printf("Sum is %d\n", local1);

    return 0;
}
```



```
int test(int param1, int param2, int param3);

// address: 0x804837f
int main(int argc, char **argv, char **envp) {
   int local5;                          // r24

   local5 = test(4, 5, 6);
   return local5;
}

// address: 0x8048354
int test(int param1, int param2, int param3) {
   int local1;                          // m[r28 - 8]
   int local3;                          // r28
```

Fig.8

What Boomerang can do?

An attempt has been made to line up equivalent original source, binary, and decompiled source code lines; this is not always possible. Comments in red are not generated by the decompiler; those in black are.

Original source code	Disassembled binary code	Decompiled source code

#include <stdio.h>
int a[10] = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10};
	8049460 01000000 02000000 03000000 04000000
	8049470 05000000 06000000 07000000 08000000
	8049480 09000000 0a000000
		int a[10] = { 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 };

int main() {	8048328: push %ebp
	8048329: mov %esp,%ebp
	804832b: sub $0x8,%esp
	804832e: and $0xfffffff0,%esp
	8048331: mov $0x0,%eax
	8048336: sub %eax,%esp
		int main(int argc, char** argv, char** envp)
		{
		int local1; // m[r28{0} - 8] // sum
		int local2; // m[r28{0} - 12] // i

int sum = 0;	8048338: movl $0x0,0xfffffffc(%ebp)	local1 = 0;

int i;
for (i=0; i < 10; i++)
{
	804833f: movl $0x0,0xfffffff8(%ebp)
	8048346: cmpl $0x9,0xfffffff8(%ebp)
	804834a: jle 804834e <main+0x26>
	804834c: jmp 8048364 <main+0x3c>
		local2 = 0;
		while (local2 <= 9)
		{

sum += a[i];	804834e: mov 0xfffffff8(%ebp),%eax 8048351: mov 0x8049460(,%eax,4),%edx 8048358: lea 0xfffffffc(%ebp),%eax 804835b: add %edx,(%eax)	local1 += a[local2]; // sum += a[i]

}	804835d: lea 0xfffffff8(%ebp),%eax
	8048360: incl (%eax)
	8048362: jmp 8048346 <main+0x1e>
		local2++; // i++
		}

printf("Sum is %d\n", sum);	8048364: sub $0x8,%esp 8048367: pushl 0xfffffffc(%ebp) 804836a: push $0x804842c 804836f: call 8048268 <printf@plt> 8048374: add $0x10,%esp	printf("Sum is %d\n", local1);
return 0;	8048377: mov $0x0,%eax	return 0;
}	804837c: leave 804837d: ret 804842c 53756d20 69732025 Sum is % 8048434 640a00 d..	}

This example shows:

- Source that is fairly readable, compiles with no warnings and runs correctly.
- Conversion of stack locations to local variables
- Detection, declaration, use, and initialisation of an array
- Correct handling of a C string through the use of the string as a parameter to a library function
- The output from sumarray-O4 (same program compiled with -O4 optimisation) looks much the same (as of September 2004), except that the pretested while loop is replaced by a posttested do while loop.

Original source code	Disassembled binary code	Decompiled source code

void main() {
int a, x;
	10684: save %sp, -112, %sp	int main(int argc, char **argv, char **envp)
		{
		int local17; // argc{37}
		int local18; // argc{73}
		// "old a"
		int local19; // local18{73}
		// a

a = 0;	10688: clr %o0	argc = 0;

do {
a = a+1;
x = a;
printf("%d ", a);
	1068c: sethi %hi(0x10400), %l0
	10690: add %o0, 1, %i0
	10694: or %l0, 872, %o0
	10698: call printf
	1069c: mov %i0, %o1
		// Compiler reuses argc for a
		local19 = argc;
		do {
		local18 = local19;
		printf("%d ", local18 + 1);

} while (a < 10);	106a0: cmp %i0, 9
	106a4: ble 0x10690
	106a8: mov %i0, %o0
		local17 = local18 + 1;
		local19 = local17;
		} while (local18 + 1 <= 9);

printf("a is %d, x is %d\n", a, x);
return 0;
	106ac: sethi %hi(0x10400), %g1
	106b0: mov %i0, %o1
	106b4: mov %i0, %o2
	106b8: call printf
	106bc: or %g1, 880, %o0
		printf("a is %d, x is %d\n", local18 + 1, local18 + 1);

}	106c0: ret
	106c4: restore %g0, 0, %o0
		return 0;
		}

This example shows:

- Boomerang can decompile SPARC binary programs
- Copes with SPARC "register windows"
- Untangles the "delay slot" instructions (after every call and branch instruction)
- local19 had to be generated as a result of transforming out of SSA form
- too many local variables

3.7.6 REC Decompiler

REC is invoked with the following command line syntax:

```
rec [{+|-}optionname ...] exec_file
```

To activate an option, precede its name with a + (plus) sign. To disable an option, precede it with a - (minus) sign. To get the list of all the options and their current value, type:

```
rec +help
```

The minimum input to REC is the binary executable file. For example:

```
rec file.exe
```

If file.exe is in one of the recognized formats, it will be read, and a file.rec will be produced using the default options, without further intervention from the user.

REC can operate in three modes:

- **Batch mode:** By default, the user must provide an executable or command file name when invoking REC. This file will be opened and analyzed, and an output file with the same name as the input file and extension .rec is produced, without further intervention by the user.
- **Full screen interactive mode:** In this mode, the user can interactively analyze the input file by disassembling or decompiling individual procedures. The

user has also access to a hexadecimal viewer, and he or she can view some of the data that REC uses internally, such as the list of strings, labels, procedures etc. REC enters interactive mode when invoked from the command line with the +interactive option.

- **HTML generation mode:** In this mode REC reads the standard input for commands, and generates an HTML page as the result of each command typed. This mode is used on UNIX to allow a web browser like Netscape to act as the user interface of the decompiler.

  A proxy program is needed to translate the browser's requests into REC's standard input commands. Check the HTTP Server setup page for a description of how to use this mode. REC uses HTML generation mode when invoked from the command line with the +html option.

The other options are used to debug the program, or to tune its output. A complete list of the options requires an understanding of the algorithms and phases that REC performs to transform an executable file in a source file. If you don't know the meaning of one option, you can experiment by enabling it and check if the output is clearer. Note that some option is only valid if another option is enabled.

The same set of options is available regardless of the host/target combination.

Interactive mode

Interactive mode is used to analyze the program being decompiled. This mode is useful to access the hexadecimal viewer, and to inspect many of the internal lists maintained by REC, such as the strings list, the labels list, etc.

To use REC in interactive mode, the user must invoke it with the following command line:

```
rec +interactive file.exe
```

REC will start analyzing file.exe to find which area contains strings, code and data. It will also build the list of labels and branches, and then will try to build a list of the procedures contained in the program.

After this phase, the main menu will be presented:

```
Reverse Engineering Compiler 1.4 (C) Giampiero Caprino (Nov. 15 1998)

    r : show regions

    d : dump regions

    l : show labels

    b : show branches

    j : show jump tables

    s : show strings

    y : show symbols

    p : show procedures

    o : show options

    D : hexdump file

    Q : quit program
```

REC's user interface is based on a simple list browser. The user can type the following keys while in the list browser:

Up arrow or BS key : moves the cursor one line up

Down arrow or Enter key : moves the cursor one line down

Page Up or Ctrl-B key : shows the previous page

Page Down or Ctrl-F key : shows the next page

Right arrow when cursor is on a highlighted word: executes the command associated with the word. If there is a menu, typing any highlighted letter from the menu executes the command associated with the letter. Left arrow or 'Q' or ESC key exits the current screen and returns to the previous screen. The exclamation mark '!' is used to request the evaluation of numeric expressions.

The forward slash '/' character is used to search a string in the current list. The question mark '?' character searches a string backwards. The 'n' character repeats the last search in the same direction. The 'N' character repeats the last search in the opposite direction.

Region List

The region list shows how the input file is organized. Structured files formats, like COFF and ELF have separate areas for code, data and auxiliary information. The region list shows which area REC will consider for decompilation (marked with the text type), and which areas will be searched for ASCII strings (marked with the data type).

The user can force REC to consider a file region to be text or data via the command file region: command.

Labels List

The labels list shows all the addresses that are the destination of a branch or call instruction. This list is used when building the procedure list. If REC incorrectly treats a data area as a text area, it can create labels that are not part of any text region. This usually causes an incorrect procedure list. The user can then change the region list until all incorrect labels are eliminated.

Branch List

The branch list shows all the addresses that have a branch, call or return instruction. This list is used when building the procedure list. If REC incorrectly treats a data area as a text area, it can create branches whose destination is not part of any text region. This usually causes an incorrect procedure list. The user can then change the region list until all incorrect branches are eliminated.

Jump Table List

The jump table list shows all those areas that may contain a table of addresses inside a text region. These are usually generated when compiling switch() statements. It is important that REC recognizes these tables because the control flow analyzer depends on this data to identify all the instructions of a procedure, and also to avoid treating data bytes as instructions.

Strings List

The string list shows those portions of data regions that may have ASCII strings. These strings will then be used as parameter to functions like printf() and strcpy(), among the others.

Symbols List

This list shows every symbolic name associated with addresses. These are usually names of procedures (belonging to a text region) or names of global variables (belonging to a data region). The symbol names and addresses are taken from the file's symbol table, if available. The symbol list also shows the list of imported symbols (from a types: or prototype file), and the list of user specified symbols (entered via the symbol: command in a .cmd file).

Procedure List

The procedure list shows all the addresses where REC has identified a user procedure. Some of these addresses may come from the Symbols List, in which case the name of the procedure is also shown. For static functions and for files without a symbol table, the entry point of the procedure is used as its name.

Options List

The option list allows the user to enable or disable each option. Some options are used to produce a better output, some to enable alternative analysis algorithms, and some enable internal debugging features.

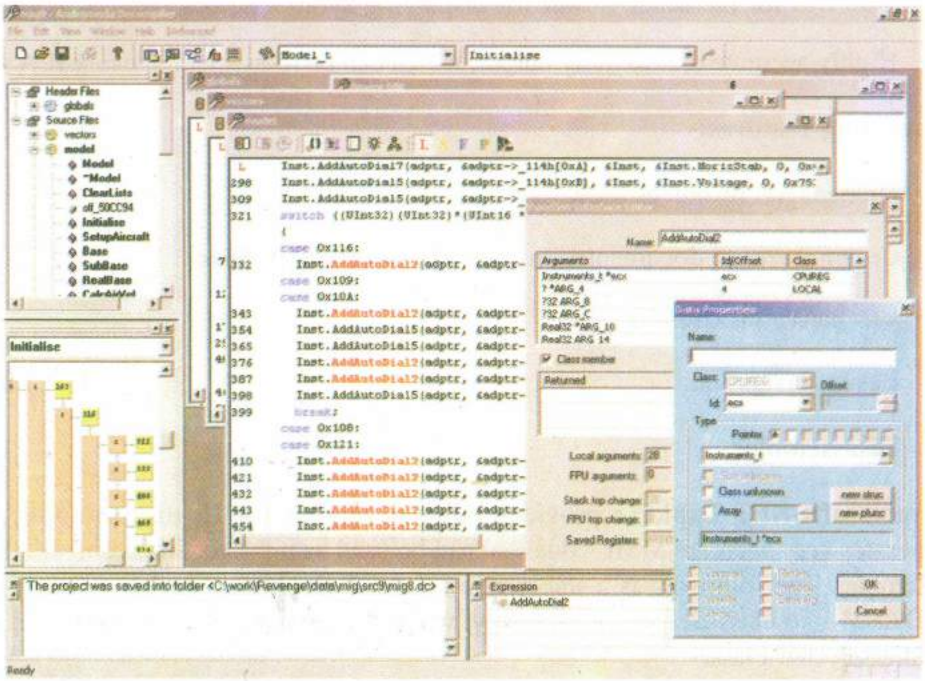
Hexdump Viewer

The hexdump viewer shows the content of the input file in hexadecimal, one page at a time. The usual cursor movement characters can be used to navigate through the dump. This mode is very useful to look at areas that REC has not recognized as code or data.

3.7.7 Andromeda Decompiler

Andromeda Decompiler (AD) - is an attempt to create the universal interactive program environment for Reverse Engineering, two main features of which are:

- Research and investigation of binary modules at a level of source codes;
- Partial or full their restoration up to re-compilable forms;



```
Inst.AddAutoDial7(adptr, &adptr->_114h[0xA], &Inst, &Inst.HorizStab, 0, 0x
Inst.AddAutoDial5(adptr, &adptr->_114h[0xB], &Inst, &Inst.Voltage, 0, 0x75
Inst.AddAutoDial5(adptr, &adptr->_
switch ((UInt32)(UInt32)*(UInt16 *
{
case 0x116:
  Inst.AddAutoDial2(adptr, &adptr-
case 0x109:
case 0x10A:
  Inst.AddAutoDial2(adptr, &adptr-
  Inst.AddAutoDial5(adptr, &adptr-
  Inst.AddAutoDial5(adptr, &adptr-
  Inst.AddAutoDial2(adptr, &adptr-
  Inst.AddAutoDial2(adptr, &adptr-
  Inst.AddAutoDial5(adptr, &adptr-
  break;
case 0x108:
case 0x121:
  Inst.AddAutoDial2(adptr, &adptr-
  Inst.AddAutoDial2(adptr, &adptr-
  Inst.AddAutoDial2(adptr, &adptr-
  Inst.AddAutoDial2(adptr, &adptr-
  Inst.AddAutoDial2(adptr, &adptr-
```

Arguments	Stk/Offset	Class
Instruments_t *ecx	ecx	CPUREG
? *ARG_4	4	LOCAL
?32 ARG_8		
?32 ARG_C		
Real32 *ARG_10		
Real32 ARG_14		

The project was saved into folder <C:\work\Revenge\data\mig\src9\mig8.dc>

Fig. 9

At present the project is in stages of development and its application is limited to the purposes of demonstration and estimation. Universality of the AD means; its ability to perceive input files from various target platforms and to give out a source code in desirable language of a high level. Though at present the program is intended only for 32-bit Intel x86-compatible frontend and C/C++ backend, its kernel is developed with this opportunity in mind. AD is an interactive decompiler. It means that the user takes active participation in the decompilation process. AD is not an automatic analyzer of programs. AD will hint you of suspicious situations, unsolved problems etc. It is your job to inform AD how to proceed. All the changes made by you are saved to disk. When you start AD again all the information about the file being decompiled is read from disk and you can continue your work.

3.7.8 Remotesoft .NET Explorer

Remotesoft .NET Explorer is a generic object browser and MSIL disassembler with professional look and feel. It offers the same functionality as Microsoft ILDASM disassembler utility, plus low level viewing of metadata and PE format. Remotesoft .NET Explorer works together with our decompiler and obfuscator, and acts as a console for easy navigation and powerful code editing and printing. This tool can be used as a source code editor, and it has a powerful syntax coloring system that recognizes many popular source files, including IL, C#, C/C++, VB, ASP, JAVA, HTML, FORTRAN, PHP, etc.

New features:

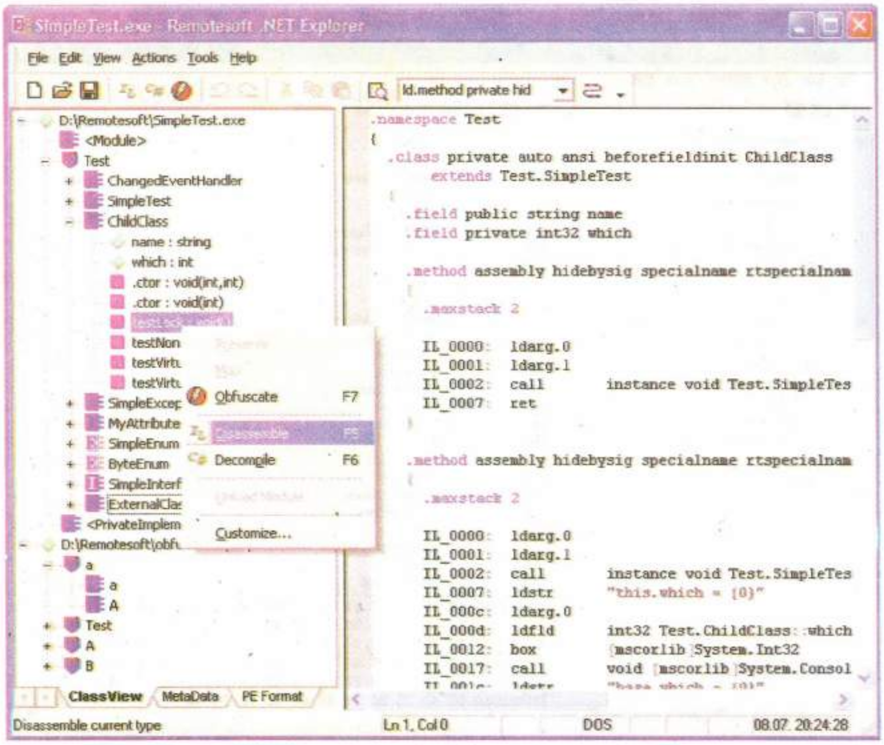
- .NET Framework 2.0 support.
- Visual Studio .NET Addin - launch from Tools > Remotesoft .NET Explorer
- Launch from right click an EXE or DLL file
- Managed resources view.
- MSIL Linker - combing assemblies/modules together (need to purchase the Linker product).
- Dependency walker, understand app.exe.config file.
- Tool tips for metadata viewer for displaying symbol names.
- Highly accurate disassembly output, which can be re-assembled using ILASM.

Upcoming features:

- Unmanaged resources view
- Comprehensive documentation with Microsoft .NET Spec
- x86 native disassembler
- Easier navigation.

1) Disassembler

Remotesoft .NET Explorer provides built in support for IL disassembling. It generates very accurate MSIL code that can be used as input for Microsoft ILASM assembler. The following is a screen shot of .NET Explorer. The left panel is the ILDASM-like class tree of an assembly, while the right panel shows the IL code of the selected class.

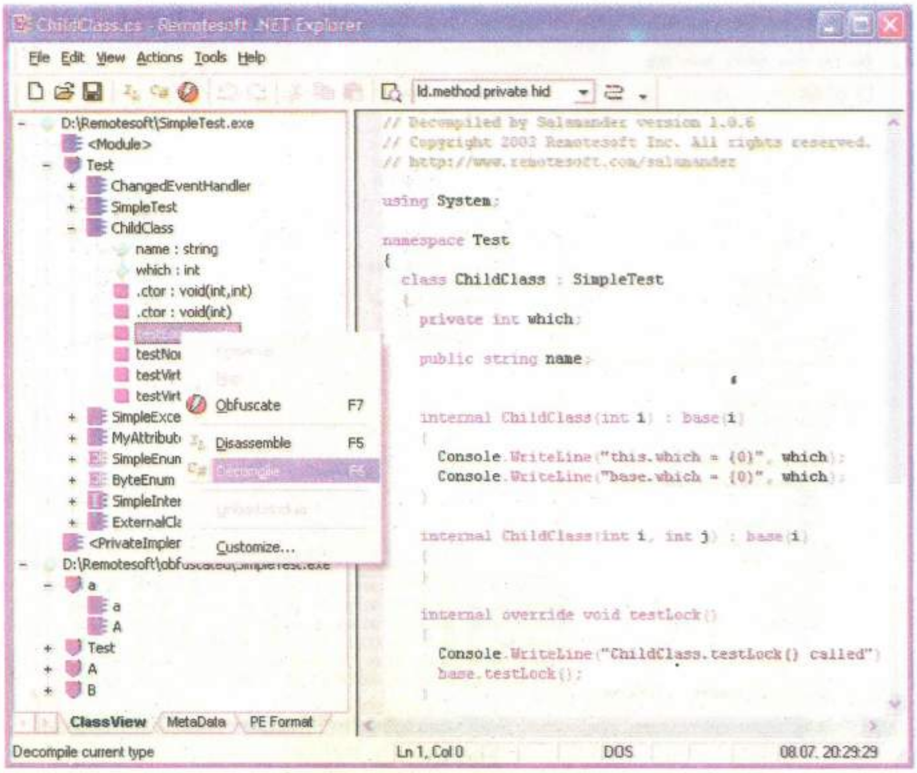


