



Computer Hacking Forensic Investigator (CHFI)

Introduction

Introductions



- Name
- Company Affiliation
- Title / Function
- Job Responsibility
- System security related experience
- Expectations

Course Materials



- Identity Card
- Student Courseware
- Lab Manual/Workbook
- CHFI Lab Files
- Knoppix CD-ROM
- Course Evaluation
- Reference Materials

Course Outline

- **Module I:** Computer Forensics in Today's World
- **Module II:** Law And Computer Forensics
- **Module III:** Computer Investigation Process
- **Module IV:** Computer Security Incident Response Team
- **Module V:** Computer Forensic Laboratory Requirements
- **Module VI:** Understanding File systems and Hard disks
- **Module VII:** Windows Forensics

Course Outline (contd.)

- **Module VIII:** Linux and Macintosh Boot processes
- **Module IX:** Linux Forensics
- **Module XX:** Data Acquisition and Duplication
- **Module XI:** Recovering Deleted Files
- **Module XII:** Image Files Forensics
- **Module XIII:** Steganography
- **Module XIV:** Computer Forensic Tools

Course Outline (contd.)

- **Module XV:** Application password crackers
- **Module XVI:** Investigating Logs
- **Module XVII:** Investigating network traffic
- **Module XVIII:** Router Forensics
- **Module XIX:** Investigating Web Attacks
- **Module XX:** Tracking E-mails and Investigating E-mail crimes

Course Outline (contd.)

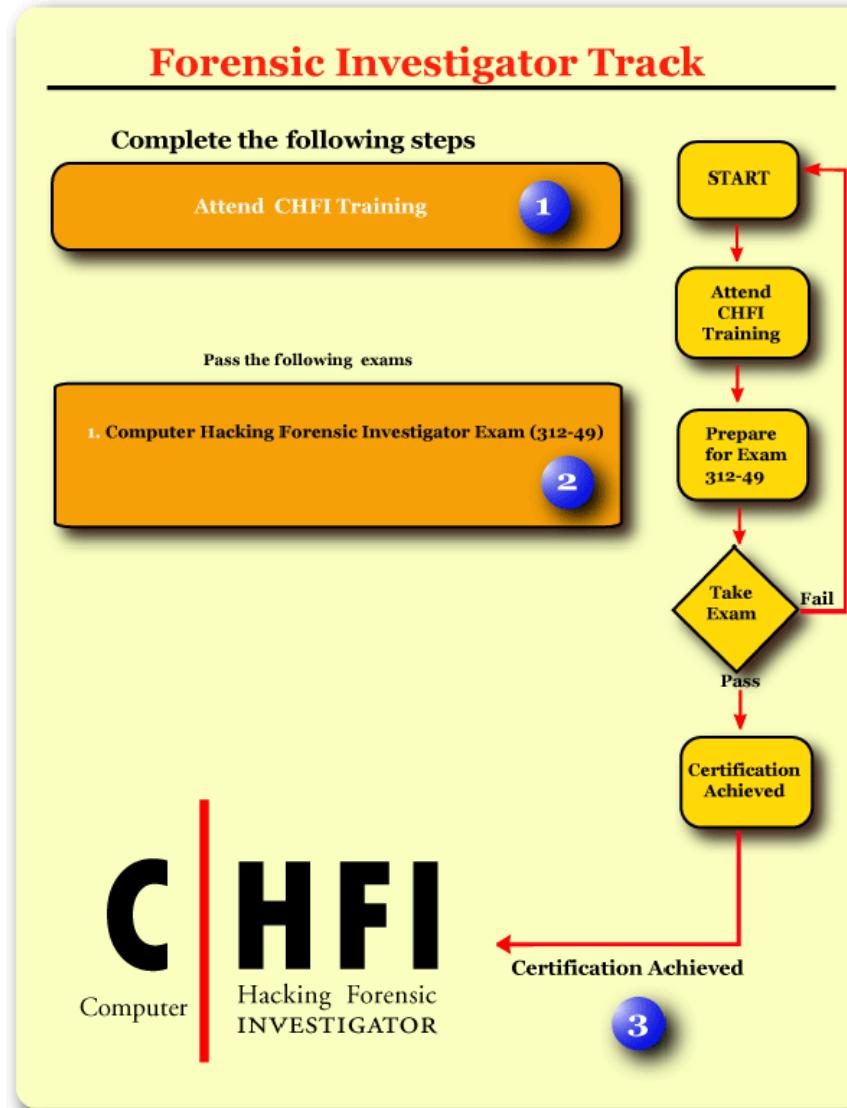
- **Module XXI:** Mobile and PDA Forensics
- **Module XXII:** Investigating Trademark and Copyright Infringement
- **Module XXIII:** Investigative Reports
- **Module XIV:** Becoming an Expert Witness
- **Module XXV:** Forensics in action

EC-Council Certified e- business Certification Program

There are several levels of certification tracks under **EC-Council** Accreditation body:

1. Certified e-Business Associate
2. Certified e-Business Professional
3. Certified e-Business Consultant
4. E++ Certified Technical Consultant
5. Certified Ethical Hacker (CEH)
6. **Computer Hacking Forensic Investigator (CHFI) ← You are here**
7. EC-Council Certified Security Analyst (ECSA)
8. EC-Council Certified Secure Programmer (ECSA)
9. Certified Secure Application Developer (CSAD)
10. Licensed Penetration Tester (LPT)
11. Master of Security Science (MSS)

EC-Council CHFI Exam

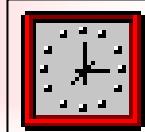


Student Facilities

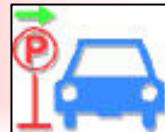
Class Hours



Building Hours



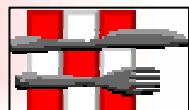
Parking



Restrooms



Meals



Phones



Messages



Smoking



Recycling



Lab Sessions



- Lab Sessions are designed to reinforce the classroom sessions
- The sessions are intended to give a hands on experience only and does not guarantee proficiency.



Computer Hacking Forensics Investigator

Module I

Computer Forensics in
Today's World

Scenario

Steven is the managing director of a respected software company. After finding pornography downloaded on his network server and a number of individual office computers, he decided to hire a computer forensics investigator to build a case for employee dismissal.

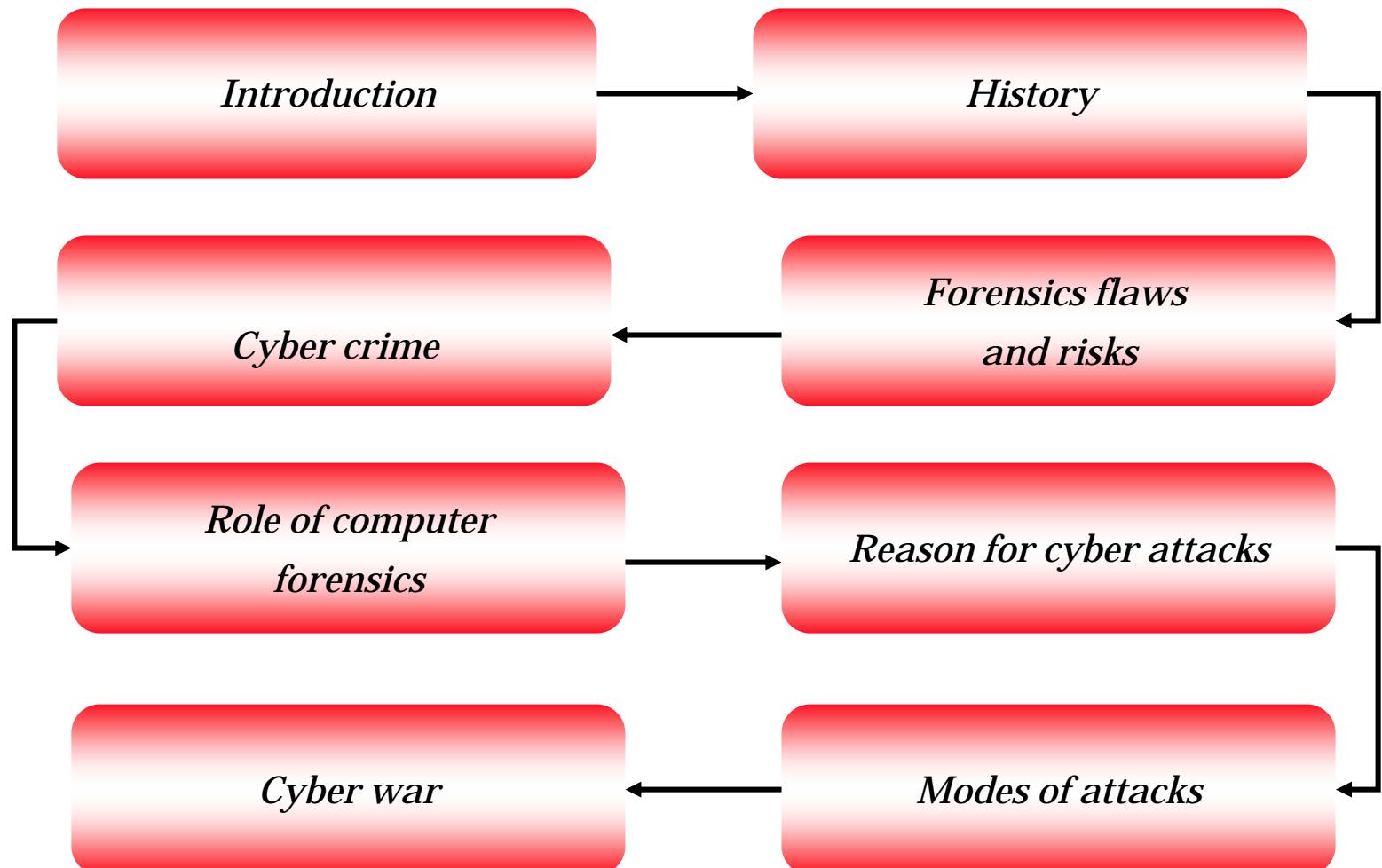
The Investigator was hired to locate deleted files if any and verify certain non-work related contents of the hard drives in question. The investigator was able to locate spy software, pornography, illegal file-sharing software from the hard drive of the suspicious employee. This led to employee dismissal.



Module Objective

- Introduction to computer forensics
- History of computer forensics
- Computer forensics flaws and risks
- Cyber crime
- Role of computer forensics
- Reason for cyber attacks
- Modes of attacks
- Cyber war

Module Flow



Introduction

- ◉ Cyber activity has become an important part of everyday life of the general public
- ◉ Importance of computer forensics:
 - 85% of business and government agencies detected security breaches
 - FBI estimates that the United States loses up to \$10 billion a year to cyber crime



History of Forensics

◎ Francis Galton (1822-1911)

- Made the first recorded study of fingerprints

◎ Leone Lattes (1887-1954)

- Discovered blood groupings (A,B,AB, & O)

◎ Calvin Goddard (1891-1955)

- Allowed Firearms and bullet comparison for solving many pending court cases

◎ Albert Osborn (1858-1946)

- Developed essential features of document examination

◎ Hans Gross (1847-1915)

- Made use of scientific study to head criminal investigations

◎ FBI (1932)

- A Lab was set up to provide forensic services to all field agents and other law authorities throughout the country



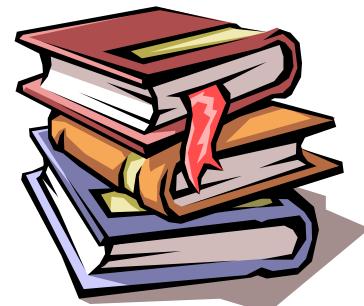
Definition of Forensic Science

Definition:

- “*Application of physical sciences to law in the search for truth in civil, criminal and social behavioral matters to the end that injustice shall not be done to any member of society*”

(Source: Handbook of Forensic Pathology College of American Pathologists 1990)

- *Aim: determining the evidential value of crime scene and related evidence*



Definition of Computer Forensics

Definition:

“A methodical series of techniques and procedures for gathering evidence, from computing equipment and various storage devices and digital media, that can be presented in a court of law in a coherent and meaningful format”

- Dr. H.B. Wolfe



What Is Computer Forensics?

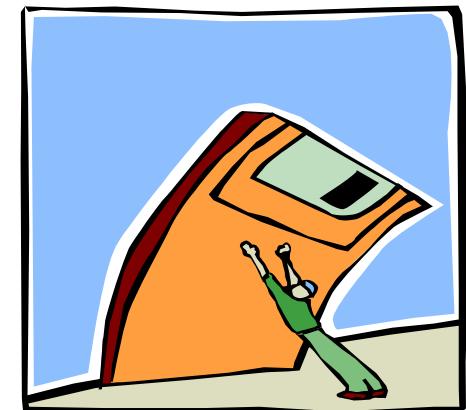
- According to Steve Hailey, Cybersecurity Institute

“The preservation, identification, extraction, interpretation, and documentation of computer evidence, to include the rules of evidence, legal processes, integrity of evidence, factual reporting of the information found, and providing expert opinion in a court of law or other legal and/or administrative proceeding as to what was found.”



Need for Computer Forensics

- ◉ “*Computer forensics is equivalent of surveying a crime scene or performing an autopsy on a victim*”.
{Source: James Borek 2001}
- ◉ Presence of a majority of electronic documents nowadays
- ◉ Search and identify data in a computer
- ◉ Digital Evidence is delicate in nature
- ◉ For recovering
 - Deleted,
 - Encrypted or,
 - Corrupted files from a system



Evolution of Computer Forensics

- 1984 - FBI Computer Analysis and Response Team (CART) emerged
- 1991 - International Law Enforcement meeting was conducted to discuss computer forensics & the need for standardized approach
- 1997 - Scientific Working Group on Digital Evidence (SWGDE) was established to develop standards
- 2001 - Digital Forensic Research Workshop (DFRWS) was held
 - <http://www.dfrws.org/>



Computer Forensics Flaws and Risks

- Computer forensics is in its early or development stages
- It is different from other forensic sciences as digital evidence is examined
- There is a little theoretical knowledge based up on which empirical hypothesis testing is done
- Designations are not entirely professional
- There is a lack of proper training
- There is no standardization of tools
- It is still more of an “Art” than a “Science”



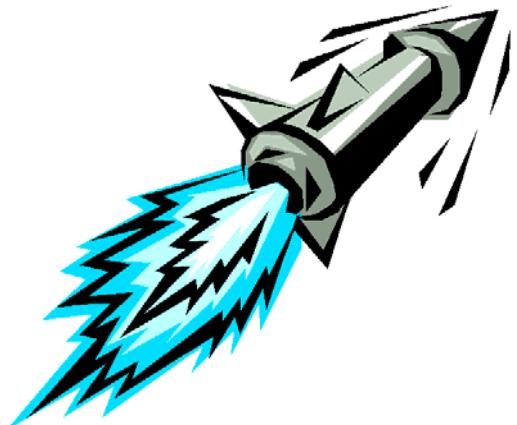
Corporate Espionage Statistics

- Corporate computer security budgets increased at an average of 48% in 2002
- 62% of the corporate companies had their systems compromised by virus
- FBI statistics reveal that more than 100 nations are engaged in corporate espionage against US companies
- More than 2230 documented incidents of corporate espionage by the year 2003



Modes of Attacks

- ◉ Cyber crime falls into two categories depending on the ways attack take place
- ◉ Following are the two types of attacks
 - 1.Insider Attacks
 - 2.External Attacks



Cyber Crime

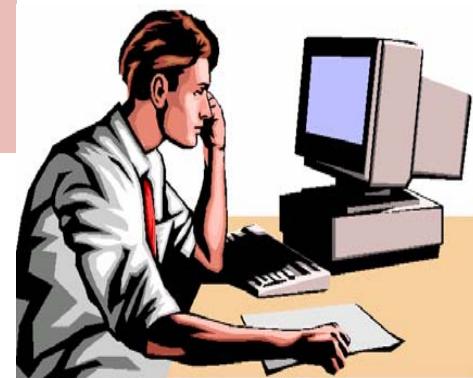
- Cyber crime is defined as
“Any illegal act involving a computer, its systems, or its applications”
- The crime must be intentional and not accidental.
- Cyber crime is divided into 3 T's
 - Tools of the crime
 - Target of the crime
 - Tangential to the crime



Examples of Cyber Crime

⦿ A few examples of cyber crime include:

- Theft of intellectual property
- Damage of company service networks
- Financial fraud
- Hacker system penetrations
- Denial of Service Attacks
- Planting of virus and worms



Reason for Cyber Attacks

- Motivation for cyber attacks
 - 1. Experimentation and a desire for script kiddies to learn
 - 2. Psychological needs
 - 3. Misguided trust in other individuals
 - 4. Revenge and malicious reasons
 - 5. Desire to embarrass the target
 - 6. Espionage - corporate and governmental



Role of Computer Forensics in Tracking Cyber Criminals

- Identifying the crime
- Gathering the evidence
- Building a chain of custody
- Analyzing the evidence
- Presenting the evidence
- Testifying
- Prosecution



Rules of Computer Forensics

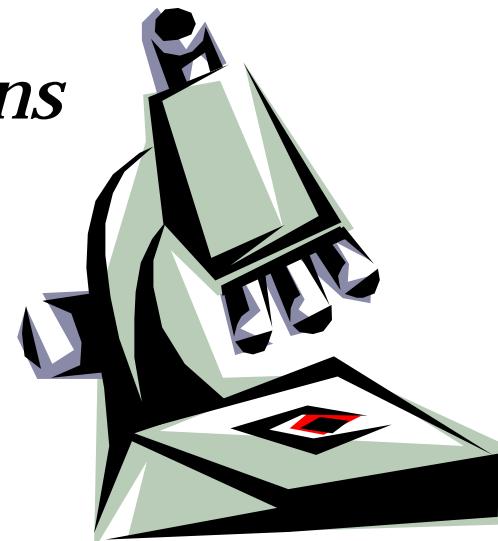
- ◉ Minimize the option of examining the original evidence
- ◉ Obey rules of evidence
- ◉ Never exceed the knowledge base
- ◉ Document any changes in evidence



Computer Forensics Methodologies

The 3 A's

- **Acquire** *evidence without modification or corruption*
- **Authenticate** *that the recovered evidence is same as the originally seized data*
- **Analyze** *data without any alterations*



Accessing Computer Forensics Resources

- Resources can be referred by joining various discussion groups such as:
 - Computer Technology Investigators Northwest
 - High Technology Crime Investigation Association
- Joining a network of computer forensic experts and other professionals
- News services devoted to computer forensics can also be a powerful resource
- Other resources:
 - Journals of forensic investigators
 - Actual case studies



Preparing for Computing Investigations

- Computing investigations fall under two distinct categories:
 1. Public Investigation
 2. Corporate Investigation



Maintaining professional conduct

- ◉ Professional conduct determines the credibility of a forensic investigator
- ◉ Investigators must display the highest level of ethics and moral integrity
- ◉ Confidentiality is an essential feature which all forensic investigators must display
- ◉ Discuss the case at hand only with person who has the right to know



Understanding Enforcement Agency Investigations

Enforcement agency investigations include:

1. Tools used to commit the crime
2. Reason for the crime
3. Type of crime
4. Infringement on someone else's rights by cyberstalking



Understanding Corporate Investigations

- Involve private companies who address company policy violations and litigation disputes
- Company procedures should continue without any interruption from the investigation
- After the investigation the company should minimize or eliminate similar litigations
- Industrial espionage is the foremost crime in corporate investigations



Investigation Process

○ Identification

- Detecting/identifying the event/crime.

○ Preservation

- Chain of Evidence, Documentation.

○ Collection

- Data recovery, evidence collection.

○ Examination

- Tracing, Filtering, Extracting hidden data.

○ Analysis

- Analyzing evidence

○ Presentation

- Investigation report, Expert witness

○ Decision

- Report



Digital Forensics

The use of scientifically unexpressed and proven methods towards the

- Preserving
- Collecting
- Confirming
- Identifying
- Analyzing
- Recording
- Presenting

A diagram illustrating the process of digital forensics. On the left, a vertical list of seven steps is enclosed in a pink-bordered box. A horizontal arrow points from the bottom right of this box to a red oval on the right. The oval contains the text "Digital evidence extracted from digital sources".

Digital evidence extracted
from digital sources

Summary

- The need for computer forensics has grown to a large extent due to the presence of a majority of digital documents
- A computer can be used as a tool for investigation or as evidence
- Minimize the option of examining the original evidence
- 3A's of Computer forensics methodologies are – Acquire, Authenticate, and Analyze
- A computer forensic investigator must be aware of the steps involved in the investigative process



Computer Hacking Forensic Investigator

Module II
**Law And Computer
Forensics**

Scenario

United States Secret Service

WWW.SECRETSERVICE.GOV



SHADOWCREW

"FOR THOSE WHO WISH TO PLAY IN THE SHADOWS....."



ACTIVITIES BY SHADOWCREW MEMBERS ARE BEING INVESTIGATED BY THE

UNITED STATES SECRET SERVICE

SEVERAL ARRESTS HAVE RECENTLY BEEN MADE...WITH MANY MORE TO FOLLOW.

Proxies, VPNs, IP Spoofing, Encryption, etc.... You Are No Longer Anonymous!!

SHADOWCREW TOPICS

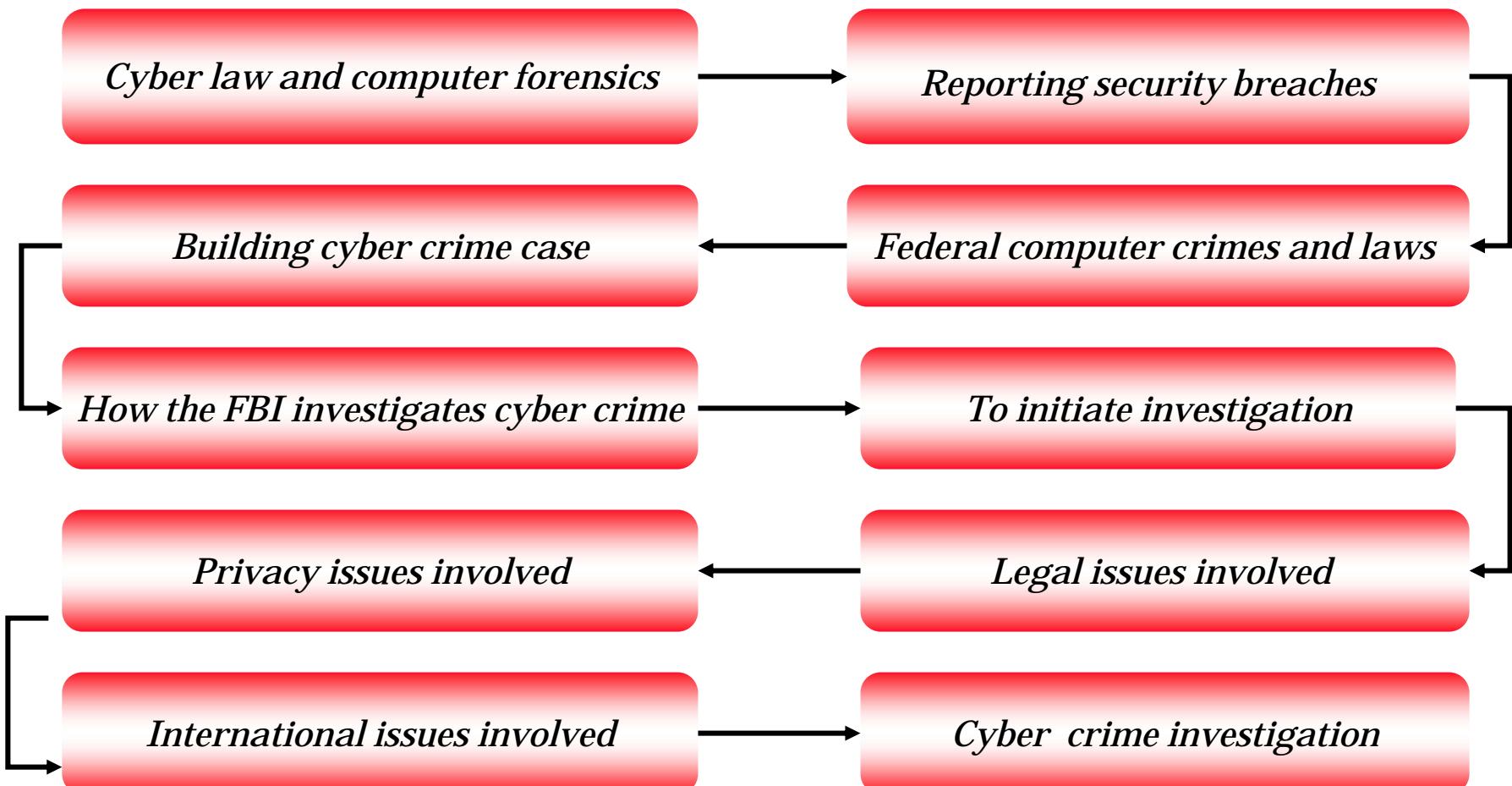
SHADOWCREW MEMBERS ARE FACING THE FOLLOWING CHARGES (*Charges are Not Limited to Below):

- TITLE 18 USC 371 - CONSPIRACY
- TITLE 18 USC 1029 - ACCESS DEVICE FRAUD
- TITLE 18 USC 1028 - FRAUD W/IDENTITY DOCUMENTS, IDENTITY THEFT, ETC.
- TITLE 18 USC 1030 - FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Module Objectives

- Introduction to cyber law and computer forensics
- Reporting security breaches to law enforcement
- Federal computer crimes and laws
- Building the cyber crime case
- How the FBI investigates computer crime
- To initiate an investigation
- Legal issues involved in seizure of computer equipments.
- Privacy issues regarding computer forensics.
- International issues related to computer forensics
- Cyber crime investigations

Module Flow



What Is Cyber Crime?

