Unit-4

Network Forensic

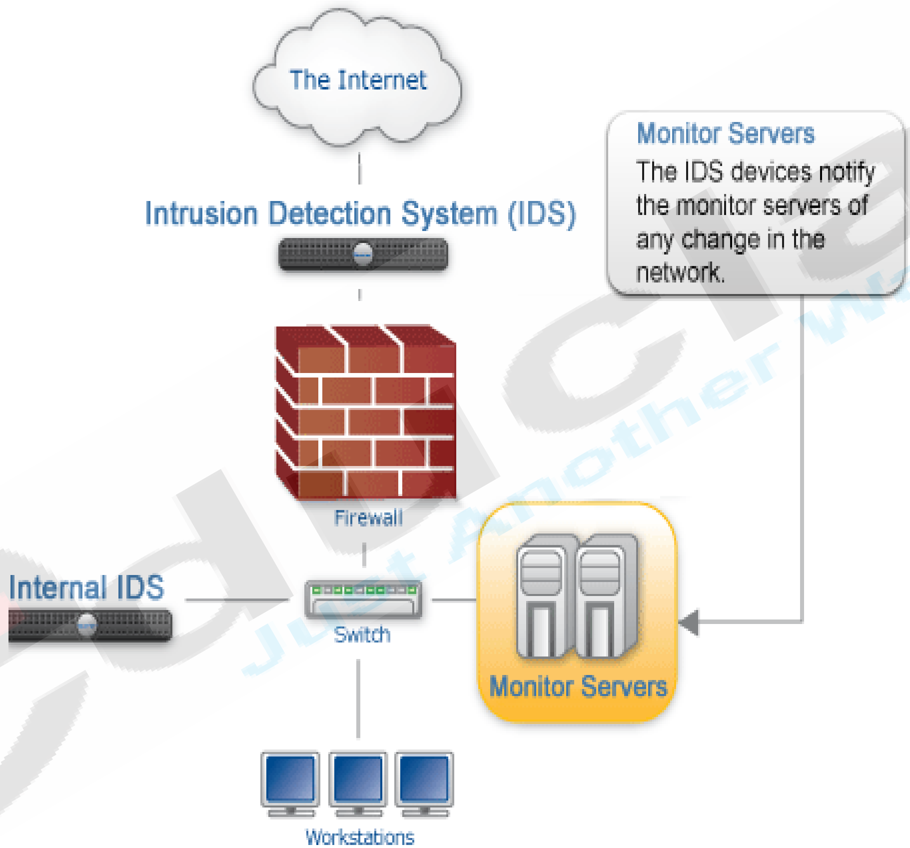
Contents

- Different attacks in network(10.1 -10.4)
- collecting and analyzing network based evidence in windows and Unix environment(ch-6.9.2,9.3)
- Email forensics for standard protocols(ch-12)

Introduction to Intrusion Detection System

- Intrusion detection system (IDs) helps information systems prepare for and deal with attacks.
- They accomplish this by collecting information from a variety of systems and network sources and then analyzing the information for possible security problems.

Intrusion detection system



In the diagram below, there are two IDS systems; one inside the network and the other outside. The IDS devices keep in constant contact of the Monitor Servers and inform them of any change in the network infrastructure.

Offering of Intrusion Detection System(IDS)

- The IDS can offer the following:
  - Add a superior degree of integrity to remainder of your infrastructure
  - Recognize and report modifications to knowledge
  - Trace user action from purpose of entry to purpose of impact
  - Automate a task of observation-the net finding out most recent attacks
  - Notice mistakes in your system configuration
  - Sense once your system is under fire
  - Make protection management of your system potential by non-expert employees
  - Guide system supervisor within important steps of building a policy for your computing assets.

Types of Intrusion Detection System

1. Active IDS
2 . Passive IDS
3. Network-Based IDS
4. Host-Based IDS
5. Knowledge-Based IDS
6. Behavior-Based IDS

Active IDS

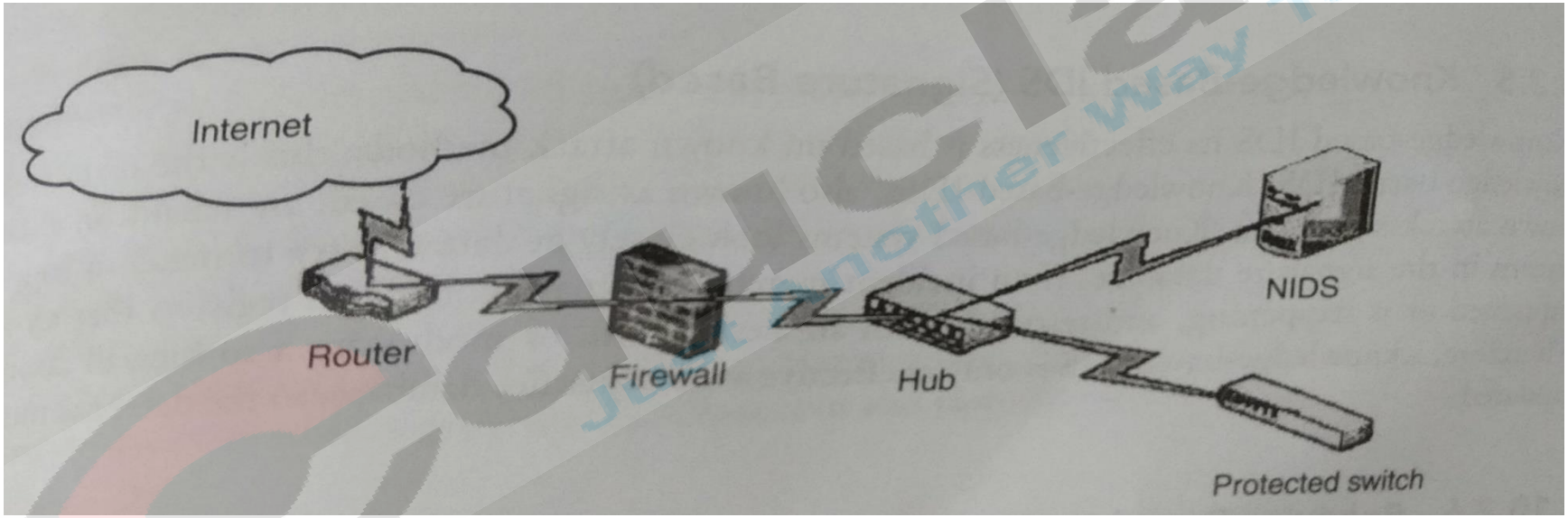
- It is also called Intrusion Detection and Prevention System(IDPS)
- System that are configured to automatically to block mistrusted attacks in progress without any interface required by an operator are called active IDS.
- IDPS has the advantage of providing real-time corrective action in reaction to an attack , but has many disadvantages also.
- To enable IDPS, itself susceptible to attack, it must be placed in-line along a network boundry.

Passive IDS

- The system that is configured only to observe and analyze network traffic activity and alert an operator to potential vulnerabilities and attack is passive IDS.
- It cannot perform any protective or corrective functions of its own.
- It only detect and alert the user about it.
- When suspicious or malicious traffic is detected, it notifies the user or administrator.
- It depends on the user or administrator to allow or block the activity
- This notification sent by e-mail, pager, cell phones and messages.
- Necessary to send notification in secure way so that attacker does not intercept or read or alter them.

Network Based IDS

- The network based IDS can be devoted hardware application, or an application running on a computer which is attached to the network.
- It observes all the traffic in a network or coming through an entry point.
- NIC of the network based IDS operates only in unrestrained mode which means that it will pick all the traffic coming from the media even when the destination or final address is not present in the IDS.
- It works on sniffer.



- Host are generally not conscious of the IDS and no extra burden is placed on the network.
- A network based IDS can observe traffic only in its native segments.
- In switched and routed network a sensor in mandatory in each segments in which network traffic is to be observed.
- When a sensor sense a probable intrusion , it will report it to a central management console which will take care of the suitable passive or active response.
- Communication between the remote sensor and the management console should be protected to avoid interference or modification by the intruder.

Host based IDS

- A host based IDS is generally a software application fixed on the system and observes activity only on local system, which has software application installed on it.
- It communicates directly with OS and has no information of the low level network traffic
- Host based IDS depends on information from audit and system log files intrusion
- They can observe system files and system resources and arriving application data.

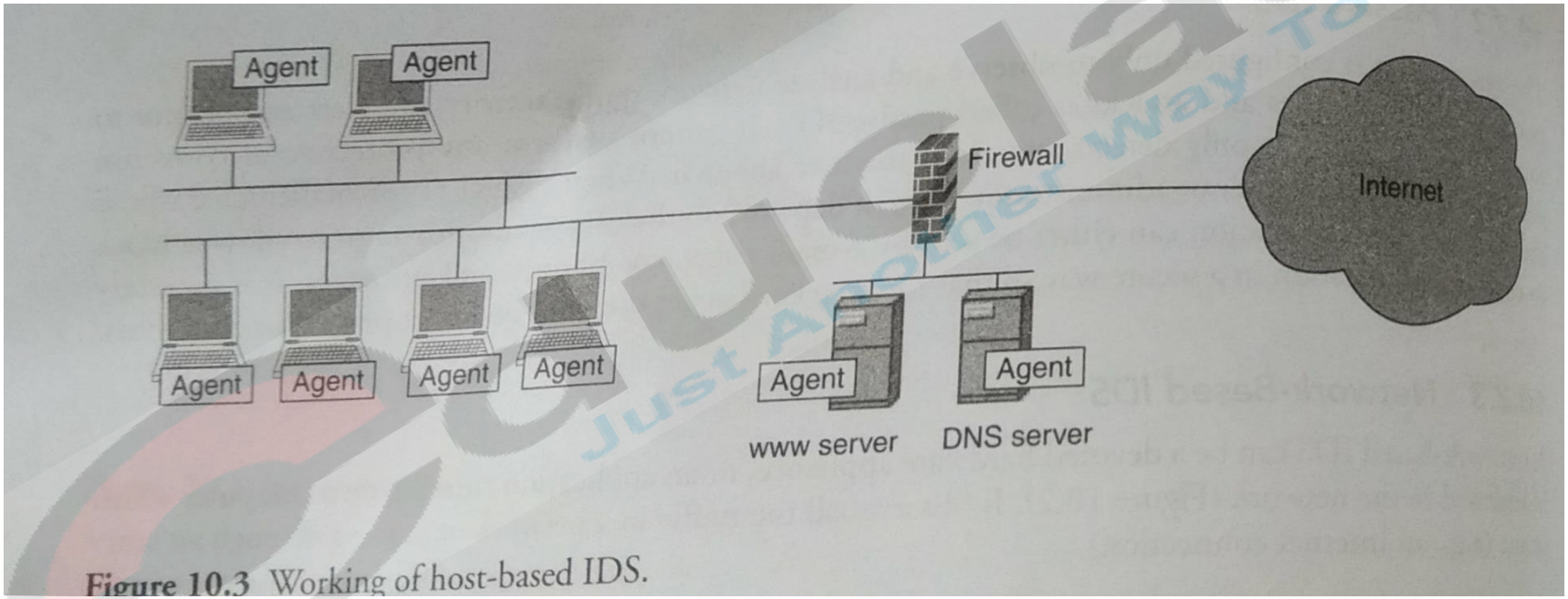


Figure 10.3 Working of host-based IDS.

- An extra administrative load is placed only on critical servers because host based IDS can yield lot of data.
- To reduce the load the IDS can report to a central console.
- Drawbacks of Host Intrusion Detection Systems (HIDS):
  - Difficult to analyse the intrusion attempts on multiple computers.
  - Host Intrusion Detection Systems (HIDS) can be very difficult to maintain in large networks with different operating systems and configurations
  - Host Intrusion Detection Systems (HIDS) can be disabled by attackers after the system is compromised.

Knowledge Based IDS (Signature Based)

- In knowledge based IDS its effectiveness is based on known attack methods; this is the main weakness of knowledge based IDS.
- It is also known as signature based, are reliant on a db of known attack signatures.
- Knowledge based system look closely at data and try to match it to a signature pattern in the signature db.
- If an incident matches a signatures , the IDS register that an attack has happened or is happening and responds with an alert , alarm or modification to firewall configuration .
- Knowledge IDS are effective for signature DB, so the DB kept updated.
- The disadvantages of Signature-based Intrusion Detection Systems (IDS) are signature database must be continually updated and maintained and Signature-based Intrusion Detection Systems (IDS) may fail to identify a unique attacks.

Behavior based IDS

- A behavior based IDS mentions a baseline or learned pattern of normal system activity to recognize active intrusion attempts.
- Behavior based intrusion detection is also know as anomaly based or statistical based intrusion detection.
- This IDs observes traffic and system activity for uncommon behavior.(or statistics)
- To distinguish between malicious activity to normal activity it need to understand normal first.
- When first time it is getting activated it will record network bandwidth, processor, disk usage, memory activities etc.
- Activity not matching with statistics/ irregular system performance the baseline will effect in an alert.
- The main advantage is dynamically adjust to new exposures.
- System behavior varies for normal causes, it generally produces a high number of false alarms.
- Deviation from this baseline or pattern cause can alarm to be activated.
- High False alarms are frequently associated with behavior-based IDS.

Advantages of IDS

- **Visibility.** An IDS provides a clear view of what's going on within your network. It is a valuable source of information about suspicious or malicious network traffic. There are few practical alternatives to an IDS that allow you to track network traffic in depth.
- **Defense.** An IDS adds a layer of defense to your security profile, providing a useful backstop to some of your other security measures.
- **Response capabilities.** Although they probably will be of limited use, you may want to enable some of the response features of the IDS. For instance, they can be configured to terminate a user session that violates policy. Obviously, you must consider the risks of taking this step, since you may accidentally terminate a valid user session. However, in certain cases it can be an important tool to prevent damage to the network.
- **Tracking of virus propagation.** When a virus first hits your network, an IDS can tell you which machines it compromised, as well as how it is propagating through the network to infect other machines. This can be a great help in slowing or stopping a virus's progress and making sure you remove it.
- **Evidence.** A properly configured IDS can produce data that can form the basis for a civil or criminal case against someone who misuses your network.