```
.namespace Test
{
  .class private auto ansi beforefieldinit ChildClass
       extends Test.SimpleTest
  {
    .field public string name
    .field private int32 which

    .method assembly hidebysig specialname rtspecialnam
    {
      .maxstack 2

      IL_0000:  ldarg.0
      IL_0001:  ldarg.1
      IL_0002:  call       instance void Test.SimpleTes
      IL_0007:  ret
    }

    .method assembly hidebysig specialname rtspecialnam
    {
      .maxstack 2

      IL_0000:  ldarg.0
      IL_0001:  ldarg.1
      IL_0002:  call       instance void Test.SimpleTes
      IL_0007:  ldstr      "this.which = {0}"
      IL_000c:  ldarg.0
      IL_000d:  ldfld      int32 Test.ChildClass::which
      IL_0012:  box        [mscorlib]System.Int32
      IL_0017:  call       void [mscorlib]System.Consol
      IL_001c:  ldstr      "base.which = {0}"
```

Fig. 10

2) Decompiler

Remotesoft .NET Explorer can be integrated with our decompiler for easy access to any methods of any assemblies. The following is a screen shot with the decompiler enabled. The left panel is the ILDASM-like class tree of an assembly, while the right panel shows the C# code of the selected class.

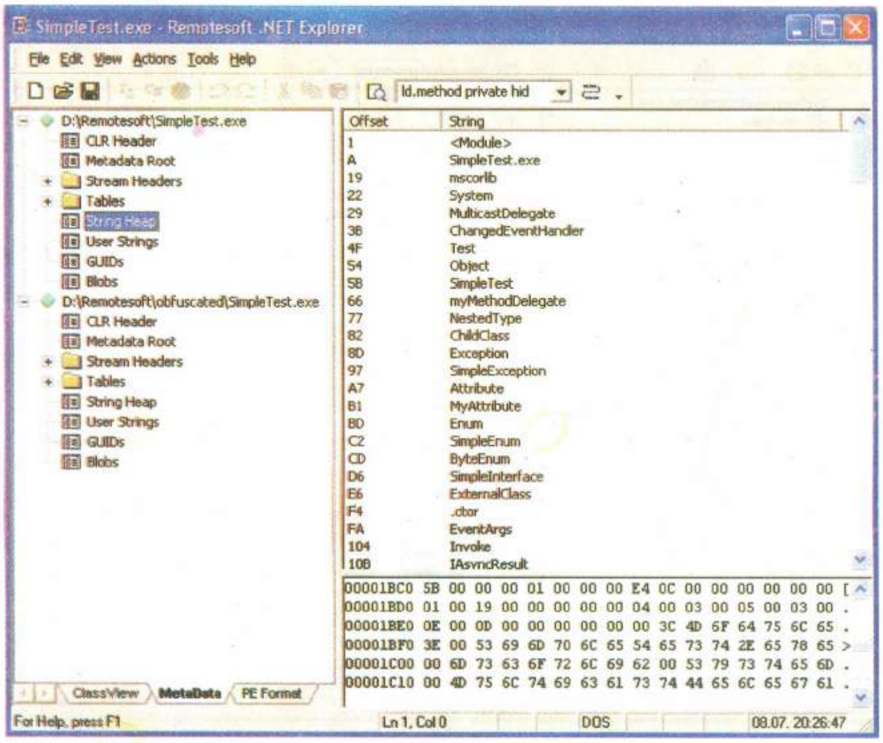


```
// Decompiled by Salamander version 1.0.6
// Copyright 2003 Remotesoft Inc. All rights reserved.
// http://www.remotesoft.com/salamander

using System;

namespace Test
{
  class ChildClass : SimpleTest
  {
    private int which;

    public string name;


    internal ChildClass(int i) : base(i)
    {
      Console.WriteLine("this.which = {0}", which);
      Console.WriteLine("base.which = {0}", which);
    }

    internal ChildClass(int i, int j) : base(i)
    {
    }

    internal override void testLock()
    {
      Console.WriteLine("ChildClass.testLock() called")
      base.testLock();
    }
```

Fig. 11

3) Metadata Viewer

Remotesoft .NET Explorer has built-in support for viewing low level .NET metadata. The following is a screen shot that shows the string heap of the selected assembly. A hex dump of the file is display in the lower right pane.



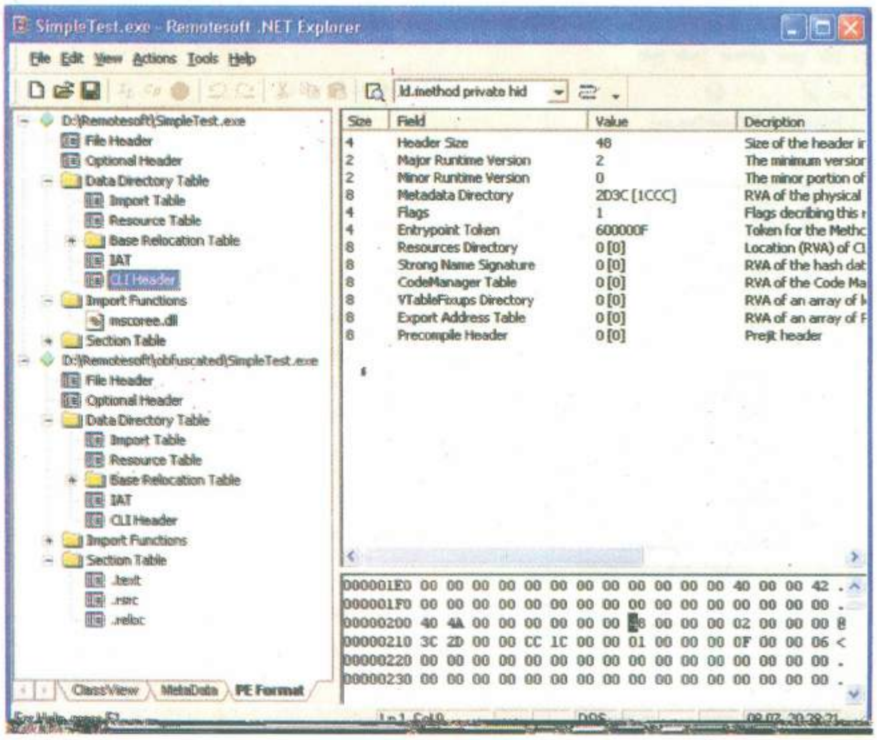
Offset	String
1	<Module>
A	SimpleTest.exe
19	mscorlib
22	System
29	MulticastDelegate
3B	ChangedEventHandler
4F	Test
54	Object
5B	SimpleTest
66	myMethodDelegate
77	NestedType
82	ChildClass
8D	Exception
97	SimpleException
A7	Attribute
B1	MyAttribute
BD	Enum
C2	SimpleEnum
CD	ByteEnum
D6	SimpleInterface
E6	ExternalClass
F4	.ctor
FA	EventArgs
104	Invoke
10B	IAsyncResult

```
00001BC0 5B 00 00 00 01 00 00 00 E4 0C 00 00 00 00 00 00 [
00001BD0 01 00 19 00 00 00 00 00 04 00 03 00 05 00 03 00 .
00001BE0 0E 00 0D 00 00 00 00 00 00 3C 4D 6F 64 75 6C 65 .
00001BF0 3E 00 53 69 6D 70 6C 65 54 65 73 74 2E 65 78 65 >
00001C00 00 6D 73 63 6F 72 6C 69 62 00 53 79 73 74 65 6D .
00001C10 00 4D 75 6C 74 69 63 61 73 74 44 65 6C 65 67 61 .
```

Fig. 12

4) PE Format Explorer

Remotesoft .NET Explorer has built-in support for viewing low level PE (Portable Executable) format. It recognizes both .NET images and native images that are compiling from C/C++. The following is a screen shot shows the CLI header of the selected assembly. A hex dump of the file is displayed in the lower right pane.



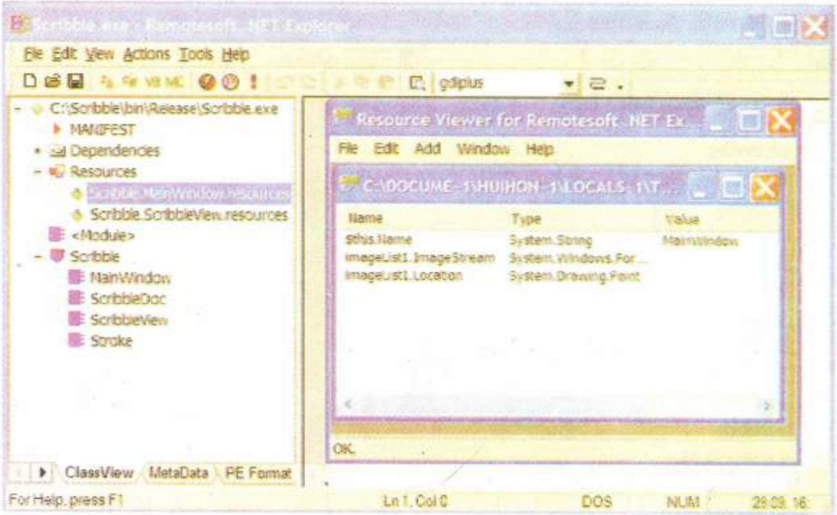
Size	Field	Value	Decription
4	Header Size	48	Size of the header ir
2	Major Runtime Version	2	The minimum versior
2	Minor Runtime Version	0	The minor portion of
8	Metadata Directory	2D3C [1CCC]	RVA of the physical
4	Flags	1	Flags decribing this r
4	Entrypoint Token	600000F	Token for the Methc
8	Resources Directory	0 [0]	Location (RVA) of Cl
8	Strong Name Signature	0 [0]	RVA of the hash dat
8	CodeManager Table	0 [0]	RVA of the Code Ma
8	VTableFixups Directory	0 [0]	RVA of an array of k
8	Export Address Table	0 [0]	RVA of an array of F
8	Precompile Header	0 [0]	Prejit header

```
000001E0 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 .
000001F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .
00000200 40 4A 00 00 00 00 00 00 48 00 00 00 02 00 00 00 @
00000210 3C 2D 00 00 CC 1C 00 00 01 00 00 00 0F 00 00 06 <
00000220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .
00000230 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .
```

Fig. 13

5) Resource viewer

Remotesoft .NET Explorer has built-in support for viewing managed resources When a managed resource is double clicked, an external viewer will be launched. A managed resource can also be saved into a file. Shown below is a screen shot that illustrate the features. Support for unmanaged resources will be gradually added into the product.


Scribble.exe - Remotesoft .NET Explorer
File Edit View Actions Tools Help
gdiplus
C:\Scribble\bin\Release\Scribble.exe
MANIFEST
Dependencies
Resources
Scribble.MainWindow.resources
Scribble.ScribbleView.resources
<Module>
Scribble
MainWindow
ScribbleDoc
ScribbleView
Stroke
Resource Viewer for Remotesoft .NET Ex...
File Edit Add Window Help
C:\DOCUME~1\HUIHON~1\LOCALS~1\T...
ClassView
MetaData
PE Format
Ln 1, Col 0
DOS
NUM
29:09:16

Name	Type	Value
$this.Name	System.String	MainWindow
imageList1.ImageStream	System.Windows.For...	
imageList1.Location	System.Drawing.Point	

OK.

For Help, press F1

Fig. 14

6) Dependency Walker

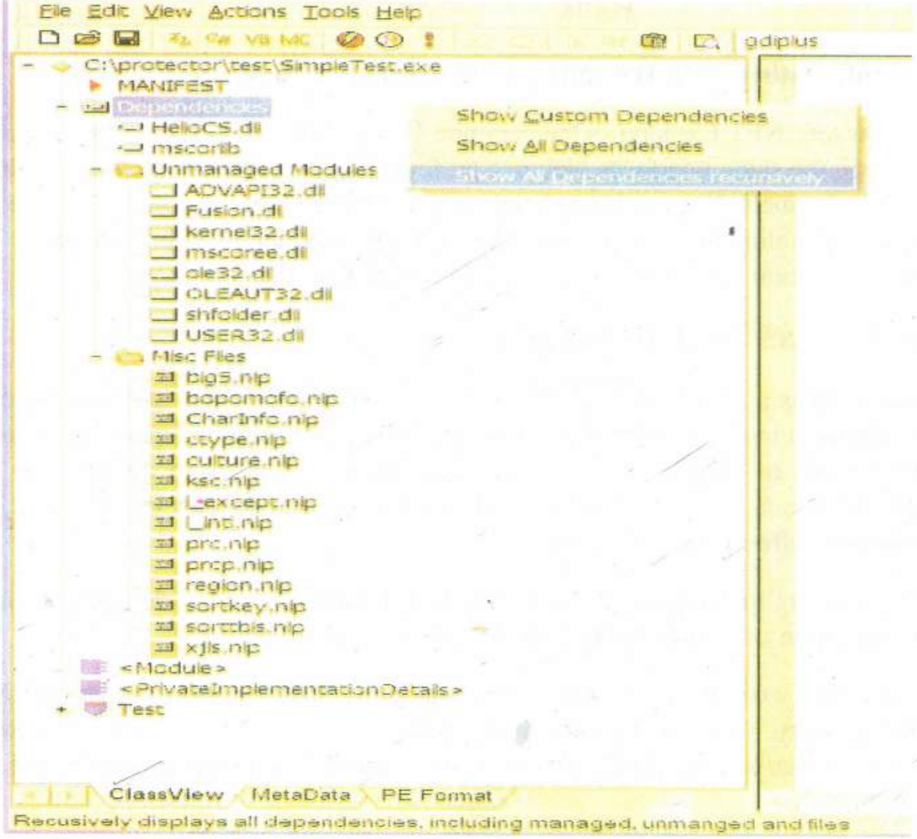
Remotesoft .NET Explorer has built-in support for viewing all dependencies of an assembly, including managed assembly/module references, unmanaged DLLs and misc file references. Shown below are two screen shots that illustrate the features.

- Dependencies can be viewed in a controlled manner: you can show only the managed references, or all dependencies recursively.

- Application configure file, app.exe.config, when existed, is parsed to locate dependencies.

- A reference, such as unmanaged DLL, can easily be loaded into the .NET Explorer for browsing and exploring.

- Dependencies of unmanaged DLL can be examined, including its import functions and export tables.



Recusively displays all dependencies, including managed, unmanged and files

Fig. 15

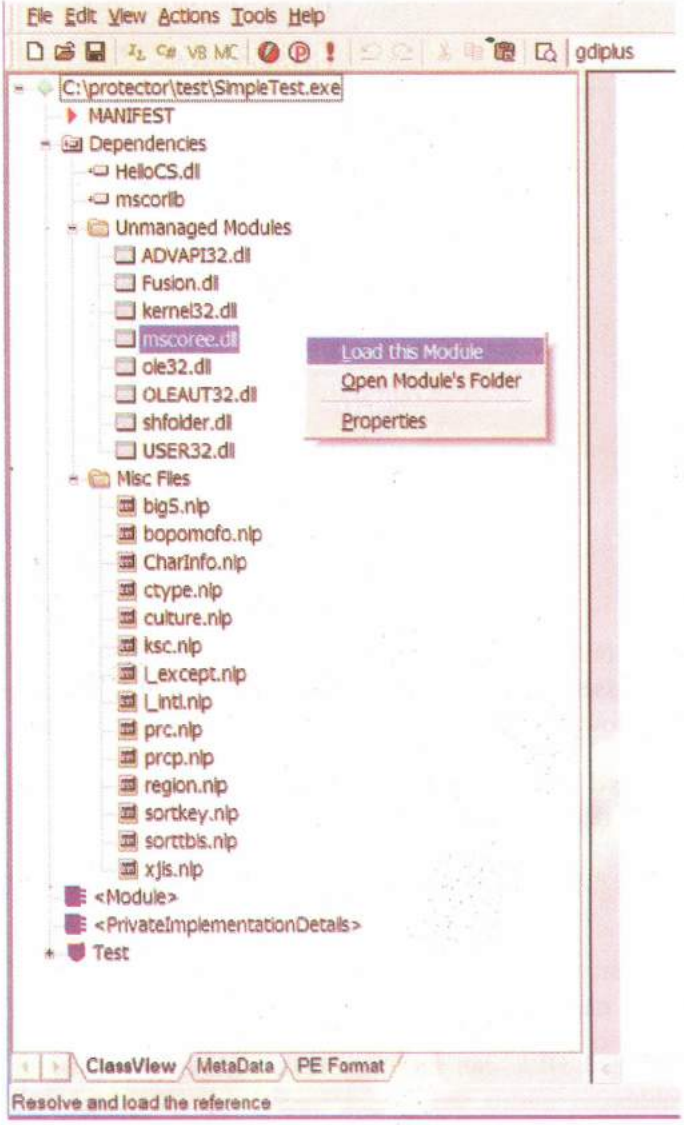


Fig. 16

7) Integrating With Decompiler, Obfuscator, Protector and Linker

Remotesoft .NET Explorer is the common GUI to interact with our other products. Through the same interfaces, you can perform linking, obfuscation, protection and mini deployment. You can immediately test the effectiveness of your code protection by disassembling and decompiling the resulting assemblies within the same GUI. The integration works only when you purchase the other products.

3.7.9 Spices .NET Decompiler

Spices.Net is a set of .NET code security and code protection, software lifecycle management tools for .NET developers, including .Net obfuscation, tamper defence tools, tools to recover source code and convert binaries to c# and VB.Net, documentation services, analysis and modelling tools in one environment that constantly offers new possibilities.

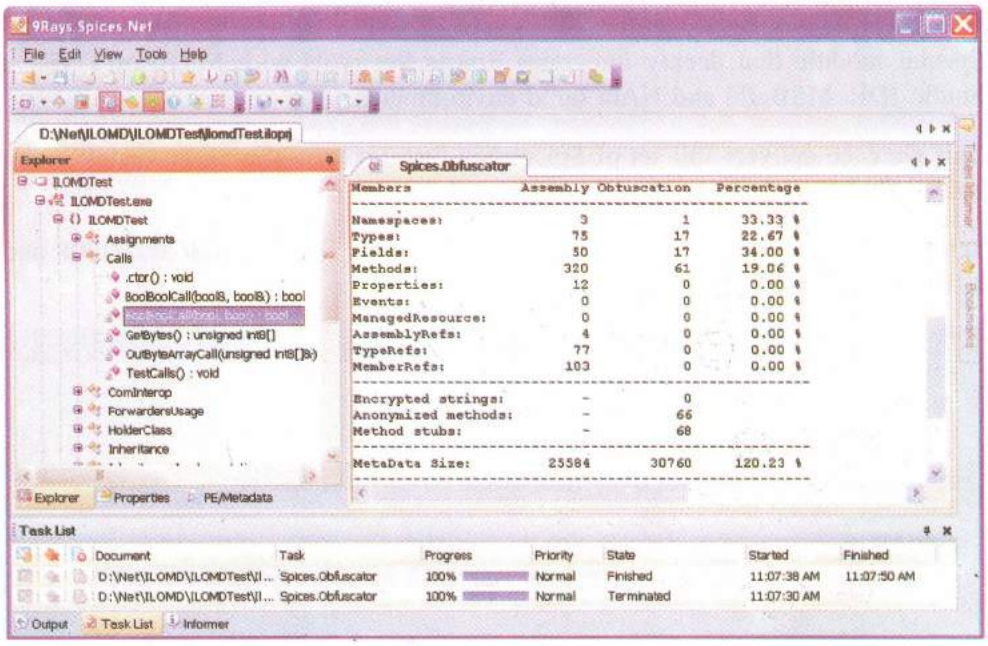
Programming in Microsoft's .NET Framework platform gives additional horizons in realization of various ideas with an extensive set of features.

Spices.Net next generation set of tools that helps .NET developers increase .NET ?ode security, safety and productivity, quality and efficiency of .NET software, that continues to offer wide range of features for developers and many more new possibilities.

Now Spices.Net Suite includes following highly integrated modules:

Spices.Net Obfuscator

Provides solutions to increase .NET code security and protect your .NET code and make it tamper resistant, localization, analysis and software lifecycle management tools and services. Make sure to keep your intellectual properties secure! Using the Spices.Net Obfuscator, you can put your code within a concentrically protective belt of security. Misinformation, blind alleys that lead to dead ends, and obtuse gibberish will greet the hacker, and send them packing for greener pastures.