- Crime directed against a computer
- Crime where the computer contains evidence
- Crime where the computer is used as a tool to commit the crime

“Any crime in which computer-related technology is encountered.”



What Is Computer Forensics ?

- Discipline using predefined procedures to thoroughly examine a computer system to extract the evidence

- Methodology:

- Acquire
- Authenticate
- Analyze



Computer Facilitated Crimes

- Dependency on computer has given way to new criminal opportunities
- Computer is used as a tool for committing crimes
- Computer crimes are posing new challenges for investigators due to the following reasons:
 - Speed
 - Anonymity
 - Fleeting nature of evidence



Reporting Security Breaches to Law Enforcement - A

Type of crime	Appropriate federal investigative Law Agencies
Computer intrusion (i.e. hacking)	<ul style="list-style-type: none">◉ FBI local office◉ U.S. Secret Service◉ Internet Fraud Complaint Center
Password trafficking	<ul style="list-style-type: none">◉ FBI local office◉ U.S. Secret Service◉ Internet Fraud Complaint Center

Reporting Security Breaches to Law Enforcement - B

Internet fraud and SPAM	<ul style="list-style-type: none">○ FBI local office○ U.S. Secret Service (Financial Crimes Division)○ Federal Trade Commission (online complaint)○ Securities and Exchange Commission (online complaint)○ The Internet Fraud Complaint Center
Internet harassment	<ul style="list-style-type: none">○ FBI local office

Reporting Security Breaches to Law Enforcement - C

Child Pornography or Exploitation	<ul style="list-style-type: none">◉ FBI local office◉ U.S. Customs and Border Patrol Protection local office◉ Internet Fraud Complaint Center
Copyright (software, movie, sound recording) piracy	<ul style="list-style-type: none">◉ FBI local office◉ If imported, U.S. Customs and Border Patrol Protection local Office◉ Internet Fraud Complaint Center

Reporting Security Breaches to Law Enforcement - D

Theft of trade secrets	Ⓐ FBI local office
Trademark counterfeiting	Ⓐ FBI local office Ⓐ If imported, U.S. Customs and Border Patrol Protection local office Ⓐ Internet Fraud Complaint Center
Trafficking in explosive or incendiary devices or firearms over the Internet	Ⓐ FBI local office Ⓐ ATF local office

National Infrastructure Protection Center

- The National Infrastructure Protection Center (NIPC) was established in the early part of 1998, with the purpose of serving as the U.S. government's center for threat assessment, warning, investigation, and response to threats or attacks against critical information infrastructures
- Infrastructures include banking, telecommunications, energy, water systems, government operations, and emergency services
- Developed the "InfraGard" initiative



FBI

- The Federal Bureau of Investigation (FBI) is the investigative division of the US Department of Justice established on July 26, 1908
- It is the leading Law Enforcement Agency, which investigate cyber attacks by foreign rivals and terrorists
- The main aim of FBI is to protect United States against terrorist, cyber based attacks and foreign intelligence operations and espionage

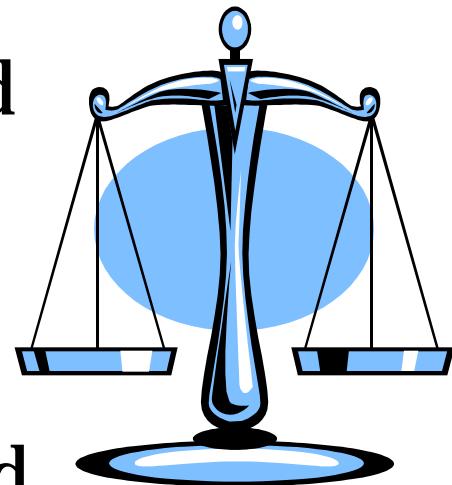


Federal Statutes

- 18 U.S.C. 875: Interstate Communications: Including Threats, Kidnapping, Ransom, Extortion
- 18 U.S.C. 1029: Fraud and related activity in connection with access devices
- 18 U.S.C. 1030: Fraud and related activity in connection with computers
- 18 U.S.C. 1343: Fraud by wire, radio or television
- 18 U.S.C. 1361: Injury to Government Property
- 18 U.S.C. 1362 Government communication systems
- 18 U.S.C. 1831 Economic Espionage Act
- 18 U.S.C. 1832 Theft of Trade Secrets

Cyber Laws

- Came into existence as conventional laws were of little use to sentence perpetrators
- Defines rules on what data is protected and what is available
- Defines ownership of data and data storage devices
- Defines rules for digital certificates and authentication algorithms



Approaches to Formulate Cyber Laws

- Formulation or extending laws by nations within their boundaries
- Multi-lateral international agreements for Internet
- Establishing a standardized international body
- Guidelines and rules from the user end



Scientific Working Group on Digital Evidence (SWGDE)

- SWGDE was established in February, 1998
- Responsible for developing cross-disciplinary guidelines and standards for recovery, preservation, and examination of digital evidence
- It drafted the standards proposed for digital evidence; definitions are also included in this document
- This document is adopted by US law enforcement agencies
 - <http://ncfs.org/swgde/index.html>

Cyber Laws Are Related to

- Computer crime
- Intellectual property
- Searching and seizing computers
- Cyberstalking
- Data protection and privacy
- Telecommunications laws



Federal Laws(Computer Crime)

⦿ 18 U.S.C. § 1029. *Fraud and Related Activity in Connection with Access Devices*

- Law is applicable if:
 - Person intentionally uses, produces or possesses one or more counterfeit access devices, and unauthorized access devices to defraud
 - obtains anything of value aggregating \$1,000 or more
- Penalty:
 - Depending on the type of offence mentioned in the Statute fine or imprisonment for not more than 10/15/20 years, or both; and

Federal Laws(Computer Crime)

◎ 18 U.S.C. § 1030. *Fraud and Related Activity in Connection with Computers*

- Law is applicable if:
 - Person intentionally accesses a computer without authorization or exceeds authorized access
 - Obtain restricted data or information that needs executive order
- Penalty:
 - Depending on the type of offence mentioned in the Statute fine or imprisonment for not more than 5/10/20 years, or both

Federal Laws (Computer Crime)

◎ 18 U.S.C. § 1362. *Communication Lines, Stations, or Systems*

- Law is applicable if:
 - Person willfully injures or destroys any of the works, property, or material of any means of communication
 - Maliciously obstructs, hinders, or delays the transmission of any communication
- Penalty:
 - a fine or imprisonment for not more than 10 years, or both

Intellectual Property Rights

Copyright Offenses

◎ 17 U.S.C. 506, Criminal Offenses

- Criminal Infringement
- Forfeiture and Destruction
- Fraudulent Copyright Notice
- Fraudulent Removal of Copyright Notice
- False Representation
- Rights of Attribution and Integrity

Intellectual Property Rights

① 18 U.S.C. 2319, *Criminal Infringement of a Copyright*

- Person applicable to submit victim impact statement include:
 - producers and sellers of legitimate works
 - holders of intellectual property rights
 - the legal representatives of such producers, sellers, and holders
- Penalty
 - imprisoned not more than 5 years, or fined for reproducing and distributing at least 10 copies or phonorecords, of 1 or more copyrighted works
 - imprisoned not more than 3 years, or fined for reproducing and distributing more than 10 copies or phonorecords, of 1 or more copyrighted works

Intellectual Property Rights

◎ **18 U.S.C. 2318**, *Trafficking in counterfeit label for phonerecords, copies of computer programs or computer program documentation or packaging, and copies of motion pictures or other audio visual works, and trafficking in counterfeit computer program documentation or packaging*

- Law is applicable if :
 - Person knowingly traffics in a counterfeit label affixed or designed to be affixed
 - Intentionally traffics in counterfeit documentation or packaging for a computer program
- Penalty:
 - fined or imprisoned for not more than five years, or both

Intellectual Property Rights

Bootlegging Offenses

◎ **18 U.S.C. 2319A**, *Unauthorized fixation of and trafficking in sound recordings and music videos of live musical performances*

- Law is applicable if:
 - Person knowingly and for purposes of commercial advantage fixes the sounds and images or reproduces copies or phonorecords
 - transmits the sound and images to the public without the consent of the performer
- Penalty:
 - imprisoned for not more than 5 years or fined or both

Intellectual Property Rights

- ◎ Trademark Offenses
- ◎ 18 U.S.C. 2320, Trafficking in counterfeit goods or services
 - Law is applicable if:
 - Person intentionally traffics or attempts to traffic in goods or services
 - knowingly uses a counterfeit mark
 - Penalty:
 - fined not more than \$2,000,000 or imprisoned not more than 10 years, or both

Intellectual Property Rights

- Trade Secret Offenses
- 18 U.S.C. 1831, *Economic espionage*
 - Law is applicable if:
 - Person knowingly steals or without authorization obtains a trade secret
 - without authorization copies or transmits a trade secret
 - receives, buys, or possesses a trade secret
 - Penalty:
 - fined not more than \$10,000,000.

Intellectual Property Rights

◎ 18 U.S.C. 1832, *Theft of trade secrets*

- Law is applicable if:
 - Person with intent to convert trade secret knowingly steals or without authorization obtains information
 - without authorization copies or transmits such information
 - receives, buys, or possesses such information
- Penalty:
 - fined not more than \$5,000,000

Intellectual Property Rights

◎ 18 U.S.C. 1833, *Exceptions to prohibitions*

- Exceptions:
 - lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State
 - reporting of a suspected violation of law to any governmental entity of the United States, a State, or a political subdivision of a State

◎ 18 U.S.C. 1834, *Criminal forfeiture*

- any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of violation
- any of the person's property used, or intended to be used to commit or facilitate violation

Intellectual Property Rights

- ◎ 18 U.S.C. 1835, *Orders to Preserve Confidentiality*
- ◎ 18 U.S.C. 1836, *Civil proceedings to enjoin violations*
- ◎ 18 U.S.C. 1837, *Applicability to conduct outside the United States*
- ◎ 18 U.S.C. 1838, *Construction with Other Laws*

Intellectual Property Rights

◎ 18 U.S.C. 1839, Definitions

- *foreign instrumentality*
 - any agency, or any legal, commercial, or business organization dominated by a foreign government
- *foreign agent*
 - representative of a foreign government
- *trade secret*
 - all forms and types of financial, business, scientific, technical, economic, or engineering information not being readily ascertainable through proper means by, the public
- *owner*
 - Person having rightful legal or equitable title to trade secret

Intellectual Property Rights

Offenses Relating to the Integrity of IP Systems

- ① **17 U.S.C. 506(c-d), *Fraudulent Copyright Notice; Fraudulent Removal of Copyright Notice***

- Offense if:
 - Person with malicious intent places a notice bearing copyright or words with false representation
 - removes or alters any notice of copyright appearing on a copy of a copyrighted work
- Penalty:
 - fined not more than \$2,500

Intellectual Property Rights

◎ 18 U.S.C. 497, *Letters patent*

- Offense if:
 - Person forges, counterfeits, or alters any letters patent granted by the President of the United States
- Penalty:
 - fined under this title or imprisoned not more than ten years, or both

◎ 35 U.S.C. 292, *False marking*

- Offense if:
 - Person without the consent of the patentee, marks upon, or affixes to, or uses in advertising in connection with anything made, used, offered for sale, or sold by such person.
- Penalty:
 - fined not more than \$500

Intellectual Property Rights

Misuse of Dissemination Systems

◎ 18 U.S.C. 1341, *Frauds and swindles*

- Offense if:
 - Person devise schemes to defraud
 - Obtain money by false representation
- Penalty:
 - fined or imprisoned not more than 20 years or both

◎ 18 U.S.C. 1343, *Fraud by wire, radio, or television*

- Offense if:
 - Person devise schemes to defraud and execute scheme by means of wire, radio, or television communication
- Penalty:
 - fined or imprisoned not more than 20 years or both

Intellectual Property Rights

- **18 U.S.C. 2512, Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited**
 - Offense if:
 - Person intentionally sends device useful for the purpose of the surreptitious interception of wire, oral, or electronic communications
 - manufactures, assembles, possesses, or sells such device knowing that it will be sent for foreign commerce
 - Penalty:
 - Fined or imprisoned not more than five years, or both

Intellectual Property Rights

◎ 47 U.S.C. 553, *Unauthorized reception of cable service*

- Offense if:
 - Person intercept or receive or assist in intercepting or receiving any communications service offered over a cable system using unauthorized way.
- Penalty:
 - fined not more than \$1,000 or imprisoned for not more than 6 months, or both

Intellectual Property Rights

④ 47 U.S.C. 605, *Unauthorized publication or use of communications*

- Practices prohibited
 - receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio
 - intercepting any radio communication and divulging or publishing the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person
 - Scrambling of Public Broadcasting Service programming
- Penalty:
 - fined not more than \$2,000 or imprisoned for not more than 6 months, or both.

Searching and Seizing Computers

◎ 18 U.S.C. § 2511 et seq. *Interception of wire, oral, and electronic communications*

- Law is applicable if:
 - Person knowingly intercepts any wire, oral, or electronic communication
 - intentionally uses, or procures any other person to use any electronic, mechanical, or other device to intercept any oral communication
 - intentionally discloses to any other person the contents of any wire, oral, or electronic communication
- Penalty:
 - fine of not less than \$500

Searching and Seizing Computers

◎18 U.S.C. § 2701 et seq. *Preservation and disclosure of stored wire and electronic communications*

- Offense if:
 - Person intentionally exceeds an authorization or without authorization to access facility providing electronic communication service
- Punishment
 - a fine under this title or imprisonment for not more than 5 years, or both if offense is for commercial advantage.
 - a fine under this title or imprisonment for not more than 1 year or both in other case

Searching and Seizing Computers

- ◎ 18 U.S.C. § 3121 et seq. *Recording of dialing, routing, addressing, and signaling information*
 - Practice Prohibited:
 - installing or using a pen register or a trap and trace device without first obtaining a court order
 - Exception:
 - Use of pen register or trap device in case relating to the operation, maintenance, and testing of a wire or electronic communication service
 - Penalty:
 - fined or imprisoned not more than one year, or both

Searching and Seizing Computers

- ◎ 42 U.S.C. § 2000aa. *Searches and seizures by government officers and employees in connection with investigation or prosecution of criminal offenses*
 - Unlawful Act:
 - to search for or seize any work product materials possessed by a person meant to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce
 - to search for or seize documentary materials possessed by a person

Cyberstalking

◎ 18 U.S.C. § 875, *Interstate communications*

- Offense:
 - Transmitting any communication containing any demand or request for a ransom
 - Transmitting any communication containing any threat to kidnap any person or to injure the person

◎ 18 U.S.C. § 2261A, *Interstate stalking*

- Offense:
 - Person travels in interstate or foreign commerce with an intent to kill or injure ,harass, or intimidate a person in another State or tribal jurisdiction

Cyberstalking

- ◎ 47 U.S.C. § 223, *Obscene or harassing telephone calls in the District of Columbia or in interstate or foreign communications*
 - Offense if:
 - Person knowingly create or transmit the obscene material to annoy or harass another person by means of telecommunication
 - makes repeated telephone calls solely to harass any person at the called number or who receives the communication
 - Penalty:
 - fined under Title 18, or imprisoned not more than two years, or both

The USA Patriot Act of 2001

“If certain conditions are met, a court may authorize so-called ‘surreptitious entry warrants’ or ‘sneak-and-peek’ warrants that excuse agents from having to notify the person whose premises are searched at the time of the search”



Patriot Act, 2001

- After 9-11, the Patriot Act increased the reach of law enforcement to pursue or capture terrorists
- Authorizes interception of wire, oral, and electronic communications relating to terrorism and to computer fraud and abuse
- Authorizes sharing of criminal investigative information



Freedom of Information Act

- The U.S. **Freedom of Information Act (FOIA)** is a law ensuring public access to U.S. government records
- Under the FOIA, all federal agencies are required to disclose records requested in writing by any person
- Applies only to federal agencies
- Does not create a right of access to records held by Congress, the courts, or by state or local government agencies
- Each state has its own public access laws that must be consulted before accessing to state and local records



Building Cyber Crime Case

- ◉ Identification of evidence
- ◉ Collecting and preserving digital evidence
- ◉ Factors that complicate prosecution
- ◉ Overcoming the obstacles



How the FBI Investigates Computer Crime

- **FBI investigates incident when:**

- Federal criminal code violation occurs
- Federal violation factors validates

- **FBI uses:**

- Various technical programs to address the complexity
- Sophisticated methods for investigation.
- Specialized cyber squads for expert assistance

How to Initiate an Investigation

- ◎ Following points to be considered:

- Reportable versus nonreportable
- Choice to go civil Instead of criminal
- Acceptable-Use policy violations



Legal Issues Involved in Seizure of Computer Equipments

- Need for technical expertise
- Limit seizure of hardware
- Impact of presence of privileged or protected material in a computer system
- Stored electronic communication
- Consent of network system administrator



Searching With a Warrant

- Law enforcement must establish "probable cause, supported by Oath or affirmation"
- Description of place, thing or person is necessary
- Drafting of warrant should be in such a way that it authorizes the agent to take necessary step
- Supporting affidavit should explain the possible search strategies

Searching Without a Warrant

- Search can be initiated without warrant if any one of the following is there:

- Consent
 - Authority has given the consent voluntarily.
 - Third party has given the consent.
 - Implied consent.
- Exigent circumstances
- Plain view
- Search incident to lawful arrest

Privacy Issues Involved in Investigations

- Reasonable Expectation of Privacy in Computers as Storage Devices
- Reasonable Expectation of Privacy and Third-Party Possession
- Private Searches
- Reasonable Expectation of Privacy in Public Workplaces



International Issues Related to Computer Forensics

- Electronic evidence located outside the borders of the country
- Seeking assistance from law enforcement authorities in different country
- Preservation of evidence
- Consistency with all legal systems
- Allowance for the use of common language
- Applicability to all forensic evidence
- Applicability at every level



Crime Legislation of EU

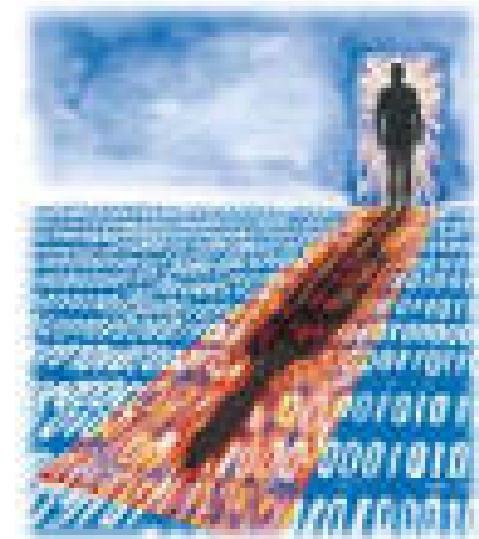
Country	Target fingerprinting	Malicious code	Denial of service	Account compromise	Intrusion attempt	Unauthorised access to information	Unauthorised access to transmission	Unauthorised modification of information	Unauthorised access to communication system
Austria	n.a.	n.a.	n.a.	Adm.	Adm.	Adm.	n.a.	n.a.	Adm.
Belgium	Crim.	Crim.	Crim.	Crim.	Crim.	Crim.	Crim.	Crim.	Crim.
Denmark	Crim	Crim	Crim	Crim	Crim	Crim	Crim	n.a.	Crim
Finland	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim
France	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim
Germany	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim
Greece	n.a.	n.a.	n.a.	Crim	Crim	Crim	n.a.	n.a.	Crim
Ireland	n.a.	n.a.	n.a.	Crim	Crim	Crim	n.a.	n.a.	Crim
Italy	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim
Luxembourg	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim
The Netherlands	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim
Portugal	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim
Spain	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim
Sweden	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim
United Kingdom	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim

Source: RAND Europe / Transcrime Research Centre

Legend:
 n.a. = no available legislation
 Adm. = Administrative sanction provided
 Crim. = Penal sanction provided

Cyber Crime Investigation

- Acquisition of the data from the system from which the digital crime has been committed
- Identification of the digital evidence from the crime
- Evaluation and analysis of the evidence
- Presentation of the evidence to the court



Summary

- Cyber crime has originated from the growing dependence on computers in modern life
- Various Law Enforcement Agencies such as FBI,NIPC investigate computer facilitated crimes and help in tracking cyber criminals
- Federal laws related to computer crime,cyberstalking, search and seizure of computer,intellectual property rights are discussed
- Building a cyber crime case and initiating investigation are crucial areas

End notes

- APPENDIX A: Sample 18 U.S.C. § 2703(d) Application and Order.
- APPENDIX B
 - Model form for IP trap and trace on a web-based email account
 - Model form for pen register/trap and trace
 - Model form for IP pen register/trap and trace on a computer network intruder
- APPENDIX C: Sample Subpoena Language
- APPENDIX D: Sample Language for Search Warrants and Accompanying Affidavits to Search and Seize Computers.
- APPENDIX G: Sample Letter for Provider Monitoring
- APPENDIX F: Standards for digital evidence.



Computer Hacking Forensic Investigator

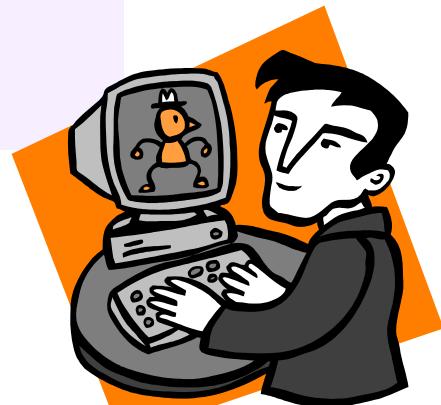
Module III

Computer Investigation Process

Scenario

Jim works as a technical resource developer in a reputed firm. As he was not meeting his deadlines Jim started working late hours.