Disadvantages of IDS

- **More maintenance.** Unfortunately, an IDS does not replace a firewall, virus scan, or any other security measure. So when you install it, it will require additional maintenance effort and will not remove much, if any, of the existing burden.
- **False positives.** IDSs are famous for setting off false positives-sounding the alarm when nothing is wrong. Although you can tweak the settings to reduce the number of false positives, you'll never completely eliminate the need to respond to false positives.
- **False negatives.** IDSs can also miss intrusions. Technologies are improving, but IDSs don't al ways catch everything.
- **Staff requirements.** Properly managing an IDS requires experienced staff. The less experienced your staff are, the more time they will spend responding to false positives. Therefore you will be creating not only more work for the IT department to handle, but more difficult work in some cases.

Understanding Network Intrusions and Attacks

Intrusion Versus Attacks

- It is important for investigators to realize the difference between an intrusion and an attack, because whether or not there was a real unauthorized entry to the network or system, it can be a significant aspect in evidencing the element of a criminal offense.
- In DOS attacks, various other attacks can be committed without attaining entry to the network or system.

- The attacker never gains access to any computer on the network as these attacks overload network resource to make the network inaccessible to genuine users.
- When no intrusion occurs, DOS attackers should not be referred to as intruders.
- Similarly, not all intruders can precisely be categorized as attackers while those who gain access and then abolish information or plant viruses are correctly named by both names.

Recognizing Direct Versus Distributed Attacks

- A direct attack is launched from a computer used by the attacker.
- Distributed attacks is more complex.
- The distributed attacks use some other individual's system for the same.
- This Type of attack includes multiple victims which include not only the target of the attacks, but also intermediary remote system from which the attacks is launched that are controlled by the attacker.

- The agent or zombies are referred by the intermediaries.
- Because the attack packets that reach the victims have multiple source address and none of these is the address of the attacks originator this type of attack make it more difficult to track down the perpetrator.
- Attackers can launch their attack simultaneously from dozen , hundreds of internet host all over the worlds using distributed method.

Step	Component	Action
1	Daemon(agent)	Announces itself to the “masters” that have been predefined
2	Master	Lists daemon as “ready and willing” to be used for attack
3	Attacker	Issues command to masters to launch attack
4	Master	Issues command to daemons on agents to launch
5	Daemon	Launches attack on specified victim

Distributed attack Process

Automated Attacks

- Attacks implements by a computer program rather than the attacker physically carrying out the phase in the attack sequence are called automated attack.
- To launch network attacks, hackers have dispersed attack tools that make it easier to accomplish it.
- Most of these tools would initiate only one attack sequence, launching complementary attack sequences which demand the interference of the human attackers.

- Tools can service different techniques, like random selection to interject pattern that would active detection by the IDS in demand to evade recognition by IDS software that depends on pattern recognition.

Accidental Attacks

- Sometimes intrusion and attacks may really be unintentional .
- Trojan horse and worms are written to spread themselves by getting into the victims address book and sending infected email to all the address found there.
- The user who appears to have sent the virus via email is frequently a victim of the attack himself / herself.
- It is very important for investigators to be aware of the culpable mental state that is specified as an element of each offense to be charged.

Preventing Intentional Internal Security Breaches

- Security breaches is an event that affects unauthorized access of data, application , services, networks and or devices by avoiding their core security mechanism
- Best position to gain access to information or block the network integrity is users inside the networks

Internal attackers are more hazardous for several reasons

- People inside the network generally know more about the company the network and the layout of the building , normal working process and other information that makes it easier for them to gain access without recognition.
- Internal attackers generally have at least some degree of legal access and could find it easy to determine password and fleapits in the current security system.
- Internal hackers know what activities will incur the most damage what information is on the network

In a high security environment actions should be taken to avert this kind of thefts

- Install computer lacking floppy drives or even totally diskless workstations.
- Apply system or group strategy that avoids users from installing software.
- Lock PC cases and cover physical access to serial ports, USB ports and the other connection points so that removable media devices cannot be connected.

Preventing Unauthorized External Intrusion

- External intrusion is that the are that must be controlled are much more focused than internal attacks.
- These are points of entry to the network from the outside.
- Unauthorized intrusion can also be defines as attacks in which the attack get access into the system by means of different hacking or cracking techniques.

Planning for Firewall Failures

The planning must take into consideration the possibility that the firewall will fail.

- If intruders do get in what is the contingency plan?
- How can they reduce the amount of damage attackers can do?
- How can the most sensitive or valuable data be protected?

When considering firewall failure organization should ask the following questions:-

- When was the last time the firewall rule set was fully verified?
- When was the firewall rule set updated ?
- When was the last time the firewall was fully tested?
- When was the last time the firewall rule set was optimized?

External Intruders with Internet access

- External intruders are basically outsiders who physically break into your facility to gain access to your network, although a true insider he or she is not authorized to be there and does not have a valid account on the network.
- The security threat assessment must be based in part on the technical aspect of the type of attack that is initiated and also on understanding the motivation of the people initiating the attacks.

Recognizing the “Face Of the Attack”

To recognize IDS use two methods:-

- **Pattern Recognition**: Investigation file, network traffic , Series in RAM or other data for recurrent or identifiable marks of attacks, like mysterious increase in file size or particular character strings.
- **Effect Recognition**:- Recognizing the result of an attack like a system crash triggered by overload or an unexpected reboot for no reason. Exploits are called “fragattacks” the when number of TCP/IP exploits use patchy packages. It is more problematic to recognize effect because the effect often look like normal network traffic or problem triggered by hardware or software faults.

Identifying and Categorizing Attack Types

- Pre intrusion/attack activities
- Password –cracking methods
- Technical exploits
- Malicious code attacks

Data Collection Introduction(ch-6)

- Digital evidence *is* "Information of value to a criminal case chat is stored or transmitted in digital form."
- The term "computer forensic" involves identification, sunder out, preparation of documents, and storing information that is *kept* or *sent* over in electronic or magnetic form basically considered as digital evidence.
- For example, in fingerprints, digital evidence is visible as the files are stored on disk that can be easily accessible by standard file management tools (like Windows Explorer), or can be hidden using special method or a software.
- The main purpose of computer forensic is to find these hidden evidences in order to increase facts value.

- Different standards have been created which are *used* co find out and preserve digital evidences. There are a number of the procedures accepted by law. Those are as follows:
  1. If evidence is not collected and handled according to the proper standards, the judge may deem the evidence inadmissible when it is presented and the jury members will never get a chance to evaluate it or consider it in making their decision.
  2. If the proof is admitted, the opposing lawyer can attack its quality by questioning the witnesses .

The Facts in a Criminal Case

- Legal process of searching, examining, preserving, and exhibiting facts or evidence is generally governed by the law of authority of the court. This process will introduce an evidence.
- As an investigator, a person should first become familiar with the applicable laws. These rules are collected in a document called “rules of evidence.“

Definition of Evidence

Evidence can generally be defined as the means by which an alleged (assumed) fact, the truth of which is subjected to scrutiny(analysis), is established or disproved. The legal significance of any given piece of evidence lies in its influence on the judge or jury at trial.

Evidence *Admissibility*

- There are certain requirements for evidence to be admissible or acceptable by court:
  1. Evidence should be competent.
  2. Evidence should be relevant.
  3. Evidence should be material.
  4. Evidence should be obtained legally.

Standards of Forensic *Examination*

- Surpassing the minimum requirements of admissibility is always safest: If extra precautions are taken by investigators, it will not only decrease the possibility of evidence being rejected by a Judge, but will also help in getting an impression by jury.
- Some organizations provide standard forensic governing examination methods or procedures for their members.

Standards regarding some digital evidence handling are:

1. The originality of the evidence should be preserved.
2. There should be an exact copy of the original, if possible, in order to maintain integrity of the evidence.
3. The copies should be preserved on a disk with no other documents available on the disk. That is, disk should be cleaned before placing copies in it.

Collection of *Digital* Evidences

- The first person to become aware of a cybercrime is always a network administrator. If the company has an IT incident response team, then this team will stop the crime progress immediately and freeze it before any law enforcement authorities take over.
- There are several people involved in the process of collecting digital evidences-the first respondent (usually an officer or a security person, who reaches the crime scene first), the investigators, and the crime scene specialists and technicians; there is also someone 'in-charge' of the crime scene able to take proper decisions. This is usually the senior investigator.
- It is also important that the members of organization should corporate in the process of investigation.
- Integrity in investigation team members is also an essential part in order to collect evidences successfully.

People involved in Data Collection Techniques

- Only specialist in computer forensic should touch the system, care has to be taken to protect computers from alteration and damage.
- There are several people involved in evidence collection techniques-first respondent (usually an officer or a security person),investigators (usually senior investigator), and the crime scene technicians (usually a person who is an expert in computer forensic). These people have been assigned with specific roles.

Role of *First Respondent*

- The first respondent is the one who appears in crime locations, usually an officer or a security person. *As* shutting down or rebooting the system may destroy some important information or even evidence, first respondent should not power off or restart the system. Nor should he access the system to seek the evidence.He should follow the process explained below:

1. **Identifying the crime location:** The person (usually an officer), who arrives first at the crime scene, should be able to identify depth of the crime and restrict access to the crime location. This location can be as wide as a room, or can consist of several rooms, or even multiple buildings. Constructing a list of computer systems that might have been involved in the crime scene is one of the tasks a first respondent should be able to do.
2. **Protecting the crime scene:** All the devices, including nonfunctional computers, mobile phones, notebooks, PDAs, or other portable devices, are considered a part of the crime scene. First respondent should freeze the condition of all the devices and wait for the IT incident response team or investigator in-charge to decide if any equipment can be excluded.
3. **Preserving temporary and tampered evidences:** An evidence that could disappear or destroyed before the arrival of investigation team should be preserved and maintained by the first respondent. If there is surveillance (CCTV) available, then it is easier to have a record of the crime. But if there is no surveillance, then identifying crime scene is a challenge for investigators.

Role of *Investigators*

- IT incident response team has authority of collecting evidences before any law enforcement team arrives. To handle all the activities at the location of crime is generally the responsibility of an investigator. He/she will be responsible for:

1. **A chain of order:** An investigator should make sure that everyone at the crime scene is aware of the chain of order. Chain of order refers to the Row investigation process. All the systems and other equipment at the crime scene should not be touched, replaced, accessed, or unplugged without the permission of a senior investigator. The role of investigator is to control and manage investigation.

   In case a senior investigator has to leave the location of crime, he/she should assign a person with similar designation to stay in contact with that person until all facts and evidences has been collected and shifted to secure storage area.

2. **Conducting the crime scene search:** Officer should seek all the systems, written documents and notes, manuals and log files related to the crime. It involves mobile phones, printers, scanners, external devices such as flash drivers, harddisks, CD/DVD, tapes .

3. **Preserving integrity of the facts or evidences:** Criminals always remove all the evidences. To Preserve all the evidences in order to take actions against the offender. Investigation should make exact copy of all the evidences, if possible should be able to analyze footprints of attacker/criminal.

Role of Crime Scene Technicians

- They are specialists or experts in computer forensic. They must have a background in the field of computer and its technology with all computer related terms like working with file systems,structure of disks and location of files where data is stored.
- Usually, crime scene experts arc responsible for:
- **Preserving temporal evidences *to* replicating disks:** Temporal data is sometimes known as volatile data located in the computer's memory such as random access memory. The disk containing evidences should be replicated or copied before shutting down the system, as there might be the possibility of disappearance of evidence after shutting down or rebooting the system.
- **Shutting down the computer system for transport:** To preserve the integrity of original evidence, shutting down the systems properly is important. All the running programs or applications should be properly closed in order to avoid corruption of files.

- **Marking and recording the evidence:** All the evidences should be noted or marked with time and dace of evidence collected, initials of the investigator, case identification number, and other related information. All these tagged or noted evidences should be recorded in evidence log files.
- **Packaging of the evidence:** All the digital evidences such as hand held, computer, laptops, PDAs, hard disks should be properly packed in antistatic bags for transport. Written documents, such as notes, manuals, and books, should be placed in plastic bags in order to protect them from damage.
- **Transporting evidence:** All the data should be securely transported to a secure evidence locker or room. The evidence should not come directly in contact with magnetic fields during transport nor left in direct contact with sunlight or any other place where temperature increases to 75°F.
- **Processing the evidence:** The disc image can be reconstructed when the copy of the disk is brought back to die lab. Special tools are used to analyze the data.

Live Data Collection

- Primary step of any digital investigation is to collect information and then deciding initial response strategy.
- Two ways of initial response:
  - Ensure there is an incident and after that obtain system's temporal data that will disappear if you power off the system
  - Investigation should be able to perform initial response using very less operation and time and should be authorized to take forensic duplication of crime scene systems.

Live Data collection from windows system

1. **CREATING A RESPONSE TOOLKIT**

   we need to plan a policy to retrieve all information without messing up with strong evidence. we have to careful about not destroying or altering the evidence and to do this we create response toolkit.