```
Members                  Assembly Obtuscation   Percentage
-----------------------------------------------------------
Namespaces:                     3           1      33.33 %
Types:                         75          17      22.67 %
Fields:                        50          17      34.00 %
Methods:                      320          61      19.06 %
Properties:                    12           0       0.00 %
Events:                         0           0       0.00 %
ManagedResource:                0           0       0.00 %
AssemblyRefs:                   4           0       0.00 %
TypeRefs:                      77           0       0.00 %
MemberRefs:                   103           0       0.00 %
-----------------------------------------------------------
Encrypted strings:              -           0
Anonymized methods:             -          66
Method stubs:                   -          68
-----------------------------------------------------------
MetaData Size:              25584       30760     120.23 %
-----------------------------------------------------------
```

Task List

Document	Task	Progress	Priority	State	Started	Finished
D:\Net\ILOMD\ILOMDTest\I...	Spices.Obfuscator	100%	Normal	Finished	11:07:38 AM	11:07:50 AM
D:\Net\ILOMD\ILOMDTest\I...	Spices.Obfuscator	100%	Normal	Terminated	11:07:30 AM	

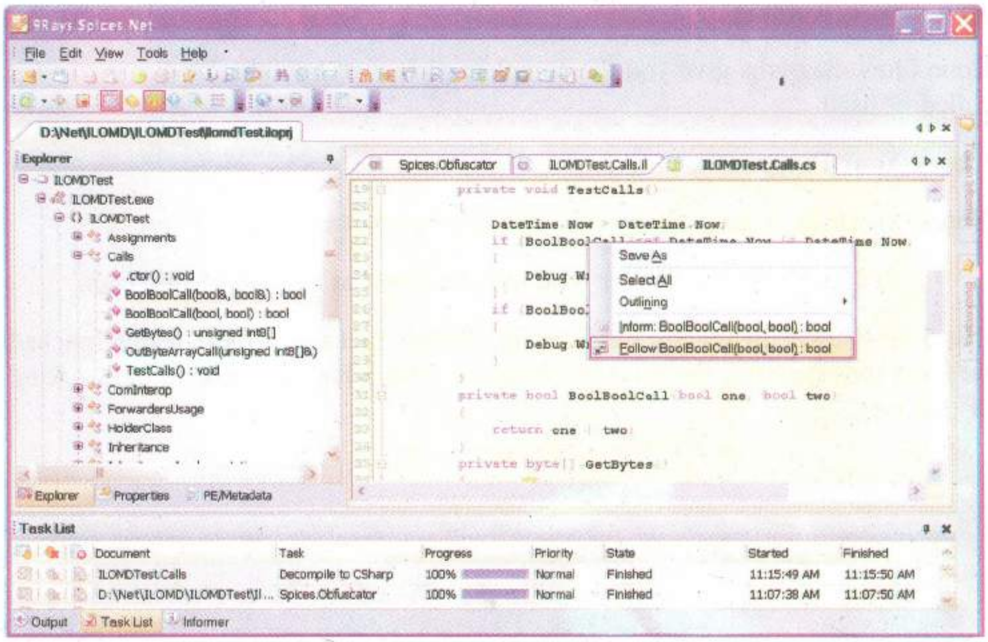
Fig. 17

Spices.Net Decompiler

Provides tools to recover source code and convert binaries to c#, VB.Net, J#, Delphi.Net and managed C++, code flow visual representation tools.

Spices.Modeler

Provides modelling and diagramming tools to visually represent various types of .NET code and assembly members relationship and structure.