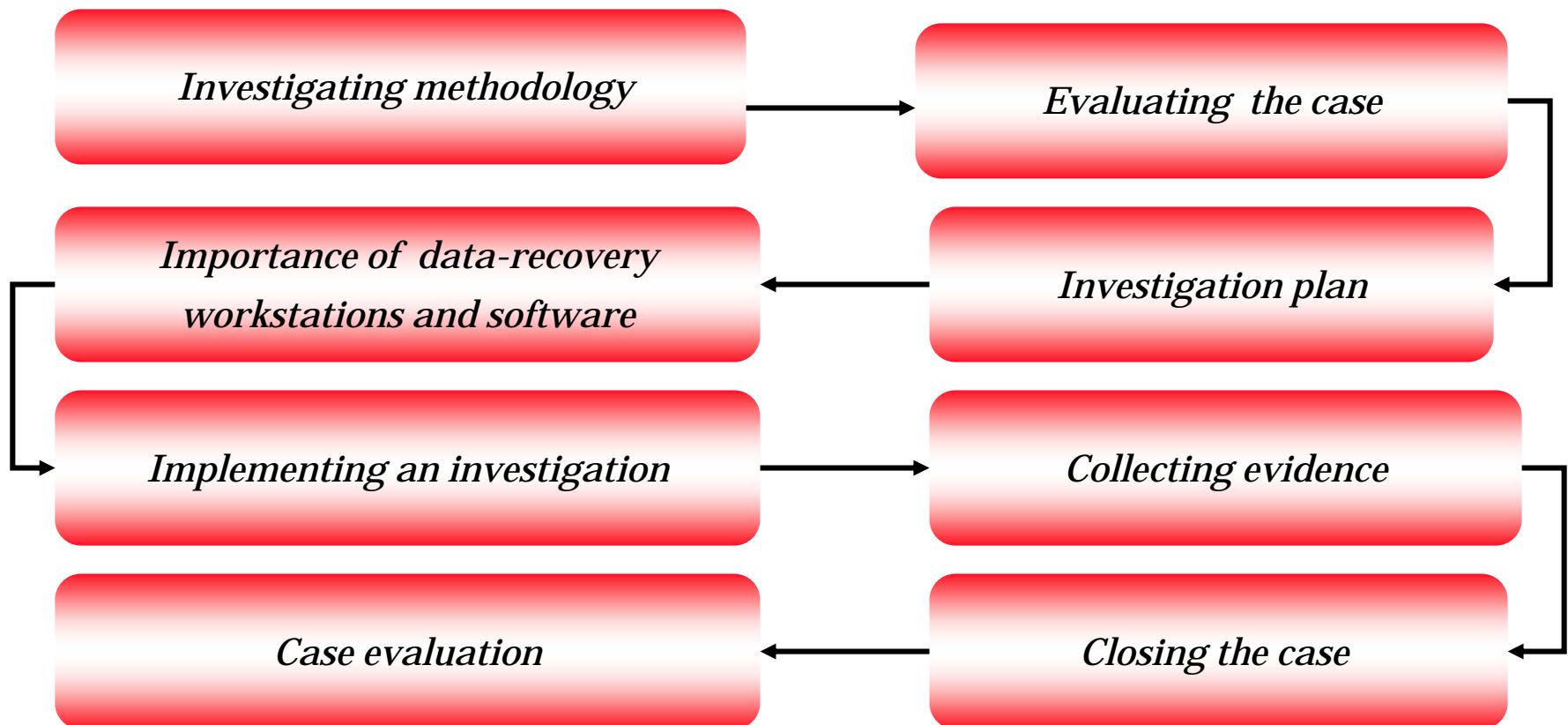
The extra effort put in by Jim did not produce any results and his Project manager got suspicious about his activities.



Module Objective

- Investigating methodology
- Evaluating the case
- Investigation plan
- Importance of data-recovery workstations and software
- Implementing an investigation
- Collecting the evidence
- Closing the case
- Case evaluation

Module Flow



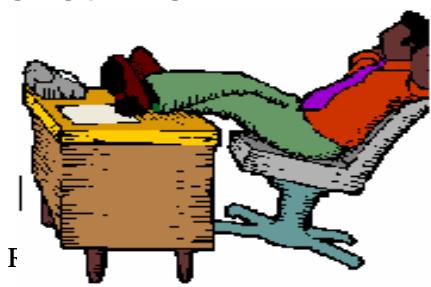
Investigating Computer Crime

- Determine if there has been an incident
- Find and interpret the clues left behind
- Do preliminary assessment to search for the evidence
- Search and seize the computer equipments

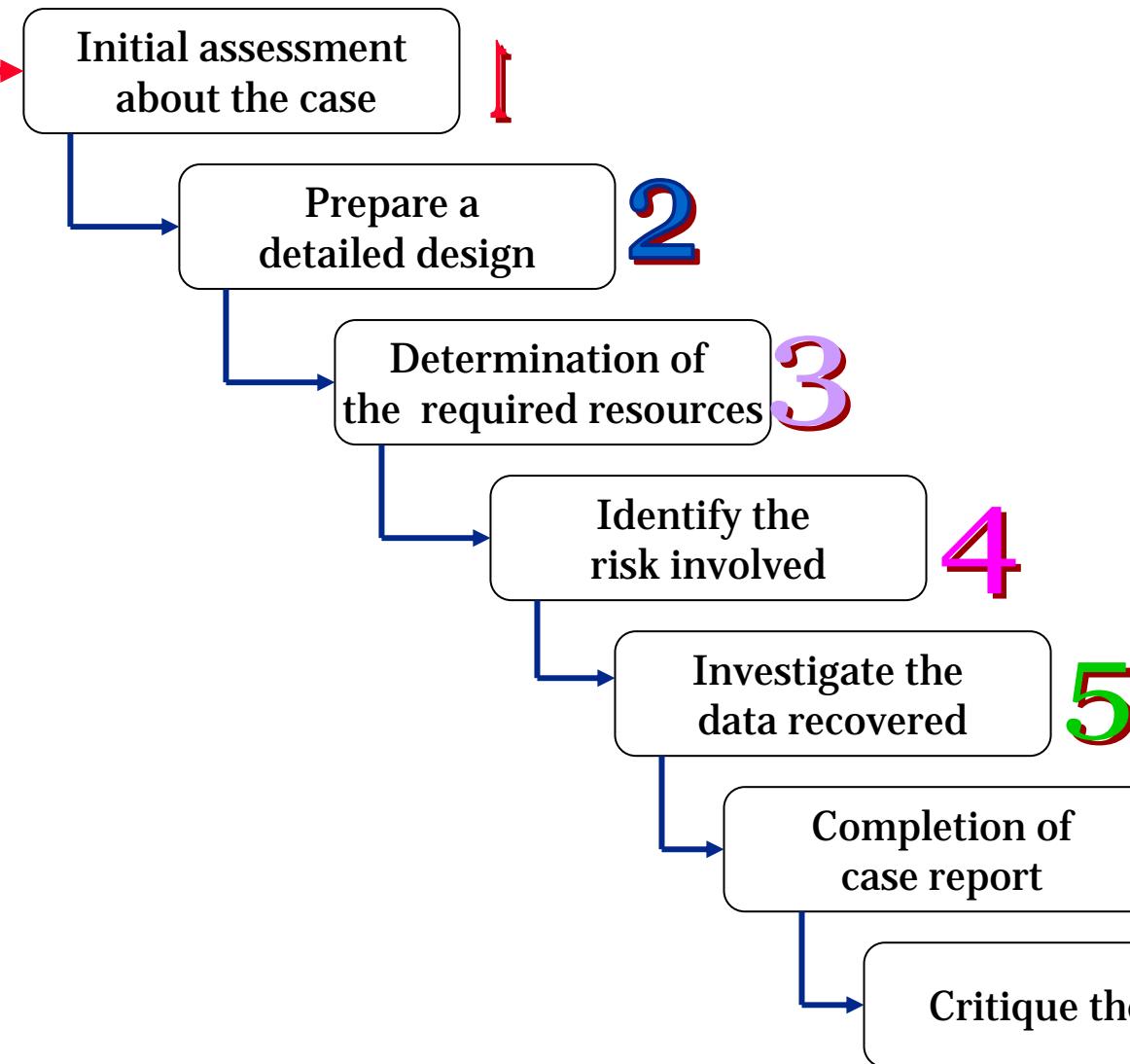


Investigating a Company Policy Violation

- ◉ All employees of the company should be informed of the company policy
- ◉ Employees using company's resources for personal use not only waste company's time and resources but they also violate company policy
- ◉ Such employees should be traced and educated about the company policy
- ◉ If the problem persists, action should be taken



Investigation Methodology



Evaluating the Case

- The case can be assessed in the following manner :

- Situation of the case
- Nature of the case
- Specifics about the case
- Type of evidence
- Operating system used by the suspect
- Known disk format
- Location of evidence
- The motive of the suspect



Before the Investigation

- Following points should be kept in mind before starting the investigation:

- Have skilled professionals
- Work station and data recovery lab
- Alliance with a local District Attorney
- Define the methodology



Document Everything

- Document the hardware configuration of the system
- Document the system date and time
- Document file names, dates, and times
- Document all findings



Investigation Plan

⦿ Following points need to be considered while planning:

- Good understanding of the technical, legal, and evidentiary aspects of computers and networks
- Proper methodology
- Steps for collecting and preserving the evidence
- Steps for performing forensic analysis



Obtain Search Warrant

- Executes the investigation
- To carry out an investigation a search warrant from a court is required
- Warrants can be issued for:
 - Entire company
 - Floor
 - Room
 - Just a device
 - Car
 - House
 - Any Company Property

Warning Banners

- Flashes at the point of access
- Warns both authorized and unauthorized users
- Unauthorized usage of the banner policy makes it easier to conduct investigation
- Employees working are warned about the consequences if the companies policies are violated

COMPUTER USAGE WARNING

This computer system is connected to the State of New York computer network, and therefore shall be governed by all local and state policies and laws concerning use of this system and available resources. This computer system, including all related equipment, networks and network devices (specifically including internet access), are provided only for authorized users. Xsecurity School District computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized Xsecurity School District and State of Arkansas Information Technology administrators to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of the Xsecurity School District computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or adverse action. Authorized or unauthorized users of the Xsecurity School District computer system shall have no expectation of privacy while using this system. If criminal activity is discovered, the information will be provided to the appropriate law enforcement officials. Suspected access violations or rule infractions should be reported to the Information Technology Director or the Network Administrator. The Information Technology Director and Network Administrator can be reached at XXXXXXXX or XXXXXXXX.

Use of this system constitutes consent to monitoring for these purposes and is also an acceptance of the Xsecurity School District Computer Usage Contract which can be found in the student handbook and/or personnel policies as well as by visiting XXXXXXXX and clicking on Board Policies.

Shutdown the Computer



- During a crime scene, should the computer be shutdown and unplugged to collect evidence?
 - Case dependant
 - Incase of ddos attack the system must be unplugged and then shutdown
 - Operating system's internal memory process handles, open files, open ports, open connections are recorded before unplugging the computer

Collecting the Evidence

- The following steps are performed to collect the evidence:

- Find the evidence
- Discover the relevant data
- Prepare an Order of Volatility
- Eradicate external avenues of alter
- Gather the evidence
- Prepare chain of custody



Chain-of Evidence Form

Metropolis Police Bureau High-Tech Investigation Unit This form is to be used for only one piece of evidence			
Case No:		Unit Number:	
Investigator:			
Nature of Case:			
Location where Evidence was obtained:			
Item # ID	Description Of the Evidence	Vendor Name	Model No./Serial No.
Evidence Recovered by:			Date & Time:
Evidence Placed in Locker:			Date & Time:
Evidence Processed by	Description of the Evidence		Date/Time

Confiscation of Computer Equipments

- Sterilize all the media to be used in the examination process
- Enter the crime scene, take snapshot of the scene and then carefully scan the data sources
- Retain and document the state and integrity of items at the crime scene
- Transport the evidence to the forensic facility

Preserving the Evidence

- Evidence for a case may include an entire computer and associated media
- Collect computer evidence in anti-static bags, anti-static pad with an attached wrist strap
- Store the evidence in an environment having pre-specified temperature and humidity



Importance of Data-recovery Workstations and Software

- ◎ **Data-recovery lab** – a place where investigations are conducted and all the equipment and software are kept
- ◎ **Computer- forensic Workstation** – a workstation set up to allow copying evidence with the help of various preloaded software ready-to-use

Configuring Windows 98 Workstation to Boot into MS-DOS

- Initiate Windows 98 and run command prompt.
- Type **msconfig** and click **Ok** button.
- Select startup settings on the General Tab.
- Click **Advanced** button.
- Click the Enable Startup **Menu** check box.
- Click **OK** to close the Advanced Troubleshooting Settings.
- Close the System Configuration Utility window.

To Add a command to the MSDOS.SYS File

The screenshot shows a Windows Notepad window titled "Untitled - Notepad". The window contains configuration settings for the MSDOS.SYS file. The text is as follows:

```
winBootDir = C:\Windows
Host WinBootDrv = C

[ Options ]
BootMulti = 1
ootGUI = 1
DoubleBuffer = 1
AutoSac = 1
WinVer = 4.10.2222
;
;The following lines are required for compatibility with other programs.
;Do not remove them ( MSDOS.SYS needs to be >1024 bytes ).
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxa
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxb
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxc
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxd
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxe
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxf
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxg
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxh
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxi
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxj
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxn
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxo
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxp
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxq
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxr
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxs
BootMenu = 1
BootMenuDelay = 59
```

Two annotations with arrows point to the "BootMenu" and "BootMenuDelay" lines. A callout box labeled "Changing setting to 59" points to the "BootMenuDelay = 59" line.

Changing
setting
to 59

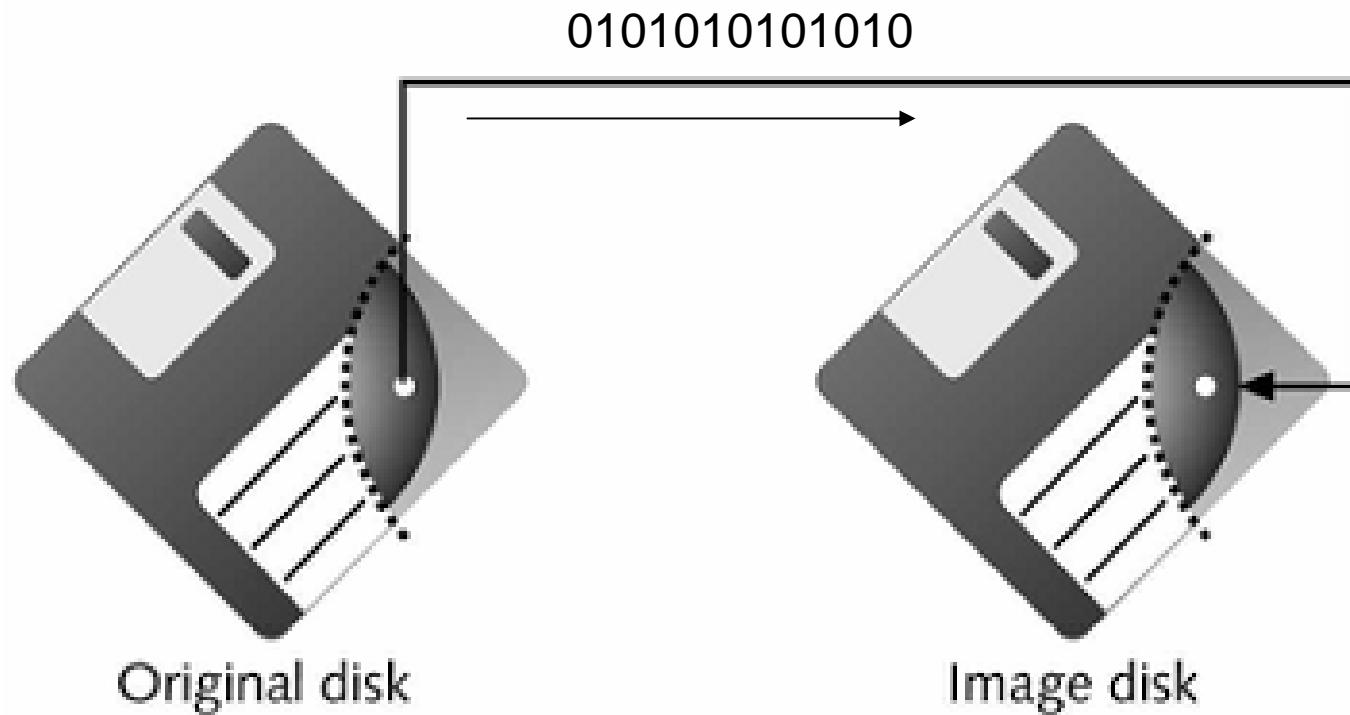
Changing
setting
to 59

Implementing an Investigation

- The items that may be needed are:

- Evidence Form
- Original evidence
- Evidence bag that is used as evidence container
- Bit-stream imaging tool
- Forensic workstation to copy and examine the evidence
- Secure evidence container

Understanding Bit-stream Copies



Imaging the Evidence Disk

- Capture an accurate image of the system as soon as possible.
- The forensic copy can be created using various techniques such as:
 - Using MS-DOS to create bit-stream copy of a floppy disk / Hard disk
 - Using Imaging software to acquire bit-stream copy of floppy disk / Hard disk

Examining the Digital Evidence

- Analysis can be carried out using various forensic analysis tool such EnCase, AccessData etc.



Closing the Case

- The investigator should include what was done and results in the final report
- Basic report includes: who,what,when,where and how
- In a good computing investigation the steps can be repeated and the result obtained are same every time
- The report should explain the computer and network processes
- Explanation should be provided for various processes and the inner working of the system and its various interrelated components



Case Evaluation

- The investigator should evaluate the case by asking the following questions:

- How could he improve his participation in the case?
- Did he use new techniques during the case?
- Did he discover new problems ? If yes, when , why and what were the problems?
- What kind of feedback did he receive from requesting source?
- Was there a match between his expectation from the case and the final outcome?



Summary

- Take a systematic approach to the investigations
- Take into account the nature of the case, instruction, and tools while planning the case
- Apply standard problem-solving techniques
- Always maintain a journal to make notes of everything
- Create bit-stream copies of files using either the Diskcopy DOS utility or the Image tool



Computer Hacking Forensic Investigator

Module IV

Computer Security Incident Response Team

Scenario

Target Company Ltd, a data warehousing has lots of important business information stored in it's huge database. The data and information present in the company's database serves as a key aspect to its next business moves.

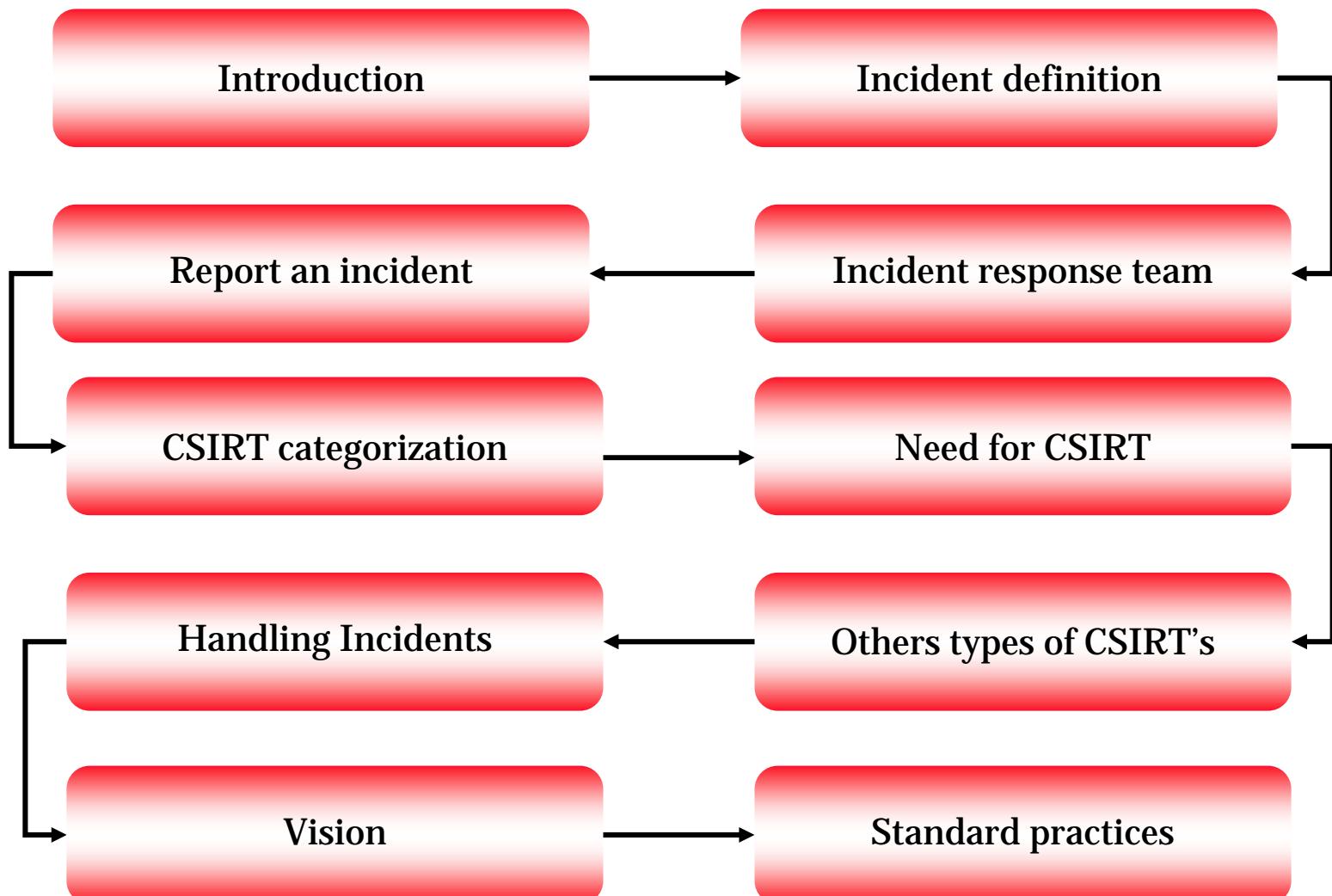
An e-mail claiming to pass all the relevant and vital business information to their competitor surprised the company's top management. A team of hackers threatens the management to expose all the business secrets of the Target Company Ltd. to the competitor unless they receive a big paycheck !!!