Tool	Description	Source
cmd.exe	The command prompt for Windows NT and Windows 2000	Built in
PsLoggedOn	A utility that shows all users connected locally and remotely	www.foundstone.com
`rasusers`	A command that shows which users have remote-access privileges on the target system	NT Resource Kit (NTRK)
`netstat`	A system tool that enumerates all listening ports and all current connections to those ports	Built in
Fport	A utility that enumerates all processes that opened any TCP/IP ports on a Windows NT/2000 system	www.foundstone.com
PsList	A utility that enumerates all running processes on the target system	www.foundstone.com
ListDLLs	A utility that lists all running processes, their command-line arguments, and the dynamically linked libraries (DLLs) on which each process depends	www.foundstone.com
`nbtstat`	A system tool that lists the recent NetBIOS connections for approximately the last 10 minutes	Built in
`arp`	A system tool that shows the MAC addresses of systems that the target system has been communicating with, within the last minute	Built in
`kill`	A command that terminates a process	NTRK

Control User Interface(CUI) Tools

Tool	Description	Source
netcat	A utility used to create a communication channel between two different systems	www.atstake.com/research/tools/network_utilities
cryptcat	A utility used to create an encrypted channel of communications	http://sourceforge.net/projects/cryptcat
PsLogList	A utility used to dump the contents of the event logs	www.foundstone.com
ipconfig	A system tool that displays interface configuration information	Built in
PsInfo	A utility that collects information about the local system build	www.foundstone.com
PsFile	A utility that shows files that are opened remotely	www.foundstone.com
PsService	A utility that shows information about current processes and threads	www.foundstone.com
auditpol	A utility used to display the current security audit settings	NTRK
doskey	A system tool that displays the command history for an open cmd.exe shell	Built in

- In Windows, there are two types of applications:
  - based on a graphical user interface(GUI)
  - based on a console user interface (CUI).
- Since GUI programs create windows, have pull-down menus, and generally do “behind-the-scenes” interaction,
- Experts advised to avoid GUI for investigation

2. **Preparing the response Toolkit:**

- You need to ensure that your toolkit will function exactly as intended and not alter the target system.
- We take several steps to prepare our toolkits for initial response:

  (a) Label the response toolkit media: A first step in evidence collection is to document the collection itself. Your response toolkit CD-ROM or floppy disks should be labeled to identify this part of your investigation. For ex, for our response floppies and CDs, we make a specialized label that has the following information on it:

  - Case number
  - Time and date
  - Name of the investigator who created the response media
  - Name of the investigator using the response media
  - Whether or not the response media (usually a floppy disk) contains output files or evidence from the victim system

  (b) Check for dependencies with File:

  It is important to determine which DLLs and files your response tools depend on.

  (C) Create a checksum for the response toolkit: One of the files on our response kit floppy (and CD and USB drive) is a text file with a checksum of all the commands on it.).

Md5sum to create a checksum for the response toolkit

Saving Information collected During Initial Response

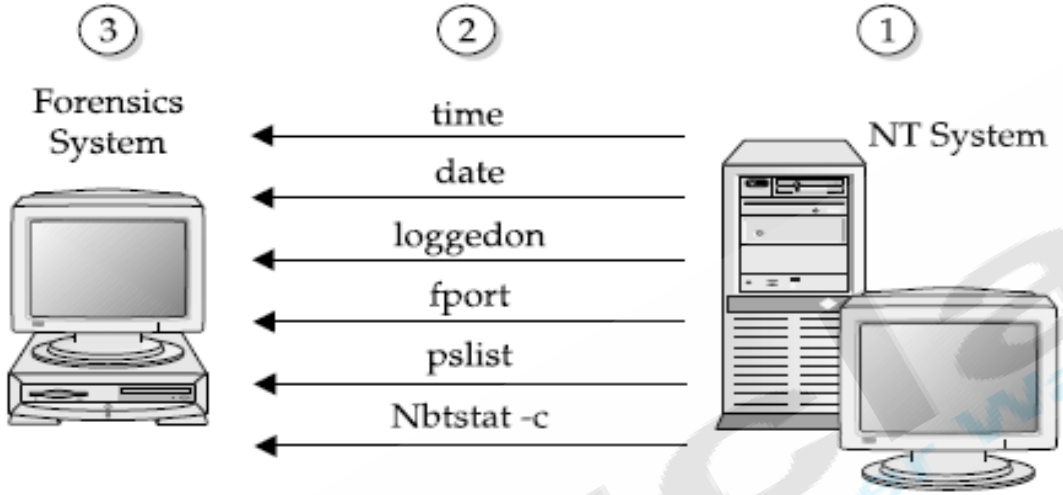
- During initial response, we collect a lot of information from the live system.
- *live to refer to a system that is relevant to an investigation, whether it is* the attacking system or the victim, and is currently powered on.
- There are four options when retrieving information from a live system:
  - Save the data you retrieve on the hard drive of the target system.
  - Record the data you retrieve by hand in a notebook.
  - Save the data you retrieve onto the response floppy disk or other removable media.
  - Save the data you retrieve on a remote "forensic system" using netcat or cryptcat.
- Saving data to the hard drive is undesirable because it alters the system

- Recording data by hand is not practical due to the volume of information.
- Floppy drives are usually not a great choice because the data will not fit on the floppy.
- Use of floppy drives are out because the storage capacity is less compared to recent storage devices which are compact in size such as removable USB drives.
- storage capabilities (up into the gigabyte range) and can be used to store your toolkit as well as the collected data. These devices have drivers built in, so they will work with any computer that sports a USB port and Windows software.
- Choose netcat to transfer the information from the target system to a remote forensic workstation.

Moving Data with Netcat

- Netcat is a freely available tool that creates a channel of communication between hosts.
- We use it during initial response to create a reliable, TCP connection between the target system and the forensic workstation used for analysis.
- All that you need to use netcat is an IP address on the target network and a laptop system with enough storage space to retain the information you gather.
- Using netcat allows you to transfer all the relevant system information and files you require to confirm whether or not an incident occurred.
- This technique of information gathering promotes two practices:
  - It lets you get on and off the target system quickly.
  - It allows you to perform an offline review of the information attained.

Using netcat during initial response to incidents



1. Run trusted commands on NT Server
2. Send output to forensics box via netcat
3. Perform off-line review
   md5sum output files

Do in an organized, forensically sound fashion

Setting up the netcat listener on the forensic workstation

- To use netcat, you initiate a netcat listener on the forensic workstation and redirect all incoming data to a file.
- Forensic workstation listening for incoming connections on port 2222.
- It will write the information received on that port to a file called pslist.
- On the target system, netcat is used to funnel the output to your response commands to the forensic workstation.
- The command line runs pslist, sending the output of the command to the forensic workstation, at IP address 192.168.0.20.
- When transferring files in this manner, netcat does not know when the data transfer is complete. You will need to break the connection after the data transfer is complete by pressing CTRL-C on the forensic workstation

OBTAINING VOLATILE DATA

- Now that you have a forensic toolkit and a methodology, you need to determine exactly which data to collect.
- At this point, you want to obtain the volatile data from the Windows NT/2000 system prior to turning off that system. At a minimum, we collect the following volatile data prior to forensic duplication:
  - System date and time
  - A list of the users who are currently logged on
  - Time/date stamps for the entire file system
  - A list of currently running processes
  - A list of currently open sockets
  - The applications listening on open sockets
  - A list of the systems that have current or had recent connections to the system

Documenting and Managing Investigation

- You need to have a methodology that is both organized and documented. There are two reasons for carefully documenting your actions when responding at the console of a victim system:
  - To gather information that may become evidence against an individual
  - To protect your own organization

Collecting Volatile Data for window system

- After knowing data should be collected and how to document response, it is now time to retrieve temporal data
- steps to use for data collection:

1. Execute a trusted cmd.exe.
2. Record the system time and date.
3. Determine who is logged in to the system (and remote-access users if applicable).
4. Record modification, creation, and access times of all files.
5. Determine open ports.
6. List applications associated with open ports.
7. List all running processes.
8. List current and recent connections.
9. Record the system time and date.
10. Document the commands used during initial response

Live data collection from UNIX System

- The initial response to prospective incidents on Unix systems is similar to the initial response for incidents on Windows systems.
- The main goal is to obtain the volatile system data before forensic duplication.
- Scope of your initial response to obtain log files, configuration files, system files, and relevant files to rapidly confirm whether or not an incident occurred.
- One difference between working with Windows and Unix systems is the difficulty of recovering deleted files on some Unix variants.
- When you execute a process in the Windows environment, you cannot delete the file corresponding to the running process from the hard drive.
- However, the Unix operating system allows you to delete a program after it has been executed—the process is running, yet the program's file has been deleted from the hard drive.
- Three steps:
  1. Creating a response Toolkit
  2. Saving information obtained at the time of initial response
  3. Obtaining volatile data before forensic duplication

Creating a response Toolkit

- Preparing your trusted toolkit is more difficult and time-consuming than it sounds, because
- practically every variant of Unix requires a unique toolkit

Saving information obtained at the time of initial response

- When you respond to an incident, you must choose where to store information retrieved during the initial response.
- You have the following storage options:
  - Store the data on the local hard drive.
  - Store the data to remote media such as floppy disks, USB drives, or tape drives.
  - Record the information by hand.
  - Use netcat (or cryptcat**) to transfer the retrieved data to a forensic** workstation over the network.
- Storing data on the local hard drive should be avoided whenever possible. If data recovery or forensic analysis is required, the data you store on the local hard drive will overwrite deleted data that was in unallocated space that may be of investigative and/or evidentiary value.
- Newer versions of Linux support USB drives, they are not as useful for data collection by direct physical connection. However, you can overcome this limitation by using netcat to transfer the data over the network to a forensic workstation equipped with a USB drive or other adequate storage.
- Weuse Linux on our forensic workstations to provide a faster response.

Obtaining volatile data before forensic duplication

- When you collect volatile data, you will want to respond to the target system at the console, rather than access it over the network.
- This eliminates the possibility of the attacker monitoring your response and ensures that you are running trusted commands.
- You should focus on obtaining the volatile system data before powering down the system.
- The volatile data includes currently open sockets, running processes, the contents of system RAM, and the location of unlinked files.
- The unlinked files are files marked for deletion when processes that access it terminate.
- The files marked for deletion will “disappear” when the system is powered down.
- Initial response should recover each type of volatile evidence, including the files marked for deletion

Collecting the Data

- At a minimum, you should collect the following information:
  - System date and time
  - A list of the users who are currently logged on
  - Time/date stamps for the entire file system
  - A list of currently running processes
  - A list of currently open sockets
  - The applications listening on open sockets
  - A list of the systems that have current or recent connections to the system

Steps for obtaining live data

1. Execute a trusted shell.
2. Record the system time and date.
3. Determine who is logged on to the system.
4. Record modification, creation, and access times of all files.
5. Determine open ports.
6. List applications associated with open ports.
7. Determine the running processes.
8. List current and recent connections.
9. Record the system time.
10. Record the steps taken.
11. Record cryptographic checksums.

1. Executing a Trusted Shell

- When you respond to a target system running Unix, you will encounter one of two scenarios:
  - The system is running in console mode.
  - The system is running X Windows, a GUI similar to the Windows desktop.
- To avoid common X Windows-based vulnerabilities that allow the attacker to log keystrokes, you should exit X Windows before you initiate your response. If you are responding to a Linux system, you may be able to switch to another *virtual console by pressing* ALT-F2.
- Log on locally at the victim console to avoid generating network traffic, and be sure to log on with root-level privileges.
- The following is the command syntax to mount a floppy drive when responding to a Linux system:
  - mount /dev/fd0 /mnt/floppy
- This command mounts your trusted toolkit on the mount point /mnt/floppy.
- When you change directories to /mnt/floppy, you will be able to access your trusted files.

2.Recording the System Time and Date

- The local date and time settings are important for later correlation of time/date stamps, and they also show when you were on the system. To capture this information, use the date command:

```
[root@conan /root]# date
Tue Dec 17 16:12:43 UTC 2003
```

3. Determining Who Is Logged on to the System

- Determining who is logged on is quite simple. Just execute the w (what) command.
- The w command displays the user IDs of logged-on users, what system they logged on from, and what they are currently executing on the system. It also provides the date and system time.

```
[root@conan /root]# w
11:39pm up 3:11, 3 users, load average: 1.27, 1.43, 1.84
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
nada ttyp0 jitter.rahul.net 8:30pm 3:02m 1:08 0.14s
telnet bothosti
bovine ttyp1 shell1.bothostin 8:35pm 3:02m 1:01 0.12s -bash
mandiak ttyp2 adsl-225-75.poto 11:38pm 0.00s 0.25s 0.11s w
[root@conan /root]#
```

- The header line in the output indicates the current system time, how long the system has been running, how many users are currently logged in, and the system load averages for the past one, five, and fifteen minutes.

4.Recording creation,alteration,and access time of each file:

- You will want to retrieve all the time/date stamps on the file system.
- As with Windows systems, Unix systems have three time/date stamps to collect for each file and directory:
- access time (atime), modification time (mtime), and the inode change time (ctime).
- You can use a trusted ls command with the proper command-line arguments to obtain these times for each file. The following lines demonstrate how to obtain the time/date stamps and save the output on a trusted floppy disk:

  ls -alRu / > /floppy/atime

  ls -alRc / > /floppy/ctime

  ls -alR / > /floppy/mtime
- The R option used in the ls command forces a recursive listing, which takes some time. On very large file systems, this data may not fit on a 1.55MB floppy, so you may be forced to use other media or netcat/cryptcat.

5.Identify open portes:

- Use the netstat –an command to view all open ports. The -n option tells netstat to not resolve hostnames, which reduces the impact on the system and speeds the execution of the command.
- The following is an excerpt from the output of netstat:

```
[root@conan /root]# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 176 66.192.0.66:22 66.192.0.26:20819
ESTABLISHED
tcp 0 0 0.0.0.0:80 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:21 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN
udp 0 0 0.0.0.0:69 0.0.0.0:*
```

- On this server, we see listening TCP ports 80, 21, and 22, and a listening UDP port 69.