```
private void TestCalls()
{
    DateTime Now = DateTime.Now;
    if (BoolBoolCall(ref DateTime.Now ... DateTime.Now
    {
        Debug.W
    }
    if (BoolBoo
    {
        Debug.W
    }
}
private bool BoolBoolCall(bool one, bool two)
{
    return one | two;
}
private byte[] GetBytes()
```

Task List

Document	Task	Progress	Priority	State	Started	Finished
ILOMDTest.Calls	Decompile to CSharp	100%	Normal	Finished	11:15:49 AM	11:15:50 AM
D:\Net\ILOMD\ILOMDTest\I...	Spices.Obfuscator	100%	Normal	Finished	11:07:38 AM	11:07:50 AM

Fig. 18

Spices.Investigator

Provides .NET metadata and assembly structure browsing tools to get detailed information about any item at low level.

Spices.Informer

Provides detailed context information about any assembly member.

Visual Studio Integration Package (VSIP)

Special module that deeply integrates Spices.Net tools with Microsoft's Visual Studio IDE, MSBuild and NAnt build environments.

This package delivers full set of Spices.Net features intp Microsoft Visual Studio and expand Visual Studio development environment functionality.

Spices.VSIP offers integration with Microsoft Visual Studio 2003/2005/2008 and 2010 and MSBuild build environments.

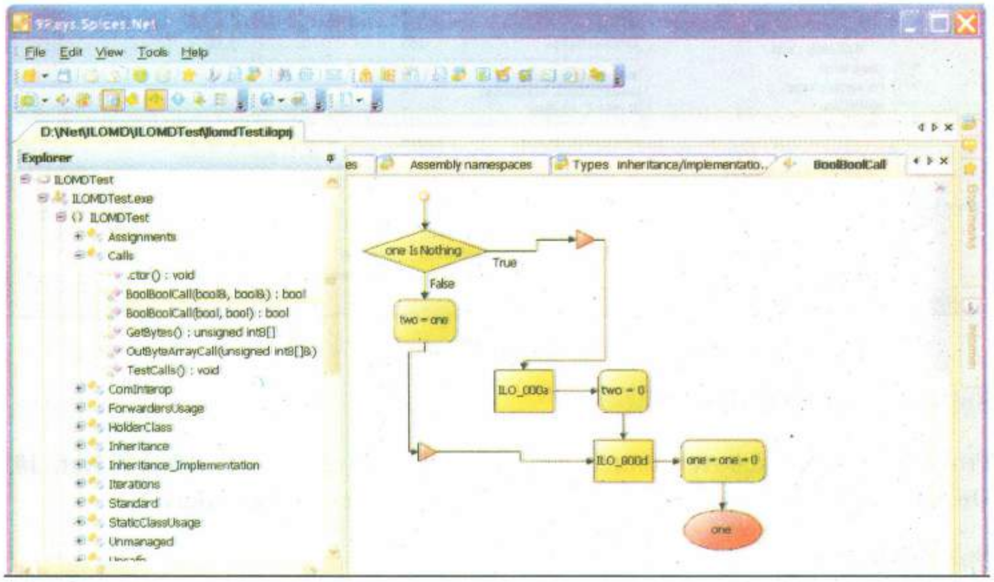


Fig. 19

Spices.Decompiler features the unique functionality that lets you easily see how your code is working.

Code Flow diagrams give you the complete picture of how this or that method is called or used.

Check Your Progress 4

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of this Unit.

List 5 tools used for reverse engineering? Which tool is the most feature-packed program for inspecting the inner workings of your software? Explain the working of that tool.

....

....

....

....

....

3.8 LET US SUM UP

This unit deals with the concept of "Reverse Engineering" which is the general process of analyzing a technology specifically to ascertain how it was designed or how it operates. This kind of inquiry engages individuals in a constructive learning process about the operation of systems and products. Reverse engineering as a method is not confined to any particular purpose, but is often an important part of the scientific method and technological development. The process of taking something apart and revealing the way in which it works is often an effective way to learn how to build a technology or make improvements to it.

There are two types of reverse engineering i.e. Software Reverse Engineering and Hardware Reverse Engineering. Software reverse engineering is done to retrieve the source code of a program because the source code was lost, to study how the program performs certain operations, to improve the performance of a program. Hardware reverse engineering involves taking apart a device to see how it works. In order to Reverse Engineer, a product or component of a system, engineers and researchers generally follow the four-stage process: 1.Identifying the product.2.Observing or disassembling the information 3.Implementing the technical data 4.Creating a new product.

This section deals with the disassembling. In the development of software, the source code in which programmers originally write is translated into object (binary) code. Another concept is software crack. It is the modification of an application's binary to cause or prevent a specific key branch in the program's execution. This is accomplished by reverse engineering the compiled program code using a debugger until the software cracker reaches the subroutine that contains the primary method of protecting the software or by disassembling an executable file.

Moreover, various tools are explained thoroughly which are used to perform the reverse engineering.

3.9 CHECK YOUR PROGRESS: THE KEY

1) Reverse engineering is taking apart an object to see how it works in order to duplicate or enhance the object.Software reverse engineering involves reversing a program's machine code (the string of 0s and 1s that are sent to the logic processor) back into the source code that it was written in, using program language statements.

   Reverse engineering can be viewed as the process of analyzing a system to:

   i) Identify the system's components and their interrelationships

   ii) Create representations of the system in another form or a higher level of abstraction

   iii) Create the physical representation of that system

   The need of reverse engineering:

   - *Interoperability:* Interoperability is a property of a product or system, whose interfaces are completely understood, to work with other products or systems, present or future, without any restricted access or implementation.

   - *Lost documentation:* Reverse engineering often is done because the documentation of a particular device has been lost or was never written, and the person who built it is no longer available. Integrated circuits often seem to have been designed on obsolete, proprietary systems, which means that the only way to incorporate the functionality into new technology is to reverse-engineer the existing chip and then re-design it.

- *Product analysis:* To examine how a product works, what components it consists of, estimate costs, and identify potential patent infringement.

- *Digital update/correction:* To update the digital version (e.g. 3D/CAD model) of an object to match an "as-built" condition.

- *Security auditing:* Determining whether vulnerabilities exist in a product

- *Learning:* learn from others' mistakes. Do not make the same mistakes that others have already made and subsequently corrected.

2) The second stage, disassembly or decompilation of the original product, is the most time-consuming aspect of the project. In this stage, Reverse Engineers attempt to construct a characterization of the system by accumulating all of the technical data and instructions of how the product works. In the third stage of Reverse Engineering, Reverse Engineers try to verify that the data generated by disassembly or decompilation is an accurate reconstruction of the original system. Engineers verify the accuracy and validity of their designs by testing the system, creating prototypes, and experimenting with the results.

3) Proprietary software developers are constantly developing techniques such as code obfuscation, encryption, and self-modifying code to make this modification increasingly difficult. Even with these measures being taken, developers struggle to combat software cracking. This is because it's very common for a professional to publicly release a simple cracked EXE or Retrium Installer for public download, eliminating the need for inexperienced users to crack the software themselves.

4) The five tools use for reverse engineering are:

   i) IDA Pro

   ii) Spices .NET Decompiler

   iii) Remotesoft .NET Explorer

   iv) PE Explorer

   v) REC Decompiler

   PE Explorer is the most feature-packed program for inspecting the inner workings of your own software, and more importantly, third party Windows applications and libraries for which you do not have source code. PE Explorer lets you open, view and edit a variety of different 32-bit Windows executable file types (also called PE files) ranging from the common, such as EXE, DLL and ActiveX Controls, to the less familiar types, such as SCR (Screensavers), CPL (Control Panel Applets), SYS, MSSTYLES, BPL, DPL and more (including executable files that run on MS Windows Mobile platform).

   PE Explorer gives you the power to look inside these PE binary files, perform static analysis, reveal a lot of information about the function of the executable, and collect as much information about the executable file as possible, without executing it. PE Explorer leaves you with only minimal work to do in order to get an analysis of a piece of software. Once you have selected the file you wish to examine, PE Explorer will analyze the file and display a summary of the PE header information, and all of the resources contained in the PE file. From here, the tool allows you to explore the specific elements within an executable file.

Besides being an effective Resource Editor, PE Explorer also provides several tools that elevate it to Power Coder status: an API Function Syntax Lookup, Dependency Scanner, Section Editor, UPX Unpacker, and a powerful yet easy-to-use Disassembler. With PE Explorer you can view and inspect unknown binaries, examine and edit the properties of EXE and DLL files, and correct and repair the internal structures of any PE (portable executable) files with the click of a button. PE Explorer is intended to be used in various scenarios such as software development, Forensics practice, Reverse Engineering extensive binary security analysis and binary auditing processes.

With PE Explorer You Can

- See what's inside an executable and what it does
- Change and customize the GUI elements of your Windows programs
- Track down what a program accesses and which DLLs are called
- Understand the way a program works, behaves, and interacts with others
- Verify the publisher and the integrity of the signed executable files
- Say good bye to digging through bloated help files just to hash out an API reference
- Open UPX-, Upack- and NsPack-compressed files seamlessly in PE Explorer, without long workarounds
- Special support for Delphi applications

UNIT 4 CRACKING METHODOLOGY

Structure

4.0 INTRODUCTION

Before testing any system, planning a basic methodology is very important. Ethical hacking involves more than just perletrating and patching. Proven techniques can help and guide you along the hacking highway and also ensure that you end up at the right destination. Planning a methodology that supports your ethical hacking goals is what separates the professionals from the amateurs.

With all of our advances in security technology, one aspect remains constant: passwords still play a central role in system security. The difficulty with passwords is that, they are the easiest security mechanism to defeat. Although we can use technology and policy to make passwords stronger, we are still fighting the weakest point in any system i.e. the human element.

Ultimately the goal is to get users to choose better passwords. However, it is not always clear how to achieve that goal. The problem is that as creative as humans are, we are way too predictable. If it is asked to make a list of totally random words, inevitably some sort of pattern, will emerge in your list automatically. Selecting good passwords requires sound security education. System administrators need to be educated and that education needs to be passed on to the end users as well. This unit is meant to bring you closer to understanding passwords in Windows operating system by addressing common password myths.

4.1 OBJECTIVES

After going through this Unit, you should be able to understand:

- What is Password Theft;
- Operating System Password Recovery;
- Application Password Recovery;
- Trojan Horses; and
- Man-In-The-Middle Attacks.

4.2 PASSWORD THEFT

Security experts have been discussing the problems with password security for years. But it seems that only few have listened and taken action to resolve those problems. If your IT environment controls authentication using passwords only, it is at greater risk for intrusion and hacking attacks than those that use some form of multifactor authentication.

The problem lies with the ever -increasing abilities of computers to process larger amounts of data in a smaller amount of time. A password is just a string of characters, typically only keyboard characters, which a person must remember and type into a computer terminal when required. Unfortunately, passwords that are too complex for a person to remember easily can be discovered by a cracking tool in a frighteningly short period of time. Dictionary attacks, brute force attacks, and hybrid attacks are all various methods which are freequently used to guess or crack passwords.

Password Cracking

Password cracking is a term used to describe the penetration of a network, system, or resource with or without the use of tools to unlock a resource that has been secured with a password. Passwords and "pass phrases" are used for everything ranging from logging into terminals to checking email accounts, from protecting Excel spreadsheets to securing the encryption keys for PKI-enabled enterprise networks. The use of the passwords in the enterprise is widespread and to provide security over and above is the biggest challenge.

Password crackers are the programs that aid in the discovery of protected passwords, usually through some method of automated guessing. Although some applications and poorly designed infrastructure equipment will encrypt or encode passwords, where most of the modern day operating systems and devices create a hash of the password instead.

Although some poor encryption mechanisms can be easily reversed, modern day hashing methods are one-way-that is, they can not be reversed and therefore decryption is not an option. Although the use of one-way algorithms can sound like a rock-solid solution, it simply makes the task at hand a little more time consuming. To circumvent the challenges created by hashing, password crackers simply employ the same algorithm used to encrypt the original password. The tools perform comparative analysis, and simply try to match their guesses with the original encrypted phrase or password hash.

4.3 OPERATING SYSTEM PASSWORD RECOVERY

It's possible that you forget Operating Systems password, especially after you have just created a new one, or you haven't used the computer for a long time, or maybe someone has changed your password. When that happens, you need to recover your password. But, how to do that? There are top 5 options for you.

Using a program anyone can automatically recover lost windows password.

Many people said the only way to reset your lost windows password is just to re-install the systems. However, this is not the better one. The best way for you is finding a program to help you recover Windows password.

4.3.1 Ophcrack

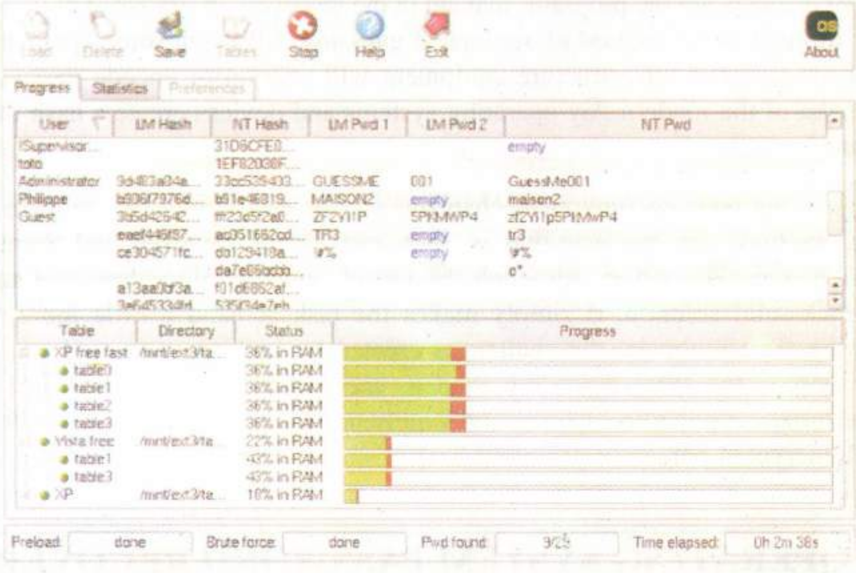
Ophcrack is an open source program that recovers passwords in a free way which is based on a time-memory trade-off using rainbow tables done by the inventors of the method. Just log into a computer and download the tool from the website and follow it's instructions to recover windows vista password.

Ophcrack will locate the users on your Windows system and begin cracking their passwords. The process is automatic – you don't usually need to type or click anything. When the passwords are displayed on screen, write them down.

On most computers, ophcrack can crack most passwords within a few minutes which mean it doesn't guarantee your password can be 100% recovered. It's just 99%, anyhow, just have a try. The disadvantage of the program is that, you may take a lot of time to download as it is very big.

Features:

- It runs on Windows, Linux/Unix, Mac OS X, ...
- It cracks LM and NTLM hashes.
- Free tables are available for Windows XP and Vista in it.
- Brute-force module is also available for simple passwords.
- Audit mode and CSV export.
- Real-time graphs to analyze the passwords.
- Live CD available to simplify the cracking.
- Loads hashes from encrypted SAM recovered from a Windows partition, Vista included.
- Free and open source software (GPL).



User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
!Supervisor...		31D6CFE0...			empty
toto		1EF82030F...			
Administrator	9d4f3a04a...	33cc535403...	GUESSME	001	GuessMe001
Philippe	b306f7976d...	b61e46819...	MAISON2	empty	maison2
Guest	3b5d42642...	ff23d5f2a0...	ZF2Y11P	5PKMWP4	zf2Y11p5PkMwP4
	eaef446f37...	ac051662cd...	TR3	empty	tr3
	ce304571fc...	d0129418a...	!#%	empty	!#%
		da7e06bdbb...			c*
	a13aa0bf3a...	f01d6852af...			
	3e6d533dfd...	535f34e7eb...			

Table	Directory	Status	Progress
XP free fast	/mnt/ext3/ta...	36% in RAM	
table0		36% in RAM	
table1		36% in RAM	
table2		36% in RAM	
table3		36% in RAM	
Vista free	/mnt/ext3/ta...	22% in RAM	
table1		43% in RAM	
table3		43% in RAM	
XP	/mnt/ext3/ta...	10% in RAM	

Preload: done Brute force: done Pwd found: 9/25 Time elapsed: 0h 2m 38s

Fig. 1

4.3.2 LophtCrack 6

LophtCrack 6 includes enhancements and additions to the critically-acclaimed LophtCrack auditor:

- **Password Scoring**

  LophtCrack 6 provides a scoring metric to quickly assess password quality. Passwords are measured against current industry best practices, and are rated as Strong, Medium, Weak, or Fail.

- **Pre-computed Dictionary Support**

  Pre-computed password files is a new advancement in password auditing. LophtCrack 6 now supports pre-computed password hashes and Password audits now take minutes instead of hours or days.

- **Unix Password Support**

  LophtCrack 6 imports and cracks Unix password files also and Perform network audits from a single interface.

- **Remote password retrieval**

  LophtCrack 6 has a built-in ability to import passwords from remote Windows and Unix machines, where previous versions of LophtCrack required a third-party utility.

- **Scheduled Scans**

  System administrators can schedule routine audits with LophtCrack 6. Audits can be performed daily, weekly, monthly, or just once, depending on the organization's auditing requirements.

- **Remediation**

  LophtCrack 6 offers remediation assistance to system administrators on how to take action against accounts that have poor passwords. Accounts can be disabled, or the passwords can be set to expire from within the LophtCrack 6 interface. Remediation works for Windows user accounts only.

- **Updated GUI**

  The user interface is improved and updated. More information is available about each user account, including password age, lock-out status, and whether the account is disabled, expired, or never expires. Information on LophtCrack 6's current session is provided in an "immediate window" with a reporting tab providing up-to-the-minute status of the current auditing session.

- **Improved reporting**

  LophtCrack 6 includes improved reporting. LophtCrack 6 now has real-time reporting that is displayed in a separate, tabbed interface. Auditing results are displayed based on auditing method, risk severity, and password character sets.

  - **Password Risk Status**

    Displays risk status in four different categories: Empty, High Risk, Medium Risk, and Low Risk.

  - **Password Audit Method**

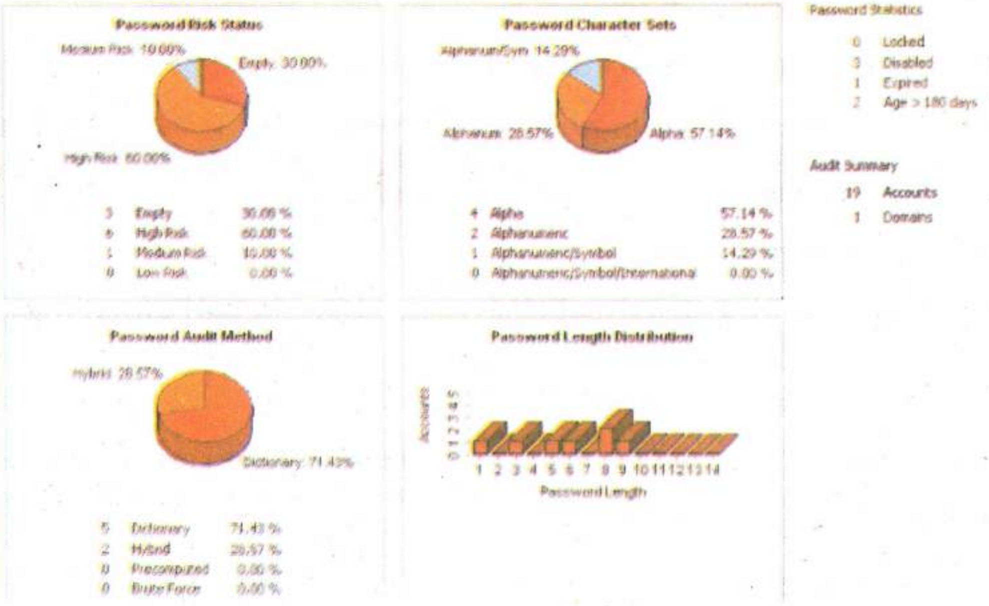
    Displays the completion of all four methods LophtCrack 6 uses: Dictionary, Hybrid, Precomputed, and Brute Force.

- **Password Character Sets**

  Reports the completion of the various character sets being audited, including, Alpha, Alphanumeric, Alphanumeric/Symbol, Alphanumeric/ Symbol/International.

- **Password Length Distribution**

  Reports the overall length of the discovered password by account.



3	Empty	30.00 %
6	High Risk	60.00 %
1	Medium Risk	10.00 %
0	Low Risk	0.00 %

4	Alpha	57.14 %
2	Alphanumeric	28.57 %
1	Alphanumeric/Symbol	14.29 %
0	Alphanumeric/Symbol/International	0.00 %

Password Statistics

0	Locked
3	Disabled
1	Expired
2	Age > 180 days

Audit Summary

19	Accounts
1	Domains

5	Dictionary	71.43 %
2	Hybrid	28.57 %
0	Precomputed	0.00 %
0	Brute Force	0.00 %

Fig. 2

The Summary Report in LophtCrack 6 shows the Password Statistics as Locked, Disabled, Expired, or if the password is older than 180 days. The Audit Summary shows the number of Accounts cracked and the number of Domains audited.

- **Foreign Password Cracking**

  LophtCrack 6 supports foreign character sets for Brute Force, as well as foreign dictionary files. Pull down menus change for language and character set. LophtCrack 6 ships with several foreign dictionaries.

Get Encrypted Passwords

- The Wizard's next dialog selects the source of encrypted passwords to audit. There are four options.
- LophtCrack 6 retrieves passwords on the machine it is installed on.
- LophtCrack 6 retrieves passwords from a remote machine on the network, provided you have administrator privileges.
- LophtCrack 6 retrieves encrypted passwords from a Windows NT Emergency Repair Disk.

  Note: Windows 2000 Emergency Repair Disks do not provide encrypted passwords.

- LophtCrack 6 sniffs the network for password hashes that are traversing it.

LophtCrack 6 audits passwords in four methods. The more rigorous and involved the audit, the longer the audit requires.

- The **Quick Password Audit** requires a few minutes to perform and tries every word in a 26,000 word dictionary file included with LophtCrack 6 to find words matching the passwords you examine.

- To adapt to **Corporate Password Policies** requiring strong passwords, the Common Password Audit programmatically varies the dictionary words by a number of characters to find modified words.
- The **Strong Password Audit** incorporates a brute force audit by attempting all combinations of letters and numbers to seek out computed passwords. This approach may take longer than a day to perform.
- The **Custom Audit** configures your audit more precisely. For example, you can change word files, change the hybrid mode parameters, or choose a different character set for the brute force audit.

Pick Reporting Style

LophtCrack 6 displays reports on the audit discoveries. Choose the reporting style to customize your report.

- **Display passwords when audited** reports on the audited passwords. Unselecting this selection reports the safety of the password without disclosing the password.
- **Display encrypted password** 'hashes' reports on encrypted passwords seen by the operating system.
- **Display how long…** reports the length of time LophtCrack 6 took to find a password.
- **Display auditing method** reports the method used to find each password.
- **Make visible notification when auditing is done** displays an alert dialog when the audit completes, even if you're working in another application.

Obtaining the Password Hashes

Approaches to obtaining password hashes differ, depending on where the password resides on the computer, and your ability to access them. LophtCrack 6 can obtain password hashes directly from remote machines, from the local file system, from backup tapes and repair disks, from Active Directory, or by recovering them as they traverse the network. Obtaining passwords over the network requires network and administrator privileges, as detailed below.

- **Import From Local Machine**

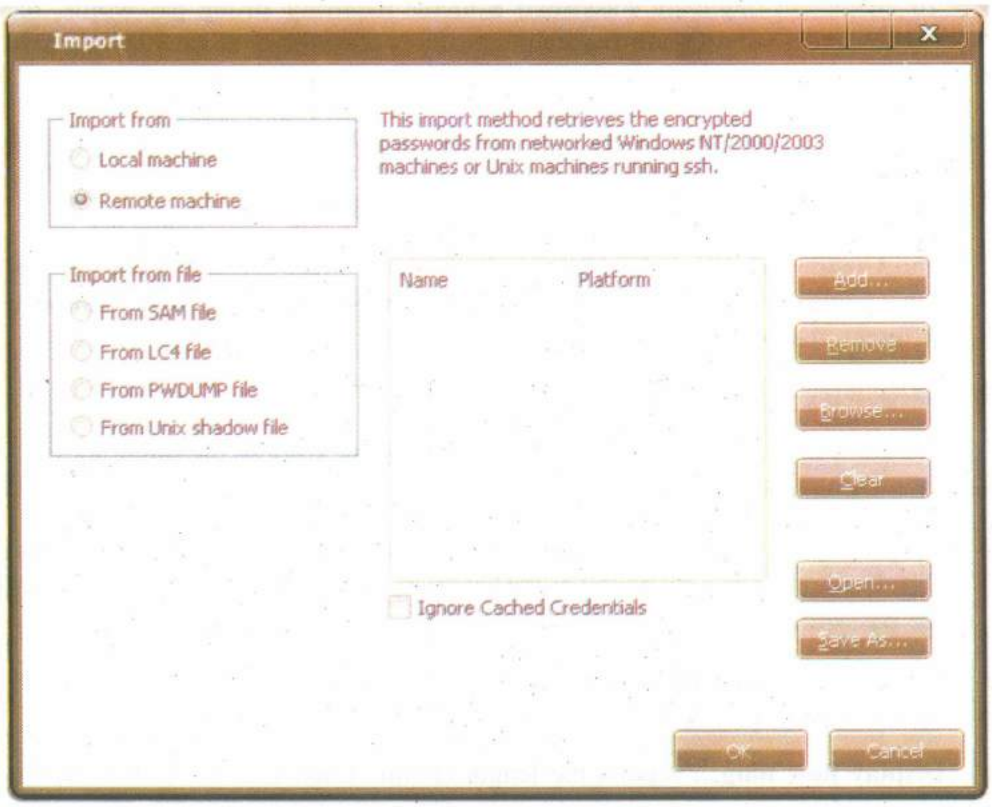
  To import passwords from a local machine, obtain administrator rights to the machine you intend to audit. From the **Session** menu, select **Import** and click the **Local Machine** option in the dialog box to retrieve the hashes. This approach works regardless of whether passwords are stored in a SAM file or in an Active Directory.

  NOTE: LophtCrack 6 is limited to dumping and opening 65,000 users. Audits with than 10,000 users require longer audit sessions.

- **Import from Remote Machine**

LophtCrack 6 incorporates remote password retrieval into the product, simplifying the process of obtaining password hashes, and reducing the need to use a third-party retrieval tool because of SYSKEY issues.

To import remote machines to the audit list, use the **Import** dialog box from the **Session** menu, and click on **Remote Machine**. Use the **Add** and **Browse** buttons to add the remote machines. Retrieving password files from remote machines requires administrative access.



Import from
○ Local machine
● Remote machine

This import method retrieves the encrypted passwords from networked Windows NT/2000/2003 machines or Unix machines running ssh.

Import from file
○ From SAM file
○ From LC4 file
○ From PWDUMP file
○ From Unix shadow file

□ Ignore Cached Credentials

Fig. 3

To save the audited group of remote machines, click Save As in the Import dialog box. Click Open from within the Import dialog box to retrieve a stored group.

LophtCrack 6 audits Unix password files from within the same interface. You are required to have an account on the remote Unix machine with access to the shadow file to perform this type of audit. LophtCrack recommends creating an auditing account on the remote machine to be used only by LoophtCrack 6. The Unix system must have the SSH (secure shell) service running for LophtCrack 6 to be able to retrieve the password hashes.

Passwords can be obtained remotely from both Windows and Unix machines, and contained in a single session. If they are both in a single session, auditing order is as follows:

- Windows Dictionary
- Unix Dictionary
- Windows Hybrid
- Unix Hybrid
- Windows Pre-computed
- Unix Pre-computed
- Windows Brute Force
- Unix Brute Force

- **SAM File**

On systems that do not use Active Directory, or SYSKEY, you may obtain password hashes directly from a password database file stored on the system, the SAM file.

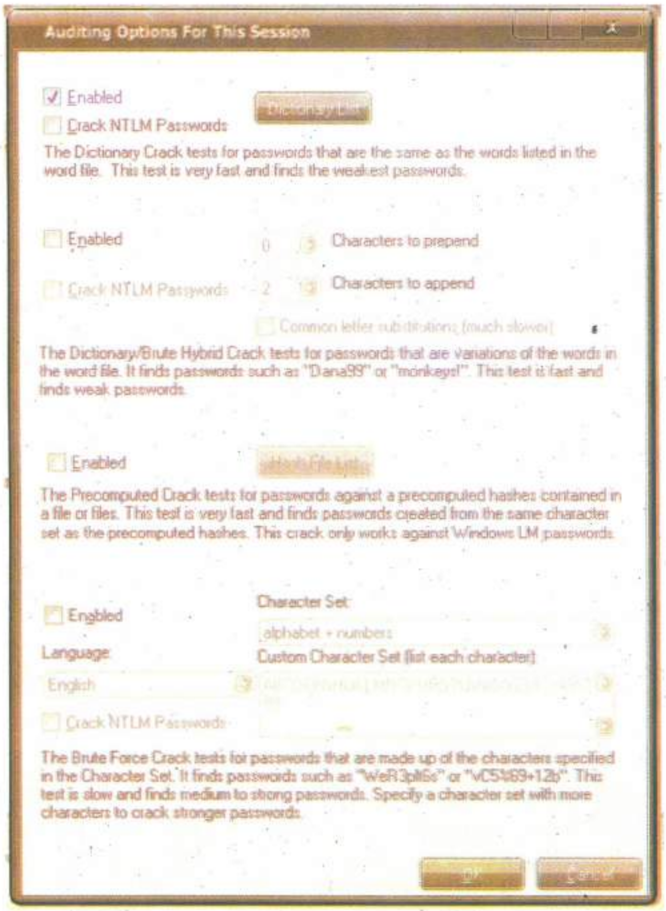
Note: This approach does not obtain password hashes from most Windows 2000 and Windows XP systems, as Windows 2000 and XP use SYSKEY by default. SYSKEY hashes cannot be found using a password cracker, due to the strong encryption Windows 2000 and XP use.

Windows NT Service Pack 3 introduced SYSKEY, which is turned off by default. SAM access works on Windows NT systems, unless SYSKEY is explicitly turned on. SYSKEY provides an additional layer of encryption to stored password hashes, however, you cannot tell by looking at the SAM or at password hashes it contains whether they have been encrypted with SYSKEY or not. LophtCrack 6 cannot crack SYSKEY-encrypted password hashes. If you do not have access to at least one administrator account on a Windows 2000 machine, you cannot obtain the password hashes required to run LophtCrack 6. In such cases, you may benefit from a password reset utility.

Password hashes cannot be read from the file system while the operating system is running, since the operating system holds a lock on the SAM file where the password hashes are stored. Copy the SAM file by booting another operating system such as DOS (running NTFSDOS), or Linux (with NTFS file system support) and retrieving it from the target system, where it is typically stored in C:\WinNT\system32\config. This is especially useful if you have physical access to the machine and it has a floppy drive.

You may also retrieve a SAM from a Windows NT Emergency Repair Disk, a repair directory on the system hard drive, or from a backup tape. Windows 2000 does not normally store a SAM file on the repair disks it generates.

Load the password hashes from a "SAM" or "SAM._" file into LophtCrack 6 using the **Import** dialog. Select to Import from file, From SAM File and specify the filename. LophtCrack 6 will automatically expand compressed "SAM._" files on NT.



Auditing Options For This Session

☑ Enabled
□ Crack NTLM Passwords

The Dictionary Crack tests for passwords that are the same as the words listed in the word file. This test is very fast and finds the weakest passwords.

□ Enabled
□ Crack NTLM Passwords
0 Characters to prepend
2 Characters to append
□ Common letter substitutions (much slower)

The Dictionary/Brute Hybrid Crack tests for passwords that are variations of the words in the word file. It finds passwords such as "Dana99" or "monkeys!". This test is fast and finds weak passwords.

□ Enabled

The Precomputed Crack tests for passwords against a precomputed hashes contained in a file or files. This test is very fast and finds passwords created from the same character set as the precomputed hashes. This crack only works against Windows LM passwords.

□ Enabled
Character Set: alphabet + numbers
Language: English
Custom Character Set (list each character)
□ Crack NTLM Passwords

The Brute Force Crack tests for passwords that are made up of the characters specified in the Character Set. It finds passwords such as "WeR3pl6s" or "vC5%69+12b". This test is slow and finds medium to strong passwords. Specify a character set with more characters to crack stronger passwords.

Fig. 4

- **Import LC4 Files**

  LophtCrack 6 can import previously saved sessions from LC4, allowing for a smooth upgrade to LophtCrack 6, as all of your LC4 session files can be used. LophtCrack 6 also has improved reporting capabilities to open previously completed sessions.

- **PWDUMP3**

  LophtCrack 6 dumps password hashes from the SAM database (and from Active Directory) of a system with Administrator privileges, regardless if SYSKEY is enabled or disabled on the system.

- **From Unix shadow file**

  LophtCrack 6 can extract the Unix password hashes from a Unix shadow file usually found on a Unix system as the /etc/shadow file. The shadow file must be in the format that Linux and Solaris systems use.

- **Packet Capture via Sniffing**

  Packet capture, or "Sniffing", is an advanced approach to obtaining password hashes that benefits from a good understanding of Ethernet networks. LophtCrack 6 supports sniffing via WinPcap packet capture software built by the Microsoft-sponsored Politecnico di Torino.

LophtCrack 6 can capture the encrypted hashes from the challenge/response exchanged when one machine authenticates to another over the network. Your machine must have one or more Ethernet devices to access the network. From the Session menu, select Import From Sniffer. If more than one network interface is detected, the Select Network Interface dialog box allows you to choose the interface to sniff on.

After choosing your interface, the SMB Packet Capture Output dialog box appears to capture any SMB authentication sessions that your network device can capture. Switched network connections only allow you to see sessions originating from your machine or connecting to your machine.

As SMB session authentications are captured, they are displayed in the SMB Packet Capture Output window. The display shows:

- Source and Destination IP addresses
- The user name
- The challenge
- The encrypted LANMAN hash
- The encrypted NTLM hash

The capture can be imported at any time using the Import button. You can capture and crack other passwords at the same time; however, password hashes captured after initiating an audit are not attempted in the running audit.

Cracking the Password Hashes

The cracking process that generates password values provides several options that balance audit rigor against the time required to crack. Effective auditing, therefore, requires an understanding the underlying business goals, and the security thresholds necessary to meet them.

To configure the cracking methods for your session, choose Session Options under the Session menu or click the Session Options button on the toolbar to open the

Auditing Options For This Session dialog box. The options for this dialog box are detailed below.

The UserName Crack

LophtCrack 6 first checks to see if any accounts have used the username as a password. These are weak passwords that you need to know about right away. This crack is performed first in every audit, because it is very quick.

Dictionary Crack

The fastest method for retrieving simple passwords is a dictionary crack. LophtCrack 6 tests all the words in a dictionary or word file against the password hashes. Once LophtCrack 6 finds a correct password, the result is displayed. The dictionary crack tries words up to the 14 character length limit (set by Windows NT, but not Windows 2000).

LophtCrack 6 uses the 25,000-word dictionary file, words-english.dic, which contains the most common English words. LophtCrack 6 also ships a 250,000 dictionary, words-english-big.dic, which can be used for more comprehensive dictionary audits. LophtCrack 6 loads this file or any other word file you select based on settings in the Session Options dialog.

LophtCrack 6 displays the result of passwords of any length located in the dictionary. The cracking process for non-dictionary words analyzes the first and last seven characters of a possible password, independently. For example, if the first seven characters of a password match those of a word in the dictionary, LophtCrack 6 reports these, even if subsequent characters do not match those in the dictionary word. Likewise, if the eighth character through the end of the word matches the corresponding characters in any dictionary word, LophtCrack 6 identifies those. When one half of a password is cracked, but the other is not, question marks (i.e. ???????) fill the un-cracked half. If neither half is cracked, the results in LophtCrack 6 are left blank.

Hybrid Crack

A Hybrid Crack builds upon the dictionary method (and its results display in the Dictionary Status area) by modifying existing dictionary words to generate additional password attempts. Many users choose passwords such as "bogus1!", or "1!bogus" in an attempt to create a memorable, yet harder to crack password, based on dictionary words slightly modified with additional numbers and symbols. Another common password substitutes numbers and symbols for letters, such as 3 for E, or $ for S. These types of passwords pass through many password filters and policies, yet still pose organizational vulnerability because they can easily be cracked.

Brute Force Crack

The most comprehensive cracking method is the brute force method, which recovers passwords up to 14 characters (Windows NT's password length limit).

The brute force crack attempts every combination of characters it is configured to use. Your choice of character sets determines how long the brute force crack takes. Common passwords, based on letters and numbers can typically be recovered in about a day using the default character set A-Z and 0-9. Complex passwords, on the other hand, that use characters such as #_}* could take up to hundreds of days to crack on the same machine.

NTLM, DES, and MD5 passwords are case-sensitive, and LophtCrack 6 tries both upper and lower case characters.

The difference between the strengths of weak versus strong passwords demonstrates the value of strong passwords in protecting your organization or machine. Using a real-world password auditing tool helps discover the strength of passwords in your organization, and gauge policy decisions such as:

- Whether users are following password policies,
- The compliance rate or non-compliance instances with such policies,
- The effectiveness of a password filter, or
- Password expiration times.

4.3.3 Password Recovery Tools

Free Windows password-cracking tools are usually Linux boot disks that have NT file system (NTFS) drivers and software that will read the registry and rewrite the password hashes for any account including the Administrators. This process requires physical access to the console and an available floppy drive but it works like a charm.

Beware!!! Resetting a user's or administrator's password on some systems (like Windows XP) might cause data loss, especially EFS-encrypted files and saved passwords from within Internet Explorer. To protect yourself against EFS-encrypted files loss you should always export your Private and Public key, along with the keys for the Recovery Agent user. Out of the following list, the only tool that will no cause any harm to EFS-encrypted files on your hard disk is the Windows Password recovery system. Here are 5 of these tools:

1) **Stellar Phoenix Password Recovery –** Simple startup utility resets a forgotten admin or users' password using a familiar Windows-like program interface instead of command-line.

2) **Password Kit** – Top rated version of Passware's Password recovery app, supports Windows Vista and RAID/SCSI/SATA drives.

3) **Petter Nordahl-Hagen's Offline NT Password & Registry Editor –** A great boot CD/Floppy that can reset the local administrator's password.

4) **Openwall's John the Ripper –** Good boot floppy with cracking capabilities.

5) **EBCD – Emergency Boot CD –** Bootable CD, intended for system recovery in the case of software or hardware faults.

Check Your Progress 1

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

Ophcrack is an open source program that recovers passwords in a free way. Justify.Which tools will not cause any harm to EFS-encrypted files on the hard disk?

....

....

....

....

....

....

4.4 APPLICATION PASSWORD RECOVERY

Do you wonder how *vulnerable* word-processing, spreadsheet, and zip files are as users send them into the wild blue yonder? Wonder no more. Some great utilities can show how easily Passwords could be cracked.

Cracking files

Most Password-protected files can be cracked in seconds or minutes. You can demonstrate this security Vulnerability to users and management. Here's a real-world scenario:

- Your CFO wants to send some confidential financial information in an Excel spreadsheet to the company's outside financial advisor.
- He protects the spreadsheet by assigning a Password to it during the file-save process in Excel.
- For good measure, he uses WinZip to compress the file, and adds another Password to make it really secure.
- The CFO sends the spreadsheet as an e-mail attachment, assuming that it will reach its destination securely.
- The financial advisor's network has content filtering, which monitors incoming e-mails for keywords and file attachments. Unfortunately, the financial advisory firm's network administrator is looking in the content filtering system to see what's coming in.
- This rogue network administrator finds the e-mail with the confidential attachment, saves the attachment, and realizes that it's Password-protected.
- The network administrator remembers some great Password-Cracking utilities from ElcomSoft (www.elcomsoft.com) that can help him out. He may see something like Figures.

4.4.1 Advanced Office Password Recovery

Gain Access to Password-Protected Documents

Forgetting a password to your personal email folder or a family budget can be annoying. Halting the work because of the lost password causes immediate monetary loss. Get control over your own documents even if they are protected with a password!

Advanced Office Password Recovery recovers, replaces, removes or circumvents instantly passwords protecting or locking documents created with Microsoft Office applications. Advanced Office Password Recovery unlocks documents created with all versions of Microsoft Office from the ancient 2.0 to the modern 2010. Recover passwords for Microsoft Word, Excel, Access, Outlook, Project, Money, PowerPoint, Visio, Publisher and OneNote. Reset MS Internet Explorer Content Advisor passwords and open any password-protected VBA project by exploiting a backdoor.

Features and Benefits

- Supports all versions of Microsoft Office applications from 2.0 to 2010
- Instant password recovery for multiple products
- Instantly unlocks documents with previously recovered passwords
- Exploits all known backdoors and tricks in the Office family for instant recovery

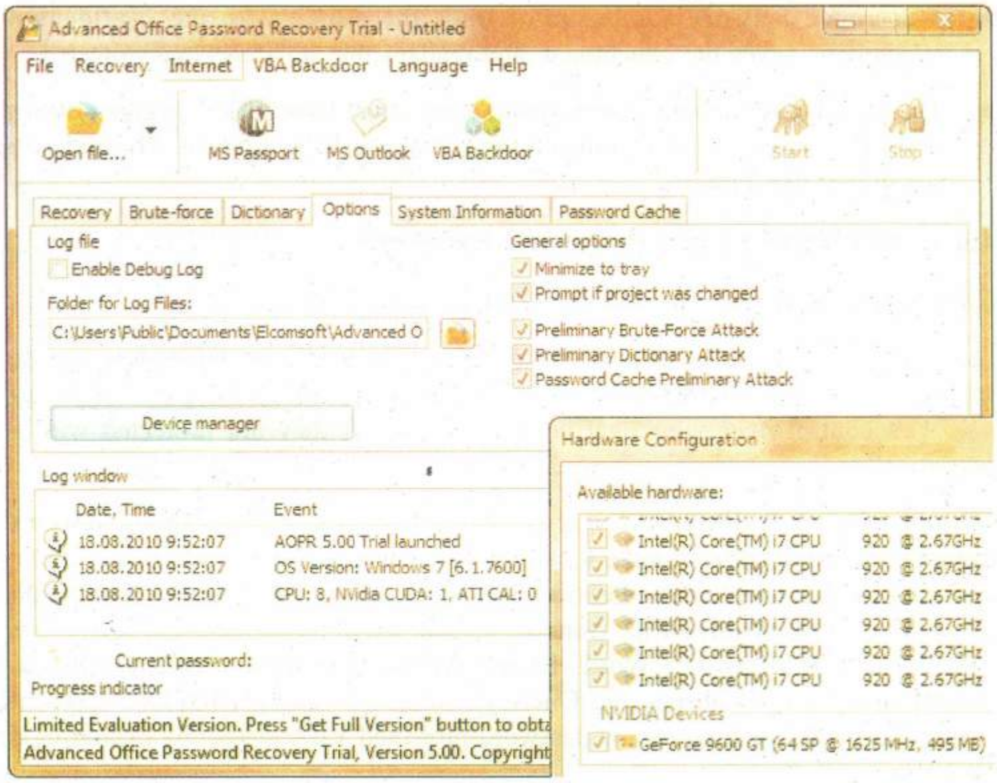
- Completely automatic preliminary attack may recover documents in less than 10 minutes
- Dictionary and brute-force attacks with user-defined masks and advanced templates
- Hardware acceleration (patent pending) reduces password recovery time by a factor of 50
- Patent-pending GPU acceleration technology with NVIDIA or ATI video cards
- Allows up to 32 CPUs or CPU cores and up to 8 GPUs
- Highly optimized low-level code for optimum performance

Selecting a file

To select a file you want to recover the password(s) for simply press the "Open File" button (or select the "File I Open File" menu item) and browse for the appropriate file (or press on a small arrow at the right to load a file you have been working with recently).

File Format will be recognized automatically with corresponding message in the Log Window. If the specified File Format is not supported by AOPR, or it's corrupted, or used by another application – the appropriate error message will be displayed.

You can clear the Recent Files list selecting the "File I Clear Files History" menu item.



Advanced Office Password Recovery Trial - Untitled

Log file

□ Enable Debug Log

Folder for Log Files: C:\Users\Public\Documents\Elcomsoft\Advanced O

General options

☑ Minimize to tray
☑ Prompt if project was changed
☑ Preliminary Brute-Force Attack
☑ Preliminary Dictionary Attack
☑ Password Cache Preliminary Attack

Log window