Module Objectives

- Introduction
- What is an incident?
- Incident response team
- How to report an incident?
- CSIRT categorization
- Need for CSIRT
- What does CSIRT do?
- Others types of CSIRT's
- Handling Incidents
- Vision
- Standard practices

Module Flow



Present Networking Scenario

- Increase in the number of companies venturing into e-business coupled with high Internet usage
- Decrease in vendor product development cycle and product's testing cycle
- Increase in complexity of Internet as a network
- Alarming increase in intruder activities and tools, expertise of hackers and sophistication of hacks
- Lack of thoroughly trained professionals as compared to the number and intensity of security breaches

Vulnerability

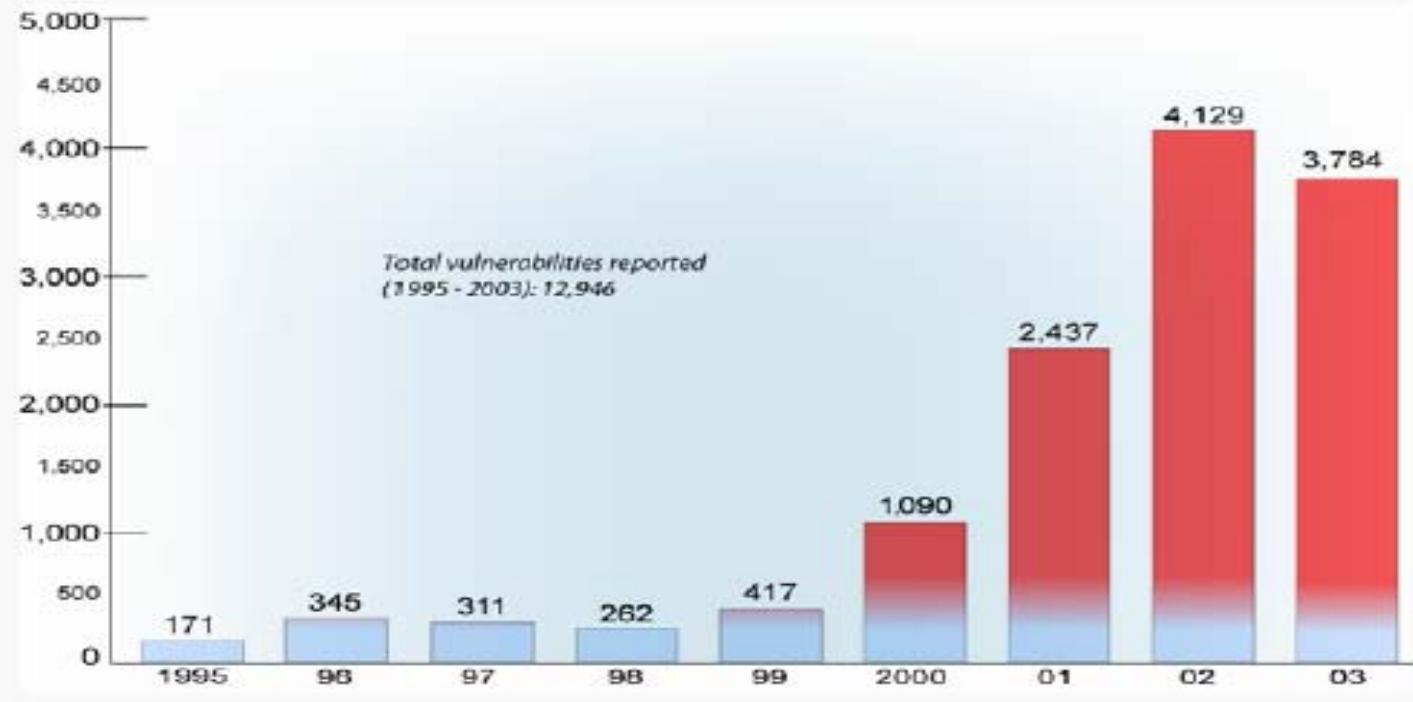
- Vulnerability is defined as “*Existence of a weakness; design or implementation error that can lead to an unexpected, undesirable event compromising the security of the system.*”

source: www.Wikipedia.com

- Some common vulnerabilities are:
 - Buffer overflows
 - SQL Injection
 - Cross side scripting
 - Default installation
 - Misconfiguration

Vulnerability Statistics

Growth in Number of Vulnerabilities Reported to the CERT/CC



Source: www.cert.org/tech_tips/incident_reporting.html

What Is an Incident?

- According to www.cert.org
Computer security incident is defined as "*Any real or suspected adverse event in relation to the security of computer systems or computer networks*"
- It also includes external threats such as gaining access to systems, disrupting their services through malicious spamming, execution of malicious codes that destroy or corrupt systems



How to Identify an Incident?

- A system alarm from an intrusion detection tool indicating security breach
- Suspicious entries in network
- Accounting gaps of several minutes with no accounting log
- Other events like unsuccessful login attempts, unexplained new user or files, attempts to write system files, modification or deleting of data
- Unusual usage patterns, such as programs being compiled in the account of users who are non-programmers

Whom to Report an Incident?

- ◉ Incident reporting is the process of reporting the information regarding the *encountered security breach* in a proper format
- ◉ The incident should be reported to the [CERT Coordination center](#), site security manager, and other site
- ◉ It can also be reported to law enforcement agencies such as [FBI](#), [USSS Electronic crimes branch](#) or [Department of Defense Contractors](#)
- ◉ It should be reported to receive technical assistance and to raise security awareness to minimize the losses

Incident Reporting

⦿ When a user encounters any breach, following should be reported:

- Intensity of the security breach
- Circumstances, which revealed vulnerability
- Shortcomings in the design and impact or level of weakness
- Entry logs related to intruder's activity
- Specific help needed should be clearly defined
- Correct time-zone of the region and synchronization information of the system with a National time server via NTP (Network Time Protocol)

Category of Incidents

- ◉ There are 3 category of incidents:
 - Low level
 - Mid Level
 - High Level

Category of Incidents - Low Level

- ◉ Low level incidents are the least severe kind of incidents
- ◉ It is recommended that they should be handled within a working day after the event occurs
- ◉ Low level incidents can be identified when the following things happen:
 - Loss of personal password
 - Suspected sharing of organization's accounts
 - Unsuccessful scans and probes
 - Presence of any computer virus or worms

Category of Incidents- Mid Level

- The incidents at this level are comparatively more serious and thus, should be handled the same day the event occurs (*normally within two to four hours of the event*).
- They can be identified by observing :
 - Violation of special access to a computer or computing facility
 - Unfriendly employee termination
 - Unauthorized storing and processing data
 - Destruction of property related to a computer incident (less than \$100,000)
 - Personal theft of data related to computer incident (\$100,000)
 - Computer virus or worms of comparatively larger intensity
 - Illegal access to buildings

Category of Incidents- High Level

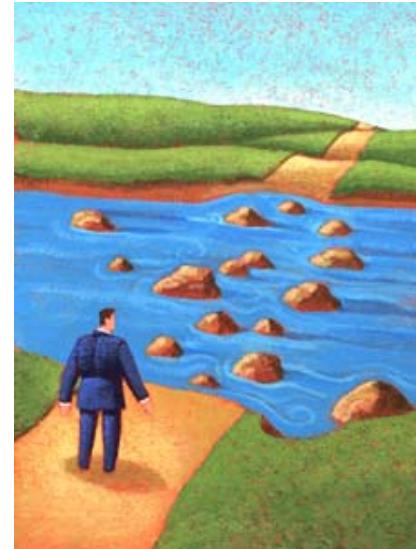
- These are the most serious incidents and are considered as “Major” in nature
- High level incidents should be handled immediately after the occurrence of the incident
- These include:
 - Denial of Service attacks
 - Suspected computer break-in
 - Computer virus or worms of highest intensity; e.g. Trojan back door.
 - Changes to system hardware, firmware or software without authentication.
 - Destruction of property exceeding \$100,000.
 - Personal theft exceeding \$100,000 and illegal electronic fund transfer or download/sale.
 - Any kind of pornography, gambling or violation of any law.

Handling Incidents

- Incident handling helps to find out trends and pattern regarding intruder activity by analyzing it
- It involves three basic functions: incident reporting, incident analysis, and incident response
- It recommends network administrators for recovery, containment, and prevention to constituents
- It allows incident reports to be gathered in one location so that exact trends and pattern can be recognized and recommended strategies can be employed
- It helps the corresponding staffs to understand the process of responding and to tackle unexpected threats and security breaches

Procedure for Handling Incident

- The incident handling process is divided into six stages
- These stages are:
 - Preparation
 - Identification
 - Containment
 - Eradication
 - Recovery
 - Follow up



- Source: FCC Computer Security incident response Team

1. Preparation

- Preparation enables easy coordination among staffs
- Provides baseline protection
- Uses virus detection and eradication tools
- Company staff is given relative training at this stage



2. Identification

- It involves validating, identifying and reporting the incident
- Determining the symptoms given in ‘how to identify an incident’
- Identifying nature of the incident
- Identifying events
- Protecting evidence
- Reporting events

3. Containment

- Limit the extent and intensity of an incident
- Avoid logging as root on the compromised system
- Conventional methods to trace back should be avoided as this may alert the attackers
- Prepare complete backups of infected systems
- Change the passwords of all unaffected systems in the LAN

4. Eradication

- Additional information along with the information gathered in the 3rd phase should be looked into to find out reasons for the particular incident
- Use standard anti-virus tools to remove virus/worms from storage medias.
- Improve security measures by enabling firewalls, router filters or assigning new IP address
- Perform vulnerability analysis

5. Recovery

- Determine the course of actions
- Monitor and validate systems
- Determine integrity of the backup itself by making an attempt to read its data
- Verify success of operation and normal condition of system
- Monitor the system by network loggers, system log files and potential back doors

6. Follow up

- Revise policies and procedures from the lessons learnt from the past
- Determine the staff time required and perform the following cost analysis:
 - Extent to which the incidents disrupted the organization
 - Data lost and its value
 - Damaged hardware and its cost

continued....

- Document the response to incident by finding answers to the following :

- Was the preparation for the incident sufficient?
- Whether the detection occurred promptly or not, and why?
- Using additional tools could have helped or not?
- Was the incident contained?
- What practical difficulties were encountered?
- Was it communicated properly?

What Is CSIRT?

- A team of trained professionals
- CSIRT members detect incidents at early stages and make reports to prevent further incidents
- CSIRT protects and secures critical information of an organization
- It secures organization's data, hardware, and critical business policy
- It provides training on security awareness, intrusion detection, and penetration testing
- Documents and develops program
- It strengthens organization's security
- Decreases the response time during any future security breach

Why an Organization Needs an Incident Response Team?

- It helps organizations to recover from computer security breaches and threats
- It is a formalized team which performs incident response work as its major job function
- As an ad-hoc team, it is responsible for ongoing computer security incident



Need for CSIRT

- CSIRT provides rapid response to maintain the security and integrity of the systems
- Experienced in handling compromised network/systems.
- Being in a network of likeminded professionals, the CSIRT team members get to know the vulnerabilities firsthand
- CSIRT helps in deploying systems that follow the security policy of the organization

Example of CSIRT

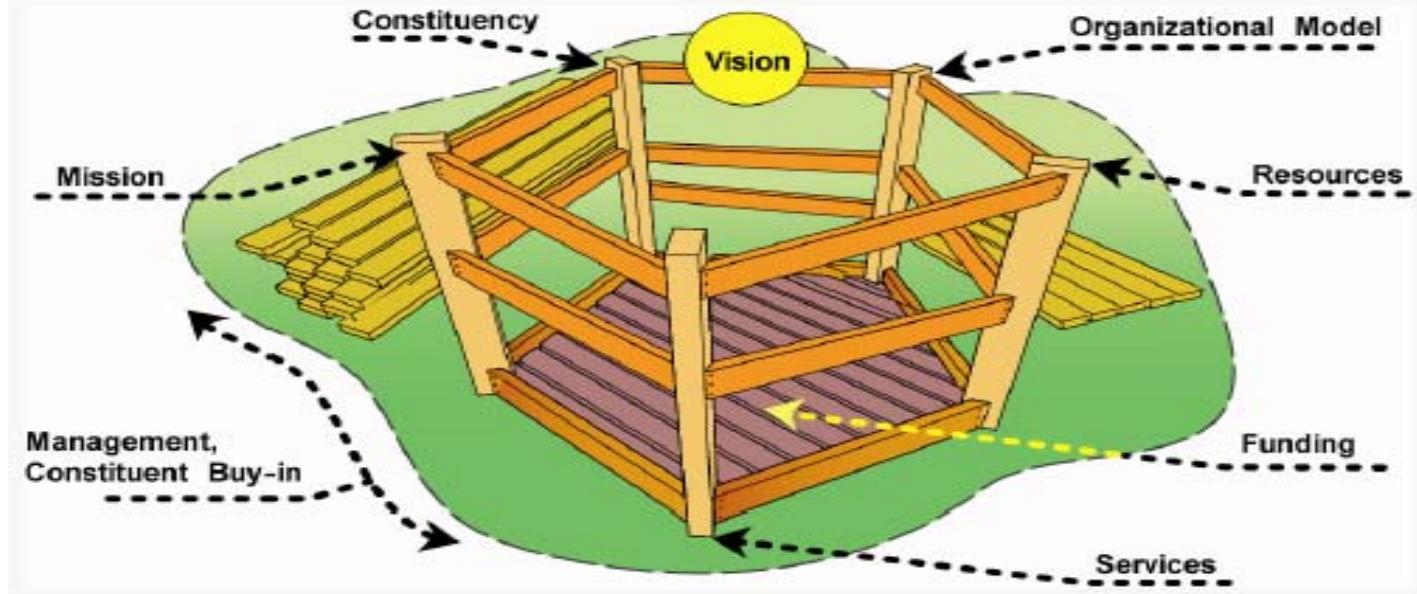
- **Internal CSIRT** provides services to their parent organization such as bank, manufacturing company, university, or any government agencies
- **National CSIRT** provides services to the entire nation example being Japan Computer Emergency Response Team Coordination Center ([JPCERT/CC](#))
- **Analysis Centers** synthesize data, determine trends and patterns in an incident activity to predict future activity or provide early warnings
- **Vendor teams** identify vulnerabilities in software and hardware products
- **Incidents Response Providers** who offer services to paid clients

CSIRT Vision

- Identify the organization
- Specify the mission, goals and objectives of CSIRT for an organization
- Select the services to be offered by the CSIRT
- Determine how the CSIRT should be structured for the organization
- Plan the budget required by the organization to implement and manage the CSIRT
- Determine the resources (equipment, staff, infrastructure) to be used by CSIRT

Vision

Building Your Vision



Source: www.cert.org/tech_tips/incident_reporting.html

Best Practices for Creating a CSIRT

- **Step 1:** Obtain management support and buy-in
- **Step 2:** Determine the CSIRT strategic plan
- **Step 3:** Gather relevant information
- **Step 4:** Design the CSIRT vision
- **Step 5:** Communicate the CSIRT vision and operational plan
- **Step 6:** Begin CSIRT implementation
- **Step 7:** Announce the operational CSIRT

Step 1: Obtain Management Support and Buy-In

- ◉ Without management approval and support, creating an effective incident response capability can be extremely difficult and problematic.
- ◉ Once the team is established, how is it maintained and expanded with budget, personnel, and equipment resources?
- ◉ Will the role and authority of the CSIRT continue to be backed by management across the various constituencies or parent organization?

Step 2: Determine the CSIRT Development Strategic Plan

- ◉ Are there specific timeframes to be met? Are they realistic, and if not, can they be changed?
- ◉ Is there a project group? Where do the group members come from?
- ◉ How do you let the organization know about the development of the CSIRT?
- ◉ If you have a project team, how do you record and communicate the information you are collecting, especially if the team is geographically dispersed?

Step 3: Gather Relevant Information

- Meet with key stakeholders to discuss the expectations, strategic direction, definitions, and responsibilities of the CSIRT. The stakeholders could include :
 - Business managers.
 - Representatives from IT.
 - Representatives from the legal department.
 - Representatives from human resources.
 - Representatives from public relations.
 - Any existing security groups, including physical security.
 - Audit and risk management specialists.

Step 4: Design your CSIRT Vision

- In creating your vision, you should

- Identify your constituency. Who does the CSIRT support and service?
- Define your CSIRT mission, goals, and objectives. What does the CSIRT do for the identified constituency?
- Select the CSIRT services to provide to the constituency (or others). How does the CSIRT support its mission?
- Determine the organizational model. How is the CSIRT structured and organized?
- Identify required resources. What staff, equipment, and infrastructure is needed to operate the CSIRT?
- Determine your CSIRT funding. How is the CSIRT funded for its initial startup and its long-term maintenance and growth?

Step 5: Communicate the CSIRT Vision

- Communicate the CSIRT vision and operational plan to management, constituency, and others who need to know and understand its operations.
- As appropriate, make adjustments to the plan based on their feedback.

Step 6: Begin CSIRT Implementation

- Hire and train initial CSIRT staff.
- Buy equipment and build any necessary network infrastructure to support the team.
- Develop the initial set of CSIRT policies and procedures to support your services.
- Define the specifications for and build your incident-tracking system.
- Develop incident-reporting guidelines and forms for your constituency.

Step 7: Announce the CSIRT

- When the CSIRT is operational, announce it broadly to the constituency or parent organization.
- It is best if this announcement comes from sponsoring management.
- Include the contact information and hours of operation for the CSIRT in the announcement.
- This is an excellent time to make available the CSIRT incident-reporting guidelines.

Source: <http://www.cert.org/csirts/Creating-A-CSIRT.html#1>

Other Response Teams Acronyms and CSIRTs around the world

CSIRT	Computer Security Incident Response Team
CIRC	Computer Incident Response Capability
CIRT	Computer Incident Response Team
IRC	Incident Response Center or Incident Response Capability
IRT	Incident Response Team
SERT	Security Emergency Response Team
SIRT	Security Incident Response Team



Asia Pacific Computer Emergency Response Team

[HOME](#) | [E-mail](#)

Meetings Schedule
Past Activities
Membership
Members
<input checked="" type="checkbox"/> group

Full Member

MEMBER

AusCERT(Australian Computer Emergency Response Team)

- Australia -

BKIS(Bach Khoa Internetwork Security Center)

- Vietnam -

CCERT(CERNET Computer Emergency Response Team)

- People's Republic of China -

KrCERT(Korea Internet Security Center)

- Korea -

CNCERT/CC(National Computer network Emergency Response technical Team / Coordination Center of China)

- People's Republic of China -

HKCERT/CC(Hong Kong Computer Emergency Response Team Coordination Center)

- Hong Kong, China -

IDCERT(Indonesia Computer Emergency Response Team)

- Indonesia -

World CSIRT

<http://www.cert-in.org.in/worldcert.htm>

◎ Asia Pacific CERTs

- Australia CERT (AUSCERT)
- Hong Kong CERT (HKCERT/CC)
- Indonesian CSIRT (ID-CERT)
- Japan CERT-CC (JPCERT/CC)
- Korea CERT (CERT-KR)
- Malaysia CERT (MyCERT)
- Pakistan CERT(PakCERT)
- Singapore CERT (SingCERT)
- Taiwan CERT (TWCERT)
- China CERT (CNCERT/CC)

◎ North American CERTs

- CERT-CC
- US-CERT
- Canadian Cert
- Cancert
- Forum of Incident Response and Security Teams
- FIRST

◎ South American CERTs

- CAIS
- CAIS- Brazilian Research Network CSIRT
- NIC BR Security Office Brazilian CERT
- NBS

◎ European CERTs

- EuroCERT
- FUNET CERT
- CERTA
- DFN-CERT
- JANET-CERT
- CERT-NL
- UNINETT-CERT
- CERT-NASK
- Swiss Academic and Research Network CERT

Summary

- Increase in the number of products and relative increase in the number of hacking tools has put *Security* in the spotlight
- Incident reporting is the process of reporting the information regarding the *encountered security breach* in a proper format
- It involves three basic functions: incident reporting, incident analysis, and incident response
- CSIRT provides rapid response to maintain the security and integrity of the systems
- Without management approval and support, creating an effective incident response capability can be extremely difficult and problematic



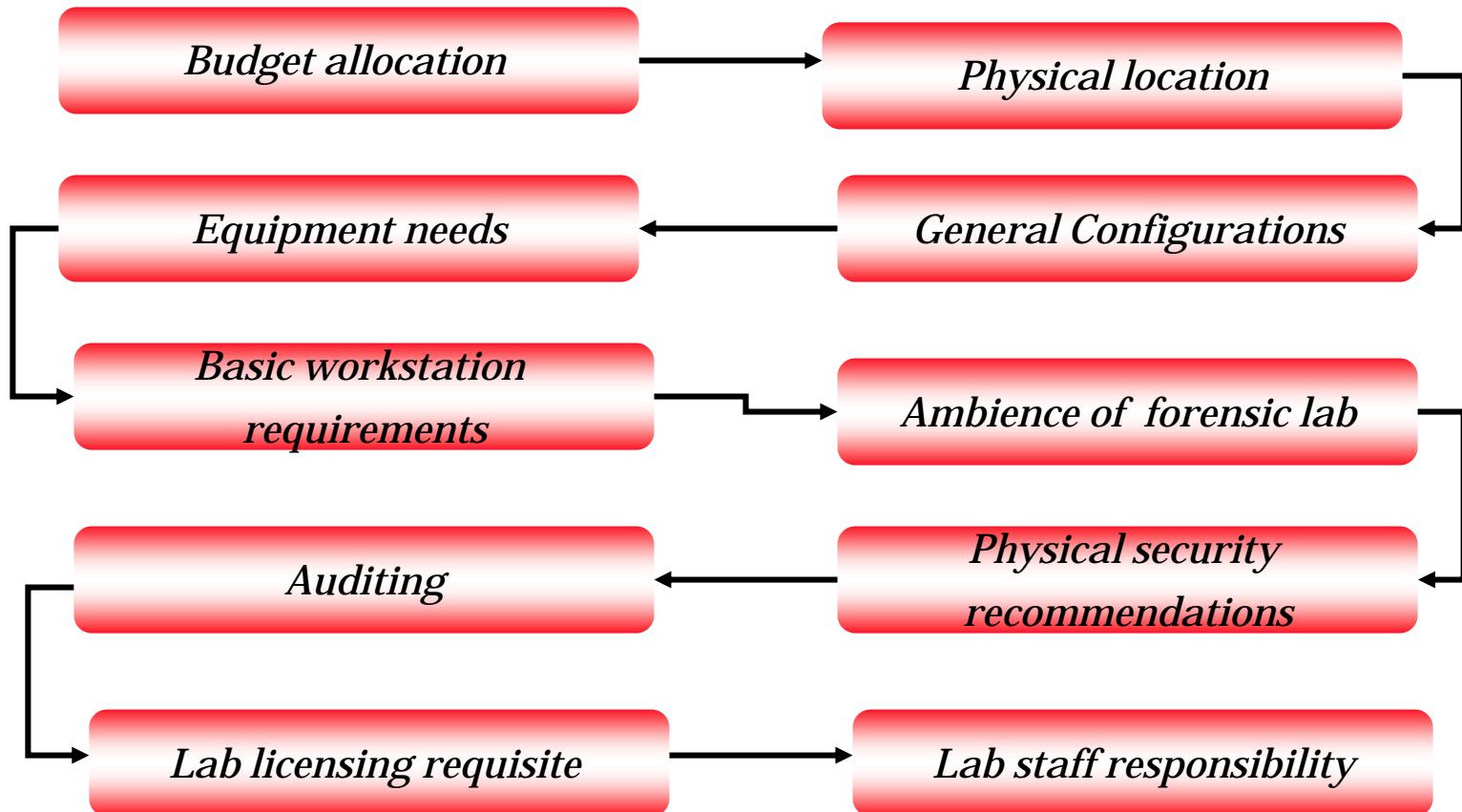
Certified Hacking Forensic Investigator

Module V Computer Forensic Laboratory Requirements

Module Objective

- Budget allocation for a forensic lab
- Physical location of a forensics lab
- General configuration of a forensics lab
- Equipment needs in a forensics lab
- Basic workstation requirements in a forensics lab
- Ambience of a forensics lab
- Physical security recommendations for a forensics lab
- Auditing for forensics lab
- Forensics lab licensing requisite
- Forensics lab staff responsibilities

Module Flow



Budget Allocation for a Forensics Lab

- Budget for a forensic lab is allocated by calculating the expected number of cases that would be examined
- Crime statistics of previous year and expected trend plays an important role in budgeting
- Space occupied, equipments required, personnel, training ,software and hardware requirements are taken into account while allocating a specific amount for the forensics lab
- The nature of forensic lab is also a determining factor



Physical Location Needs of a Forensic Lab

- Physical location requirements of a forensic lab:

- Site of the lab
- Access to the emergency services
- Lighting at the lab
- Physical milieu of the lab
- Structural design of parking



Work Area of a Computer Forensics Lab

- An ideal lab consists of two forensic workstations and one ordinary workstation with Internet connectivity
- Number of forensics workstations varies according to the number of cases and process handled in the lab
- The work area should have ample space so that there is space for case discussions among investigators.