6. Listing Applications Associated with Open Ports

- On Linux, the netstat command has a -p option that maps the name of the application and its process ID (PID) to the open ports.

```
[root@conan /root]# netstat -anp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q  Local Address   Foreign Address  State
PID/Program name
1) tcp       0      0 0.0.0.0:143     0.0.0.0:*        LISTEN   385/inetd
2) tcp       0      0 0.0.0.0:22      0.0.0.0:*        LISTEN   395/sshd
3) tcp       0      0 0.0.0.0:512     0.0.0.0:*        LISTEN   385/inetd
4) tcp       0      0 0.0.0.0:513     0.0.0.0:*        LISTEN   385/inetd
5) tcp       0      0 0.0.0.0:514     0.0.0.0:*        LISTEN   385/inetd
6) tcp       0      0 0.0.0.0:23      0.0.0.0:*        LISTEN   385/inetd
7) tcp       0      0 0.0.0.0:21      0.0.0.0:*        LISTEN   385/inetd
8) udp       0      0 0.0.0.0:69      0.0.0.0:*                 385/inetd
9) raw       0      0 0.0.0.0:1       0.0.0.0:*                 7
   -
10) raw      0      0 0.0.0.0:6       0.0.0.0:*                 7
```

This output displays seven open TCP sockets and one open UDP socket. Line 9 indicates a raw socket is listening for ICMP, and line 10 reveals that the kernel is also listening for TCP packets. If you examine line 2, you can see that the secure shell daemon, sshd, with a PID of 395, is listening for connections on TCP port 22. Lines 1, 3, 4, 5, 6, and 7 show that the inetd, with a PID of 385, is listening on TCP ports 143, 512, 513, 514, 23, and 21.

7.Determining the Running Processes

- It is critical to take a snapshot of all the running processes during the initial response. This can be accomplished by using the standard ps (process status) command

```
[root@conan]# ps -aux
USER    PID %CPU %MEM  VSZ  RSS TTY   STAT START TIME COMMAND
root      1  0.1  0.7 1060  480 ?     S    17:52 0:03 init [3]
root      2  0.0  0.0    0    0 ?     SW   17:52 0:00 [kflushd]
root      3  0.0  0.0    0    0 ?     SW   17:52 0:00 [kupdate]
root      4  0.0  0.0    0    0 ?     SW   17:52 0:00 [kpiod]
root      5  0.0  0.0    0    0 ?     SW   17:52 0:00 [kswapd]
root      6  0.0  0.0    0    0 ?     SW<  17:52 0:00 [mdrecoveryd]
root    259  0.0  0.2  348  136 ?     S    17:52 0:00 /sbin/dhcpcd eth0
root    316  0.0  0.8 1112  556 ?     S    17:52 0:00 syslogd -m 0
root    326  0.0  1.1 1360  756 ?     S    17:52 0:00 klogd
daemon  341  0.0  0.7 1084  492 ?     S    17:52 0:00 /usr/sbin/atd
root    356  0.0  0.9 1272  608 ?     S    17:53 0:00 crond
```

8. Listing Current and Recent Connections

- The netstat command provides information about another aspect of live response: current and recent connections.

9. Recording System Time

- Use the date command again (repeat step 2) to record the current system time.

10. Record the Steps Taken

- Finally, record all of the commands you have issued to the system. There are several possibilities
- here: use script, history, or even vi if you performed your live response
- from the editor. Since you issued all commands from a trusted shell, using the history
- command will record all of the commands you've executed. However, a better choice is

11. Recording Cryptographic Checksums

- Finally, record the cryptographic checksums of all recorded data. Simply run the md5sum program against all files in the data directory, as shown here:

  [root@conan /root]# md5sum * > md5sums.txt

Storing Information obtained during Initial response

- Most Unix flavors keep their log files in /var/adm or /var/log subdirectories.
- We use a combination of netcat, cryptcat, dd, and des to obtain the log files on a system.
- At a minimum, you want to acquire the three binary log files and the common ASCII text log files.
- The following binary log files are of particular interest:
  - The utmp file, accessed with the w utility
  - The wtmp file, accessed with the last utility
  - The lastlog file, accessed with the lastlog utility
- Process accounting logs, accessed with the lastcomm utility
- The following are the common ASCII text log files:
  - Web access logs (/var/log/httpd/access_log)
  - Xferlog (ftp logs)
  - History files

- **Obtaining Important Configuration Files**
- Unix maintains certain configuration files that are commonly accessed or altered by attackers.
- It is important to review each one of these configuration files to locate backdoors, unauthorized trust relationships, and unauthorized user IDs.
  - /etc/passwd, to look for unauthorized user accounts or privileges
  - /etc/shadow, to ensure every account requires password authentication
  - /etc/groups, to look for escalation in privileges and scope of access
  - /etc/hosts, to list the local Domain Name System (DNS) entries
  - /etc/hosts.equiv, to review trusted relationships
  - /etc/rc, to look in the startup files
  - crontab files, to list scheduled events

- **Dumping System RAM**
- There is no proper way to dump the system RAM on Unix machines.
- We usually transfer the /proc/kmem or /proc/kcore file from the target system.
- This file contains the contents of system RAM in a discontinuous manner.

Investigating Window Systems

Following Investigative steps:-

- Review all pertinent logs
- Perform Keyword Searches
- Review relevant files
- Identifying unauthorized user accounts or group
- Identifying rouge process and services
- Look for unusual or hidden files/ directories
- Check for illegal entry points
- Inspect jobs run by scheduler services
- Analyze trust relationship
- Review security Identifiers.

Where evidence resides on window systems:

1. Volatile data in kernel structures
2. Slack spaces where you obtain info from previously deleted files that are unrecoverable.
3. Free or unallocated space where you can obtain previously deleted files including damaged or inaccessible clusters.
4. The logical file system.
5. The event logs
6. The Registry which you should think of as an enormous log file.
7. Application logs not managed by the window event log services
8. The printer spool
9. Sent or received email such as the.pst files for outlook mail.

Reviewing All Pertinent Logs

1. Determine which user have been accessing specific files
2. Determine who has been successfully logging on to a system
3. Determine who has been trying unsuccessfully to log on a system
4. Track usage of special application
5. Track alteration to the audit policy
6. Track changes to user permission (such as increased access)

Performing Keyword Searches

- Keyword Search utilities provide a “window” of information around the keyword or phrase .
- This allows the reviewer to determine its applicability to the investigation.
- Plan keyword searches carefully to minimize exposure while balancing the requirement for discovery of data relevant to your investigation
- In most disk search tools that are marketed cannot read a drive that is running a window OS, because various types of tools require that you boot the target system from a controlled boot floppy or media and run the tool

Reviewing Relevant Files

- Third party software can augment the monitoring and record keeping that window system perform.
- Third party firewall software provides fantastic audit trail for investigator to piece together incoming and outgoing activity on a system.
- Most firewall application record every website a system visits , tap virus and provide an audit tail for every known on the system.

Identifying Unauthorized User Accounts or Groups

- There are several ways to audit user account or groups:
  - Look in the User Manager for unauthorized user accounts (during a live system response).
  - Use usrstat from the NTRK to view all domain accounts on a domain controller, looking for suspicious entries.
  - Examine the Security log using Event Viewer, filtering for event ID 624 (addition of a new account), 626 (user account enabled), 636 (changing an account group), and 642 (user account changed).
  - Check the \%systemroot%\Profiles directories on the system. If the user account exists, but there is no corresponding \%systemroot%\Profiles\ directory, that user account has not been used to log in to the system yet. If that directory does exist, but the user account is no longer listed in the User Manager or Registry (at HKLM\SAM\Domains\Account\Users\ Names), that user ID did exist at one time but no longer exists.

Identifying Rogue Process

- The easiest solution is to run the most up to date virus scanner on the whole logical volume of evidence
- Make sure that the volume is mounted read only when you choose to run a virus checking against the file system of the restored image.
- PestPatrol is best tool that identifies Trojan, backdoor ,keystroke and other malware.

Looking for Unusual or hidden files

Once an attacker gains unlawful access to a Windows system she needs to hide her files for later use. Once an insider chooses to perform unauthorized or unacceptable deeds on his system, he may choose to make a few files “invisible.” Both of these attackers can take advantage of NTFS file streams to hide data behind legitimate files

1. Programming by JD Glaser
2. Usage-sfind [path]/ns
3. [dirpath] Directory to search none equal current
4. -ns Skip sub directories
5. -or/either switch statement can be used
6. -?Help

Checking for Unauthorized Access Points

1. Terminal Server
2. SQL/Oracle
3. Third- party telnet daemons on Window NT
4. Windows 2000 Telnet Server
5. Third –party FTP daemons
6. Web servers (such as Apache and IIS)
7. Virtual network computing(TCP port 5800) and PC anywhere(TCP port 5631)
8. Remote access services (PPP and PPTP)
9. X servers

Examining Jobs Run by the Scheduler Service

- A common trick by attackers is to have a scheduled event start backdoor programs for them, change the audit policy, or perhaps even something more sinister such as scheduled wiping of files.
- Consider the following batch file running the NTRK tool remote on an NT system:

remote /s "cmd.exe" batman5

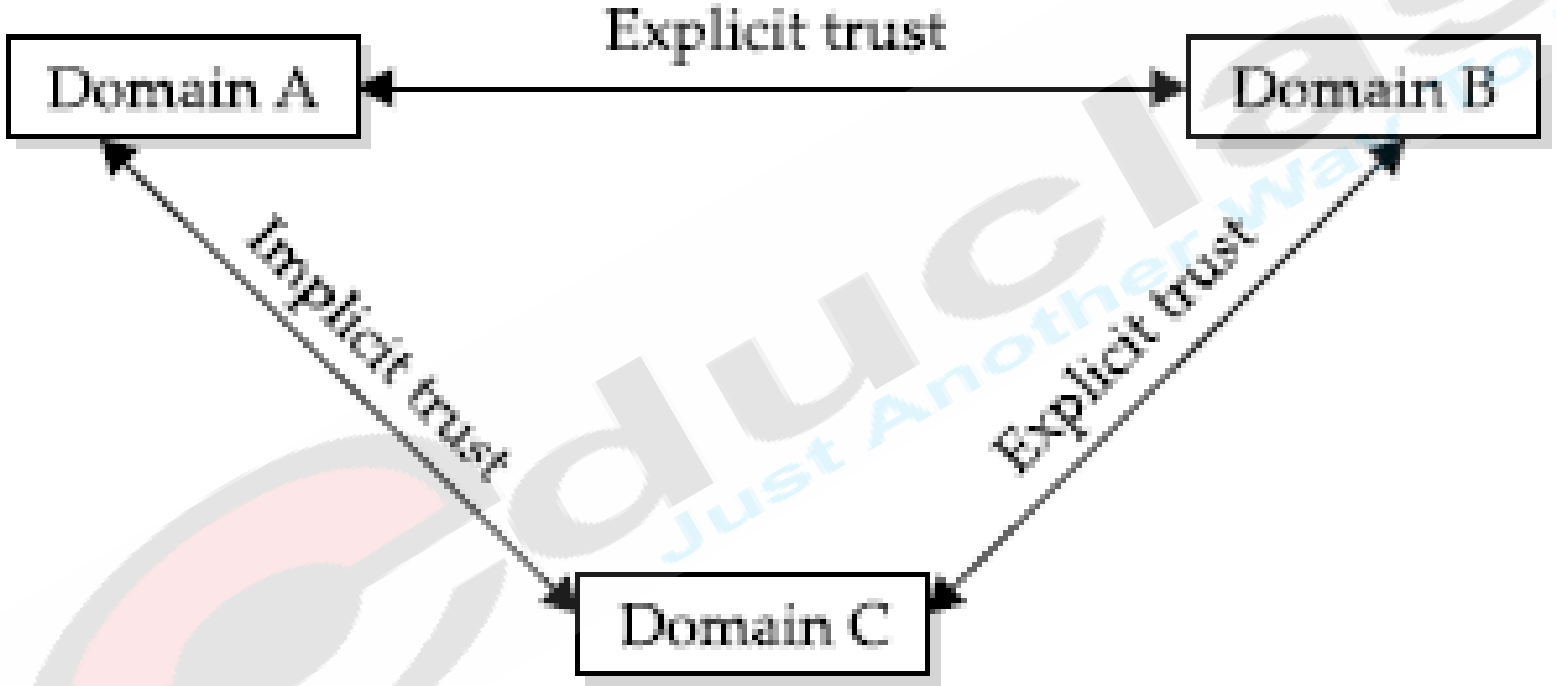
- If this command line were run at a specific time, someone could connect to the system using the following command line:

remote /c <hostname> batman5

- The <hostname> is the NetBIOS name of the remote system, and batman5 is the key phrase to connect.
- The person can now execute any commands desired.
- scheduled jobs are typically scheduled by using the at or soon utility.
- The at command, with no command-line arguments, will show any jobs that have been scheduled.

Analyzing Trust Relationships

- Trust relationships among domains can certainly increase the scope of a compromise should a valid user ID and password be stolen by an attacker.
- Access to one machine may mean logical access to many others.
- Trust relationships may increase the scope of a compromise and raise the severity of the incident.
- Determining trust within a Windows domain is not as simple as it is in the Unix environment.
- Windows NT supports *nontransitive, or one-way, trust. This means that access and* services are provided in one direction only.
- If your NT PDC trusts another domain, it does not need to trust your PDC. Therefore, users on the trusted domain can use services on your domain, but not vice versa.
- Windows 2000 can provide a two-way, or *transitive, trust relationship.*
- *Domains located* within an Active Directory forest require two-way trusts to communicate properly.
- For example, in Windows 2000 Active Directory Services, if Domain A trusts Domain B, and Domain B trusts Domain C, then Domain A trusts Domain C. This relationship is illustrated in Figure



Reviewing Security Identifiers (SIDs)

- To establish the actions of a specific user ID, you may need to compare SIDs found on the victim machine with those at the central authentication authority.
- SIDs can contribute to incident response.
- The SID is used to identify a user or a group uniquely. Each system has its own identifier, and each user has his own identifier on that system. The computer identifier and the user identifier are combined to make the SID. Thus, SIDs can uniquely identify user accounts. SIDs do not apply to share security.
- For example, the following is a SID that belongs to the administrator account:

S-1-5-21-917267712-1342860078-1792151419-500

- The S denotes the series of digits as a SID. The 1 is the revision level, the 5 is the identifier- authority value, and 21-917267712-1342860078-1792151419 includes the subauthority values. The 500 is the relative identifier.
- with help of usernames and passwords Access to shares is accomplished. However, SIDs do apply when remote access to a domain is provided.
- A SID with the server's unique sequence of numbers is placed in the Registry of the workstation after the first successful logon to that server.
- SIDs can be the digital fingerprints that prove that a remote system was used to log on to a machine and access a domain.