```
Date, Time            Event
18.08.2010 9:52:07    AOPR 5.00 Trial launched
18.08.2010 9:52:07    OS Version: Windows 7 [6.1.7600]
18.08.2010 9:52:07    CPU: 8, NVidia CUDA: 1, ATI CAL: 0
```

Current password:

Progress indicator

Limited Evaluation Version. Press "Get Full Version" button to obta

Advanced Office Password Recovery Trial, Version 5.00. Copyright

Hardware Configuration

Available hardware:

☑ Intel(R) Core(TM) i7 CPU 920 @ 2.67GHz
☑ Intel(R) Core(TM) i7 CPU 920 @ 2.67GHz
☑ Intel(R) Core(TM) i7 CPU 920 @ 2.67GHz
☑ Intel(R) Core(TM) i7 CPU 920 @ 2.67GHz
☑ Intel(R) Core(TM) i7 CPU 920 @ 2.67GHz
☑ Intel(R) Core(TM) i7 CPU 920 @ 2.67GHz

NVIDIA Devices

☑ GeForce 9600 GT (64 SP @ 1625 MHz, 495 MB)

Fig. 5

Result

After the File selection, the dialog box with results will be displayed automatically. The following situations may occur as the result of the File Processing:

All or some Passwords were recovered. The dialog box with Passwords is displayed. Password fields may contain those auxiliary messages:

- None - the Password is not set;
- Cannot be found instantly - the Password cannot be recovered instantly, you must select the Attack Options and Start the Attack to recover this Password. You can create a Project to save the Attack parameters to the file.
- Can be changed - the Password cannot be recovered, but can be changed or deleted. In this case a Dialog with results contains two additional buttons: "Change Password" and "Delete Password". You can change or delete the Password simply clicking those buttons. Selected File must not be write-protected to complete this operation successfully.
- Not available – the Passwor
- Selected File Format does not have such Password
- Password that decrypts a document is not found yet
- Error - an error occurred while Password Recovery process. The error message box is displayed to explain the error.

Any found Password can be copied to the Clipboard. Simply press the "Copy to Clipboard" button located at the right of the corresponding Password. You can insert the copied Password to any field by pressing the "Ctrl-V" buttons combination (usually the Paste menu item is disabled, but the keyboard shortcut always works). A Password which contains international symbols can be displayed incorrectly on Windows® 95, 98 and Me. These Windows® versions don't support Unicode and therefore we recommend using Windows® NT, 2000 or XP to recover Passwords with international symbols. Path to the selected File is displayed under "File Path:" caption. You can open the File simply clicking the "Open..." button.

Creating a project

If you need to recover the "open" password for a document and this password cannot be recovered instantly, you may create a project. Project file contains all information about the source File, selected Options and Character Set. You can simply copy the Project File to another computer and you don't need to copy the source File -- the Project contains all information needed to recover a Password.

When you open the file for password recovery and this Password cannot be recovered instantly, the program creates a new Project automatically. Project files have an ".AOPR" extension. By default the Project name is equal to the source File name. For example if you're opening the "test.doc" file, the Project name is "test.opr".

Saving a project

When the file is loaded, you can save your project -- all the changes you've made will be reflected in the project file. The name for the project is selected automatically based on the name of the file. If you want to give an alternative name - use "File | Save Project As..." menu item. If you don't want to change the name, just use the "File | Save Project" menu item.

If a Project was created and you're trying to quit AOPR, the Saving Project Prompt will be displayed. You can disable this Prompt unckecking the "Prompt if project was changed" checkbox at the Options tab.

Type of Attack

If a Password cannot be recovered instantly you must use one of the Attack Types. The following Attack Types are available in AOPR:

- Brute-Force Attack. This Attack will try all possible characters combinations in the specified Range. The Range is defined by Password Length and Brute-Force Range Options.

Password length

This is one of the most important options affecting checking time. You can check all 4-character (and shorter) passwords in a few minutes. But for longer passwords you have to have patience and/or some knowledge about the password (including the character set which has been used, or even better - the mask).

AOPR allows you to set a Password Length range by defining the Minimal and Maximal Length. These values can be set using the "Password Length" controls at the "Brute-Force" tab. The minimal length cannot be set to a value greater than maximal one. In this case the appropriate error message will be displayed.

If the Minimal and Maximal Lengths are not the same, the program tries the shorter passwords first. For example, if you set Minimal=3 and Maximal=7, the program will start from 3-character Passwords, then try 4-character ones and so on -- up to 7. While AOPR is running, it shows the current Password Length, as well as the current Password, Average Speed, Elapsed and Remaining Time, and Total and Processed number of passwords (some of these Parameters are displaying in the "Extended Statistics" Dialog. All of this information except average speed and elapsed time, which are global, is related only to the current length.

Brute-force range options

In MS Office documents passwords may contain the following Characters: latin letters (both small and capital), digits, special symbols (like @, #, $ etc) and national languages' symbols. You can select these Ranges separately, or define your own Password Range. To define your own range, check the box "Custom charset" and press the "Custom charset…" button.

The Predefined Passwords Ranges contain the following Characters:

- "a - z": abcdefghijklmnopqrstuvwxyz
- "A - Z": ABCDEFGHIJKLMNOPQRSTUVWXYZ
- "0 - 9": 0123456789
- "!@..." (special characters): !@#$%^&*()_+-=<>,./?[]{}~:;`'|"\
- "All Printable": contains all Ranges defined above

Password mask

If you already know some characters in the Password, you can specify the Mask to decrease the total number of passwords to be verified. At the moment, you can set the Mask only for fixed-length Passwords, but doing this can still help.

For example, you know that the Password contains 8 characters, starts with 'x', and ends with '99'; the other symbols are small or capital letters. So, the Mask to be set is "x?????99", and the charset has to be set to All caps and All small.

With such options, the total number of the passwords that AOPR will try will be the same as if you're working with 5-character passwords which don't contain digits; it is much less than if the length was set to 8 and All Printable options were selected. In the above example, the '?' chars indicate the unknown symbols.

If you know that the password contains character '?', you can choose a different Mask Character to avoid having one character, '?', represent both an unknown pattern position and a known character. In this case, you could change the Mask

Symbol from '?' ' to, for example, '#' or '*' ', and use a mask pattern of "x######?" (for mask symbol '#') or "x******?" (for mask symbol '*').

The Mask and Mask Symbol can be defined in the "Mask / Mask Character" control at the "Brute-Force" tab.

Custom Charset

You can define your own Character Set for the Brute-Force Attack. Click the "Define Custom Charset" button at the "Brute-Force" tab. The following Dialog will appear:

custom_charset

You can enter the Custom charset either in text and HEX format. In HEX format the Unicode symbols must be separated by Spaces. You can Load, Save, Clear and Add Charset by pressing the corresponding buttons. After entering the Charset AOPR checks for duplicate characters and removes them automatically.

The following char sets are included in AOPR distribution:

- Arabic (all Arabic symbols according to Unicode standard)
- Armenian
- Czech (splitted to caps and small letters)
- French (splitted to caps and small letters)
- German (splitted to caps and small letters)
- Greek (all symbols according to Unicode standard)
- Greek (letters only)
- Hebrew
- Japanese (Katakana)
- Japanese (Hiragana)
- Korean (Hangul Jamo)
- Russian (Cyrillic)

If the "Additional char sets" option was selected in installation, these char sets are placed in the "\char sets" directory.

- **Brute-Force with Mask.** This Attack is useful when you remember a part of Password. For example if you remember that length of your password was 5 characters and password begins from "A", you can define the mask "A????" and save the time by trying 4 symbols instead of 5. A Password Mask must be defined to use this Attack.
- **Dictionary Attack.** This Attack verifies the words stored in the specified Dictionary File. The dictionary is just a Unicode text file with one word at a line; lines are separated with line breaks. You can set additional Dictionary Options for this Attack. A Dictionary Attack is much faster than Brute-Force so we recommend to run it first. AOPR has supplied with one small Dictionary File containing English words. Additional Dictionaries can be obtained on a CD with any Elcomsoft program.

Dictionary Options

At first you have to select the desired Dictionary File. Click the "Select Dictionary File..." button at the ""Dictionary" tab and select the needed file.

In that Attack the program will try all words from it as passwords for the selected Document. It really helps when the Password has some meaning, i.e. the whole word. You can select an option "Smart mutations" or "Try all possible upper/ lower case combinations" – it may really help if you're not sure about the register the Password has been typed in. For example, let's assume that the next word in dictionary is "PASSword" (the case, actually, doesn't matter here). With the second option enabled, the program will just try all possible combinations, like:

password

passworD

passwoRd

passwoRD

passwOrd

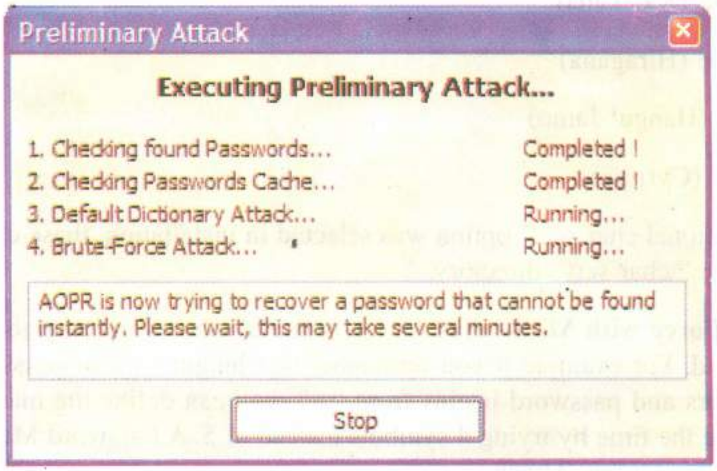
...

Default Dictionary

Default Dictionary is used when the Preliminary Attack is running. To select the Default Dictionary click the "Select Default Dictionary..." at the "Dictionary" tab. Please note, this Dictionary Attack is running with "Smart Mutations" Option and a long Dictionary File may slow down the Preliminary Attack.

- **Preliminary Attack**

  Preliminary Attack is the set of predefined Attacks which are tried when a password cannot be recovered instantly. When this Attack is running the following dialog is displayed:



Executing Preliminary Attack...

1. Checking found Passwords... Completed !
2. Checking Passwords Cache... Completed !
3. Default Dictionary Attack... Running...
4. Brute-Force Attack... Running...

AOPR is now trying to recover a password that cannot be found instantly. Please wait, this may take several minutes.

Fig. 6

Preliminary Attack consists of four independent attacks which can be enabled/ disabled in program options.

- **Found Passwords Attack**. This attack is always available. It checks all passwords that were found in the document prior to finding the current password. For example Microsoft® Word® files may have a VBA project password. This password is checked first because many users use the same passwords in different places.

- **Password Cache Attack**. This attack checks the Password Cache (all passwords found in other documents by AOPR). This attack can be enabled/

disabled by "Password Cache Preliminary Attack" checkbox at the "Options" tab.

- **Preliminary Dictionary Attack.** Performs the Dictionary Attack by Default Dictionary with "Smart Mutations" Option. This attack can be enabled/disabled by "Preliminary Dictionary Attack" checkbox at the "Options" tab.

Preliminary Brute-Force Attack. Performs the Brute-Force Attack by several predefined Character Sets. This Attack can be enabled/ disabled by "Preliminary Brute-Force Attack" at the "Options" tab.

- **Other options**

AOPR Options can be adjusted at the "Options" tab.

The "Device Manager" button allows selecting a hardware that will be used for password searching. By default AOPR uses all available CPU cores and graphic cards to achieve the best performance. But you can disable some CPUs or GPUs using the Device Manager.

"Enable Debug log" option creates a separate log file ("aoxppr_debug_log.txt") with the detailed information needed for resolving problems. Normally this option must be switched off.

Folder for log files: select the folder where "axppr_debug_log.txt" and other log files files will be created.

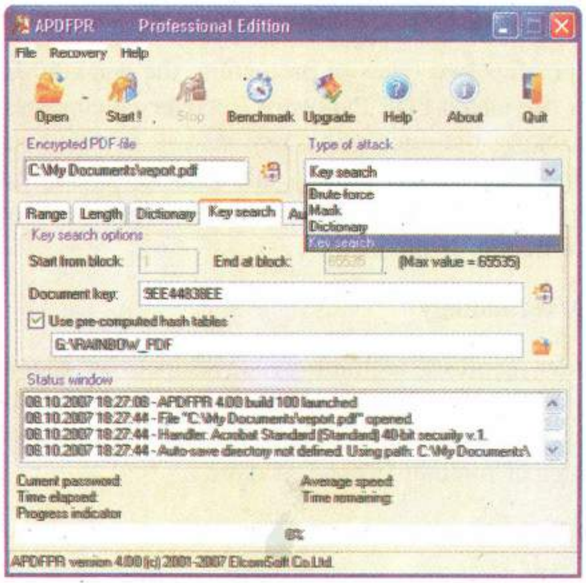
If you select the Minimize to tray option, the program will hide itself from the screen when being minimized (so you will not see an appropriate button on Windows® toolbar), but small icon will be created in the tray (near the system tray). Double-click on it to restore.

By disabling the Prompt if project was changed option, you instruct AOPR not to display the messages like "The project has been changed. Save?", when you've changed some options and open an another project, or creating a new one.

4.4.2 Advanced PDF Password Recovery

Get access to password-protected PDF files quickly and efficiently! Instantly unlock restricted PDF documents by removing printing, editing and copying restrictions!

Advanced PDF Password Recovery recovers or instantly removes passwords protecting or locking PDF documents created with all versions of Adobe Acrobat or any other PDF application.



Encrypted PDF-file: C:\My Documents\report.pdf

Type of attack: Key search

Key search options

Start from block: 1 End at block: 65535 (Max value = 65535)

Document key: 9EE44838EE

☑ Use pre-computed hash tables

G:\RAINBOW_PDF

Status window