General Configuration of a Forensic Lab

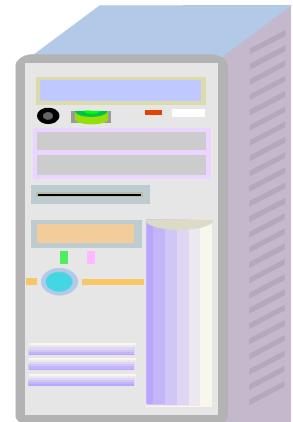
- A forensics lab should satisfy the minimum requirements needed for a forensic lab
- Following is a list of elements that a forensics lab should have:

- Workstation; both forensic and non- forensic
- UPS as a preventive measure against power failure
- Bookracks for the library
- Necessary software
- Reference materials
- Safe locker to store evidence
- LAN and Internet connectivity
- Storage shelves for unused equipments

Equipment Needs in a Forensics Lab

- Equipments required for a forensics lab depend on the nature of forensics investigation carried out in the lab
- Below listed are the common equipments that are necessary in a computer forensics lab:

- Forensic towers
- Printers
- Scanners
- Additional hard drives
- Tape drives



Ambience of a Forensics Lab

- ◉ Investigators spend long hours in a forensics lab, so it is of utmost importance that the lab environment is comfortable
- ◉ The height of ceilings, make of ceilings, walls, flooring etc all contribute to the ambience of a forensics lab
- ◉ Ergonomics, lighting, room temperature, communications form an important factor while considering the ambience of a computer forensics lab.



Ambience of a Forensics Lab:- Ergonomics

- Taken from Greek words
 - “Ergon” which means “work”;
 - “Nomoi” which means “natural laws”;
- Ergonomics is defined as the :

“The study of conniving equipment to meet the human requirements of comfort without affecting the efficiency.”



Environmental Conditions

- The following are the environmental conditions required for proper lab functioning
 - Large dimensions of the room.
 - High exchange rate of air per minute(in the lab)
 - Good cooling system to overcome excess heat generated by work station.
 - Allocation of workstations as per the room dimensions
 - Arrangement of computers as per the architecture of the lab.
 - It must be able to handle RAID server's heat output.

Recommended Eyestrain Considerations

- The following are the recommended to avoid eyestrain:

- Optimum distance from the monitor
- Ensure proper height of monitor and material
- Zoom option can be used to vary font size
- Screen filters must be used to clear the glare
- Lab must have proper ventilation
- Direct light on the monitor must be purged
- Eye check ups at regular intervals
- Take breaks at frequent intervals



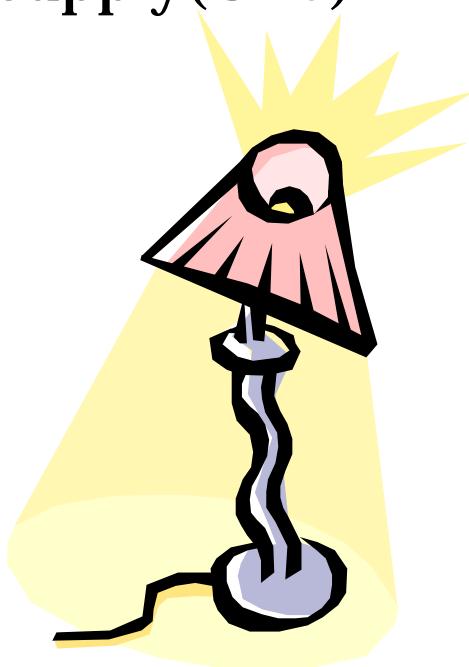
Structural Design Considerations

- The following are structural design considerations for a lab:
 - It must be a secure place
 - It must be constructed with heavy materials
 - It must not have any openings in the walls, ceilings and floors
 - It must not have windows in lab exterior
 - Check if computers are facing any internal or external windows



Electrical Needs

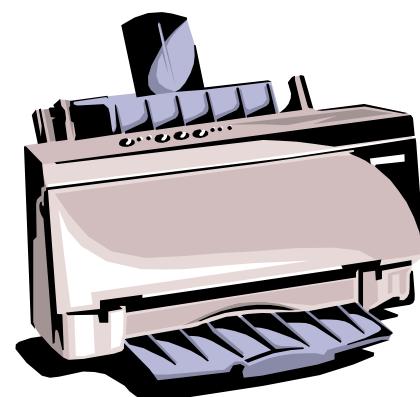
- The following are electrical needs of the lab:
 - The lab must be supplied with good amperage.
 - It must have easy electrical outlets.
 - There must be an uninterrupted Power supply(UPS) installed on all the computer systems



Communications

- The following are the communication considerations:

- Dedicated ISDN for network and voice communications
- Dial-up internet access must also be available
- Disconnect the forensic workstation from the network
- A dedicated network is preferred for the forensic computers



Basic Workstation Requirements in a Forensic Lab

- A basic forensics workstation should have the following:

- Processor with high computing speed
- 512 Mb RAM for satisfying minimum processing requirements.
- CD-ROM with read/write facility
- Motherboard which supports IDE, SCSI ,USB; slot for LAN/WAN card and a fan attached for cooling the processor
- Tape drive, USB drive
- Removable drive bays
- Monitor , keyboard , mouse according to comfort of investigator
- Minimum two hard drives for loading two different OS on each
- Extra RAM, hard disk incase of any need

Consider stocking the following hardware peripherals:

- The following hardware peripherals must be stocked as back-up:
 - 40-pin 18-inch and 36-inch IDE cables, both ATA-33 and ATA-100 or faster
 - Ribbon cables for floppy disks
 - Extra SCSI cards
 - Graphics cards, PCI and AGP
 - Extra power cords
 - A variety of hard disk drives
 - Laptop hard drive connectors
 - Handheld devices

Maintain Operating System and Application Inventories

- The following are the application inventories and operating systems that must be maintained:
 - Office XP, 2000, 97, 95
 - Quicken
 - Programming language applications such as Visual Studio
 - Specialized viewers such as QuickView and ACDC
 - Corel Office Suite
 - StarOffice/OpenOffice
 - Peachtree accounting applications

Common Terms

- ◉ Configuration Management:

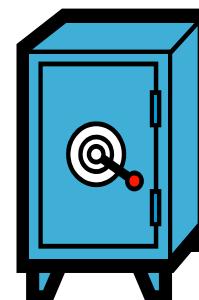
“The process of keeping track of all upgrades and patches you apply to your computer operating system and application software.”

- ◉ Risk Management:

“It is determining the amount of risk that is agreeable for process or operation.”

Physical Security Recommendations for a Forensic Lab

- Recommended to have only one entrance to a forensics lab
- Windows should not be kept open as a preventive measure against unauthorized access
- Log book at the entrance of the lab to log in the timings and name of the person visited
- An intrusion alarm system should be placed in the entrance
- Fire fighting equipments should be placed within and outside the lab



Fire-Suppression Systems

- The following are the fire suppression system considerations:
 - Install a dry chemical fire-suppression system.
 - Check the installation of sprinklers.
 - Accessibility to chemical fire extinguishers.



Evidence Locker Recommendations

- The following are the evidence locker recommendations:
 - The locker must be located at in the restricted area that is only accessible to lab personnel.
 - Authorization to the locker must be minimum.
 - All the lockers must be monitored properly and they must be locked when they are not under supervision.



Evidence Locker Combination Recommendations

- The following are the combinations of the evidence locker:
 - There must be equal security to both combination of container and content of the container
 - Destroy old combination after the new combination is created
 - Only authorized personnel must change the combination
 - Lock combination must be changed after every six months and when an authorized personnel leaves the company

Evidence Locker Padlock Recommendations

- The following are the evidence locker Padlock recommendations:
 - Custodian for distributing the keys
 - Sequential number for every duplicate key
 - Record the listing of the assigned key
 - Monthly audit to ensure no key is lost
 - Inventory of all keys must be maintained
 - Locks and keys must be changed annually
 - Master key must not used for several keys

Facility Maintenance

- ◉ The following are the facility maintenance steps:
 - Damages must be repaired immediately
 - Anti static pads must be used
 - Separate trash containers must be maintained.

Auditing a Computer Forensics Lab

- Steps to audit the computer forensic lab:
 - Scrutinize the ceiling, floor, roof, and exterior walls
 - Scrutinize the doors and locks
 - Check if the locks are working properly
 - Go through the visitors log
 - Examine the logs for evidence containers
 - Acquire evidence that is not being processed and store it at a secure place

Auditing a Forensics Lab

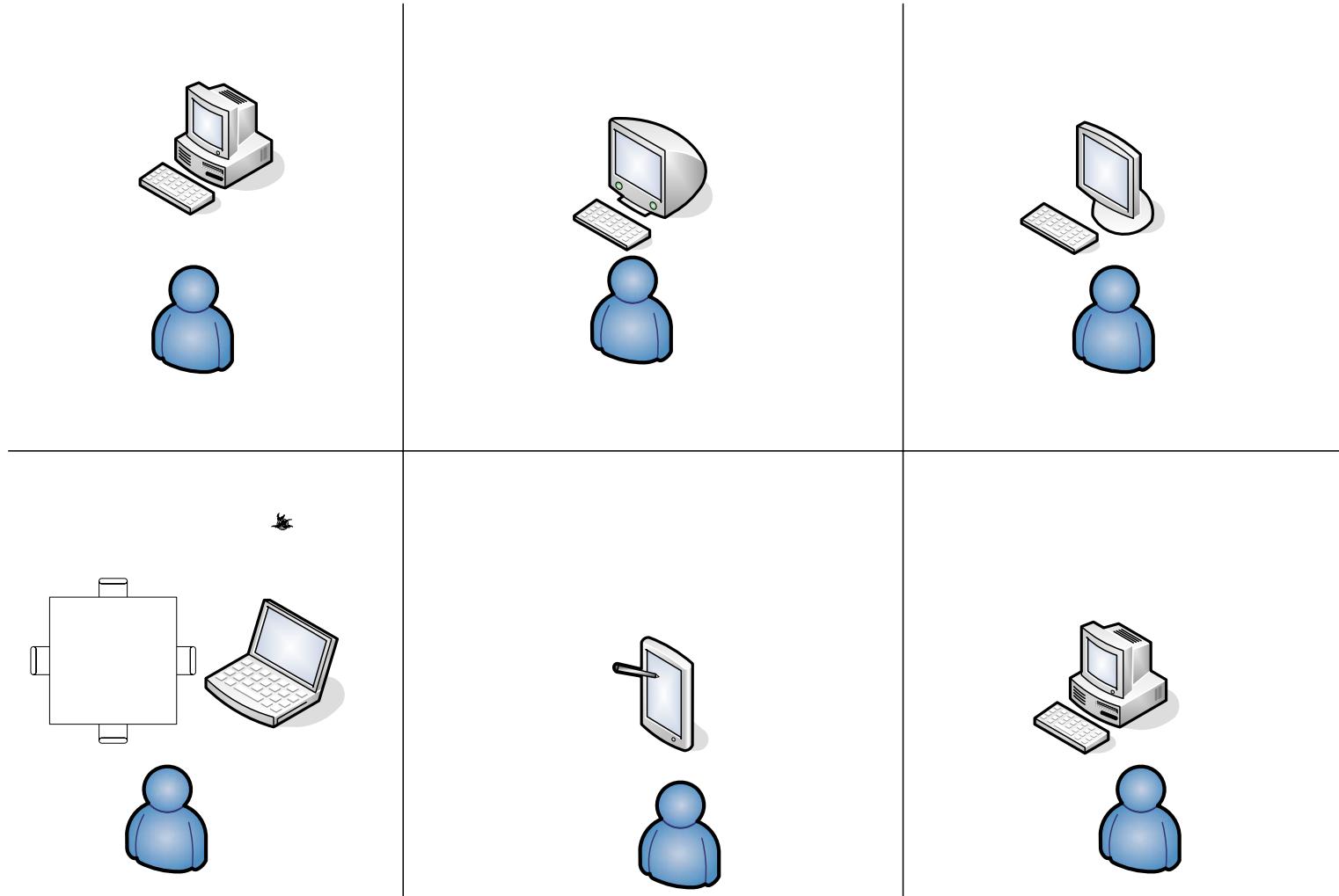
- Forensics lab should be under surveillance to protect it from intrusions
- The lab should be inspected on a regular basis to check if the policies and procedures implemented are followed or not
- The log file at the entrance of the lab should be verified
- Fire extinguishers should be manually checked to ensure its function



Forensics Lab



Mid Sized Lab



Forensic Lab Licensing Requisite

- The American Society of Crime Laboratory Directors (ASCLD) is an international body certifying forensics labs that investigate criminal cases by analyzing evidences
- Forensics labs around the globe seeking ASCLD/LAB certificate have to adhere to
 - **ISO/IEC 17025:1999**, General Requirements for the Competence of Testing and Calibration Laboratories and
 - **ASCLD/LAB**-International Supplemental Requirements for the Accreditation of Forensic Science Testing and Calibration Laboratories.

Forensic Lab Manager Responsibilities

⦿ The American Society of Crime Laboratory Directors has given guidelines for managers and supervisors of forensics lab. Following are few of them:

- Lab managers should ensure quality and efficient work
- Lab managers are responsible to ensure productivity
- Lab managers are responsible for the people they hire
- Development of the staff is the responsibility of the lab manager
- Lab managers should ensure a safe and sound working environment

Summary

- Budget for a forensic lab is allocated by calculating the expected number of cases that would be examined
- An ideal lab consists of two forensic workstations and one ordinary workstation with Internet connectivity
- The lab should be inspected on a regular basis to check if the policies and procedures implemented are followed or not
- The American Society of Crime Laboratory Directors (ASCLD) is an international body certifying forensics labs that investigate criminal cases by analyzing evidences



Computer Hacking Forensic Investigator

Module VI
**Understanding File systems
and Hard disks**

Introduction

In this networked world organizations need to manage systems, network, and applications running over them, which can enable effective data and resource sharing

No operating system can guarantee 100% security to the available resources and data. There are several shortcomings in their designs

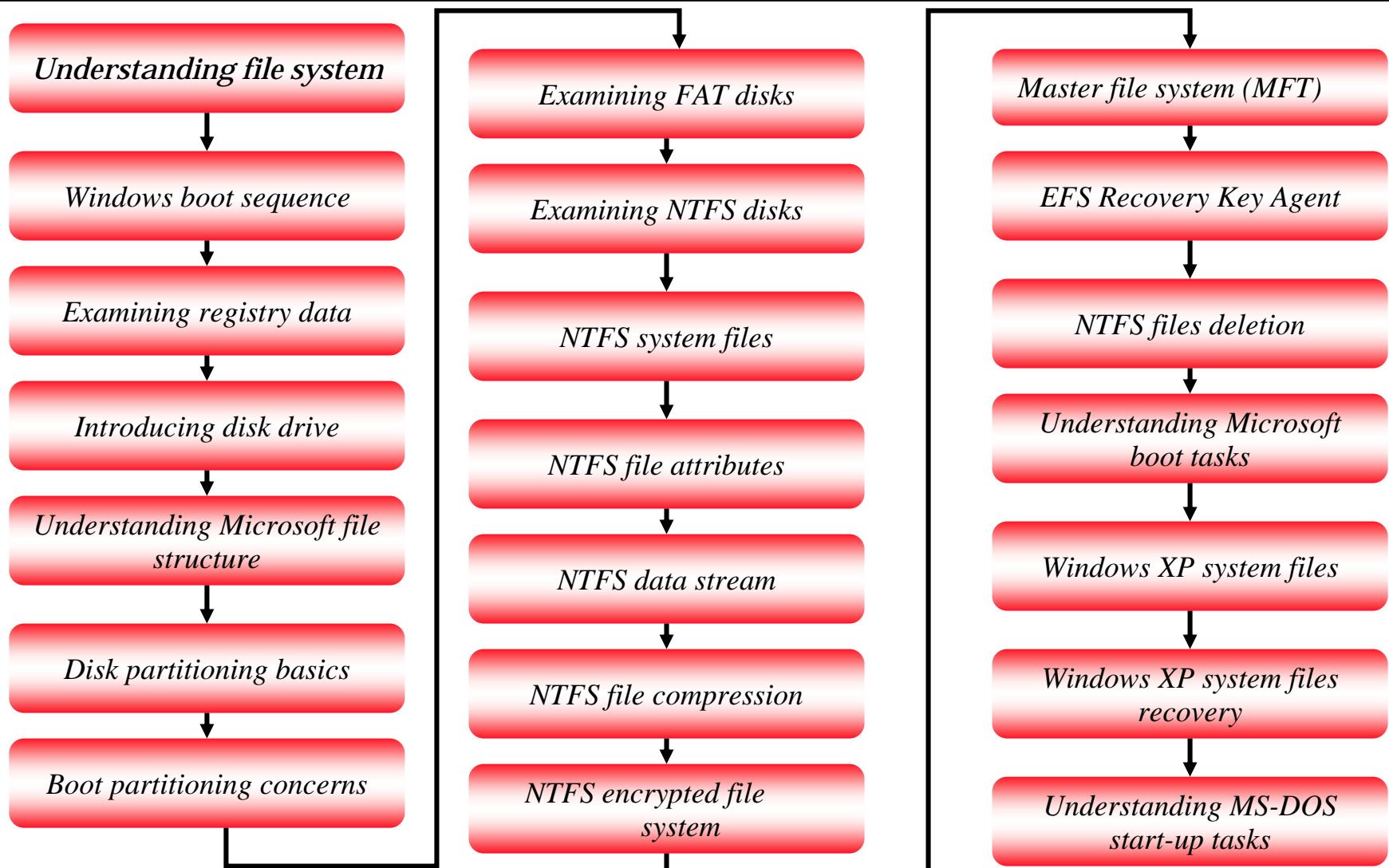
This situation, if exploited well by hackers can lead to end of any organization's business !!

The pitiable thing is that, end users are unaware of the vulnerabilities

Module Objective

- Understanding file systems
- Understanding the boot sequence
- Examining registry data
- Disk drive overview
- Exploring Microsoft file structures
- Disk partition concerns
- Boot partition concerns
- Examining FAT disks
- Examining NTFS disks
- NTFS system files
- NTFS attributes
- NTFS data streams
- NTFS compressed files
- NTFS Encrypted File Systems(EFS) and Master File Table(MFT)
- EFS Recovery Key Agent
- Deleting NTFS files
- Understanding Microsoft boot tasks
- Windows XP, 2000, and NT startup
- Windows XP system files
- Understanding MS-DOS startup tasks
- Other DOS operating systems

Module Flow



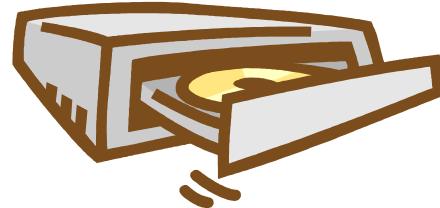
Disk Drive Overview - I

- ◉ There are two types of Disk drives:
 - Fixed storage drives
 - External storage drives
- ◉ Few of removable storage drives are:
 - Floppy disks
 - Compact Disks
 - Digital Versatile Disk (DVD)
 - ZIP Disks
 - r/m Drives

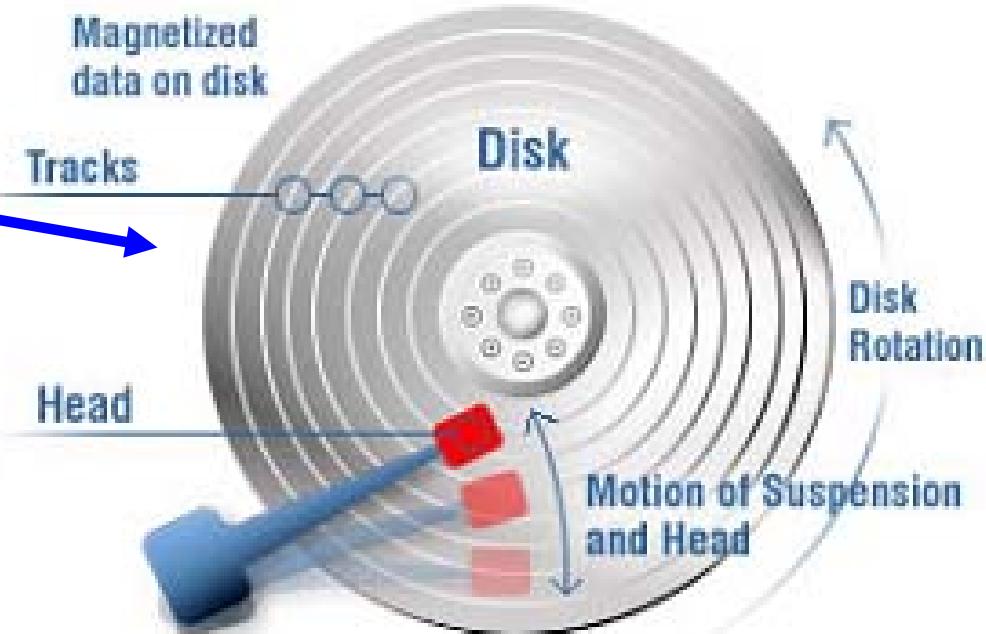


Disk Drive Overview - II

- Hard disk drive is a good example for permanent storage device
- The data is recorded magnetically onto the hard disk
- Main components of hard disk are:
 - Cylinders
 - Head
 - Platter
- The data is stored on the tracks of the sectors



Hard Disk



Disk Drive Overview-III

- The data is recorded onto the hard disk using the zoned bit recording
- Zoned Bit Recording:

It is the task of grouping the tracks by zones to ensure the same size of all the tracks

- The densities of the data on the disk drive are of two types namely:
 - Track density: It is the space between tracks on a disk
 - Areal density: It is defined as the number of bits per square inch on a platter
 - Bit density: It is bits per unit length of track

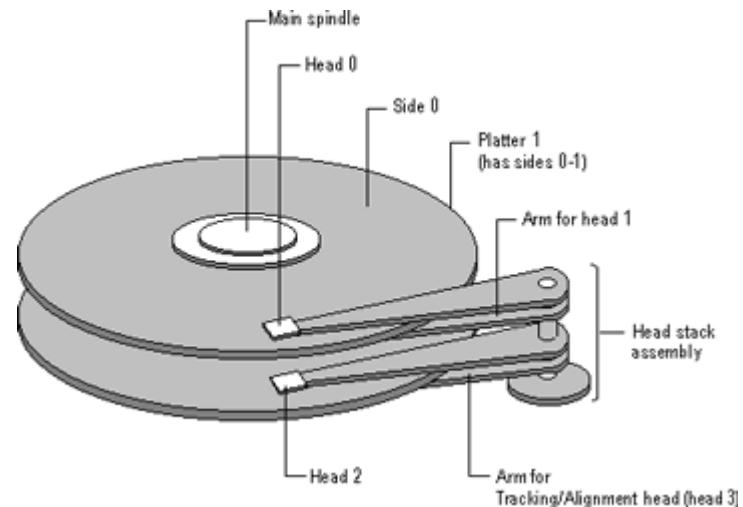


Hard Disk

- A hard disk is a sealed unit containing a number of platters in a stack. Hard disks may be mounted in a horizontal or a vertical position

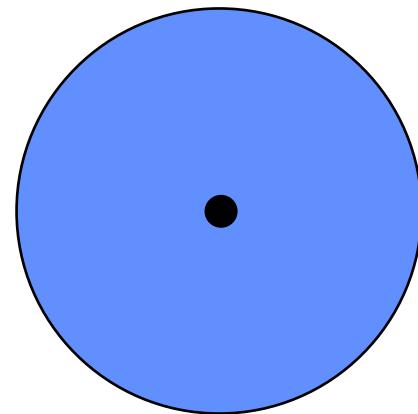
- Electromagnetic read/write heads are positioned above and below each platter