Investigating UNIX System(9.2 and 9.3)

- The Unix operating system is powerful, flexible, and extremely functional.
- The functionality that makes it so useful also makes it a challenge to protect and investigators.
- Once you are ready to begin investigating the Unix system, the following actions provide the most likely way to identify relevant evidence:
  - Review all pertinent logs
  - Perform keyword searches
  - Review relevant files
  - Identify unauthorized user accounts or groups
  - Identify rogue processes
  - Check for unauthorized access points
  - Analyze trust relationships
  - Check for kernel module rootkits
- These steps are not listed chronologically or in order of importance. You may not need to take all of the steps for every incident. Your approach depends on the specific incident and the goals of your response.
- As you conduct your investigation, be aware that, in the event of root compromise, anything can happen. An attacker with root access to a system can modify just about anything on the operating system, including the evidence that you are reviewing

Reviewing Pertinent Logs

- Unix operating systems have a variety of log files that can yield important clues during incident response.
- Not only are system activities such as logons, startups, and shutdowns logged, but also events associated with Unix network services.
- Most log files are located in a common directory, usually /var/log. However, some flavors of Unix will use an alternate directory, such as /usr/adm or /var/adm. Some logs are placed in nonintuitive locations, such as /etc.
- consult operating system-specific documentation, When in doubt.
- Additionally, not all log files are even on the system in question. You may find pertinent logs on a network server or security device, such as a firewall or an IDS.

Performing Keyword Searches

- Keyword searches are a critical part of almost every incident response investigation, ranging from email harassment to remote network compromise cases.
- Keywords can be a wide range of ASCII strings, including an attacker's backdoor password, a username, a MAC address, or an IP address.
- You can conduct keyword searches on the logical file structure or at the physical level, examining the contents of an entire drive.
- Here, we'll concentrate on how to perform string searches using Unix utilities.

String Searches with grep

- The powerful, flexible grep command is a primary tool for string searches. To perform a string search within a file, use the grep command as follows:

  [root@lucky]# grep root /etc/passwd

  root:x:0:0:root:/root:/bin/bash

- Notice that the line in the passwd file with the string root inside appears as output. The passwd file is a text file.
- Now, let's try grep on a binary file:

  [root@lucky]# grep PROMISC /sbin/ifconfig

- Binary file /sbin/ifconfig matches
- This time, the string does not appear. Instead, you see a notification that a file of type binary has a matching entry. If you want to see the match, use the -a option to handle binary files:

  [root@lucky]# grep -a PROMISC /sbin/ifconfig

[NO FLAGS] UP BROADCAST DEBUG LOOPBACK POINTOPOINT NOTRAILERS RUNNING NOARP PROMISC ALLMULTI SLAVE MASTER MULTICAST DYNAMIC

REVIEWING RELEVANT FILES

- It is a near certainty that many files will harbor evidence related to any given incident.
- However, your success in identifying all of the relevant files is much less certain.
- To help identify which files are likely to be relevant to any given incident.
- These techniques include identifying relevant files by their time/date stamps and by the information gained during the initial response to Unix.
- We also search configuration and system files commonly abused by attackers.

Incident Time and Time/Date Stamps

- In order to search for files and directories that were accessed, modified, or created around the time of a suspected incident, you must first know the time of the suspected incident.
- The timeframe may be very specific, such as when a network IDS discovered and logged the attack as it happened.
- On the other hand, the timeframe may be general, such as in the case where a system administrator connected the system to the Internet two weeks ago and evidence of compromise was found today.
- If you have a good record from an outside source (such as network IDS) of when the attack occurred, the first step is to make sure that the system time on the IDS matches that of the victim system.
- The goal in reviewing time/date stamps is to follow up on the relevant time windows that you have already determined.
- All of the files or directories accessed, modified, or created during this time are likely candidates as relevant items.

Identifying Unauthorized User Accounts Or Groups

- Attackers will often modify account and group information on victim systems.
- This modification can come in the form of additional accounts or escalations in privilege of current accounts.
- The goal is usually to create a backdoor for future access.
- You should audit user and group accounts on suspected victim systems to validate that an attacker did not manipulate this information.
- Auditing Unix system account information is a straightforward process.

User Account Investigation

- User information is stored in the /etc/passwd file.
- This is a text file that you can easily review through a variety of mechanisms.
- Every user on a Unix system has an entry in the /etc/passwd file.
- A typical entry looks like this:

lester:x:512:516:Lester Pace:/home/lester:/bin/bash

- The entry consists of seven colon-delimited fields: the username (lester), the password (shadowed in this case), the user ID (512), groupID (516), GECOS field (for comments; Lester Pace in this case), home directory, and default login shell.
- Any extra user accounts not created by the system administrator are cause for alarm.

Group Account Investigation

- Groupaccounts use the groupID shown in the /etc/passwd file as well as the /etc/groups file.
- A typical /etc/group file looks like this:
  1. $ cat /etc/group
  2. root::0:root,ashunn
  3. bin::2:root,bin,daemon
  4. sys::3:root,bin,sys,adm
  5. adm::4:root,adm,daemon
  6. uucp::5:root,uucp
- The file lists the groups, along with the users that are associated with that group.
- It is important to note that an entry in the groupfile does not need to exist for a group to exist.
- Group membership is based on the group ID in the password file.

IDENTIFYING ROGUE PROCESSES

- Identifying rogue processes is much easier when examining a live system.
- During the initial investigation, you should have recorded all listening ports and running processes.
- You should carefully examine the running processes to verify their validity.
- Review all binaries associated with listening services and running processes to ensure that they have not been modified.

What Can Happen

- During your initial investigation, you dutifully record listening ports and running processes.
- Upon further examination, you notice an anomaly with FTP:

```
[root@victim]# netstat –anp
tcp 0 0 0.0.0.0:23 0.0.0.0:* LISTEN 519/inetd
tcp 0 0 0.0.0.0:21 0.0.0.0:* LISTEN 519/ftpd
```

CHECKING FOR UNAUTHORIZED ACCESS POINTS

- Unix is a fully functional, robust operating system.
- Unix has continually added functionality, and network services are no exception.
- A default installation of Unix offers a dazzling array of network services, including the Network File System (NFS), telnet, finger, rlogin, and many others.
- Any one of the networked services on Unix systems can potentially allow some degree of remote access to unwanted intruders, as can a phone line connected to a modem.
- Some of the most common access points that we have seen intruders take advantage of include X Servers, FTP, telnet, TFTP, DNS, sendmail, finger, SNMP, IMAP, POP, HTTP, and HTTPS.
- As you conduct your investigation of the Unix system, you will need to examine all network services as potential access points.
- Network services could be vulnerable, allowing intruders access to your system, or network services could already be trojaned by a successful intruder.

ANALYZING TRUST RELATIONSHIPS

- Trust relationships within Unix systems were once a primary mechanism of attack.
- Trust can be established between Unix systems with a variety of services, the most popular of which include rlogin, rsh, the Network Information Service (NIS and NIS+), NFS, and ssh.
- Trust relationships can be convenient time-savers for system administrators and users.
- If machine A trusts machine B, then the user on machine B can access machine A with no additional credentials.
- If you are a system administrator with dozens of systems to maintain, using this feature can be very enticing.
- Trust relationships are usually configured through files such as /etc/hosts.equiv or any .rhosts file in a user's home directory.
- Trust relationships can be established with ssh through shared keys and through NFS shares.
- Another type of trust is created through network topology. Networked computers that share a common network segment must trust their peers. This means that an attacker who compromises a single host can view network traffic on the same segment, even in a switched environment.

DETECTING TROJAN LOADABLE KERNEL MODULES

- Loadable kernel modules (LKMs), or kernel extensions, are found on the various flavors of Linux, BSD, and Solaris.
- They extend the capabilities of the base operating system kernel, typically to provide additional support within the operating system for device and file system drivers.
- LKMs can be dynamically loaded by a user with root-level access, and they run at the kernel level instead of at a normal user-process level.
- Several intrusion-based LKMs have been developed, and once a malicious user obtains privileged access to your system, she can install one.
- Some common malicious LKMs include Adore, Knark, and Itf.
- These LKMs provide several capabilities for attackers, such as providing remote root access and hiding files, processes, and services

LKMs on Live Systems

- Detecting trojan LKMs on a live system can be complicated because these tools actually intercept system calls (such as ps or directory listing) to provide false information.
- They are specifically designed to prevent detection with traditional response methods.
- However, in many cases, you can find them by combining externally executed commands with local commands to detect anomalies or discrepancies.

Email Forensic

- The important reason for designing and implementing such technologies is to work out forensics investigation on demo emails to accurately identify the information like recipients name, the route used for transportation of email, client side application used to create email, the time when the email was created a separate message id and more
- The examination and disclosing of the key information or data from the email is called email forensics

Importance of Email as Evidence

- Email can be pivotal(essential) evidence in a case
- Due to its informal nature it does not always represent corporate policy
- Email evidence is in the email itself
- Email evidence is left in arrears as it travels from sender to recipient
  - contained in the various logs
  - Maintained by system administrator
- Law enforced can use a writ issued by a government agency to collect email
  - Headers and Logs

Working Of Email

- Email servers controls the transfer of email from the sending end to the receiving end
- Once the server are configured and are ready for use , the user across the globe register to these email servers and et up his/her personal email account.
- There are two standard methods for sending and receiving emails

  A) client/server application

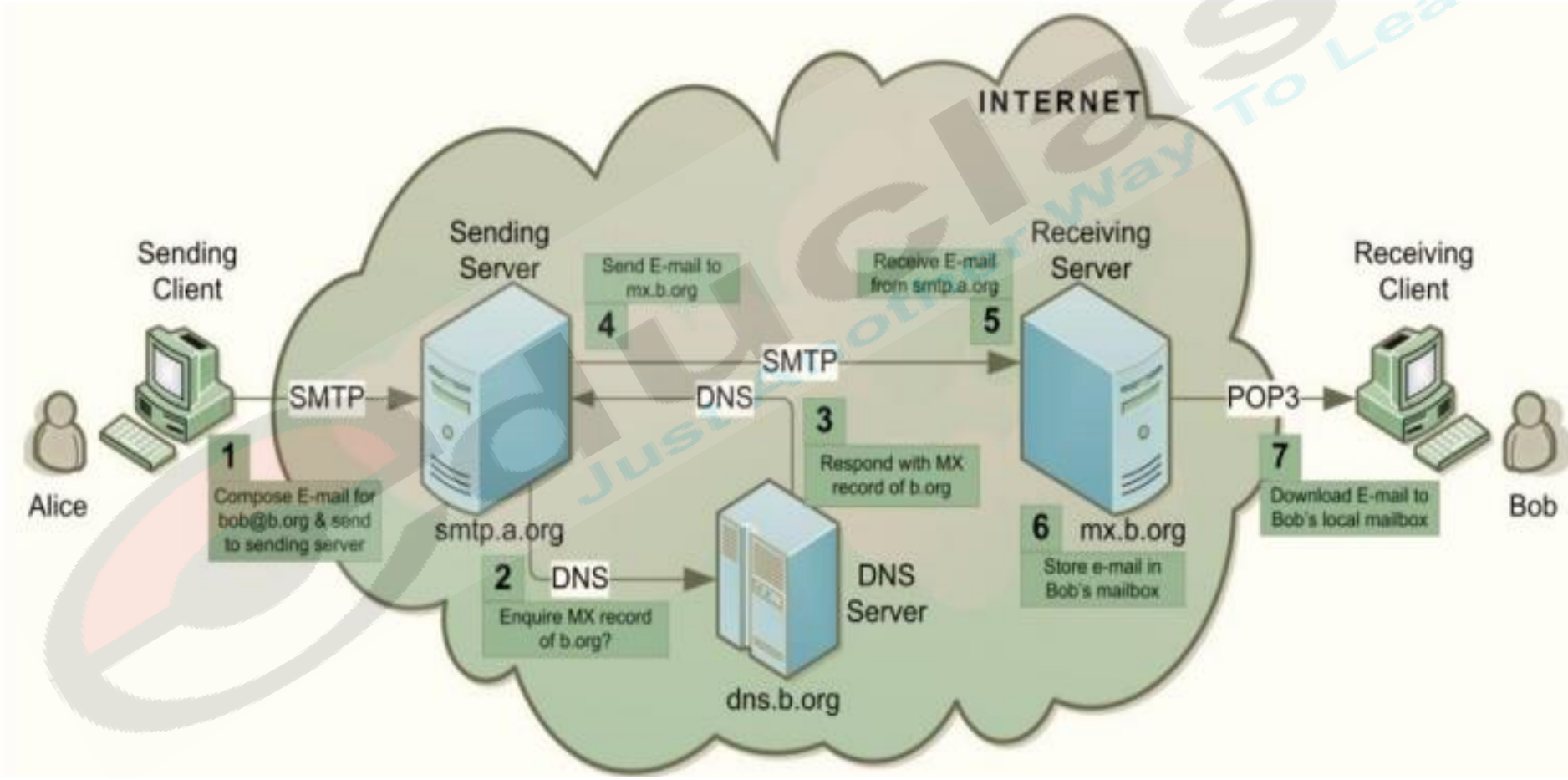
  B)Webmail

Steps in the Email communication

- An e-mail communication between a sender ‘Alice’ having e-mail address ‘alice@a.com’ and recipient ‘Bob’ having e-mail address ‘bob@b.com’ is shown in figure

1. ‘Alice’ composes an e-mail message on her computer called client for ‘Bob’ and sends it to her sending server ‘smtp.a.org’ using SMTP protocol.
2. Sending server performs a lookup for the mail exchange record of receiving server ‘b.org’ through Domain Name System (DNS) protocol on DNS server ‘dns.b.org’. The DNS server responds with the highest priority mail exchange server ‘mx.b.org’ for the domain ‘b.org’.
3. The DNS server replies with uppermost important mail exchange server mx.b.org for the domain b.org.
4. Sending server establishes SMTP connection with the receiving server and delivers the e-mail message to the mailbox of ‘Bob’ on the receiving server.
5. The receiving server receives the incoming e-mail message.
6. The receiving server stores e-mail message on Bob’s mailbox.
7. ‘Bob’ downloads the message from his mailbox on receiving server to local mailbox on his client computer using POP3 or IMAP [3] protocols. Optionally, ‘Bob’ can also read the message stored in his server mailbox without downloading it to the local mailbox by using a Webmail program.