```
08.10.2007 18:27:08 - APDFPR 4.00 build 100 launched
08.10.2007 18:27:44 - File "C:\My Documents\report.pdf" opened.
08.10.2007 18:27:44 - Handler: Acrobat Standard (Standard) 40-bit security v.1.
08.10.2007 18:27:44 - Auto-save directory not defined. Using path: C:\My Documents\
```

Current password:
Average speed:
Time elapsed:
Time remaining:
Progress indicator

0%

APDFPR version 4.00 (c) 2001-2007 ElcomSoft Co.Ltd.

Fig. 7

Features and Benefits

- Supports all versions of Adobe Acrobat, including Acrobat 9
- Supports GPU acceleration
- Supports all third-party products producing PDF files
- Instantly unlocks PDF documents with printing, copying and editing restrictions
- Removes "owner" and "user" passwords
- Recovers passwords to open
- Supports 40-bit and 128-bit RC4 encryption as well as 128-bit and 256-bit AES encryption
- Patent-pending Thunder Tables® technology recovers 40-bit passwords in a matter of minutes
- Dictionary and brute-force attacks with user-defined masks and advanced templates
- Three editions to satisfy the most demanding and savvy customers
- Optionally removes JScript code, form fields and digital signatures
- Batch mode allows automatic processing of multiple files
- Highly optimized low-level code optimized for modern multi-core CPUs

Instant Access to Restricted PDF Documents

Remove annoying restrictions from PDF files! Advanced PDF Password Recovery instantly unlocks PDF documents that restrict you of printing, editing or copying of data to clipboard.

This is by far the most common protection found in PDF files. If you can open a document without a password, but cannot print it at all or are restricted to low-quality output, or if you cannot copy data to clipboard or cannot edit the document, read no further and get Advanced PDF Password Recovery Standard edition!

Passwords to Open

What if you can't open a PDF document at all without knowing the correct password? In that case, you'll need the password recovery feature found in the Professional and Enterprise editions of Advanced PDF Password Recovery.

The PDF format specifies two types of protection: the weak 40-bit and the strong 128-bit encryption. Advanced PDF Password Recovery guarantees the recovery of 40-bit keys by attacking the encryption key instead of attempting to guess the password. While the Professional edition takes up to several days to recover a PDF document protected with a 40-bit key, the Enterprise edition can unlock an encrypted PDF in a matter of minutes!

Thunder Tables® Technology

The unique Thunder Tables® technology developed by ElcomSoft uses pre-computed tables to significantly speed up the recovery of 40-bit keys. The technology is available in the Enterprise edition, and will unlock a protected document in a matter of minutes instead of days.

Strong Password Recovery

If the PDF is protected with a strong 128-bit or 256-bit key, Advanced PDF

Password Recovery performs a range of attacks on the PDF file document in order to obtain the original password. But even then you're not left without options!

Dictionary Attack

Most passwords used by living beings are based on a word or phrase. Performing a dictionary attack by attempting different combinations of cases and variations of words and characters before reverting to a comprehensive brute-force attack allows for considerate time savings.

Brute Force Attack

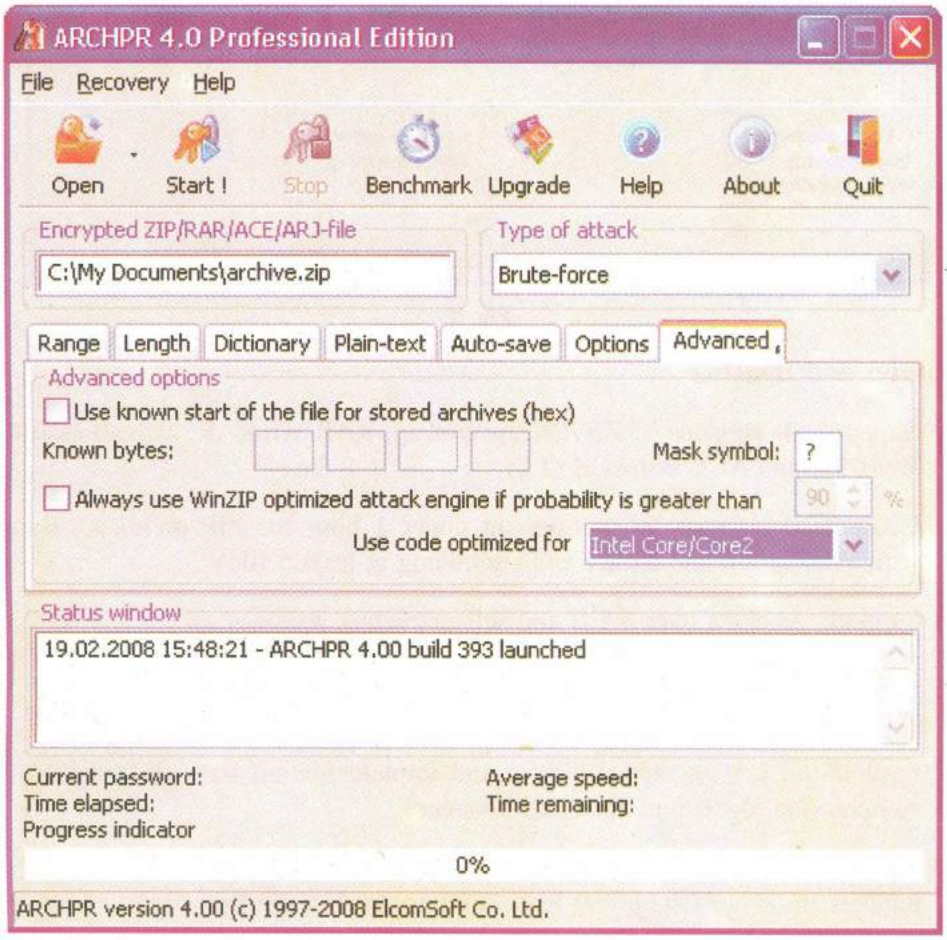
If the password does not fall into any dictionary, Advanced PDF Password Recovery attempts all possible combinations of passwords by performing the brute force attack. The highly optimized low-level code provides the best-in-class performance for the brute-force password recovery. Multi-threaded optimization ensures optimum performance on the modern multi-core CPUs.

Additional Notes

Mac Computers: Advanced PDF Password Recovery may not run on Mac running Windows 2000/XP/Vista on a virtual machine (using Virtual PC, VMWare, Parallels or other virtualization software).

DRM and Third-Party Security Plug-ins: Advanced PDF Password Recovery does not support PDF files protect using Digital Rights Management (DRM) technology or any third-party party security plug-ins such as FileOpen (FOPN_fLock).

Version 5.0 works with PDF files created in Adobe Acrobat 9 (with 256-bit AES encryption), with multi-core and multi-processor support and hardware acceleration using NVIDIA cards.



Encrypted ZIP/RAR/ACE/ARJ-file: C:\My Documents\archive.zip

Type of attack: Brute-force

Advanced options

□ Use known start of the file for stored archives (hex)

Known bytes:

Mask symbol: ?

□ Always use WinZIP optimized attack engine if probability is greater than 90 %

Use code optimized for Intel Core/Core2

Status window

```
19.02.2008 15:48:21 - ARCHPR 4.00 build 393 launched
```

Current password:

Average speed:

Time elapsed:

Time remaining:

Progress indicator

0%

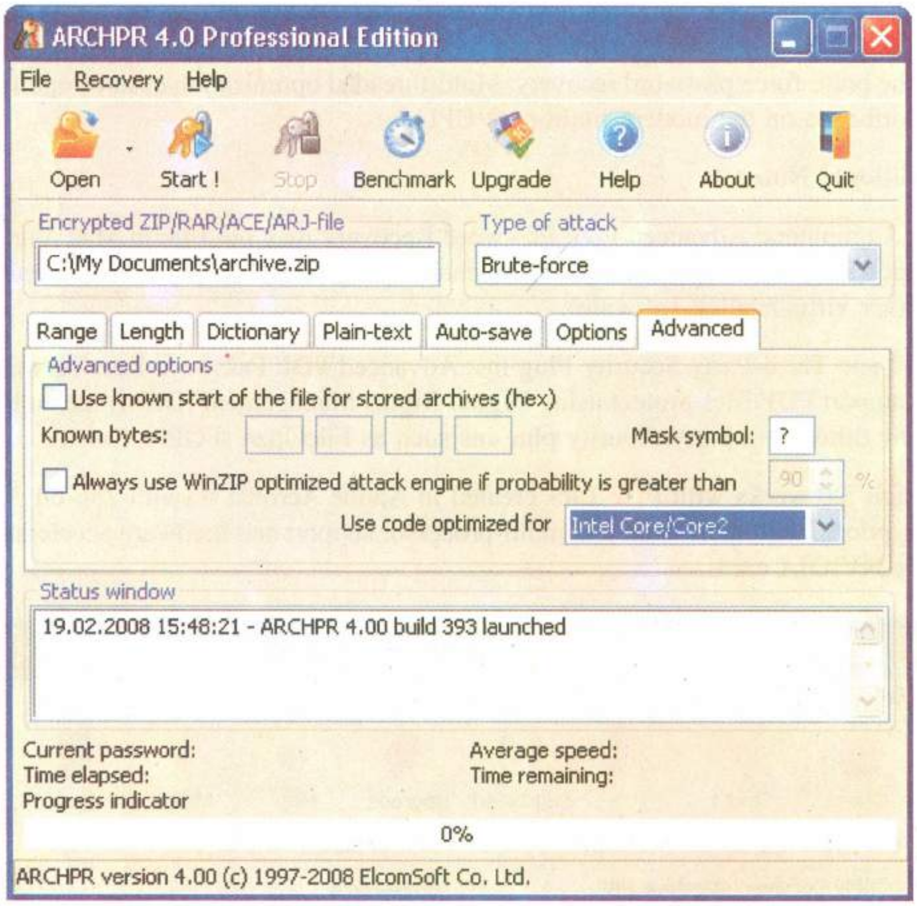
ARCHPR version 4.00 (c) 1997-2008 ElcomSoft Co. Ltd.

Fig. 8

4.4.3 Advanced Archive Password Recovery

Advanced Archive Password Recovery recovers protection passwords or unlocks encrypted ZIP and RAR archives created with all versions of popular archivers. Recover passwords for plain and self-extracting archives created with PKZip and WinZip, RAR and WinRAR automatically or with your assistance. Guaranteed unlocking of archives created with WinZip 8.0 and earlier in under one hour is possible by exploiting an implementation flaw.

Advanced Archive Password Recovery features ultimate compatibility among the various types of archives, knows weaknesses of certain types of protection, and provides best-in-class performance in unlocking all types of archives.



Encrypted ZIP/RAR/ACE/ARJ-file: C:\My Documents\archive.zip

Type of attack: Brute-force

Advanced options

□ Use known start of the file for stored archives (hex)

Known bytes: Mask symbol: ?

□ Always use WinZIP optimized attack engine if probability is greater than 90 %

Use code optimized for Intel Core/Core2

Status window

```
19.02.2008 15:48:21 - ARCHPR 4.00 build 393 launched
```

Current password: Average speed:
Time elapsed: Time remaining:
Progress indicator
0%

ARCHPR version 4.00 (c) 1997-2008 ElcomSoft Co. Ltd.

Fig. 9

Features and Benefits

- Supports all versions of ZIP/PKZip/WinZip, RAR/WinRAR, as well as ARJ/WinARJ, and ACE/WinACE (1.x)
- Guaranteed recovery of archives in under 1 hour for ZIP archives created with WinZip 8.0 and earlier and containing at least 5 files
- Supports archives over 4 GB and self-extracting archives
- Supports strong AES encryption found in WinRAR and the new versions of WinZip
- Exploits all known vulnerabilities and implementation flaws in the various compression algorithms for faster recovery
- Speedy known-plaintext attack recovers certain ZIP and ARJ archives in minutes (user must supply at least one unprotected file from that archive)
- Interrupt and resume operation at any time

- Supports background operation by utilizing idle CPU cycles only
- Dictionary and brute-force attacks with user-defined masks and advanced templates
- Highly optimized low-level code for optimum performance

Universal Compatibility

Supporting a wide range of compression and encryption algorithms, all versions of popular archivers and multiple archive formats, Advanced Archive Password Recovery comes as close to being a truly universal recovery tool as no one else. Advanced Archive Password Recovery unlocks archives compressed with various methods from legacy Shrinking, Reducing, Imploding, and Tokenizing to modern Inflating and recent WavPack, BZip2 and PPMd.

Certain ZIP and ARJ archives can be unlocked and decrypted in just minutes, provided that you have at least one unprotected file from that archive at your discretion. It does not matter how long and complex the password is! If you have a file from the encrypted ZIP archive in your hands, the whole archive can be usually unlocked in minutes by applying the known-plaintext attack. Similar ARJ archives are unlocked instantly. Fast recovery available only in case of "classical" encryption, not AES.

Guaranteed Recovery: Special Cases

After carefully analyzing the algorithms and implementations of password protection in different versions of WinZip, ElcomSoft developed a work-around solution to allow quick guaranteed decryption of certain ZIP archives instead of performing lengthy attacks. If an encrypted ZIP archive was created with WinZip version 8 or earlier, and if the archive contains 5 or more files, Advanced Archive Password Recovery can unlock the archive and decrypt its content - guaranteed! A modern PC takes just under one hour to finish the job. Guaranteed recovery available only in case of "classical" encryption, not AES.

Advanced Archive Password Recovery is well aware of the various methods of password protection, and implements all the tricks that allow you to recover protected archives as quickly as possible.

Strong AES Encryption Support

Advanced Archive Password Recovery supports latest encryption technologies, including the complex AES encryption used in WinRAR and the recent versions of WinZip.

Advanced Encryption Standard (AES) is a strong cipher used as an encryption standard by the U.S. government, military and Special Forces. AES has been extensively analyzed by cryptography specialists worldwide, and is a proven international standard for strong data protection.

If nothing else helps, Advanced Archive Password Recovery performs a range of attacks on a protected archive in order to obtain the original password. Even then you're not left without options! If you remember something about the password, that information will be used to speed up the recovery. Don't take anything for a given! Just specifying your company security policy can increase the speed of the attack tenfold. Remember how many characters your password had, or that it was certainly longer than a certain length? Sure your password had numbers or letters, or both? Maybe you can recollect the first or the last character, or remember whether it was a letter or a number? Every little bit of extra information helps to speed up the recovery.

Dictionary Attack

Most passwords used by human beings are based on a single word or a combination of words from a certain language. Before reverting to the brute force attack, Advanced Archive Password Recovery performs a full-scaled comprehensive attack based on a dictionary.

Use a small built-in dictionary or specify your own dictionaries no matter the language, and Advanced Archive Password Recovery will attempt single words and word combinations in different cases and variations.

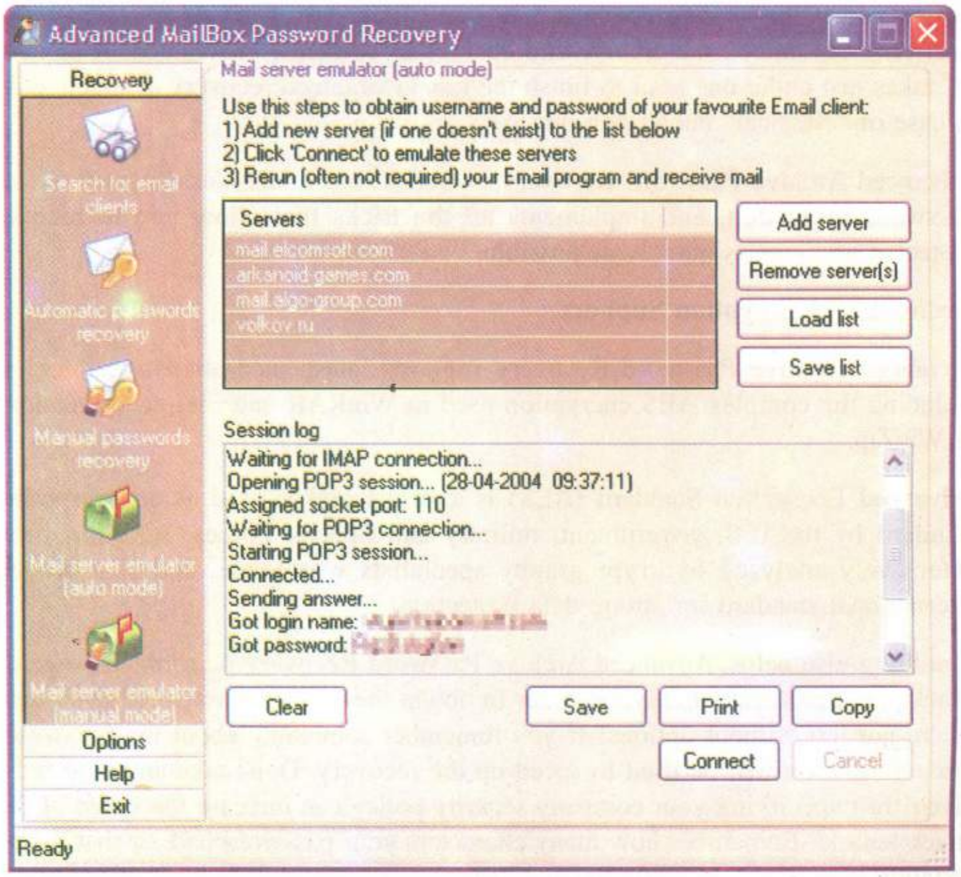
Brute Force Attack

If you're blank about the password, Advanced Archive Password Recovery will revert to the last resort: the brute force attack. Thanks to the highly optimized low-level code, Advanced Archive Password Recovery provides the best-in-class performance for the brute-force password recovery, attempting millions different password combinations per second on a typical ZIP archive with a modern CPU. As many people tend to choose short, simple passwords, the brute-force attack remains a viable option for password recovery.

4.4.4 Advanced Mailbox Password Recovery

Recover Passwords to Email Accounts and Profiles

Advanced Mailbox Password Recovery instantly retrieves the locally stored login and password information protecting email accounts and profiles, and supports many popular email clients. With the help of the included POP3/IMAP Server Emulator, Advanced Mailbox Password Recovery retrieves passwords to POP3 and IMAP accounts from all email clients in existence.


Advanced MailBox Password Recovery
Recovery
Search for email clients
Automatic passwords recovery
Manual passwords recovery
Mail server emulator (auto mode)
Mail server emulator (manual mode)
Options
Help
Exit
Add server
Remove server(s)
Load list
Save list
Clear
Save
Print
Copy
Connect
Cancel
Ready

Mail server emulator (auto mode)

Use this steps to obtain username and password of your favourite Email client:
1) Add new server (if one doesn't exist) to the list below
2) Click 'Connect' to emulate these servers
3) Rerun (often not required) your Email program and receive mail

Servers
mail.elcomsoft.com
arkanoid-games.com
mail.algo-group.com
volkov.ru

Session log