- As the platters spin, the drive heads move in toward the center surface and out toward the edge

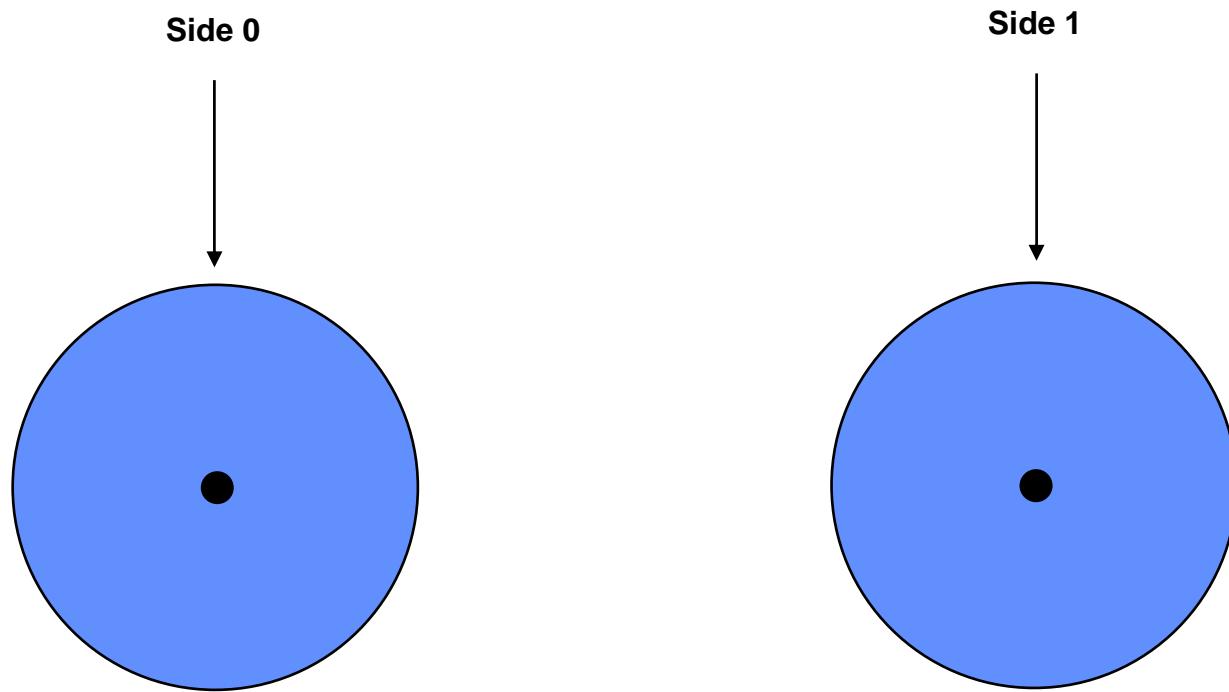


Disk Platter

- ◉ An aluminum alloy is used to make disk platter
- ◉ Glass and ceramic is used for modern day platters
- ◉ Magnetic media coating is done on the part where data resides
- ◉ Coating is done by iron oxide substance or cobalt alloy



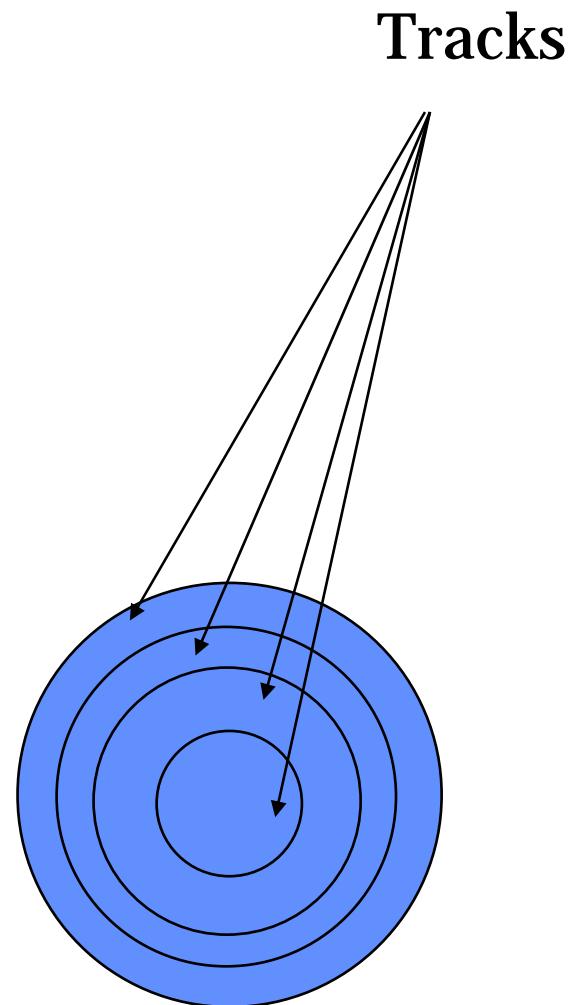
Disk Platter



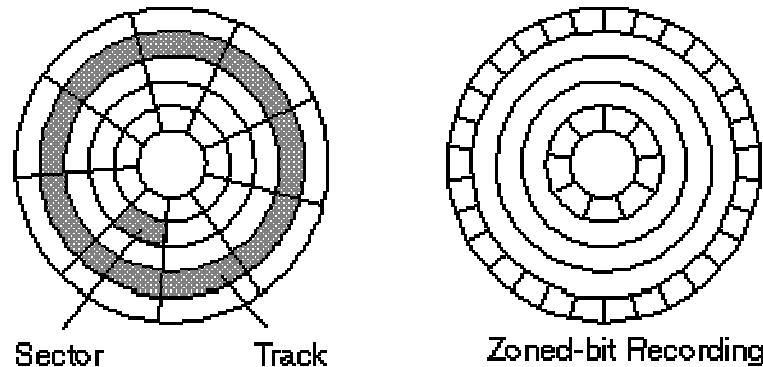
- Data is written on both sides of a hard disk platter
- Numbering is done on both the sides as ***side 0*** and ***side 1***

Tracks

- A circular ring on one side of the platter is known as track
- Drive head can access this circular ring in one position at a time
- Tracks are numbered for their identification
- Data exists in thin concentric bands on a hard disk
- A 3.5-inch hard disk consists of more than a thousand tracks



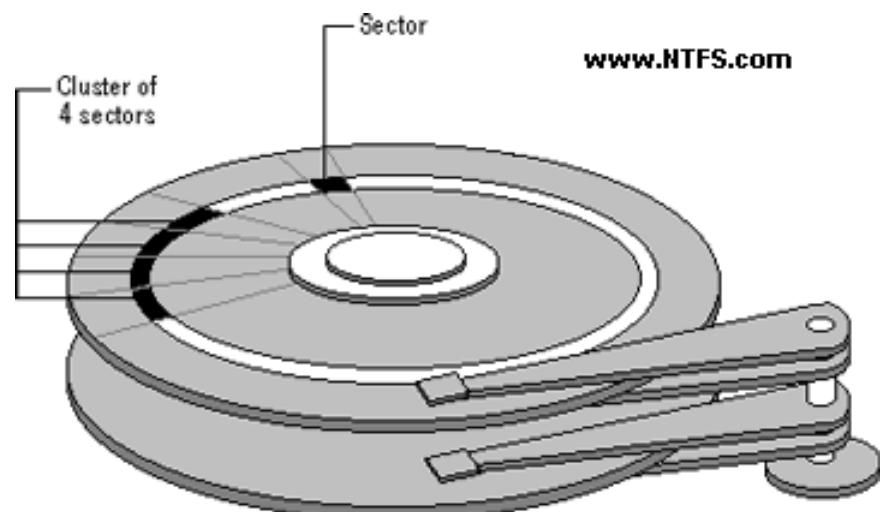
Tracks Numbering



- ① Tracks numbering begins from 0 at outer edge and moves towards center reaching the value of typically 1023
- ② A cylinder is formed when tracks are lined up

Sector

- Smallest physical storage unit on the disk
- Normally 512 bytes in size
- Factory track-positioning data determines labeling of disk sector
- Data is stored on the disk in contiguous series
- For example, if the file size is 600 bytes, two 512 k sectors are allocated for the file



Sector addressing

- Cylinders, heads and sectors determine address of individual sectors on the disk
- For example, on formatting a disk have 50 tracks divided into 10sectors each
- Track and sector numbers are used by operating system and disk drive to identify the stored information

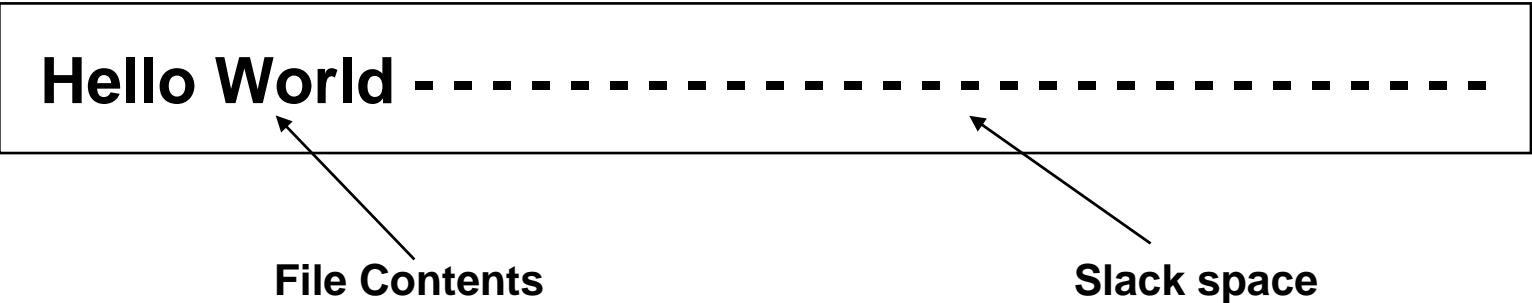
Cluster

- Smallest allocation unit of a hard disk
- Relevant formatting scheme determines range of tracks and sectors from 2 to 32
- Minimum size can be of one sector (1 sector / cluster)
- Allocation unit can be made of two or more sectors (2 sectors / cluster)
- Any read or write operation consumes space of at least 1 cluster
- Lot of slack space or unused space is wasted in the cluster beyond the data size in the sector

Cluster Size

- ◉ For optimum disk storage cluster size can be altered
- ◉ Larger cluster size(greater than one sector) will encounter the following points :
 - minimize fragmentation problem
 - greatly increases the probability for unused space in the cluster
 - reduces disk storage area to save information
 - also reduces unused area on the disk

Slack Space



- Slack space is the free space on the cluster after writing data on that cluster
- Dos and Windows utilizes fixed size clusters for file system
- If the size of stored data is less than the cluster size, the unused area remains reserved for the file resulting in slack space
- DOS and FAT 16(file allocation table) file system in the Windows utilizes very large sized clusters
- For example, if the partition size is 4 GB, each cluster will be 32 K. Even if a file needs only 10 K, the entire 32 K will be allocated, resulting in 22 K of slack space.

Lost Clusters

- Operating system marks cluster as used but not allocate them to any file such clusters are known a lost cluster
- Lost clusters can be reassigned data making disk space free
- ScanDisk utility has the capability to identify lost clusters in DOS and Windows operating system

Bad Sector



- ① A damaged portion of a disk on which no read/write operation can be performed
- ② Formatting a disk enables operating system to identify unusable sector and marks them as bad
- ③ Special software is used to recover the data on a bad sector

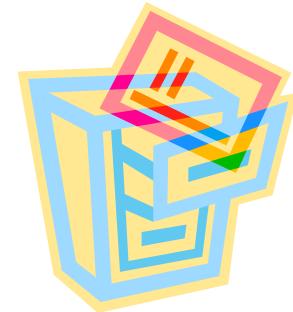
Understanding File Systems

- File system is a set of data types, which is employed for storage, hierarchical categorization, management, navigation, access, and recovering the data
- File system can use storage devices like hard disks, CD-ROM or floppy disk
- Command line or graphical user interface can be used to access the files
- File systems are arranged into tree-structured directories and directories require access authorization



Types of File System

- File system are classified into four types. They are:
 - Disk file systems
 - Network file systems
 - Database file systems
 - Special purpose file systems



List of Disk File Systems

- ◉ ADFS – Acorn filing system, successor to DFS.
- ◉ BFS – the Be File System used on BeOS
- ◉ EFS – Encrypted filesystem, An extension of NTFS
- ◉ EFS (IRIX) – an older block filing system under IRIX.
- ◉ Ext – Extended filesystem, designed for Linux systems
- ◉ Ext2 – Extended filesystem 2, designed for Linux systems
- ◉ Ext3 – Extended filesystem 3, designed for Linux systems, (ext2+journalling)
- ◉ FAT – Used on DOS and Microsoft Windows, 12 and 16 bit table depths
- ◉ FAT32 – FAT with 32 bit table depth
- ◉ FFS (Amiga) – Fast File System, used on Amiga systems. Nice for floppies, but fairly useless on hard drives.
- ◉ FFS – Fast File System, used on *BSD systems
- ◉ Files-11 – OpenVMS filesystem
- ◉ HFS – Hierarchical File System, used on older Mac OS systems

- HFS Plus – Updated version of HFS used on newer Mac OS systems
- HFSX – Updated version of HFS Plus to remove some backward compatibility limitations.
- HPFS – High Performance Filesystem, used on OS/2
- ISO 9660 – Used on CD-ROM and DVD-ROM discs (Rock Ridge and Joliet are extensions to this)
- JFS – IBM Journaling Filesystem, provided in Linux, OS/2, and AIX
- kfs
- LFS – Log-structured filesystem
- MFS – Macintosh File System, used on early Mac OS systems
- Minix file system – Used on Minix systems
- NTFS – Used on Windows NT based systems
- OFS – Old File System, on Amiga.

List of Disk File Systems

- PFS – and PFS2, PFS3, etc. Technically interesting filesystem available for the Amiga, performs very well under a lot of circumstances. Very simple and elegant.
- ReiserFS – Filesystem which uses journaling
- Reiser4 – Filesystem which uses journaling, newest version of ReiserFS
- SFS – Smart File System, available for the Amiga.
- Sprite – The original log-structured filesystem.
- UDF – Packet based filesystem for WORM/RW media such as CD-RW and DVD.
- UFS – Unix Filesystem, used on older BSD systems
- UFS2 – Unix Filesystem, used on newer BSD systems
- UMSDOS – FAT filesystem extended to store permissions and metadata, used for Linux.
- VxFS – Veritas file system, first commercial journaling file system; HP-UX, Solaris, Linux, AIX
- XFS – Used on SGI IRIX and Linux systems
- ZFS – Used on Solaris 10

List of Network file systems

- AFS (Andrew File System)
- AppleShare
- CIFS (Microsoft's documented version of SMB)
- Coda
- GFS
- InterMezzo
- Lustre
- NFS
- OpenAFS
- SMB (sometimes also called Samba filesystem)

Special Purpose File systems

- acme (Plan 9) (text windows)
- archfs (archive)
- cdfs (reading and writing of CDs)
- cfs (caching)
- Davfs2 (WebDAV)
- DEVFS
- ftpfs (ftp access)
- Infs (long names)
- LUFS (replace ftpfs, ftp ssh ... access)
- nntpfs (netnews)
- plumber (Plan 9) (interprocess communication – pipes)
- PROCFS
- ROMFS
- TMPFS
- wikifs (wiki wiki)

Popular Linux File systems

○ EXT (Extended File System)

- First filesystem for the Linux operating system to overcome certain limitations of the Minix file system
- Quickly replaced by the second extended file system

○ EXT2 (Second Extended File System)

- Standard filesystem with improved algorithms used on the Linux operating system for a number of years
- Not a journaling file system

○ EXT3 (Third Extended File System)

- Journalled filesystem used in the GNU/Linux operating system
- Can be mounted and used as an Ext2 filesystem
- Can use file system maintenance utilities (like fsck) for maintaining and repairing alike Ext2 filesystem

Sun Solaris 10 File system - ZFS

- ZFS is a filesystem first used in Sun Microsystems Solaris 10
 - Uses 128-bit addressing to perform read/write operation referred to as a "giga-terabyte" (a zettabyte)
 - Any modification to this filesystem will never increase its storage capacity
- Main Features:
 - Facilitates immediate backup as the file is written
 - Introduced Logical Volume Management(LVM) features into the filesystem
 - File systems are portable between little-endian and big-endian systems
 - Provides data integrity to detect and correct errors
 - HA Storage+ feature provides cluster/failover compatibility in case of any interruption(only one server is empowered to perform write operation on the disk)
 - Creates many copies of the single snapshot with minimum overheads
 - Deletes all the unused memory space out of files
 - Supports full range of NFSv4/Windows NT-style ACLs

Windows File systems

- **FAT (File Allocation Table)**

- 16 bit file system developed for MS-DOS
- Used in consumer versions of Microsoft Windows till Windows Me
- Considered relatively uncomplicated and became popular format for devices like floppy disks, USB devices, Digital cameras, flash disks

- **FAT32**

- 32 bit version of FAT file system with storage capacity up to 2 GB

- **NTFS (New Technology File System)**

- NTFS has three versions
 - v1.2 (v4.0) found in NT 3.51 and NT 4
 - v3.0 (v5.0) found in Windows 2000 and
 - v3.1 (v5.1) found in Windows XP and Windows Server 2003
- Newer versions added extra features like quotas introduced by Windows 2000. In NTFS, anything such as file name, creation date, access permissions and even contents is written down as metadata

Mac OS X File system

◉ HFS (Hierarchical File System)

- Developed by Apple Computer to support Mac Operating System
- Traditionally used by floppy and hard disks but now also used by CD-ROMs

◉ UFS (UNIX file system)

- Derived from the Berkeley Fast File System (FFS) that was originally developed at Bell Laboratories from first version of UNIX FS
- All BSD UNIX derivatives including FreeBSD, NetBSD, OpenBSD, NeXTStep, and Solaris use a variant of UFS
- Acts as a substitute for HFS in Mac OS X

CD-ROM / DVD File system

- ISO 9660 (International Organization for Standardization) defines a file system for CD-ROM and DVD-ROM media
- To exchange data it supports various computer operating systems like Microsoft Windows, Mac OS, and UNIX based systems
- There are some extensions to ISO 9660 to cope up its demerits
 - Longer ASCII coded names and UNIX permissions are facilitated by Rock Ridge
 - Unicode naming (like non roman scripts)are also supported by Joliet
 - Bootable CDs are facilitated by El Torito
- ISO 13490 is combination of ISO 9660 with multisession support

File system Comparison

File system:	NTFS	FAT32	Mac OS X UFS	HFS+	ext2	ext3	ReiserFS	XFS	JFS	FFS	Be File System
Creator	Microsoft, Gary Kimura, Tom Miller	Microsoft	Apple	Apple	R&D Card	Stephen Tweedie	Namesys	SGI	IBM	Marshall McKusick	Be Inc., D. Giampaolo, C. Meurillon
Original operating system	Windows NT	Windows 95 ¹⁰	Mac OS X	Mac OS	Linux	Linux	Linux	IRIX	AIX ¹¹	BSD	BeOS
<i>Limits</i>											
Maximum filename length	255 bytes	255 bytes	?	255 characters ¹	255 bytes	255 bytes	4096 bytes/255 characters	255 bytes	?	?	?
Allowable filename characters	Space plus any printable except\ / : ? * " > <	Space plus any printable except\ / : ? * " > <	Any Non-null except /	Any Unicode ² except :	Any Non-null except /	Any Non-null except /	Any Non-null except /	Any Non-null except /	?	Any Non-null except /	?
Maximum pathname length	32767 bytes	at least 260 bytes	?	?	No limit defined ³	No limit defined ³	?	?	?	?	?
Maximum file size	16EB	4GB	?	8EB	16GB to 2TB ⁴	16GB to 2TB ⁴	8TB ⁸	9EB ⁹	8EB	8TB	?
Maximum volume size	16EB	2-8TB ^{4,7}	?	?	2TB to 32TB ⁴	2TB to 32TB ⁴	16TB	9EB ⁹	512TB to 4PB ⁴	?	?
<i>Features</i>											
File type metadata	None (file extensions)	None (file extensions)	rich (type and creator)	rich (type and creator)	None (file extensions or magic numbers)	None (file extensions or magic numbers)	?	rich (extended attributes)	?	None (file extensions)	rich
Stores file owner	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
POSIX file permissions	No ⁵	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Access control lists	Yes	No	No	No	No ⁶	No ⁶	No ⁶	No ⁶	No ⁶	No	No
Hard links	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Soft links	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Alternate data stream / resource fork	Yes	No	No	Yes	No	No	No	No	No	No	No
Journaling	Yes	No	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes
File system:	NTFS	FAT32	Mac OS X UFS	HFS+	ext2	ext3	ReiserFS	XFS	JFS	FFS	Be File System

Boot Sector

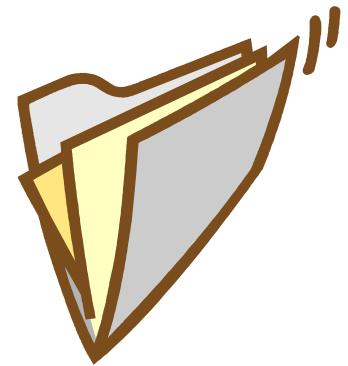
- Boot Sector is the first sector (512 bytes) of a FAT file system
- Unix-like terminology defines it as superblock

```
000000 eb 3c 90 4d 53 44 4f 53 35 2e 30 00 02 01 01 00
000010 02 e0 00 40 0b f0 09 00 12 00 02 00 00 00 00 00
000020 00 00 00 00 00 00 29 ca 18 39 19 4d 53 44 4f 53
000030 20 20 20 20 20 20 46 41 54 31 32 20 20 20 fa 33
000040 c0 8e d0 bc 00 7c 16 07 bb 78 00 36 c5 37 1e 56
000050 16 53 bf 3e 7c b9 0b 00 fc f3 a4 06 1f c6 45 fe
000060 0f 8b 0e 18 7c 88 4d f9 89 47 02 c7 07 3e 7c fb
000070 cd 13 72 79 33 c0 39 06 13 7c 74 08 8b 0e 13 7c
000080 89 0e 20 7c a0 10 7c f7 26 16 7c 03 06 1c 7c 13
000090 16 1e 7c 03 06 0e 7c 83 d2 00 a3 50 7c 89 16 52
0000a0 7c a3 49 7c 89 16 4b 7c b8 20 00 f7 26 11 7c 8b
0000b0 1e 0b 7c 03 c3 48 f7 f3 01 06 49 7c 83 16 4b 7c
0000c0 00 bb 00 05 8b 16 52 7c a1 50 7c e8 92 00 72 1d
0000d0 b0 01 e8 ac 00 72 16 8b fb b9 0b 00 be e6 7d f3
0000e0 a6 75 0a 8d 7f 20 b9 0b 00 f3 a6 74 18 be 9e 7d
0000f0 e8 5f 00 33 c0 cd 16 5e 1f 8f 04 8f 44 02 cd 19
000100 58 58 58 eb e8 8b 47 1a 48 48 8a 1e 0d 7c 32 ff
000110 f7 e3 03 06 49 7c 13 16 4b 7c bb 00 07 b9 03 00
000120 50 52 51 e8 3a 00 72 d8 b0 01 e8 54 00 59 5a 58
000130 72 bb 05 01 00 83 d2 00 03 1e 0b 7c e2 e2 8a 2e
000140 15 7c 8a 16 24 7c 8b 1e 49 7c a1 4b 7c ea 00 00
000150 70 00 ac 0a c0 74 29 b4 0e bb 07 00 cd 10 eb f2
000160 3b 16 18 7c 73 19 f7 36 18 7c fe c2 88 16 4f 7c
000170 33 d2 f7 36 1a 7c 88 16 25 7c a3 4d 7c f8 c3 f9
000180 c3 b4 02 8b 16 4d 7c b1 06 d2 e6 0a 36 4f 7c 8b
000190 ca 86 e9 8a 16 24 7c 8a 36 25 7c cd 13 c3 0d 0a
0001a0 47 65 65 6e 20 73 79 73 74 65 65 6d 73 63 68 69
0001b0 6a 66 20 6f 66 20 73 63 68 69 6a 66 66 6f 75 74
0001c0 0d 0a 56 65 72 76 61 6e 67 20 64 69 73 6b 65 74
0001d0 74 65 20 65 6e 20 64 72 75 6b 20 6f 70 20 74 6f
0001e0 65 74 73 0d 0a 00 49 4f 20 20 20 20 20 20 53 59
0001f0 53 4d 53 44 4f 53 20 20 20 53 59 53 00 00 55 aa
```

Exploring Microsoft File Structures

- **Filesystems:**

- File Allocation Tables (FAT)
- New technology File system(NTFS)
- High Performance File system



- Windows supports two types of file systems on CD-ROM and Digital Versatile Disk (DVD):

- Compact Disc File System (CDFS)
- Universal File System (UDF)

- A file system can be chosen as per the storage needs of the organization and the type of operating system used

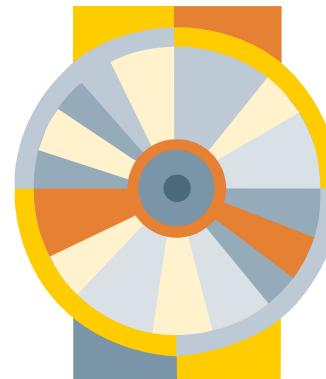
Exploring Microsoft File Structures

FAT vs. NTFS:

File Allocation Table(FAT)	New Technology File System(NTFS)
A table, which tracks all the system storage changes.	A latest file system developed specially for Windows 2000.
Versions available are FAT12,FAT16,FAT32	NTFS is the only version.
Supported in all versions of windows operating system	Supports all the operating systems after windows 2000
Doesn't support large file names.	Supports large file names.
Doesn't support extremely large storage media.	Supports extremely large storage media.
Doesn't support file system recovery.	Supports file system recovery.