Steps in the Email communication



Client Protocols

Different Protocol along with their characteristics

Post Office Service	Protocol	Characteristics
Stores only incoming messages.	POP	Investigation must be at the workstation.
Stores all messages	IMAP MS' MAPI Lotus Notes	Copies of incoming and outgoing messages might be stored on the workstation or on the server or on both.
Web-based send and receive.	HTTP	Incoming and outgoing messages are stored on the server, but there might be archived or copied messages on the workstation. Easy to spoof identity.

SMTP Header

Reviewing e-mail headers can offer clues to true origins of the mail and the program used to send it

Common e-mail header fields include:

- Bcc
- Cc
- Content-Type
- Date
- From
- Message-ID
- Received
- Subject
- To
- X-Priority

SMTP Header

- Example of a message header for an email sent from MrJones@emailprovider.com to MrSmith@gmail.com

```
Delivered-To: MrSmith@gmail.com
Received: by 10.36.81.3 with SMTP id e3cs239nzb;Tue, 29 Mar 2005 15:11:47
-0800 (PST)
Return-Path: MrJones@emailprovider.com
Received: from mail.emailprovider.com (mail.emailprovider.com
[111.111.11.111]) by mx.gmail.com with SMTP id h19si826631rnb; Tue, 29
Mar 2005 15:11:47 -0800 (PST)
Message-ID: <20050329231145.62086.mail@mail.emailprovider.com>
Received: from [11.11.111.111] by mail.emailprovider.com via HTTP; Tue,
29 Mar 2005 15:11:45 PST
Date: Tue, 29 Mar 2005 15:11:45 -0800 (PST)
From: Mr Jones
Subject: Hello
To: Mr Smith
```

Received Header

- Received is the most essential field of the email header: it creates a list of all the email servers through which the message traveled in order to reach the receiver
  - The best way to read are from bottom to top
    - ❖ The bottom "Received" shows the IP address of the sender's mail server
    - ❖ The top "Received" shows the IP address of receiver mail server
    - ❖ The middle "Received" shows the IP address of the mail server through which email passes from sender to receiver

Example:

From mail.emailprovider.com to mx.gmail.com

```
Received: from mail.emailprovider.com (mail.emailprovider.com
[111.111.11.111]) by mx.gmail.com with SMTP id h19si826631rnb; Tue, 29
Mar 2005 15:11:47 -0800 (PST)


Received: from [11.11.111.111] by mail.emailprovider.com via HTTP; Tue,
29 Mar 2005 15:11:45 PST
```

SMTP Protocol

- Neither IMAP or POP are involved relaying messages between servers.
- Simple Mail Transfer Protocol: SMTP
  - Easy, but can be spoofed easily.

```
S: 220 www.example.com ESMTP Postfix
C: HELO mydomain.com
S: 250 Hello mydomain.com
C: MAIL FROM: <sender@mydomain.com>
S: 250 Ok
C: RCPT TO: <friend@example.com>
S: 250 Ok
C: DATA
S: 354 End data with .
C: Subject: test message
C: From: sender@mydomain.com
C: To: friend@example.com
C:
C: Hello,
C: This is a test.
C: .
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye
```

Email Services Protocols

- Basically 3 protocols:
  - SMTP
  - POP3
  - IMAP

SMTP

- SMTP stands for Simple Mail Transfer Protocol.
- SMTP is used either when email is delivered from the client (like Gmail) to the email server or when email is delivered from one server to another.
- Port number 25 is used for SMTP.

POP3

- POP3 stands for Post office Protocol
- It allows the client to download the email from the server
- POP3 is a very simple protocol and it does not support any other feature except download.
- The design of POP3 assumes that the client download all the available email from the server and deletes the email from the serve and then disconnected.
- Port number 110 is used from POP3

IMAP

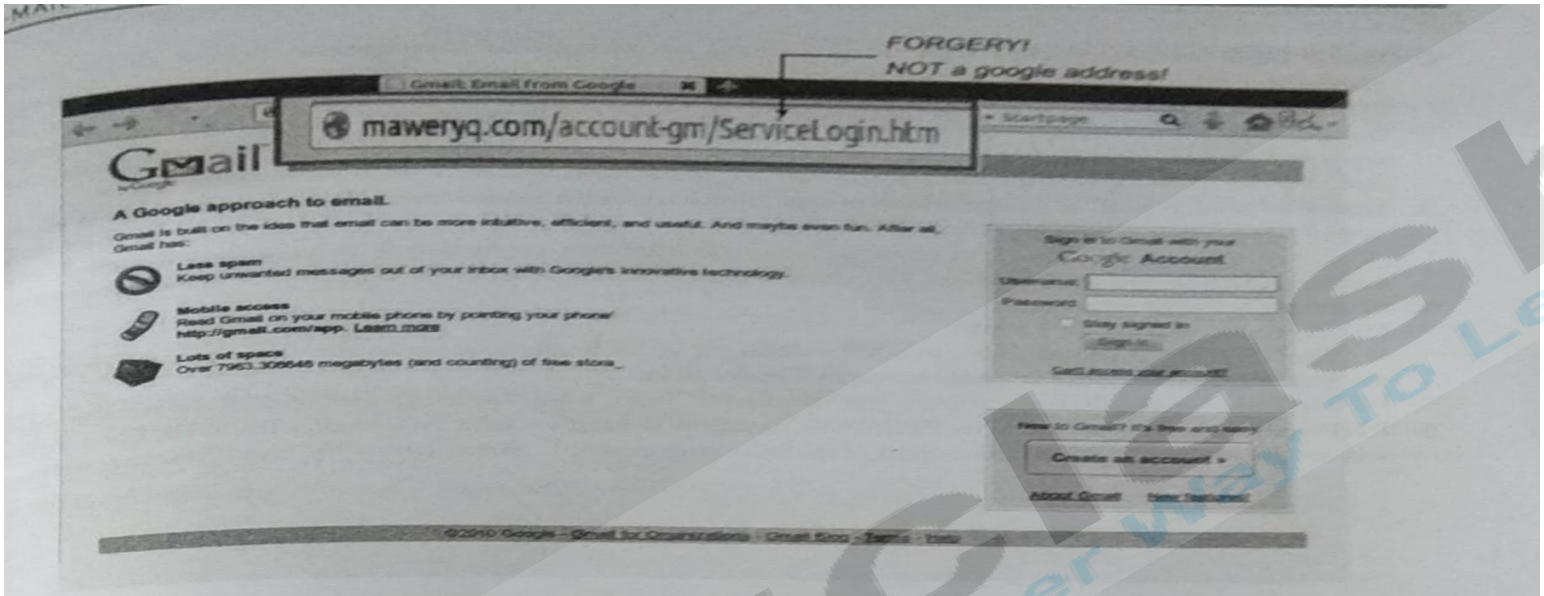
- IMAP stands for Internet Message Access Protocol.
- Features of IMAP are almost similar to POP3.
- This Protocol can be used by the client to download email from the server
- Many feature are added which are not included in POP3
- IMAP is designed to allow the end users to store their emails on the server
- It requires more disk space on the server for storing the emails
- It requires more CPU resources for processing over the servers
- More space and CPU resources are needed as compared to POP3.
- Port number 143 is used for IMAP.

Internet Fraud

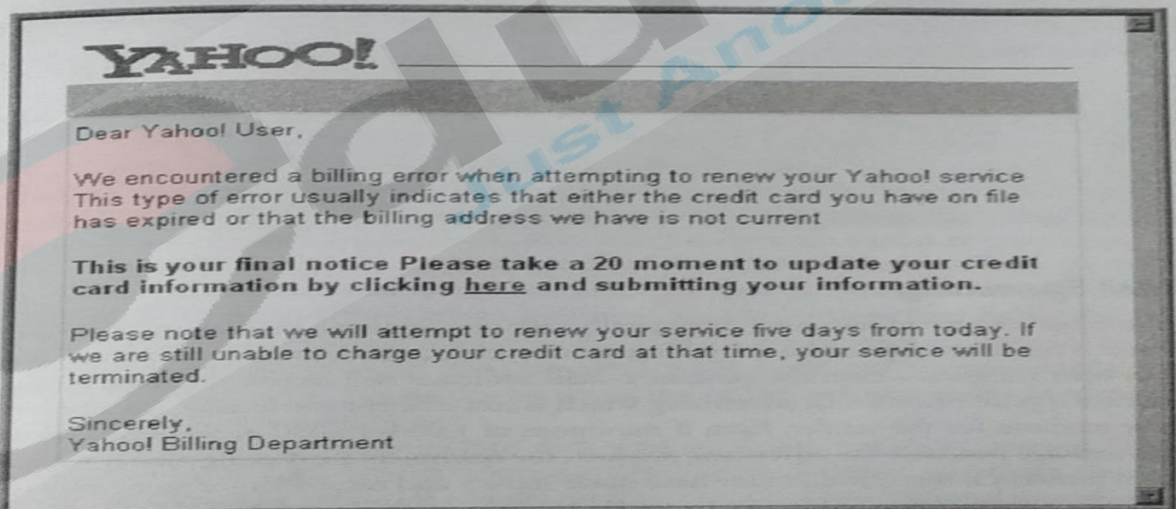
- Internet fraud refers to any kind of fraud scheme which uses email services, websites, forums or chat rooms, or messages to trap a person and make them the victim of the same.
- They conduct may fraud transaction or transfer the funds to fraud accounts and many other various connected schemes

Email Spoofing

- Email spoofing is fake of the email header, which denotes that the message is sent from the original and genuine source. Spammers often use this technique as an attempt to get the user to open such attractive email and expect a reply from the user to trap them and make them a victim.
- There exists many ways to send fake emails and trap the user without knowing the passcode or password of the email ID
- Email spoofing is very easy to do. All that a hacker needs to spoof any email address is SMTP server (like Gmail)and efficient and effective email software.
- Many hosting services provide SMTP servers in their hosting package. It is also feasible and possible to send any email from our own system or devices all you need to do is install the SMTP server on it. Many ISP will block port number 25(this port no is required to send the email out).



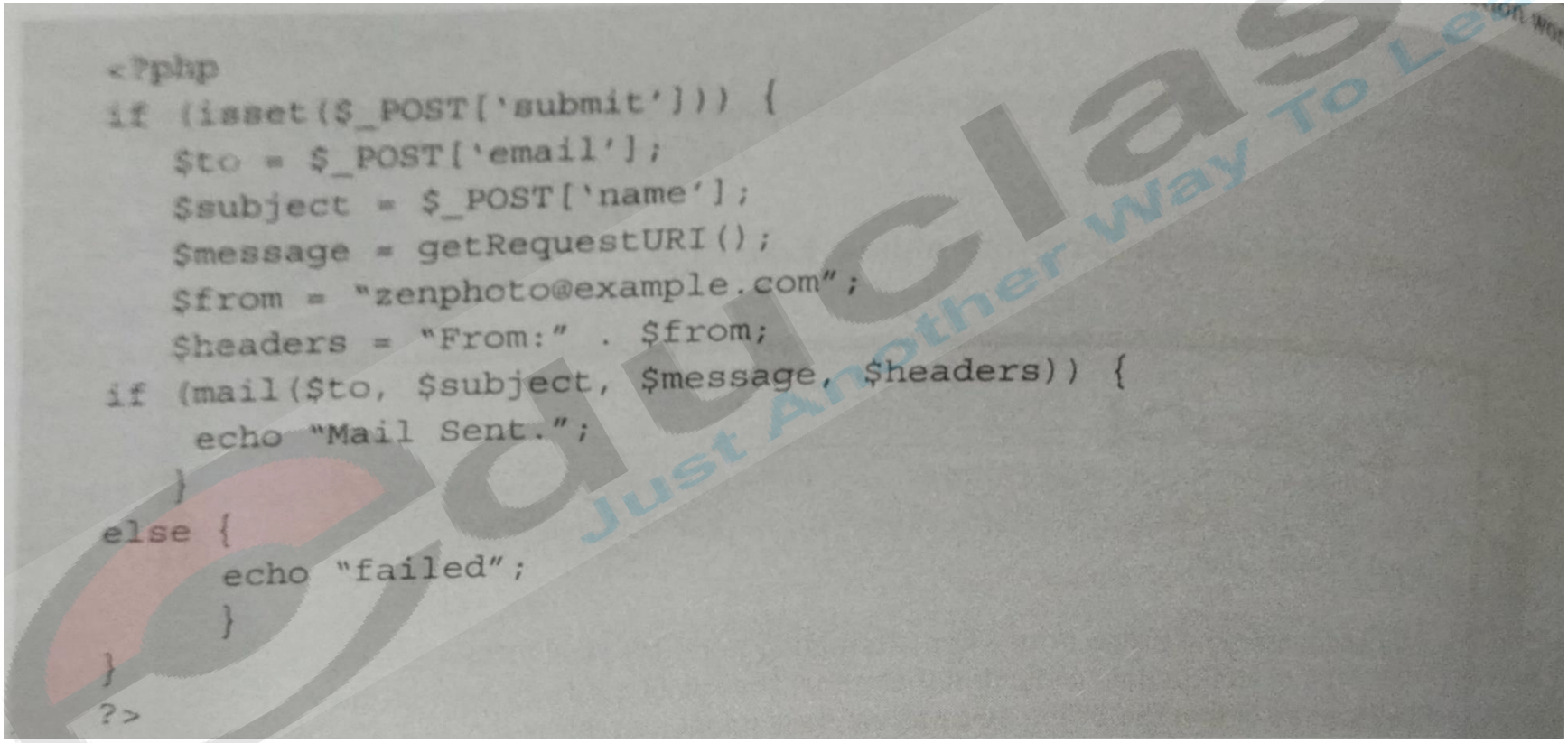
gure 12.3 Hacking Gmail account password online: Fake Page.