```
Waiting for IMAP connection...
Opening POP3 session... (28-04-2004  09:37:11)
Assigned socket port: 110
Waiting for POP3 connection...
Starting POP3 session...
Connected...
Sending answer...
Got login name: [redacted]
Got password: [redacted]
```

Fig. 10

Features and Benefits

- Recovers passwords to multiple email clients

- Recovers passwords to all accounts
- Retrieves send (SMTP) and receive (POP3/IMAP) passwords
- Recovers profile passwords and master-passwords
- Recovers POP3/IMAP passwords in all email clients with the POP3/IMAP Server Emulator
- Retrieves passwords to uninstalled email clients
- Recovers corrupted email databases and installations
- Fully automatic operation displays all passwords at once
- Fully manual operation supports corrupted email clients and databases

Universal Compatibility

Advanced Mailbox Password Recovery can recover login and password information to POP3 and IMAP accounts from any email client in existence. The included POP3/IMAP Server Emulator intercepts the login and password information sent to an email server.

Mobile Clients

Forgetting a POP3 or IMAP password on a mobile client such as a cell phone or Windows Mobile communicator may be impossible to recover without Advanced Mailbox Password Recovery, but could not be easier with it. Just replace the POP3/IMAP server on the mobile device with the address of POP3/IMAP Server Emulator, and Advanced Mailbox Password Recovery will intercept and display the password the moment your mobile device connects to the server to check for new messages.

Instant Recovery

Run Advanced Mailbox Password Recovery and see all email passwords at once! Advanced Mailbox Password Recovery scans your system and retrieves all types of passwords to supported email clients in just seconds.

Passwords to Corrupted Mailboxes

In manual mode, Advanced Mailbox Password Recovery recovers passwords to corrupted email databases, and can operate even if an email client has been uninstalled.

Supported Email Clients

- Microsoft Internet Mail and News
- Eudora
- TheBat! and TheBat! Voyager
- Netscape Navigator/Communicator Mail
- Pegasus mail
- Calypso mail
- FoxMail
- Phoenix Mail
- IncrediMail
- @nyMail

- QuickMail Pro
- MailThem
- Opera mail
- Kaufman Mail Warrior
- Becky!
- Internet Mail

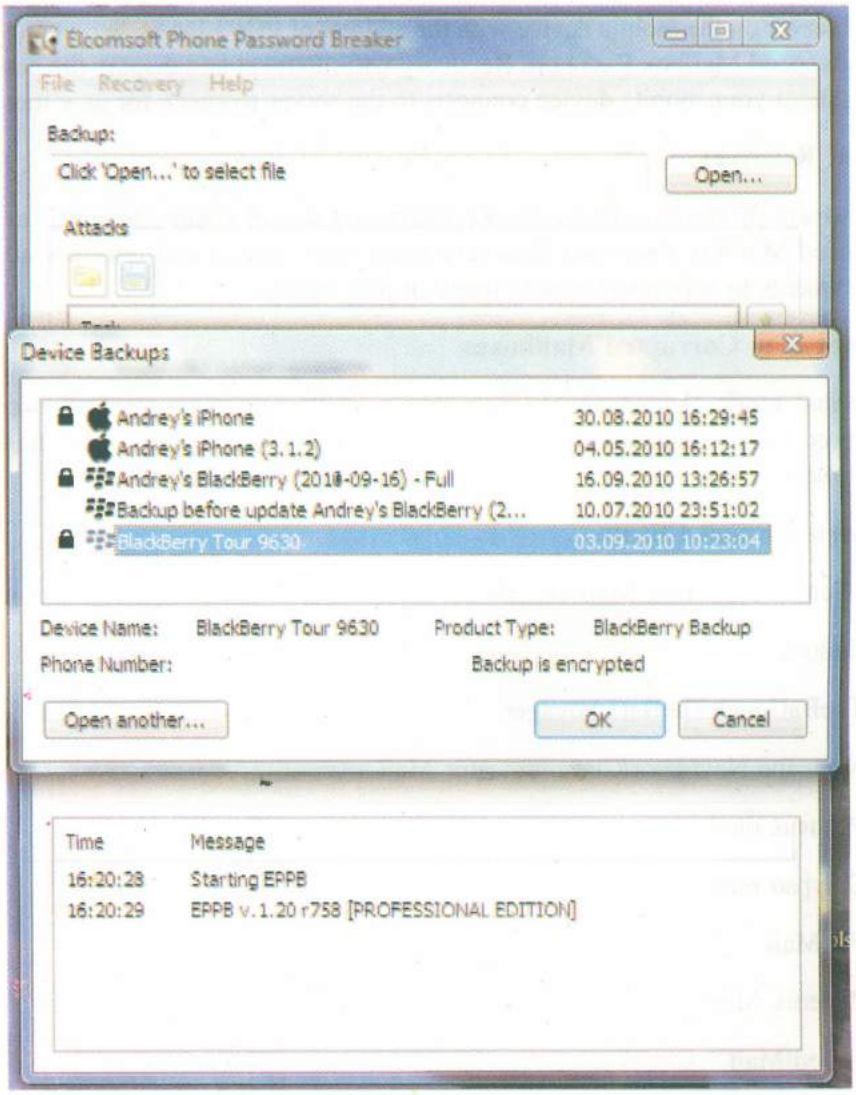
Local Account Operation

Please note that Advanced Mailbox Password Recovery can recover lost or forgotten password from the local account only, and requires you to be logged in to the system. This product cannot be used to retrieve somebody else's passwords.

4.4.5 Elcomsoft Phone Password Breaker

Recover Password-Protected BlackBerry and Apple Backups

Elcomsoft Phone Password Breaker enables forensic access to password-protected backups for smart phones and portable devices based on RIM BlackBerry and Apple iOS platforms. The password recovery tool supports all Blackberry smart phones as well as Apple devices running iOS including iPhone, iPad and iPod Touch devices of all generations released to date, including the latest iPhone 4 and iOS 4.1.



```
Andrey's iPhone                                      30.08.2010 16:29:45
Andrey's iPhone (3.1.2)                              04.05.2010 16:12:17
Andrey's BlackBerry (2010-09-16) - Full              16.09.2010 13:26:57
Backup before update Andrey's BlackBerry (2...       10.07.2010 23:51:02
BlackBerry Tour 9630                                 03.09.2010 10:23:04
```

Device Name: BlackBerry Tour 9630

Product Type: BlackBerry Backup

Phone Number:

Backup is encrypted

```
Time        Message
16:20:28    Starting EPPB
16:20:29    EPPB v.1.20 r758 [PROFESSIONAL EDITION]
```

Fig. 11

Unlock Apple and BlackBerry Backups

The new tool recovers the original plain-text passwords protecting encrypted backups for Apple and BlackBerry devices. The backups contain address books, call logs, SMS archives, calendars and other organizer data, camera snapshots, voice mail and email account settings, applications, Web browsing history and cache.

Fast GPU Acceleration

To unlock Apple backups even faster, the tool engages the company's patent-pending GPU acceleration technology. Elcomsoft Phone Password Breaker is the first GPU-accelerated iPhone/iPod password recovery tool on the market, and the only product to read and decrypt key chains (saved passwords to mail accounts, web sites and 3rd party applications) from password-protected backups (if password is known or recovered).

Features and Benefits

- Gain access to information stored in password-protected iPhone, iPad and iPod Touch backups
- Decrypt encrypted BlackBerry backups
- Recover original plain-text passwords
- Read and decrypt keychain data (email account passwords, Wi-Fi passwords, and passwords you enter into websites and some other applications)
- Save time with cost-efficient GPU acceleration when one or several ATI or NVIDIA video cards are installed*
- Hardware acceleration on Tableau TACC1441 hardware
- Perform advanced dictionary attacks with highly customizable permutations
- Perform offline attacks without Apple iTunes or BlackBerry Desktop Software installed
- Recover passwords to backups for original and 'jailbroken' iPhone, iPhone 3G, iPhone 3GS, iPhone 4, iPad, and iPod Touch 1st to 4th Gen devices
- Recover passwords to all BlackBerry smart phones released to date
- Compatible with all versions of iTunes (incl. 10.0) and iOS (3 and 4, incl. 4.1) and BlackBerry Desktop Software
- iPhone backup decryption using known password
- Using AES-NI instructions to speed up BlackBerry backups' password recovery
- AMD Radeon HD 6970 and NVIDIA GTX 580 support

Advanced Attacks

Elcomsoft Phone Password Breaker supports an advanced dictionary attack with customizable permutations. According to multiple security researches, the majority of users choose meaningful, dictionary-based passwords that are easier for them to remember. Elcomsoft Phone Password Breaker is able to recover such passwords and their variations quickly and efficiently no matter which language they are. Elcomsoft Phone Password Breaker supports a variety of permutations of dictionary words, trying hundreds of variants for each dictionary word to ensure the best possible chance to recover the password.

Extract and Decrypt Stored Passwords

In Apple iPhone devices, passwords to email accounts, Web sites, and certain third-party software are stored securely in key chains that are encrypted with hardware keys unique to each individual device.

Prior to the release of iOS 4, key chains remained encrypted with a device-specific hardware key; but with the release of Apple iOS4, the key chains are stored encrypted only with backup's master password. Elcomsoft Phone Password Breaker is able to instantly read and decrypt all keychain data including stored passwords if a backup password is known or recovered.

Offline Backups

Elcomsoft Phone Password Breaker does not use Apple iTunes or BlackBerry Desktop Software, and does not need to have those products installed. All password recovery operations are performed offline.

4.4.6 Advanced EFS Data Recovery

Restore Access to EFS-Encrypted Files

Microsoft Encrypting File System (EFS) is an integral part of Microsoft Windows operating systems that enables users to protect their files against unauthorized access even from those who gain physical access to the hard disk or the computer that contains the encrypted files.

Advanced EFS Data Recovery decrypts the protected files, and works in all versions of Windows 2000, XP, 2003, Vista, Windows Server 2008 and Windows 7. The recovery is still possible even when the system damaged, is not bootable, or when some encryption keys have been tampered with.

Advanced EFS Data Recovery recovers EFS-encrypted data that becomes inaccessible because of system administration errors such as removing users and user profiles, misconfiguring data recovery authorities, transferring users between domains, or moving hard disks to a different PC.

Advanced EFS Data Recovery is a powerful data recovery tool that helps recovering the encrypted files under various circumstances.

- EFS-protected disk inserted into a different PC
- Deleted users or user profiles
- User transferred into a different domain without EFS consideration
- Account password reset performed by system administrator without EFS consideration
- Damaged disk, corrupted file system, unbootable operating system
- Reinstalled Windows or computer upgrades
- Formatted system partitions with encrypted files left on another disk

Why Encrypted Files Become Inaccessible

The EFS appears completely transparent to the user, providing on-the-fly encryption and decryption of data with strong cryptographic algorithms. The ease of use and complete transparency to the end user creates false impression of impeccability of the Encrypting File System in the eyes of the user, who often forget about the encrypted files when they re-install Windows or transfer a disk into a new, upgraded computer.

Recovering Encrypted Files

Advanced EFS Data Recovery decrypts files protected with EFS quickly and efficiently. Scanning the hard disk directly sector by sector, Advanced EFS Data Recovery locates the encrypted files as well as the available encryption keys, and decrypts the protected files. The direct access to the file system allows Advanced EFS Data Recovery to recover encrypted files in the most difficult cases even if the disk with data is only available without a valid user account to login into system, or when some encryption keys have been tampered with.

Instant Access

With Advanced EFS Data Recovery, instant access to EFS-protected files is often possible. The product is well aware of the EFS encryption weakness present in Windows 2000, allowing quickest recovery of the encrypted files. Supplying a valid password to the user account (or a previously used password if the password has been reset by a system administrator, causing EFS-protected files to become inaccessible) or an account that serves as a data recovery agent (Administrator account by default) can often provide on-the-fly decryption of the protected files.

The Professional edition locates master and private keys in the deleted files as well, scanning the disk sector by sector and using patterns to locate the keys, allowing the recovery of re-formatted disks and overwritten Windows installations.

4.4.7 Elcomsoft Wireless Security Auditor

Elcomsoft Wireless Security Auditor allows network administrators to verify how secure a company's wireless network is by executing an audit of accessible wireless networks. Featuring patent-pending cost-efficient GPU acceleration technologies, Elcomsoft Wireless Security Auditor attempts to recover the original WPA/WPA2-PSK text passwords in order to test how secure your wireless environment is.

- Determine how secure your wireless network is
- Built-in wireless network sniffer (with AirPCap adapters)
- Test the strength of WPA/WPA2-PSK passwords protecting your wireless network
- Save time with patent-pending GPU acceleration technology when one or more compatible NVIDIA or ATI video cards are present
- Hardware acceleration on Tableau TACC1441 hardware
- Run advanced dictionary attacks with highly configurable variations
- Perform attacks from inside or outside of your network

4.4.8 Advanced VBA Password Recovery

Advanced VBA Password Recovery (or simply AVPR) is a program to recover or remove lost or forgotten passwords to view and edit Visual Basic for Applications (VBA) projects source code in Microsoft Office documents: Word, Excel, Outlook, Project, Access, PowerPoint, Visio. AVPR can also unlock protected Excel add-ins.

In addition, allows to open all documents with VBA projects (not only Microsoft ones) via the "backdoor", so no password is needed to view the code (works with all Office components and all other VBA-enabled applications like Corel WordPerfect Office, AutoCAD). All versions of Microsoft Office (from 97 to 2007) are supported – either directly or through the backdoor.

4.4.9 Elcomsoft Internet Password Breaker

Reveal Stored Internet Passwords

Elcomsoft Internet Password Breaker instantly reveals Internet passwords, retrieves login and password information protecting a variety of Web resources and mailboxes in various email clients. The new password recovery tool supports instant password recovery for passwords, stored forms and AutoComplete information in Microsoft Internet Explorer, mailbox and identity passwords in all versions of Microsoft Outlook Express, passwords to all types of accounts and PST files in Microsoft Outlook, and passwords protecting email accounts in Windows Mail and Windows Live Mail. Apple Safari, Google Chrome, Mozilla Firefox* and Opera Web browsers are also supported.

Features and Benefits

- Instant password recovery for a variety of applications
- Supports all versions of Microsoft Internet Explorer, including IE7 and IE8
- Supports all versions of Microsoft Outlook and Outlook Express
- Supports Windows Mail and Windows Live Mail passwords
- Instantly recovers passwords cached in Apple Safari, Google Chrome, Mozilla Firefox and Opera Web browsers
- Reveals stored POP3, IMAP, SMTP and NNTP passwords for all supported applications
- Recognizes and works around enhanced security model of Internet Explorer 7 and 8
- Reveals Microsoft Passport information in Windows Live Mail
- Retrieves Microsoft Outlook PST passwords
- Recovers login and password information to a variety of resources

Check Your Progress 2

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

How Advanced Office Password Recovery is useful in passwords protecting documents created with Microsoft Office applications? What are the attacks available in Advanced Office Password Recovery?

....

....

....

....

....

....

....

....

....

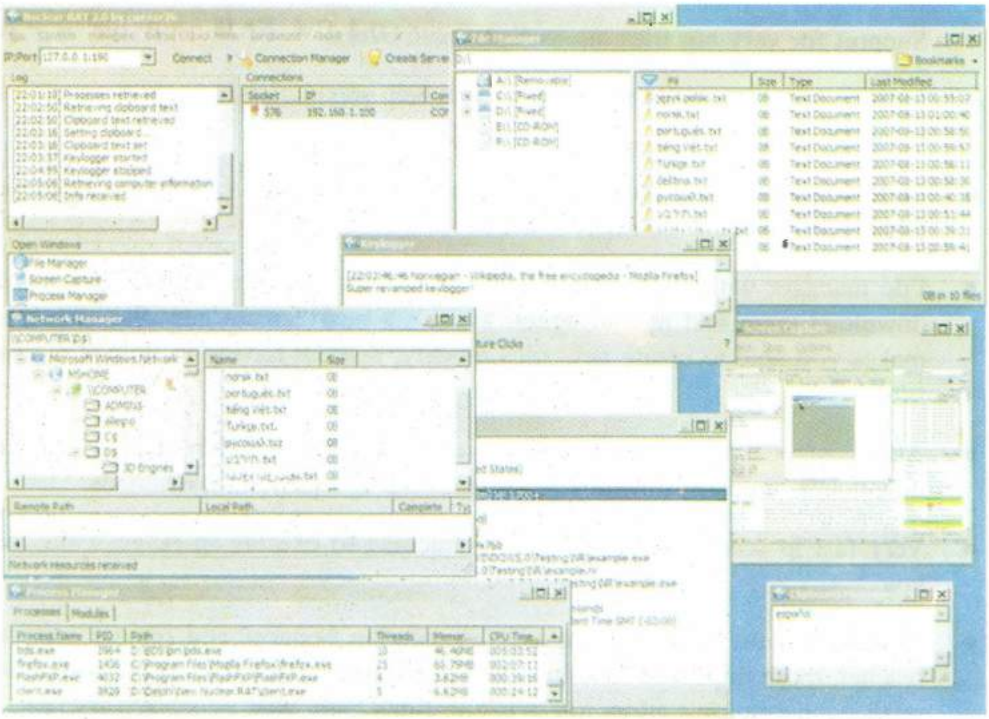
4.5 TROJAN HORSES

A Trojan horse is a continuing threat to all forms of IT communication. Basically, a Trojan horse is a malicious payload surreptitiously delivered inside a benign host. You are sure to have heard of some of the famous Trojan horse malicious payloads such as Back Orifice, NetBus, and SubSeven. But the real threat of Trojan horses is not the malicious payloads you know about, its ones you don't. A Trojan horse can be built or crafted by anyone with basic computer skills. Any malicious payload can be combined with any benign software to create a Trojan horse. There are countless ways of crafting and authoring tools designed to do just that. Thus, the real threat of Trojan horse attack is the unknown.

The malicious payload of a Trojan horse can be anything. This includes programs that destroy hard drives, corrupt files, record keystrokes, monitor network traffic, track Web usage, duplicate e-mails, allow remote control and remote access, transmit data files to others, launch attacks against other targets, plant proxy servers, host file sharing services, and more. Payloads can be grabbed off the Internet or can be just written code authored by the hacker. Then, this payload can be embedded into any benign software to create the Trojan horse. Common hosts include games, screensavers, greeting card systems, admin utilities, archive formats, and even documents.

All a Trojan horse attack needs to be successful is a single user to execute the host program. Once that is accomplished, the malicious payload is automatically launched as well, usually without any symptoms of unwanted activity. A Trojan horse could be delivered via e-mail as an attachment, it could be presented on a Web site as a download, or it could be placed on a removable media (memory card, CD/DVD, USB stick, floppy, etc.). In any case, your protections are automated malicious code detection tools, such as modern anti-virus protections and other specific forms of Malware scanners, and user education.

4.5.1 Nuclear RAT V2.1.0