Exploring Microsoft File Structures

- Cluster is defined as the smallest amount of space allocated by the operating system to hold a file
- Cluster is more efficient if size of the cluster is small
- There is no default size for the cluster
- The cluster address allocated by the operating system is called logical address
- The physical addresses are the addresses that exists at firmware or hardware level



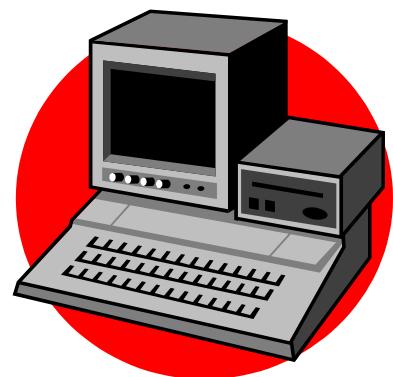
Disk Partition Concerns

- Partitioning of hard disk drive is done for effective storage management of data
- Partition is logical part of the disk that holds data
- It can be divided into
 - Primary Partition
 - Extended Partition
- A basic disk can have one primary partition and any number of extended partition
- Windows look for primary partition to start the computer. This active partition contains the boot files used to start an operating system
- Inter-partition gap is unused or void space between the primary and first logical partition



Boot Partition Concerns

- The information regarding the files on the disk, their location, size and other important data is stored in the Master Boot Record file
- Every disk has Master Boot Record that contains the information about partitions on the disk
- User can choose the operating system by using the third party boot utilities, which change the Master Boot record



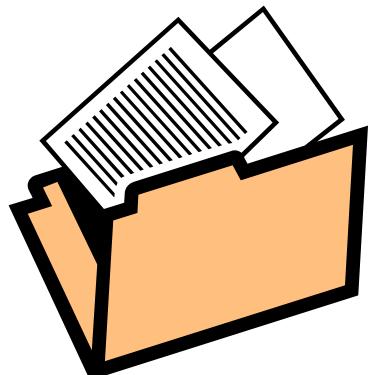
Examining FAT

- When a file is deleted from the operating system it replaces the first word of the file name by a lower case Greek letter. The space is made available for new files
- These files can be recovered using forensic tools
- Few tools which can be used for forensics are:
 - WINHEX
 - UNDELETE
 - FILE SCAVENGER



NTFS

- New Technology File System was introduced by Microsoft
- In NTFS every data written on the disk is considered as the file
- Partition Boot Sector is the first data set on the disk
- After the PBS, the first file set is Master File Table, which occupies space 12.5% to 50% of disk space
- NTFS uses UNICODE data format



NTFS System Files

File name	Description
\$attrdef	Contains definitions of all system and user-defined attributes of the volume
\$badclus	Contains all the bad clusters
\$bitmap	Contains bitmap for the entire volume
\$boot	Contains the volume's bootstrap
\$logfile	Used for recovery purposes
\$mft	Contains a record for every file
\$mftmirr	Mirror of the MFT used for recovering files
\$quota	Indicates disk quota for each user
\$upcase	Converts characters into uppercase Unicode
\$volume	Contains volume name and version number

NTFS Partition Boot Sector

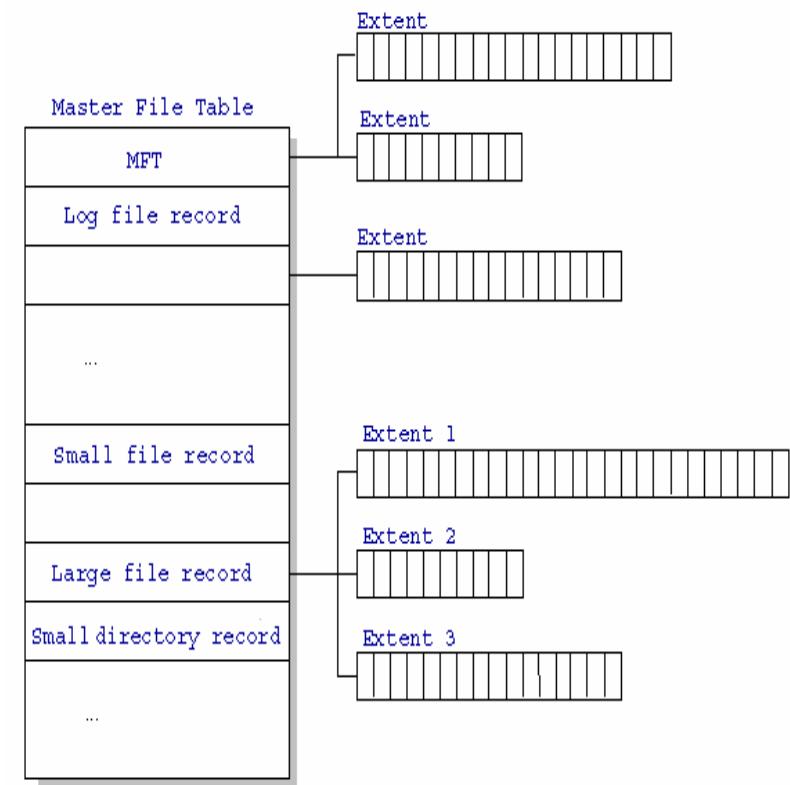
- When you format an NTFS volume, the format program allocates the first 16 sectors for the boot sector and the bootstrap code.

```
Physical Sector:Cyl 0, Side 1, Sector 1
00000000:EB 52 90 4E 54 46 53 20 -20 20 20 20 00 02 08 00 00 .R.NTFS .....
00000010:00 00 00 00 00 F8 00 00 -3F 00 FF 00 3F 00 00 00 .....?....?
00000020:00 00 00 00 80 00 80 00 -4A F5 7F 00 00 00 00 00 .....J.....
00000030:04 00 00 00 00 00 00 00 -54 FF 07 00 00 00 00 00 .....T.....
00000040:F6 00 00 00 01 00 00 00 -14 A5 1B 74 C9 1B 74 1C .....t.t.
00000050:00 00 00 00 FA 33 C0 8E -D0 BC 00 7C FB B8 C0 07 ....3.....|....
00000060:8E D8 E8 16 00 B8 00 0D -8E C0 33 DB C6 06 0E 00 .....3.....
00000070:10 E8 53 00 68 00 0D 68 -6A 02 CB 8A 16 24 00 B4 ..S.h..hj....$..
00000080:08 CD 13 73 05 B9 FF FF -8A F1 66 0F B6 C6 40 66 ...s.....f...@f
00000090:0F B6 D1 80 E2 3F F7 E2 -86 CD C0 ED 06 41 66 0F .....?.....Af.
000000A0:B7 C9 66 F7 E1 66 A3 20 -00 C3 B4 41 BB AA 55 8A ..f..f....A..U.
000000B0:16 24 00 CD 13 72 0F 81 -FB 55 AA 75 09 F6 C1 01 .$.r...U.u....
000000C0:74 04 FE 06 14 00 C3 66 -60 1E 06 66 A1 10 00 66 t.....f`..f...f
000000D0:03 06 1C 00 66 3B 06 20 -00 0F 82 3A 00 1E 66 6A ....f;.....fj
000000E0:00 66 50 06 53 66 68 10 -00 01 00 80 3E 14 00 00 .fP.Sfh....>...
000000F0:0F 85 0C 00 E8 B3 FF 80 -3E 14 00 00 0F 84 61 00 .....>....a.
00000100:B4 42 8A 16 24 00 16 1F -8B F4 CD 13 66 58 5B 07 .B..$.....fx [...]
00000110:66 58 66 58 1F EB 2D 66 -33 D2 66 0F B7 0E 18 00 fx_fx.-f3.f.....
00000120:66 F7 F1 FE C2 8A CA 66 -8B D0 66 C1 EA 10 F7 36 f.....f..f....6
00000130:1A 00 86 D6 8A 16 24 00 -8A E8 C0 E4 06 0A CC B8 .....$.....
00000140:01 02 CD 13 0F 82 19 00 -8C C0 05 20 00 8E C0 66 .....f
00000150:FF 06 10 00 FF 0E 0E 00 -0F 85 6F FF 07 1F 66 61 .....o....fa
00000160:C3 A0 F8 01 E8 09 00 A0 -FB 01 E8 03 00 FB EB FE .....  

00000170:B4 01 8B F0 AC 3C 00 74 -09 B4 0E BB 07 00 CD 10 .....<.t.....
00000180:EB F2 C3 0D 0A 41 20 64 -69 73 6B 20 72 65 61 64 .....A disk read
00000190:20 65 72 72 6F 72 20 6F -63 63 75 72 72 65 64 00 error occurred.
000001A0:0D 0A 4E 54 4C 44 52 20 -69 73 20 6D 69 73 73 69 ..NTLDR is missi
000001B0:6E 67 00 0D 0A 4E 54 4C -44 52 20 69 73 20 63 6F ng...NTLDR is co
000001C0:6D 70 72 65 73 73 65 64 -00 0D 0A 50 72 65 73 73 mpressed...Press
000001D0:20 43 74 72 6C 2B 41 6C -74 2B 44 65 6C 20 74 6F Ctrl+Alt+Del to
000001E0:20 72 65 73 74 61 72 74 -0D 0A 00 00 00 00 00 00 restart.....
000001F0:00 00 00 00 00 00 00 00 -83 A0 B3 C9 00 00 55 AA .....U.
```

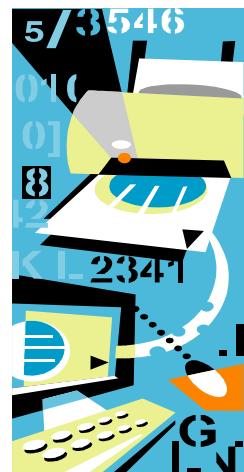
NTFS Master File Table (MFT)

- Each file on an NTFS volume is represented by a record in a special file called the master file table (MFT).
- NTFS reserves the first 16 records of the table for special information.
- The first record of this table describes the master file table itself, followed by a MFT mirror record.
- If the first MFT record is corrupted, NTFS reads the second record to find the MFT mirror file, whose first record is identical to the first record of the MFT.
- The locations of the data segments for both the MFT and MFT mirror file are recorded in the boot sector. A duplicate of the boot sector is located at the logical center of the disk.
- The third record of the MFT is the log file, used for file recovery. The seventeenth and following records of the master file table are for each file and directory (also viewed as a file by NTFS) on the volume.

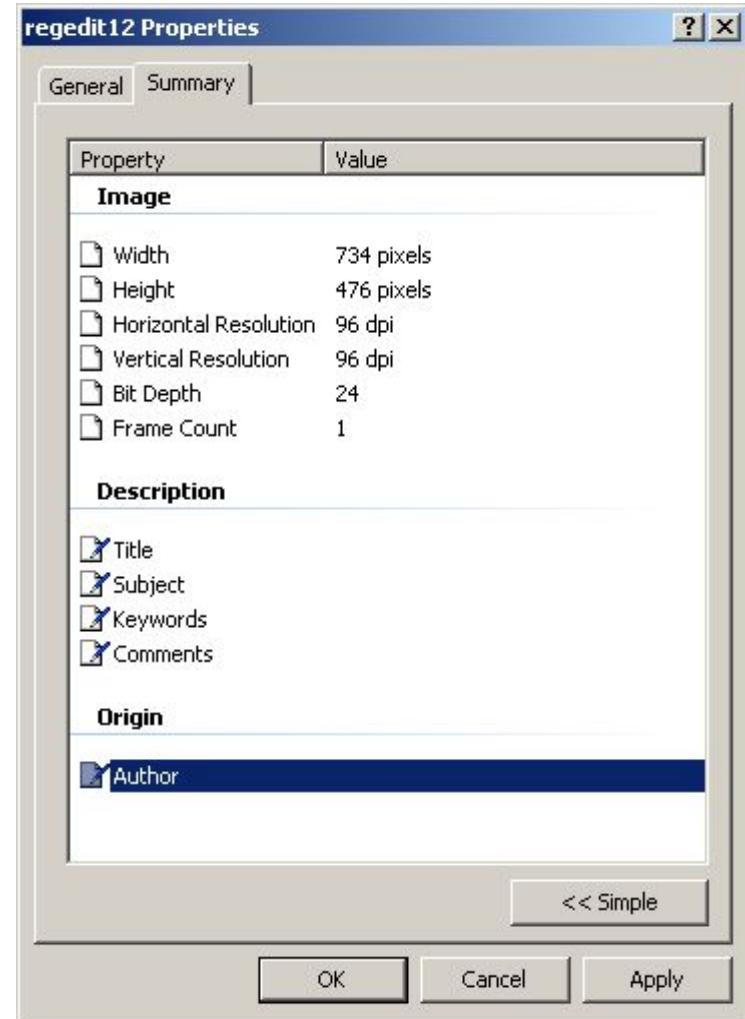
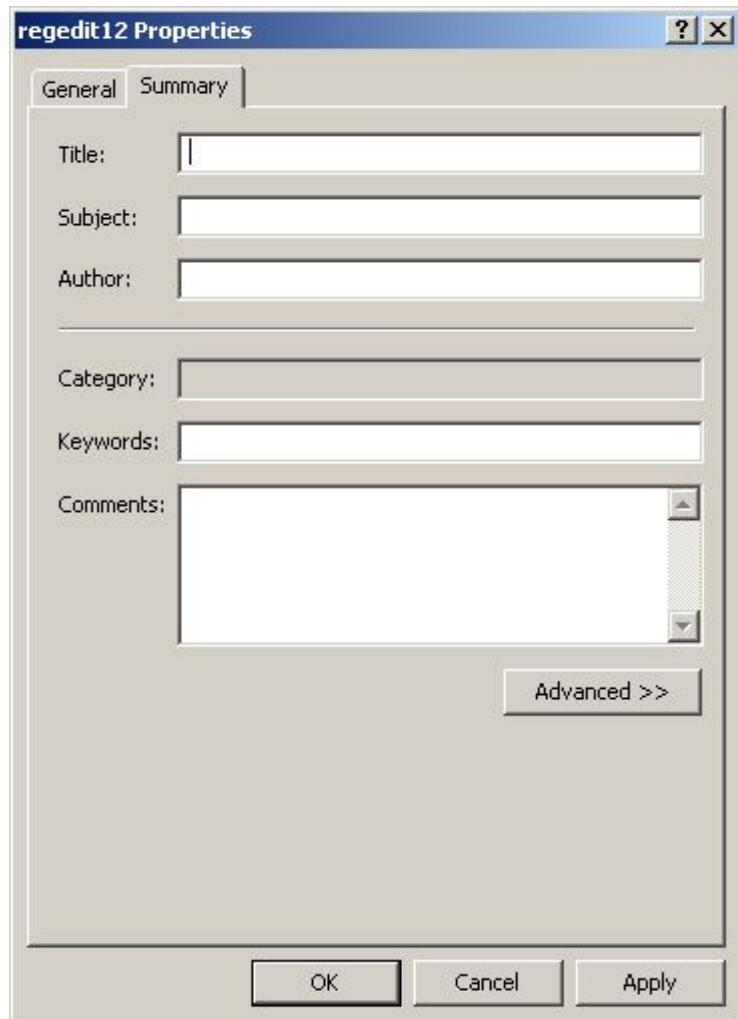


NTFS Attributes-I

- Every file has a unique identities like
 - Name
 - Security information and
 - It can also contain metadata of file system in the file.
- Every attribute is identified by an attribute type code.
- There are two categories of attributes:
 - *Resident attributes* : These are the attributes that are contained in the MFT.
 - *Non-resident attributes*: These are the attributes that are allocated one or more clusters of disk space.



NTFS Attributes-II



NTFS Data Stream-I

- A sequence of bytes is called data stream
- Data can be added to the stream when examining the attributes of the file
- Data streams can create obscure data intentionally or by coincidence
- In this file system data stream becomes an data attribute of the a file
- Data stream can be created by using the following command

```
C:\ECHO text_message > myfile.txt  
:stream1
```



NTFS Data Stream-II

1

```
C:\Command Prompt  
C:\pqr>dir  
Volume in drive C has no label.  
Volume Serial Number is 30FC-7EDD  
  
Directory of C:\pqr  
  
04/08/2005  06:47p      <DIR> .  
04/08/2005  06:47p      <DIR> ..  
                0 File(s)          0 bytes  
                2 Dir(s)   6,036,811,776 bytes free  
  
C:\pqr>
```

2

```
C:\Command Prompt  
C:\pqr>dir  
Volume in drive C has no label.  
Volume Serial Number is 30FC-7EDD  
  
Directory of C:\pqr  
  
04/08/2005  06:47p      <DIR> .  
04/08/2005  06:47p      <DIR> ..  
                0 File(s)          0 bytes  
                2 Dir(s)   6,036,811,776 bytes free  
  
C:\pqr>ECHO text_message > myfile.txt:stream1  
  
C:\pqr>
```

NTFS Data Stream-III

3

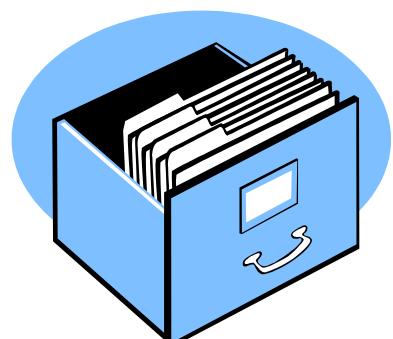
```
C:\ Command Prompt  
C:\pqr>dir  
Volume in drive C has no label.  
Volume Serial Number is 30FC-7EDD  
  
Directory of C:\pqr  
  
04/08/2005  06:47p      <DIR>          .  
04/08/2005  06:47p      <DIR>          ..  
                0 File(s)   0 bytes  
                2 Dir(s)  6,036,811,776 bytes free
```

```
C:\pqr>ECHO text_message > myfile.txt  
  
C:\pqr>more < myfile.txt:stream1  
text_message  
  
C:\pqr>  
  
C:\ Command Prompt  
C:\pqr>ECHO text_message > myfile.txt:stream1  
  
C:\pqr>more < myfile.txt:stream1  
text_message  
  
C:\pqr>dir  
Volume in drive C has no label.  
Volume Serial Number is 30FC-7EDD  
  
Directory of C:\pqr  
  
04/08/2005  06:49p      <DIR>          .  
04/08/2005  06:49p      <DIR>          ..  
04/08/2005  06:49p      0 myfile.txt  
                1 File(s)   0 bytes  
                2 Dir(s)  6,036,721,664 bytes free  
  
C:\pqr>
```

4

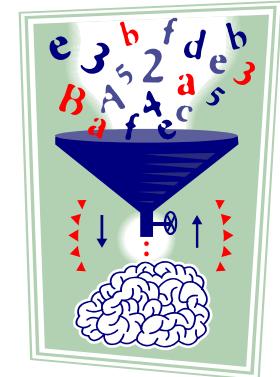
NTFS Compressed Files

- The compressed files present on the NTFS volume can be accessed, read or modified by any Windows application without decompressing the file
- When an application like Microsoft word or operating system commands like copy command requests to access, file is decompressed by the filter driver
- NTFS compression algorithms supports cluster sizes of up to 4 KB



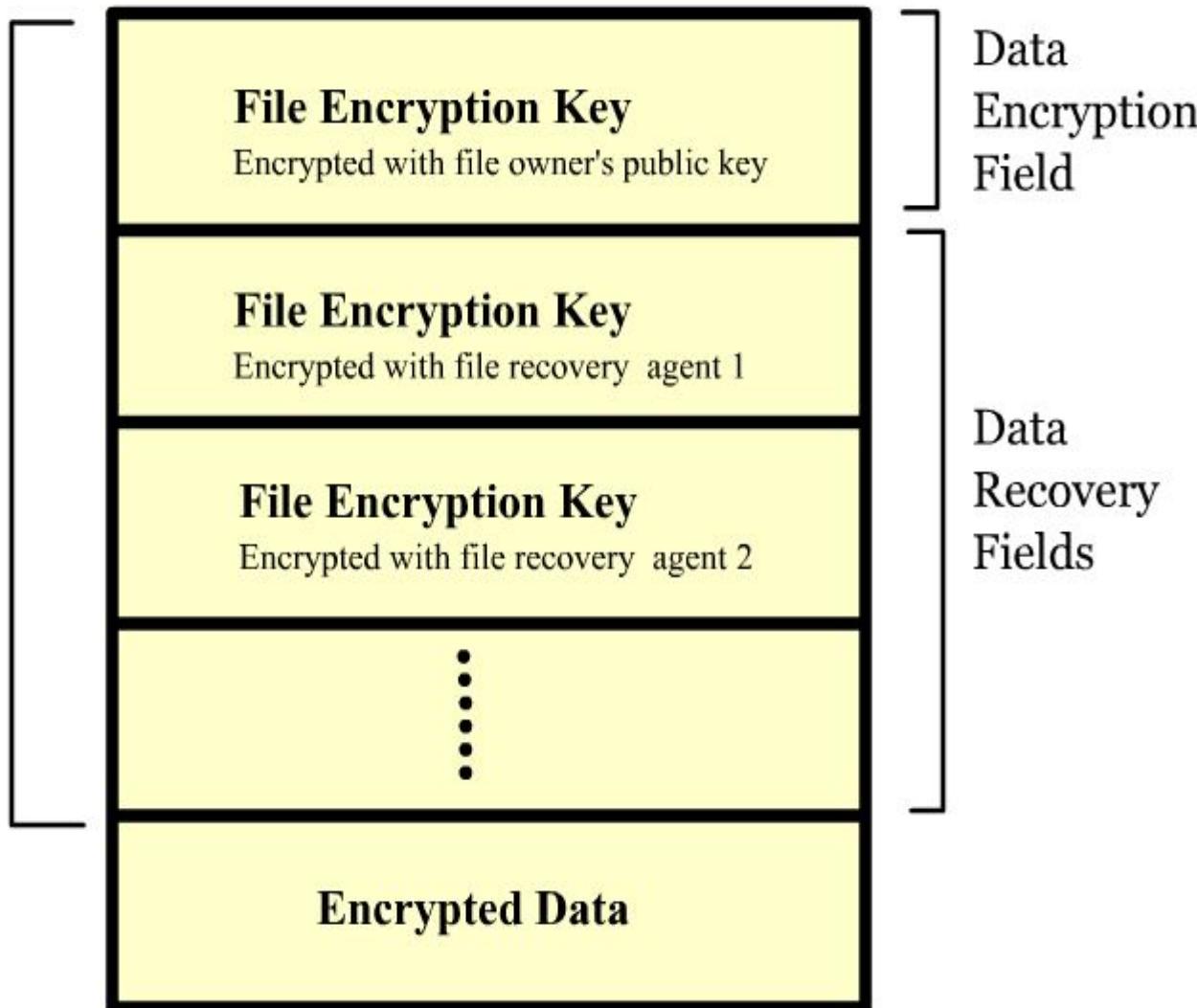
NTFS Encrypted File Systems (EFS)