How can I Protect Myself from Being Spoofed?

- USE your spam filter
- Never click an unexpected link or download an unfamiliar attachment.
- Learn to read email message header and check domain names and IP addresses
- Spotting spoofed messages.
- PHP mail sending Script

PHP mail sending Script

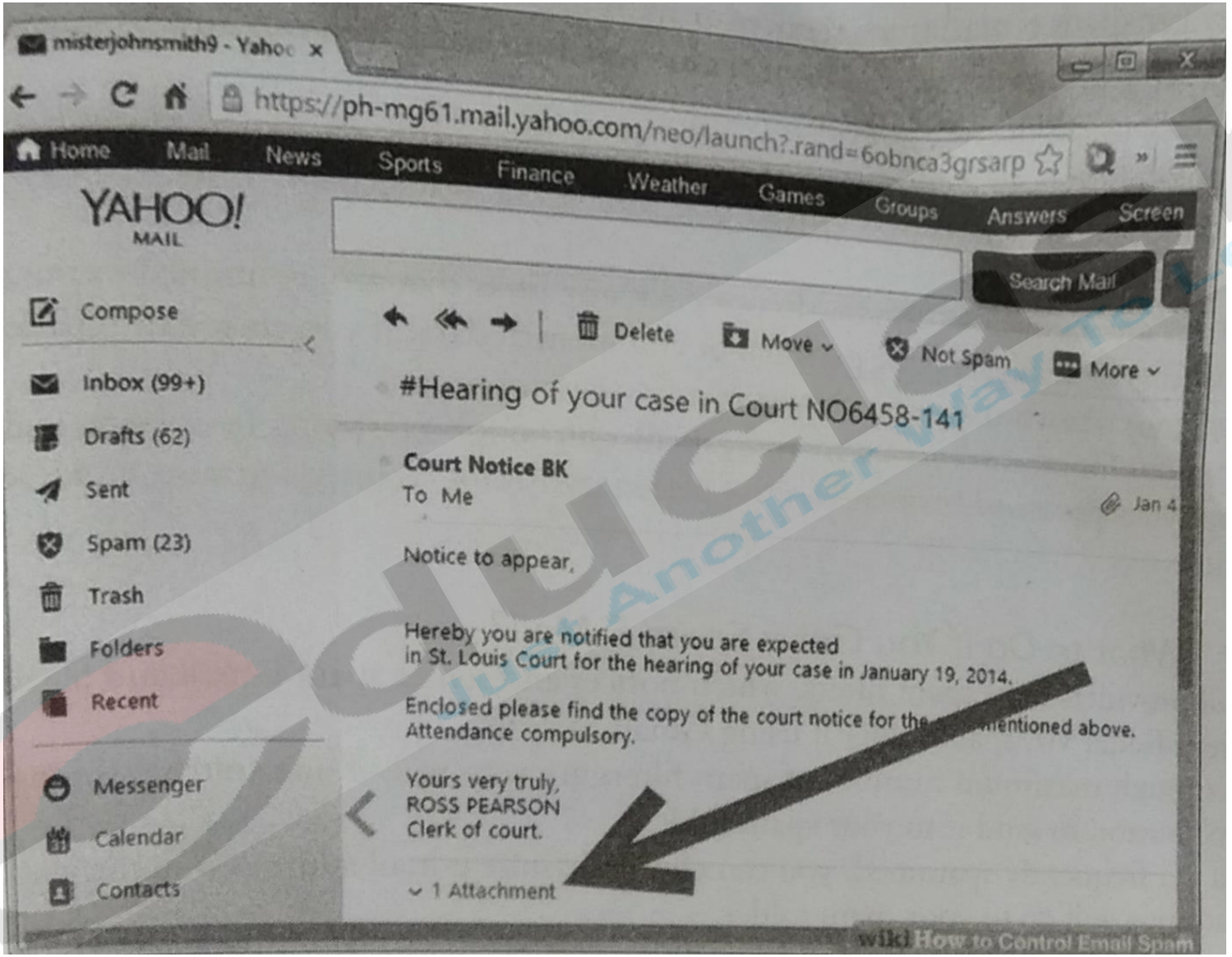


```
<?php
if (isset($_POST['submit'])) {
    $to = $_POST['email'];
    $subject = $_POST['name'];
    $message = getRequestURI();
    $from = "zenphoto@example.com";
    $headers = "From:" . $from;
if (mail($to, $subject, $message, $headers)) {
     echo "Mail Sent.";
    }
else {
        echo "failed";
        }
}
?>
```

Email Spamming

- Email spamming is a type of bombing. It generally refers to sending email to multiple user. This can become worse if the user respond back to this kind of email, which in turn make them the victim for the same.
- Spam email is a type of commercial advertising which is cost efficient and feasible, because email is very cost effective medium for the sender. The spammer are making money without any effort and the spam problem is successful as they have made money and earned lots of profit from it.
- Spammer collect the recipient address from the publicly available and hack able or accessible sources using programs or spider to collect the email address over the web and make use of dictionaries to make the automated assumptions at the common and simple usernames at a given website.

- Spamming is a topic of debate for political reasons in several countries. Hacker often forge the original source of message, ISPs rules and regulation and snit spammer lists which are used by the anti spam software.
- Developing spam fighting tools are on the increase and are very useful and important for the end user of any email service user.
- Spam is spreading over the internet like virus with multiple copies of the same data or message. Cost of sending the spam is minimal, but the maximum cost of such spam is paid by the user who become the victim of the such scam.
- Spam is divided into two main types and each of them have different effect on the user who use internet. Cancellable Usenet spam is the one and only message which is sent to 20 or more Usenet newsgroup. Usenet spam steals the user who are of use in the newsgroup by the burdening them with a load of advertising or the other spam posts.
- Email spam select their target or victim with sending direct email or messages. The spam list for the sending email is often developed by referring to the Usenet posting obtaining the internet mailing lists or searching over the internet for email address.



Email Tracing

- Tracing an email means locating the original sending and getting to know the IP address of the network from which the email was actually generated.
- To get the information about the sender of the email we must first know the structure of the email.
- We all are aware how email travel from one end to the other. Each message has exactly one header, which is structured into fields.
- Each field has a name and a value. Header of the email contains all the valuable information about the path and the original sender of the email.

Why would you want to find out the identity of the sender? Well, you may have heard of shady e-mail scams or e-mails supposedly from PayPal inviting you to reenter your personal information. Now, you can determine if an e-mail is truly from the authentic source.

Accessing the e-mail header is different for every e-mail provider or e-mail application, and sometimes it is even hidden. In most of the cases, however, the option to reveal the full header will be somewhere in the area where the subject and sender name are provided.

Any individual can trace an e-mail from where it is received. Figure 12.6 shows how we can trace the header in the browser.

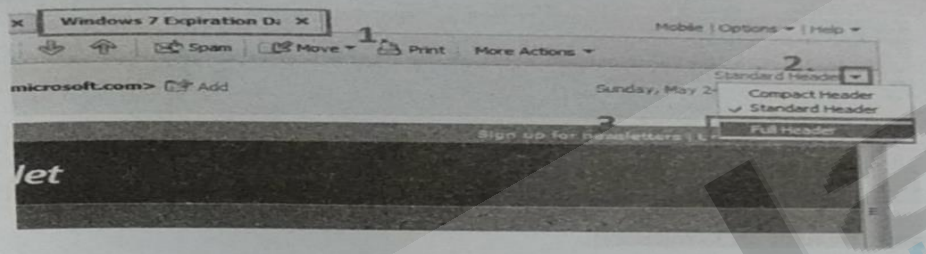


Figure 12.6 Example of e-mail header tracing.

For example, the Yahoo Mail header is in the upper right corner of the sender box. When you click Show Original, a text file will open in a new tab. This file contains all the necessary headers at the start. Figure 12.7 represents the full e-mail header information that appears in Yahoo Mail.

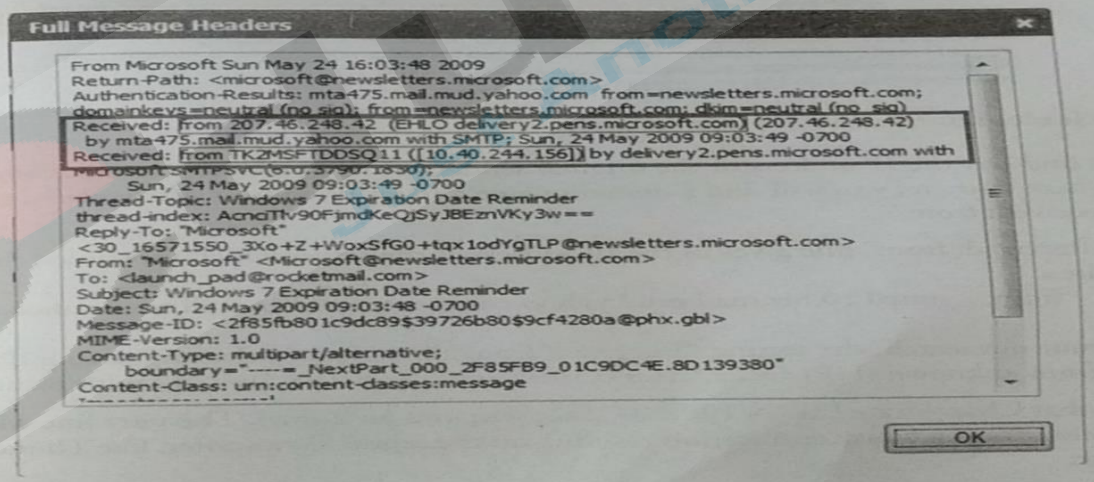
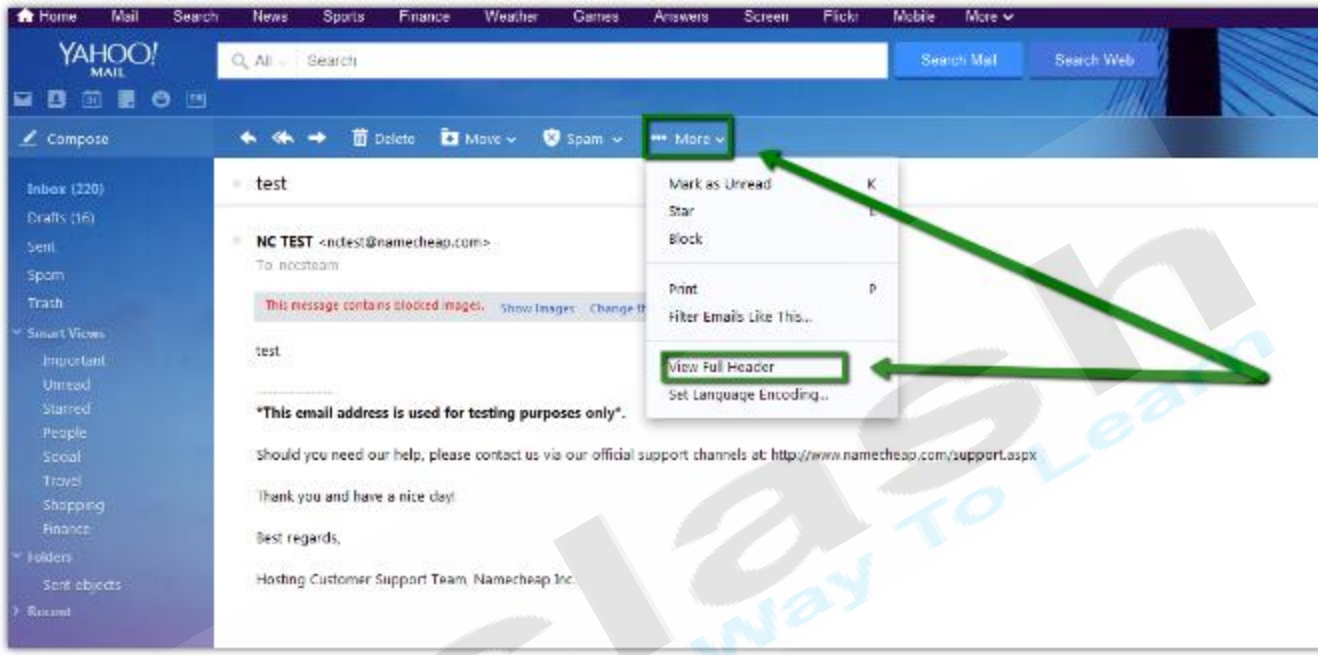


Figure 12.7 Full e-mail header in Yahoo mail.



Full Message Headers

```
From Microsoft Sun May 24 16:03:48 2009
Return-Path: <microsoft@newsletters.microsoft.com>
Authentication-Results: mta475.mail.mud.yahoo.com  from=newsletters.microsoft.com;
domainkeys=neutral (no sig); from=newsletters.microsoft.com; dkim=neutral (no sig)
Received: from 207.46.248.42  (EHLO delivery2.pens.microsoft.com) (207.46.248.42)
  by mta475.mail.mud.yahoo.com with SMTP; Sun, 24 May 2009 09:03:49 -0700
Received: from TK2MSFTDDSQ11 ([10.40.244.156]) by delivery2.pens.microsoft.com with
Microsoft SMTPSVC(6.0.3790.1830);
       Sun, 24 May 2009 09:03:49 -0700
Thread-Topic: Windows 7 Expiration Date Reminder
thread-index: AcncTlv90FjmdKeQjSyJBEznVKy3w==
Reply-To: "Microsoft"
<30_16571550_3Xo+Z+WoxSfG0+tqx1odYgTLP@newsletters.microsoft.com>
From: "Microsoft" <Microsoft@newsletters.microsoft.com>
To: <launch_pad@rocketmail.com>
Subject: Windows 7 Expiration Date Reminder
Date: Sun, 24 May 2009 09:03:48 -0700
Message-ID: <2f85fb801c9dc89$39726b80$9cf4280a@phx.gbl>
MIME-Version: 1.0
Content-Type: multipart/alternative;
     boundary="----=_NextPart_000_2F85FB9_01C9DC4E.8D139380"
Content-Class: urn:content-classes:message
```

OK

For Gmail, the header is hidden under "Show Original" which shows you the complete e-mail in plain text, including the header (Figure 12.8).