```
[22:01:10] Processes retrieved
[22:02:50] Retrieving clipboard text
[22:02:50] Clipboard text retrieved
[22:03:16] Setting clipboard...
[22:03:16] Clipboard text set
[22:03:37] Keylogger started
[22:04:55] Keylogger stopped
[22:05:06] Retrieving computer information
[22:05:06] Info received
```

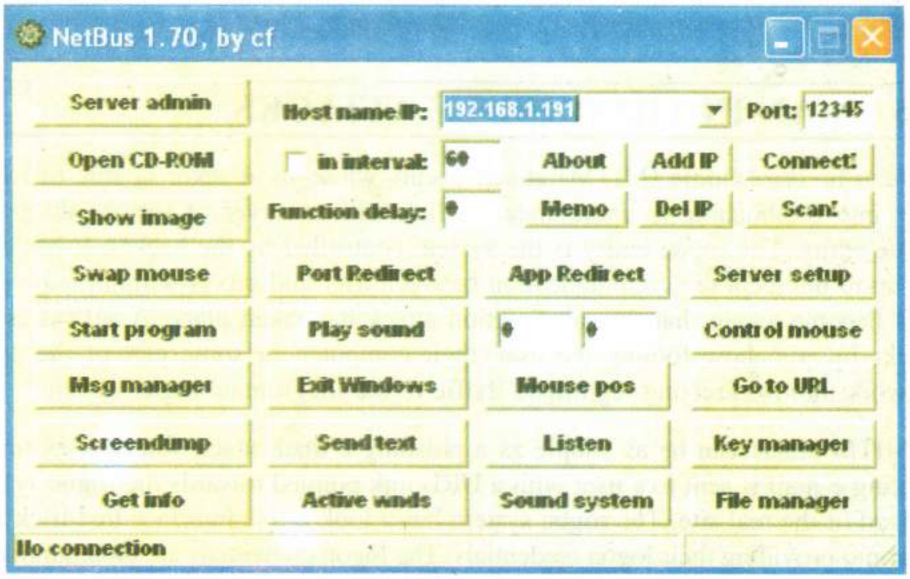
Fig. 12

Feature highlight

- Unicode support, you can see folders, windows, text, in any world language, that windows can support. Tested with Korean, Japanese, Arabian, Vietnamese, Chinese, Portuguese, Spanish, Russian, and more! (check the screenshot)
- Very fast and secure listings (for windows, file manager, network manager, etc). Navigate through the remote computer like if you were opening on your local computer! Use the "go to" commands to reach the folder you want, perfectly fast. The same applies to the registry!
- Improved key logger, get a smooth result from the key logger, and easy to read text.
- Network manager allows you to browse the other computers in the same LAN (that are already authenticated), upload, download and delete files from those other computers in LAN, no need for installing a server on another pc (just to browse the lan shares)
- Hybrid support for both direct and reverse connection modes. you can receive connections on your client at the same time you connect to direct connection servers
- Huge list of possibilities for process injection, decide where to inject your server, where to install, startup methods, and have full control over your server creation. inject to default browser, custom windows, start any type of program, inject to winsock enabled applications, inject to all applications, etc
- Multiple transfers at once (multi-threaded) or queue transfers system.
- Very powerful plug-in system, where you may add anything your mind could think of. Add net limiters, socks, encryption, root kits, compression, password stealers, cd key stealers, offline key loggers, anything!
- Support for very big files, up to 5 pb (peta byte).
- Intrinsic help system, clicking the "?" will help you understand certain functions from the program.
- Multi-language support for the client, see the program on your primary language (should be available soon).
- File manager with quick edit feature: edit plain text files without having to download them and upload again. There's a new "create new file" feature, makes you able to create new files quickly, without having to upload a new file!
- All transfers have "resume" feature, even network transfers. resume folder downloads, uploads, downloads and network uploads and downloads.
- Very fast ip scanner, use the remote machine to execute ip range scans for you
- Two other new revamped features: connection bouncer and remote service reacher. those improved functions will help you to reach the remote computer services that doesn't allow direct connections from wan

4.5.2 NetBus

NetBus or Netbus is a software program for remotely controlling a Microsoft Windows computer system over a network. It was created in 1998 and has been very controversial for its potential of being used as a backdoor.



Host name/IP: 192.168.1.191

Port: 12345

□ in interval: 60

Function delay: 0

0 0

No connection

Fig. 13

There are two components to the client-server architecture. The server must be installed and run on the computer that should be remotely controlled. The filename is "patch.exe" which we need to deploy to the target computer. Where "Netbus.exe" is the file which we need to run on the hackers computer. Onces, the server would install on the host computer, which modify the Windows registry so that it starts automatically on each system startup. The server is a faceless process, listening for connections on port 12345 (in some versions, the port number can be adjusted). The client was a separate program presenting a graphical user interface that allowed the user to perform a number of activities on the remote computer.

Examples of its capabilities

- Keystroke logging
- Keystroke injection
- Screen captures
- Program launching
- File browsing
- Shutting down the system
- Opening/closing CD-tray
- Tunneling protocol (NetBus connections through a number of systems.)

Check Your Progress 3

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

Explain Trojan Horse?

....

....

....

....

....

4.6 MAN-IN-THE-MIDDLE ATTACKS

A Man-In-The-Middle (MITM) attack occurs when an attacker is able to fool a user into establishing a communication link with a server or service through a rogue entity. The rogue entity is the system controlled by the hacker. It has been set up to intercept the communication between user and server without letting the user become aware that the misdirection attack has taken place. A MITM attack works by somehow fooling the user, their computer, or some part of the user's network into re-directing legitimate traffic to the illegitimate rogue system.

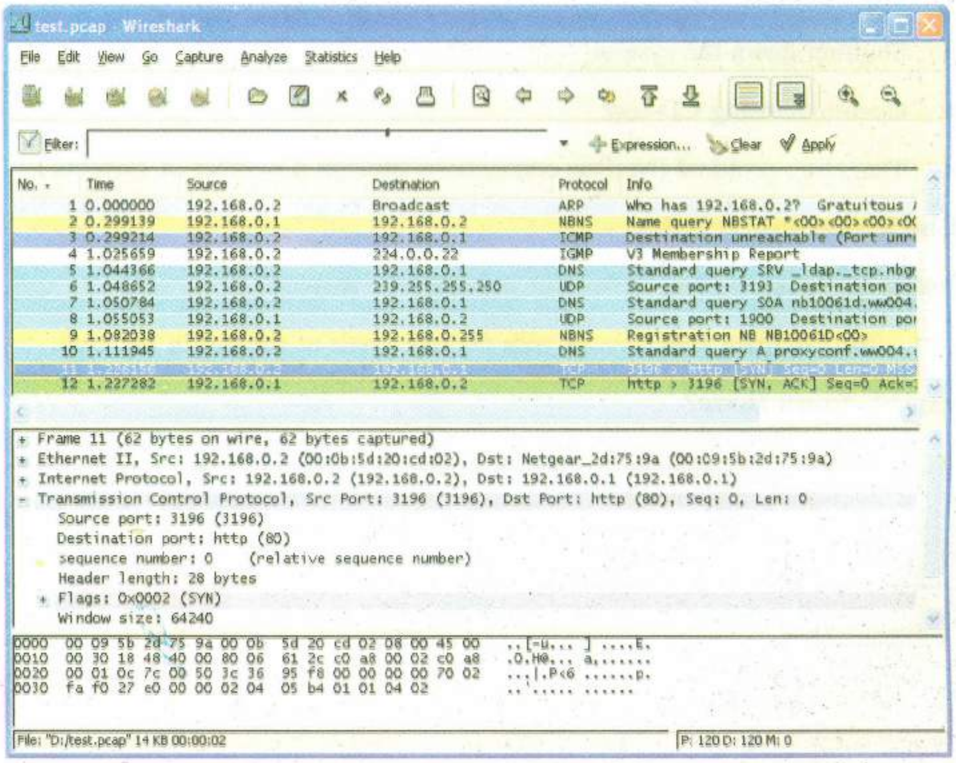
A MITM attack can be as simple as a phishing e-mail attack where a legitimate looking e-mail is sent to a user with a URL link pointed towards the rogue system instead of the real site. The rogue system has a look a-like interface that tricks the user into providing their logon credentials. The logon credentials are then duplicated and sent on to the real server. This action opens a link with the real server, allowing the user to interact with their resources without the knowledge that their communications have taken a detour through a malicious system that is eavesdropping on and possibly altering the traffic.

MITM attacks can also be waged using more complicated methods, including MAC (Media Access Control) duplication, ARP (Address Resolution Protocol) poisoning, router table poisoning, fake routing tables, DNS (Domain Name Server) query poisoning, DNS hijacking, rogue DNS servers, HOSTS file alteration, local DNS cache poisoning, and proxy re-routing. And that doesn't mention URL obfuscation, encoding, or manipulation that is often used to hide the link misdirection.

To protect yourself against MITM attacks, you need to avoid clicking on links found in e-mails. Furthermore, always verify that links from Web sites stay within trusted domains or still maintain SSL encryption. Also, deploy IDS (Intrusion Detection System) systems to monitor network traffic as well as DNS and local system alterations.

4.6.1 Wireshark

Wireshark is a network packet analyzer.



```
No. -  Time        Source         Destination       Protocol  Info
     1 0.000000    192.168.0.2    Broadcast         ARP       Who has 192.168.0.2?  Gratuitous /
     2 0.299139    192.168.0.1    192.168.0.2       NBNS      Name query NBSTAT *<00><00><00><0(
     3 0.299214    192.168.0.2    192.168.0.1       ICMP      Destination unreachable (Port unr
     4 1.025659    192.168.0.2    224.0.0.22        IGMP      V3 Membership Report
     5 1.044366    192.168.0.2    192.168.0.1       DNS       Standard query SRV _ldap._tcp.nbgr
     6 1.048652    192.168.0.2    239.255.255.250   UDP       Source port: 3193  Destination poi
     7 1.050784    192.168.0.2    192.168.0.1       DNS       Standard query SOA nb10061d.ww004.
     8 1.055053    192.168.0.1    192.168.0.2       UDP       Source port: 1900  Destination poi
     9 1.082038    192.168.0.2    192.168.0.255     NBNS      Registration NB NB10061D<00>
    10 1.111945    192.168.0.2    192.168.0.1       DNS       Standard query A proxyconf.ww004.:
    11 1.226156    192.168.0.2    192.168.0.1       TCP       3196 > http [SYN] Seq=0 Len=0 MSS
    12 1.227282    192.168.0.1    192.168.0.2       TCP       http > 3196 [SYN, ACK] Seq=0 Ack=:
```

```
+ Frame 11 (62 bytes on wire, 62 bytes captured)
+ Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)
+ Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
- Transmission Control Protocol, Src Port: 3196 (3196), Dst Port: http (80), Seq: 0, Len: 0
    Source port: 3196 (3196)
    Destination port: http (80)
    sequence number: 0    (relative sequence number)
    Header length: 28 bytes
  + Flags: 0x0002 (SYN)
    Window size: 64240
```

```
0000  00 09 5b 2d 75 9a 00 0b  5d 20 cd 02 08 00 45 00   ..[-u... ] ....E.
0010  00 30 18 48 40 00 80 06  61 2c c0 a8 00 02 c0 a8   .0.H@... a,......
0020  00 01 0c 7c 00 50 3c 36  95 f8 00 00 00 00 70 02   ...|.P<6 ......p.
0030  fa f0 27 e0 00 00 02 04  05 b4 01 01 04 02         ..'..... ......
```

Fig. 14

A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible. You could think of a network packet analyzer as a measuring device used to examine what's going on inside a network cable, just like a voltmeter is used by an electrician to examine what's going on inside an electric cable (but at a higher level, of course). In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, all that has changed. Wireshark is perhaps one of the best open source packet analyzers available today.

Features

Wireshark is software that "understands" the structure of different networking protocols. Thus, it is able to display the encapsulation and the fields along with their meanings of different packets specified by different networking protocols. Wireshark uses pcap to capture packets, so it can only capture the packets on the types of networks that pcap supports.

- Data can be captured "from the wire" from a live network connection or read from a file that recorded already-captured packets.
- Live data can be read from a number of types of network, including Ethernet, IEEE 802.11, PPP, and loopback.
- Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, tshark.
- Captured files can be programmatically edited or converted via command-line switches to the "editcap" program.
- Data display can be refined using a display filter.
- Plug-ins can be created for dissecting new protocols.
- VoIP calls in the captured traffic can be detected. If encoded in a compatible encoding, the media flow can even be played.
- Raw USB traffic can be captured with Wireshark.This feature is currently available only under Linux.

Wireshark's native network trace file format is the libpcap format supported by libpcap and WinPcap, so it can read capture files from applications such as tcpdump and CA NetMaster that use that format, and its captures can be read by applications that use libpcap or WinPcap to read capture files. It can also read captures from other network analyzers, such as snoop, Network General's Sniffer, and Microsoft Network Monitor.

Check Your Progress 4

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of this Unit.

How MITM attack helps the attacker to fool a user by establishing a communication link with a server?

....

....

....

....

....

....

....

....

....

....

4.7 LET US SUM UP

This unit deals with "Cracking Methodology". Planning a methodology that supports your ethical hacking goals is what separates the professionals from the amateurs. The goal is to get users to choose better passwords. Passwords are used for everything ranging from logging into terminals to checking email accounts. Password crackers are programs that aid in the discovery of protected passwords, usually through some method of automated guessing. It's possible for you to forget Operating Systems password, especially after you have just created a new one, or you haven't used the computer for a long time, or maybe someone has changed your password. When that happens, you need to recover your password. Ophcrack, LophtCrack 6, LophtCrack 6 are the tools for recovering the operating system passwords.

Further the section emphasis on Advanced Office Password Recovery recovers, replaces, removes or circumvents instantly passwords protecting or locking documents created with Microsoft Office applications. And highlighting the concept of Trojan Horse. Lastly it throws light on the Man In The Middle Attack. A MITM attack occurs when an attacker is able to fool a user into establishing a communication link with a server or service through a rogue entity.

4.8 CHECK YOUR PROGRESS: THE KEY

1) **Ophcrack** is an open source program that recovers passwords in a free way. It is based on a time-memory trade-off using rainbow tables done by the inventors of the method. Just log in to a computer and download the tool from the website and follow it's instructions to recover windows vista password.

   Ophcrack will locate the users on your Windows system and begin cracking their passwords. The process is automatic – you don't usually need to type or click anything. When the passwords are displayed on screen, write them down. On most computers, ophcrack can crack most passwords within a few minutes which mean it doesn't guarantee your password can be 100% recovered. It's just 99%, anyhow, just have a try.

   The tool that will not cause any harm to EFS-encrypted files on your hard disk is the Windows Password recovery system. Here are 5 of these tools:

   i) **Stellar Phoenix Password Recovery** – Simple startup utility resets a forgotten admin or users' password using a familiar Windows-like program interface instead of command-line.

   ii) **Password Kit** – Top rated version of Passware–s Password recovery app, supports Windows Vista and RAID/SCSI/SATA drives.

   iii) **Petter Nordahl** – Hagen's Offline NT Password & Registry Editor – A great boot CD/Floppy that can reset the local administrator's password.

iv) **Openwall's John the Ripper** – Good boot floppy with cracking capabilities.

v) **EBCD – Emergency Boot CD** – Bootable CD intended for system recovery in the case of software or hardware faults.

2) **Advanced Office Password Recovery** unlocks documents created with all versions of Microsoft Office from the ancient 2.0 to the modern 2010. Recover passwords for Microsoft Word, Excel, Access, Outlook, Project, Money, PowerPoint, Visio, Publisher and OneNote. Reset MS Internet Explorer Content Advisor passwords and open any password-protected VBA project by exploiting a backdoor.

Features and Benefits

- Supports all versions of Microsoft Office applications from 2.0 to 2010
- Instant password recovery for multiple products
- Instantly unlocks documents with previously recovered passwords
- Exploits all known backdoors and tricks in the Office family for instant recovery
- Completely automatic preliminary attack may recover documents in less than 10 minutes
- Dictionary and brute-force attacks with user-defined masks and advanced templates
- Hardware acceleration (patent pending) reduces password recovery time by a factor of 50
- Patent-pending GPU acceleration technology with NVIDIA or ATI video cards
- Allows up to 32 CPUs or CPU cores and up to 8 GPUs
- Highly optimized low-level code for optimum performance.

The attacks available in Advanced Office Password Recovery are:-

i) **Brute-Force Attack**: This Attack will try all possible characters combinations in the specified Range. The Range is defined by Password Length and Brute-Force Range Options.

ii) **Brute-Force with Mask:** This Attack is useful when you remember a part of Password. For example if you remember that length of your password was 5 characters and password begins from "A", you can define the mask "A????" and save the time by trying 4 symbols instead of 5. A Password Mask must be defined to use this Attack.

iii) **Dictionary Attack:** This Attack verifies the words stored in the specified Dictionary File. The dictionary is just a Unicode text file with one word at a line; lines are separated with line breaks. You can set additional Dictionary Options for this Attack. A Dictionary Attack is much faster than Brute-Force so we recommend to run it first. AOPR has supplied with one small Dictionary File containing English words. Additional Dictionaries can be obtained on a CD with any Elcomsoft program.

3) **Trojan horse** is a malicious payload surreptitiously delivered inside a benign host. You are sure to have heard of some of the famous Trojan horse malicious payloads such as Back Orifice, NetBus, and SubSeven. But the real threat of Trojan horses is not the malicious payloads you know about, its ones you don't. A Trojan horse can be built or crafted by anyone with basic computer

skills. Any malicious payload can be combined with any benign software to create a Trojan horse. There are countless ways of crafting and authoring tools designed to do just that. Thus, the real threat of Trojan horse attack is the unknown.

The malicious payload of a Trojan horse can be anything. This includes programs that destroy hard drives, corrupt files, record keystrokes, monitor network traffic, track Web usage, duplicate e-mails, allow remote control and remote access, transmit data files to others, launch attacks against other targets, plant proxy servers, host file sharing services, and more. Payloads can be grabbed off the Internet or can be just written code authored by the hacker. Then, this payload can be embedded into any benign software to create the Trojan horse. Common hosts include games, screensavers, greeting card systems, admin utilities, archive formats, and even documents.

All a Trojan horse attack needs to be successful is a single user to execute the host program. Once that is accomplished, the malicious payload is automatically launched as well, usually without any symptoms of unwanted activity. A Trojan horse could be delivered via e-mail as an attachment, it could be presented on a Web site as a download, or it could be placed on a removable media (memory card, CD/DVD, USB stick, floppy, etc.). In any case, your protections are automated malicious code detection tools, such as modern anti-virus protections and other specific forms of Malware scanners, and user education.

4) **A MITM attack** occurs when an attacker is able to fool a user into establishing a communication link with a server or service through a rogue entity. The rogue entity is the system controlled by the hacker. It has been set up to intercept the communication between user and server without letting the user become aware that the misdirection attack has taken place. A MITM attack works by somehow fooling the user, their computer, or some part of the user's network into re-directing legitimate traffic to the illegitimate rogue system.

A MITM attack can be as simple as a phishing e-mail attack where a legitimate looking e-mail is sent to a user with a URL link pointed towards the rogue system instead of the real site. The rogue system has a look a-like interface that tricks the user into providing their logon credentials. The logon credentials are then duplicated and sent on to the real server. This action opens a link with the real server, allowing the user to interact with their resources without the knowledge that their communications have taken a detour through a malicious system that is eavesdropping on and possibly altering the traffic.

MITM attacks can also be waged using more complicated methods, including MAC (Media Access Control) duplication, ARP (Address Resolution Protocol) poisoning, router table poisoning, fake routing tables, DNS (Domain Name Server) query poisoning, DNS hijacking, rogue DNS servers, HOSTS file alteration, local DNS cache poisoning, and proxy re-routing. And that doesn't mention URL obfuscation, encoding, or manipulation that is often used to hide the link misdirection.

Student Satisfaction Survey

Student Satisfaction Survey of IGNOU Students

Enrollment No.	
Mobile No.	
Name	
Programme of Study	
Year of Enrolment	
Age Group	□ Below 30 □ 31-40 □ 41-50 □ 51 and above
Gender	□ Male □ Female
Regional Centre	
States	
Study Center Code	

Please indicate how much you are satisfied or dissatisfied with the following statements

Sl. No.	Questions	Very Satisfied	Satisfied	Average	Dissatisfied	Very Dissatisfied
1.	Concepts are clearly explained in the printed learning material	□	□	□	□	□
2.	The learning materials were received in time	□	□	□	□	□
3.	Supplementary study materials (like video/audio) available	□	□	□	□	□
4.	Academic counselors explain the concepts clearly	□	□	□	□	□
5.	The counseling sessions were interactive	□	□	□	□	□
6.	Changes in the counseling schedule were communicated to you on time	□	□	□	□	□
7.	Examination procedures were clearly given to you	□	□	□	□	□
8.	Personnel in the study centers are helpful	□	□	□	□	□
9.	Academic counseling sessions are well organized	□	□	□	□	□
10.	Studying the programme/course provide the knowledge of the subject	□	□	□	□	□
11.	Assignments are returned in time	□	□	□	□	□
12.	Feedbacks on the assignments helped in clarifying the concepts	□	□	□	□	□
13.	Project proposals are clearly marked and discussed	□	□	□	□	□
14.	Results and grade card of the examination were provided on time	□	□	□	□	□
15.	Overall, I am satisfied with the programme	□	□	□	□	□
16.	Guidance from the programme coordinator and teachers from the school	□	□	□	□	□

After filling this questionnaire send it to:
Programme Coordinator, School of Vocational Education and Training,
Room no. 19, Block no. 1, IGNOU, Maidangarhi, New Delhi- 110068

SoVET-IGNOU/P.O. 1T/July, 2011

ISBN-978-81-266-5443-7