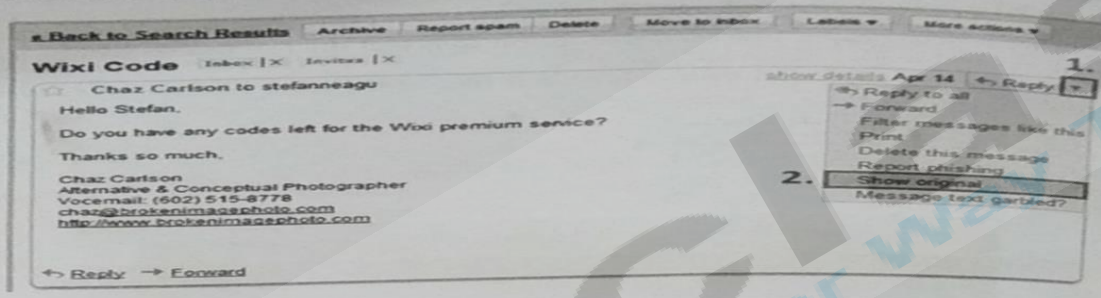


Figure 12.8 Full e-mail header in Gmail.

The example in Figure 12.9 is the header from an e-mail received in Gmail.

```
Return-Path: <chaz@brokenimagephoto.com>
Received: from smtp110.biz.mail.mud.yahoo.com (smtp110.biz.mail.mud.yahoo.com
    by mx.google.com with SMTP id 27s112052374gxk.26.2009.04.14.03.42.27;
    Tue, 14 Apr 2009 03:42:27 -0700 (PDT)
Received-SPF: neutral (google.com: 68.142.201.179 is neither permitted nor der
Authentication-Results: mx.google.com; spf=neutral (google.com: 68.142.201.179
Received: (qmail 13418 invoked from network); 14 Apr 2009 10:42:26 -0000
Received: from unknown (HELO ?192.168.0.100?) (chaz@68.108.204.242 with plain)
    by smtp110.biz.mail.mud.yahoo.com with SMTP; 14 Apr 2009 10:42:26 -0000
X-Yahoo-SMTP: 1Ert9wOswDA8qqQ3AQWQTdj17xIWn_kcCMaCBHvJJP2sgwpO4eQ-
X-YMail-OSG: 4m835uoVM1mNGeuKro04OMGE_PRCan1ZIUrOOqKvYF1KZI7J10B_GbRnFD14ERy7c
X-Yahoo-Newman-Property: ymail-3
MIME-Version: 1.0 (Apple Message framework v753.1)
```

Figure 12.9 Header information in Gmail account.

In order to find out the IP address of the original sender, we need to look closely at the first half of the header. Somewhere in there, you will find a domain name and an IP address. Particularly, take a closer look at the term "Received: from":

1. The first "Received: from" line gives us the IP address of the server which forwarded the e-mail to your Gmail address.
2. Received: from smtp110.biz.mail.mud.yahoo.com(smtp110.biz.mail.mud.yahoo.com [68.142.201.179]).
3. If we continue our search, the second "Received: from" line gives us the originating IP address.
4. Received: from unknown (HELO?192.168.0.100?) (chaz@68.108.204.242 with plain).

This means that Chaz, located at 68.108.204.242, sent you an e-mail. The next line will only appear if the e-mail was sent using an e-mail application residing on the sender's computer, like Thunderbird or Apple Mail. In our case:

X-Mailer: Apple Mail (2.753.1)

Keystroke Logger

- Keystroke logger captures the target keystroke and either save them in a file to be read or mentioned later, or communicate them to a prearranged end point available to the hacker.
- Since Keystroke logging program record every single keystroke keyed in through the keyboard they can capture a widespread diversity of private information together with password, credit card number and set apart email communication , name, address and phone number

How can keystroke Logger Harm?

- It can be used by your rival or colleague to get sensitive information like your username and code word, bank credit card details, or any other action you do on your workstation.
- For example you login in to your FB account from a computer in which the key logger is setup then your username and password will be taken.

Types of Key logger

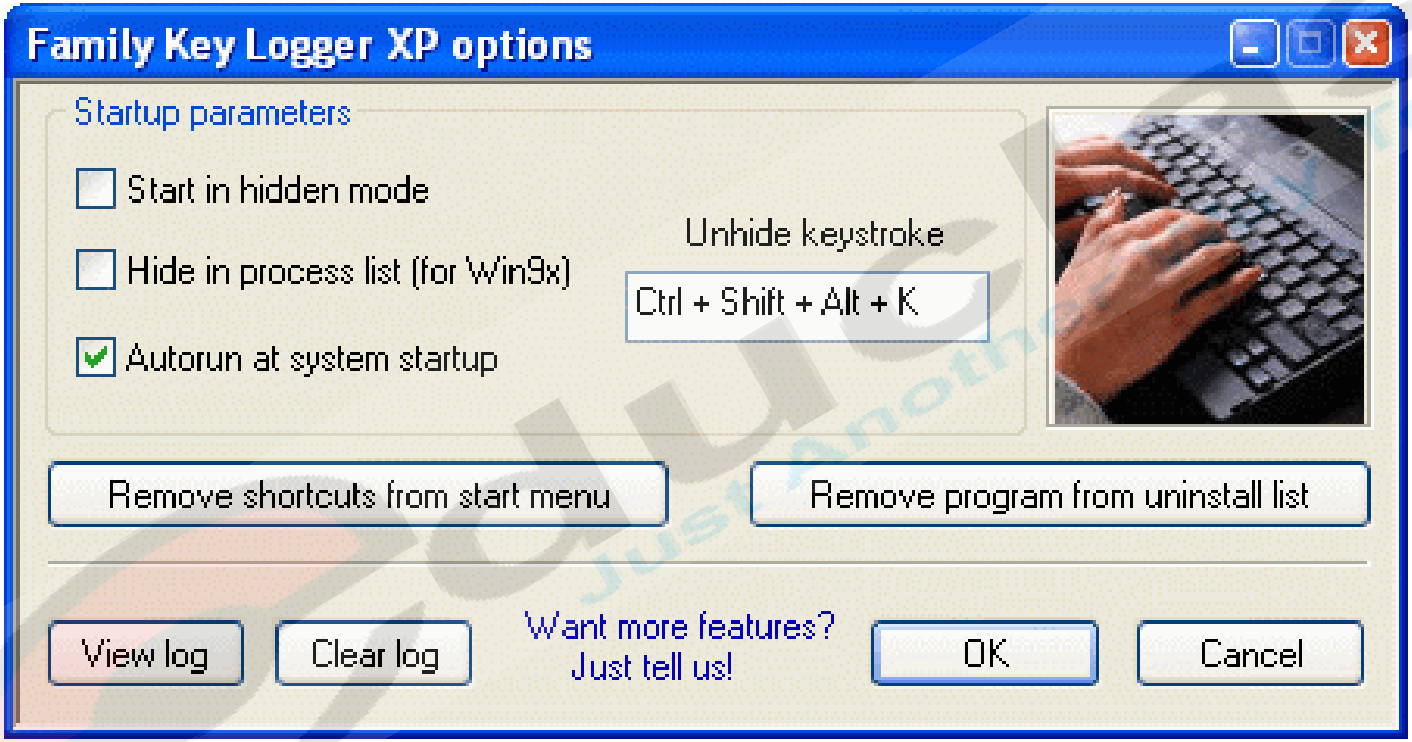
1.Hardware Key logger

- It is a hardware based spy that monitor the keyboard keys pressed by a user and then records the input data secretly. It need no installation as it is already within the physical system on a computer.
- A type of key logger is acoustic key logger which records the sound of the keys pressed by a user.
- As each sound is unique it is possible to predict which key it is.

Types of Key logger

2.Software Keylogger

- It is essential program that monitors a computer OS .
- It can be memory injection software which is typical Trojan virus that alter the memory tablet of a system in order to bypass online security.
- Another type is form grabbing based software which controls the form submitted online and essentially tracks all the information a user puts in any form including all the personal details.



Various Key logger names

- Award Keylogger Pro3.2
- Ultimate Keylogger free
- Black Box security monitor
- Refog free keylogger
- Super Winspy
- Pykey logger
- Personal keylogger
- Koom Keylogger

Securing Your Email Account

- Use a strong Password
- Beware of public PCs
- Protect your address
- Lock it up
- Do not be fooled
- Use Encryption

1. **Use a Strong Password.** You give out your email address all the time; it's not really private information. That being the case, the only thing protecting your account from misuse is the password. A malefactor who guesses your too-weak password gains full control of your email account. Protect your account with a **strong password**, especially if you use a Web-based email provider like Gmail or Yahoo mail.
2. **Beware Public PCs.** If you check your email on a public computer in a library or Internet café, be absolutely sure you've logged out before leaving. Even then, you might be leaving behind traces that could give the next user too much information about you. Follow PCMag's advice to **Use Public Computers Safely**.
3. **Protect Your Address.** It's true that you give out your email address every time you send a message, but there's no need to give it to the whole world. Don't include your email address in comments on blog posts, or in social media posts. Spammers and scammers scrape pages all the time looking for new victims.
4. **Lock It Up.** If you step away from your desk, lock the Windows desktop or close your email client. Otherwise a sneaky co-worker could read your mail or even reset your login password. Hold the Windows key and press L to lock the desktop instantly.
5. **Don't Be Fooled.** Oh, dear. Your email provider has sent you notification of a security breach, with a link to reset your password. Don't click that link! It's almost certainly a fraud, designed to steal your email account password. If you have any doubts, navigate to the email provider's site directly and double-check.
6. **Use Encryption.** Sometimes you just have to send sensitive information by email. To keep your data safe, save it as a document and use your word processing application's built-in encryption, or store the document in an encrypted ZIP file. Then share the password with the recipient separately. If you need encryption frequently, try a free email encryption product like **PrivateSky**or **Enlocked**.

Email Recovery

- Check the trash section
- Search your Inbox
- Check any folder or labels you have created
- Check your archived message in Gmail
- Contact the email services
- Check the trash and other location
- Check the web services that your client connect to
- Recover deleted messages in outlook
- Check with the server administrator

E-mail Forensic Analysis steps

- E-mail forensics refers to the study of source and content of e-mail as evidence to identify the actual sender and recipient of a message, data/time of transmission, detailed record of e-mail transaction, intent of the sender, etc.
- It involves investigation of metadata, keyword searching, port scanning, etc. for authorship attribution and identification of e-mail scams.

1. Header analysis:

   Meta data in the e-mail message in the form of control information i.e. envelope and headers including headers in the message body contain information about the sender and/or the path along which the message has traversed. Some of these may be spoofed to conceal the identity of the sender. A detailed analysis of these headers and their correlation is performed in header analysis.

2. 5.2. Bait Tactics In bait tactic investigation an e-mail with http: “” tag having image source at some computer monitored by the investigators is send to the sender of e-mail under investigation containing real (genuine) e-mail address. When the e-mail is opened, a log entry containing the IP address of the recipient (sender of the e-mail under investigation) is recorded on the http server hosting the image and thus sender is tracked. However, if the recipient (sender of the email under investigation) is using a proxy server then IP address of the proxy server is recorded. The log on proxy server can be used to track the sender of the e-mail under investigation. If the proxy server’s log is unavailable due to some reason, then investigators may send the tactic email containing a) Embedded Java Applet that runs on receiver’s computer or b) HTML page with Active X Object. Both aiming to extract IP address of the receiver’s computer and e-mail it to the investigators. 5.3. Server Investigation In this investigation, copies of delivered e-mails and server logs are investigated to identify source of an e-mail message. E-mails purged from the clients (senders or receivers) whose recovery is impossible may be requested from servers (Proxy or ISP) as most of them store a copy of all e-mails after their deliveries. Further, logs maintained by servers can be studied to

- trace the address of the computer responsible for making the e-mail transaction. However, servers store the copies of e-mail and server logs only for some limited periods and some may not co-operate with the investigators. Further, SMTP servers which store data like credit card number and other data pertaining to owner of a mailbox can be used to identify person behind an e-mail address. 5.4. Network Device Investigation In this form of e-mail investigation, logs maintained by the network devices such as routers, firewalls and switches are used to investigate the source of an e-mail message. This form of investigation is complex and is used only when the logs of servers (Proxy or ISP) are unavailable due to some reason, e.g. when ISP or proxy does not maintain a log or lack of cooperation by ISP's or failure to maintain chain of evidence. 5.5. Software Embedded Identifiers Some information about the creator of e-mail, attached files or documents may be included with the message by the e-mail software used by the sender for composing e-mail. This information may be included in the form of custom headers or in the form of MIME content as a Transport Neutral Encapsulation Format (TNEF). Investigating the e-mail for these details may reveal some vital information about the senders e-mail preferences and options that could help client side evidence gathering. The investigation can reveal PST file names, Windows logon username, MAC address, etc. of the client computer used to send e-mail message. 5.6. Sender Mailer Fingerprints Identification of software handling e-mail at server can be revealed from the Received header field and identification of software handling e-mail at client can be ascertained by using different set of headers like "X-Mailer" or equivalent. These headers describe applications and their versions used at the clients to send e-mail. This information about the client computer of the sender can be used to help investigators devise an effective plan and thus prove to be very useful