- Main file encryption technology used to store encrypted files in the NTFS
- Encryption of the file or folder can be read or modified, just like any other file or folder
- EFS uses public and private keys to encrypt the files, folders, and disk volumes
- Encrypted files can be accessed only if the user has the private key and the operating system has the public key
- If an intruder tries to modify, copy or rename the files then the intruder receives an access denied message



EFS File Structure

Header



Metadata File Table (MFT)

- MFT is a relational database, which consists of information regarding the files and the file attributes
- The rows consists of file records and the columns consists of file attributes
- It has information of every file on the NTFS volume including information about itself
- MFT has 16 records reserved for system files
- MFT for small folder is represented as follows

Standard Information	File or Directory Name	Data or index	Unused space
----------------------	------------------------	---------------	--------------

EFS Recovery Key Agent-I

- ◉ A recovery policy is always associated with a encryption policy. A recovery agent decrypts the file if encryption certificate of an encrypted file is lost
- ◉ The recovery agent is used in following conditions:
 - When a user loses a private key
 - When a user leaves the company
 - Whenever a law enforcement agency makes a request



EFS Recovery Key Agent -II

- The Windows administrator can recover key from the Windows or from the MS-DOS command prompt
- The keys can be recovered from command prompt using the following commands:
 - CIPHER
 - COPY
 - EFSRECVR
- Recovery agent information of an encrypted file can be viewed using the efsinfo tool



Deleting NTFS Files

- On deletion from Windows Explorer the file is moved into the recycle bin
- If the file is deleted from command prompt then recycle bin is bypassed. It can be recovered only by using the forensic tools
- When a file is deleted the following tasks are performed by the operating system in the NTFS:
 - The clusters are made available for the new data
 - MFT attribute \$BITMAP is updated
 - File attribute of the MFT is marked available
 - Any linking inodes and VFN/LCN cluster locations are removed from MFT
 - The list of links to the cluster locations is deleted

Understanding Microsoft Boot Tasks

- ⦿ These are the steps that are followed by NTFS during the startup:
 - Power-on self test (POST)
 - Initial startup
 - Boot loader
 - Hardware detection and configuration
 - Kernel loading
 - User logon



Windows XP system files

⦿ Essential system files used by windows XP:

File name	Description
Ntoskrnl.exe	The executable and kernel of Windows XP
Ntkrnlpa.exe	Physical address support program(for >4GB)
Hal.dll	Used for OS kernel to communicate with computer's hardware
Win32k.sys	Kernel mode for Win32 subsystem
Ntdll.dll	Supports internal functions and dispatches the stubs to executive functions.
Kernel32.dll	Win32 subsystem DLL files
Advapi32.dll	
User32.dll	
Gdi32.dll	

Understanding Boot Sequence DOS

- Boot sequence steps are as follows:
 - Computer waits for power good signal
 - Processor executes the BIOS boot program
 - BIOS performs Power on self test(POST)
 - BIOS initializes the system settings from CMOS settings
 - PCI initializes and displays the configuration and status of devices
 - BIOS locates and loads Disk operating system(DOS)



Understanding Boot Sequence DOS

- BIOS then loads the Master Boot Record(MBR)
 - Volume boot sector is loaded and tested
 - Loads and executes IO.SYS
 - IO.SYS searches for MSDOS.SYS, loads it and executes the file
 - COMMAND.COM is loaded and executed for interpreting and reading CONFIG.SYS and AUTOEXEC.BAT
- ① After this point the operating system takes control of the computer



Understanding MS-DOS Startup Tasks

- IO.SYS – It contains all instructions used by the operating system to interact with the hardware. It is the first file loaded after bootstrap detects the operating system
- MSDOS.SYS – It is the kernel in MS-DOS and loads COMMAND.COM and AUTOEXEC.BAT
- COMMAND.COM – It provides internal DOS commands
- CONFIG.SYS – It contains the commands that are required during the startup
- AUTOEXEC.BAT – It contains customized settings for the MS-DOS



Other DOS Operating Systems

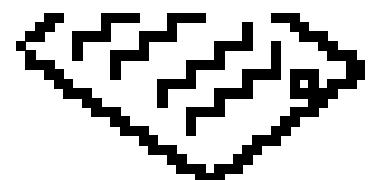
Following are the useful disk operating system other than Microsoft's DOS:

- 4DOS: It has more commands, better editor, online help and flow control commands like; DO WHILE, RERURN, IFF..THEN...ELSE
- Dr- DOS: It is DOS compatible and offers pre-emptive multitasking and 32-bit protected mode etc
- Caldera OpenDOS: It's a MS-DOS compatible OS. It is the descendant of DR DOS and Novell DOS
- Novell DOS: A full feature DOS built for workstations on Novell networks



Other DOS Operating Systems

- PTS-DOS: Simple graphical user interface DOS; which supports FAT32, big hard drives, and CD-ROMs. *Partition Manager Easy* makes it easy to partition the hard drives;
- QDOS: A 16MB OS created for CP/M operating system
- FreeDOS: It is cheaper than IBM's and Microsoft's and is being used in China on HP PC's

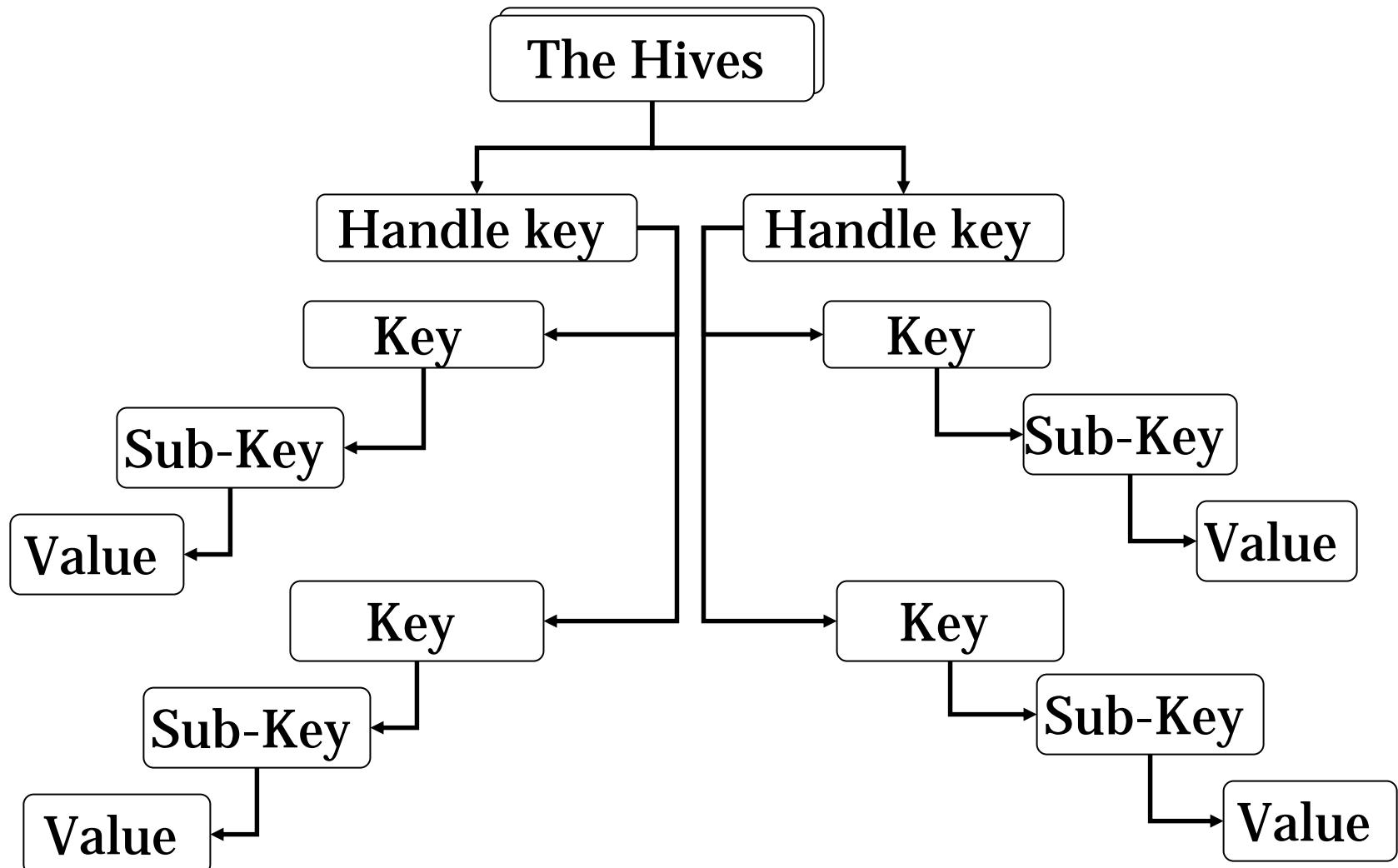


Registry Data-I

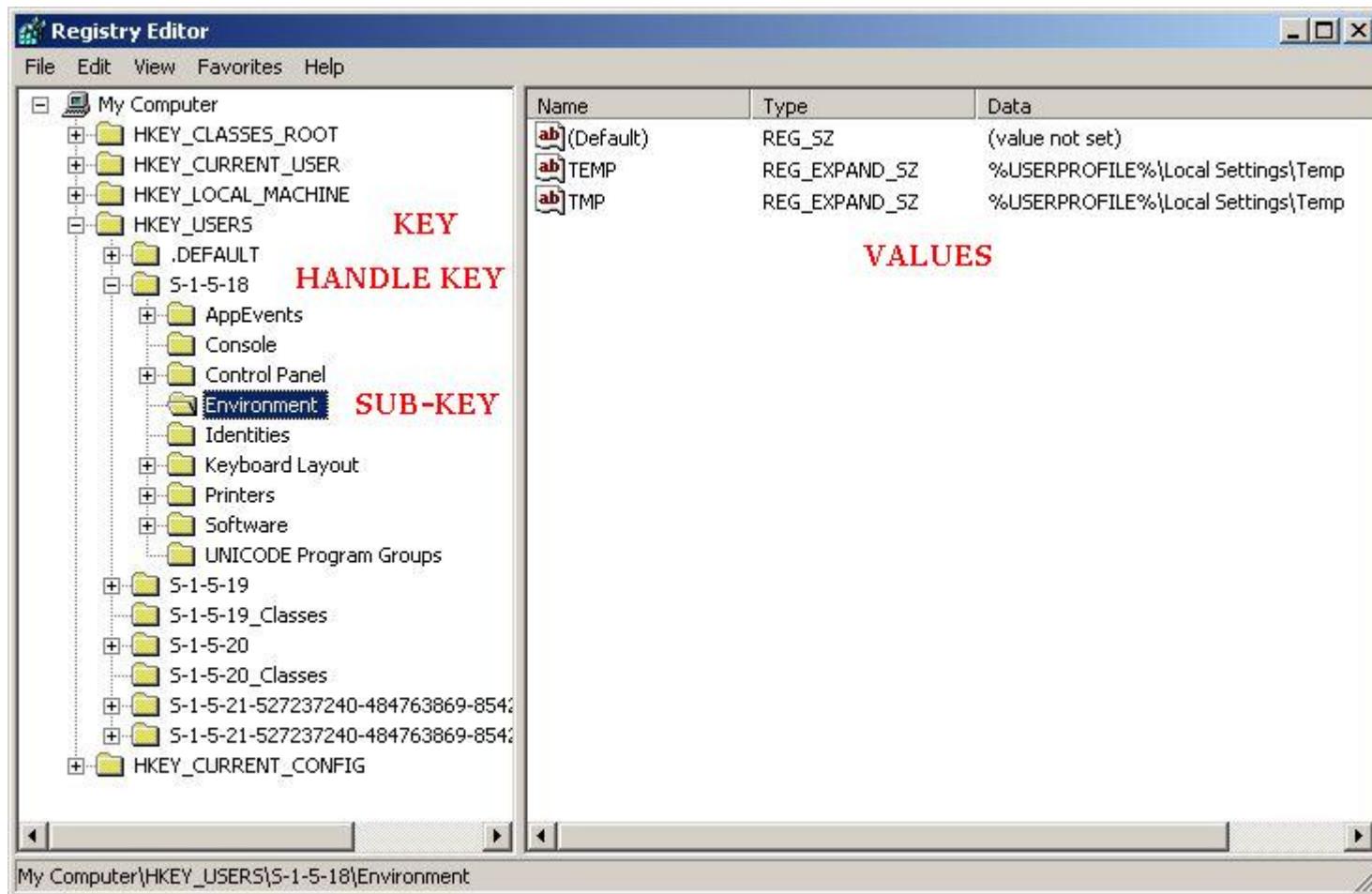
- Registry is the hierarchical database
- Used to store the information regarding the users, applications, and the hardware devices
- Windows continuously refers the registry for the information during the execution of the application
- The data in the registry is saved in the form of binary files



Registry Data-II



Registry Data-III



Examining Registry Data

- Registry has predefined set of keys for every folder
- A registry hive is defined as a set of keys, sub keys, and values in the used in the windows registry, which has a group of supporting files that contain backups of its data
- Registry can be examined manually using the register editor
- Registry can be examined using the tools like:
 - Registry Monitor
 - Registry Checker



Summary

- File system is a set of data types, which is employed for storage, hierarchical categorization, management, navigation, access, and recovering the data
- Registry is the hierarchical database
- The data is recorded onto the hard disk using the zoned bit recording
- Partitioning of hard disk drive is done for effective storage management of data
- Every disk has Master Boot Record that contains the information about partitions on the disk

Summary

- FAT is located at the sector zero (starting) on a disk
- Drive Slack is the void or the free space allocated for files (in clusters) by the operating system
- EFS is the main file encryption technology used to store encrypted files in the NTFS.
- MFT is a relational database, which consists of information regarding the files and the file attributes
- Few of the other useful disk operating system are 4DOS, Dr-DOS and Caldera OpenDOS



Computer Hacking Forensic Investigator

Module VII Windows Forensics

Scenario

Ethan works as a technical consultant in a reputed IT firm.

He plans of using a P2P program to download full length movies into his computer, which would definitely breach companies policies.

Not aware of a trojan being loaded into his system, he downloads his favorite movie, Phone booth and watches it.

To his shock, Ethan's Windows 2000 based system failed to reboot the next day.

His system administrator, Jake checks his system and changes the hard disk.

A week later, when the reports came in from the forensic investigator, Ethan was fired for company policy breach.

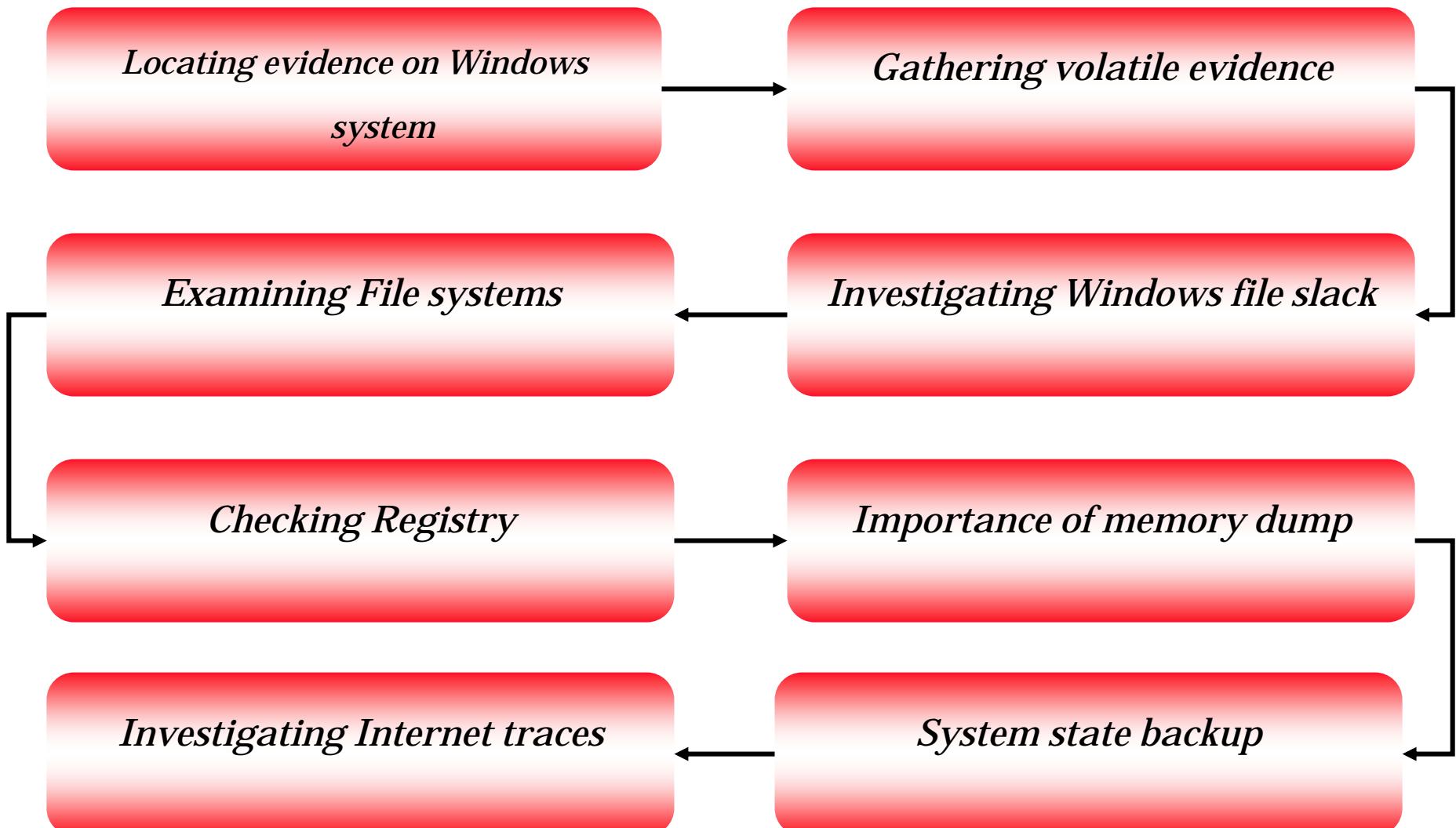
But how did the forensic investigator find out about Ethan's activities?



Module Objective

- Locating evidence on Windows systems
- Gathering volatile evidence
- Investigating Windows file slack
- Examining file systems
- Checking Registry
- Importance of Memory dump
- System state backup
- Investigating Internet traces

Module Flow



Locating Evidence on Windows Systems

- Hidden files
- Assessing file attributes to find file signature
- The registry
- Searching Index.dat files

Areas to look for evidence

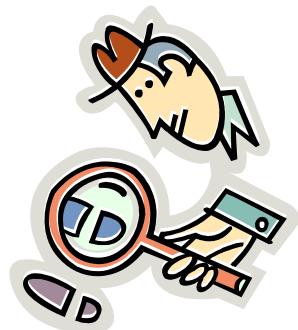
- Files
- Slack space
- Swap file
- Unallocated clusters
- Unused partitions
- Hidden partitions



Gathering Volatile Evidence

Collecting volatile data using command prompt in Windows NT/2000

- System date and time
 - C:/>date ; C:/>time
- Currently running processes
 - Tool - pslist
- Currently open sockets
 - C:/>netstat
- Applications listening on open sockets
 - Tool - fport
- Current users logged on
 - Tool - psloggedon
- Systems currently or recently connected.
 - C:/>nbstat



Forensic Tool: Pslist

- Supports Windows NT/2000/XP
- Lists all currently running processes on the system.
- Information include:
 - Time of the process when executed
 - Time the process has executed in kernel and user modes
 - Physical memory that the OS has assigned the process

Name	Pid	Pri	Thd	Hnd	Priv	CPU Time	Elapsed Time
Idle	0	0	1	0	0	3:47:06.187	0:15:43.328
System	8	8	40	201	24	0:00:13.781	0:15:43.328
SMSS	180	11	6	33	1076	0:00:00.453	0:00:00.000
CSRSS	204	13	10	422	1524	0:00:15.953	0:00:00.000
WINLOGON	224	13	19	409	6252	0:00:11.156	0:00:00.000
SERVICES	252	9	36	537	3280	0:00:02.421	0:00:00.000
LSASS	264	9	16	292	2720	0:00:01.156	0:00:00.000

Forensic Tool: fport

- Lists all open TCP/IP and UDP ports
- Maps the ports to their running processes with their
 - PID,
 - Process name, and
 - Path
- Useful in locating unknown open ports and their related applications

```
G:\Windows_Forensics\Tools\fport>fport /a
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

      Pid  Process          Port  Proto  Path
      648  MTask            ->  1025  TCP    C:\WINNT\system32\MTask.exe
          System           ->  1026  TCP
          System           ->  139   TCP
          System           ->  445   TCP
        1460  isafe            ->  1499  TCP    C:\WINNT\system32\ZoneLabs\isafe.exe
        1460  isafe            ->  1500  TCP    C:\WINNT\system32\ZoneLabs\isafe.exe
        452   svchost          ->  135   TCP    C:\WINNT\system32\svchost.exe
       784   svchost          ->  1952  TCP    C:\WINNT\system32\svchost.exe
      1368  vsmon            ->  1503  TCP    C:\WINNT\system32\ZoneLabs\vsmon.exe
      1368  vsmon            ->  1504  TCP    C:\WINNT\system32\ZoneLabs\vsmon.exe
      1368  vsmon            ->  1637  TCP    C:\WINNT\system32\ZoneLabs\vsmon.exe

      968  IEXPLORE          ->  2119  UDP   C:\Program Files\Internet Explorer\IEXPLORE.EXE
     1280  IEXPLORE          ->  2128  UDP   C:\Program Files\Internet Explorer\IEXPLORE.EXE
          System           ->  137   UDP
          System           ->  138   UDP
          System           ->  445   UDP
        264   lsass             ->  4500  UDP   C:\WINNT\system32\lsass.exe
        264   lsass             ->  500   UDP   C:\WINNT\system32\lsass.exe
```

Forensic Tool - Psloggedon

- Displays locally logged on users
- Also displays users who are logged on through resources for either the local or a remote computer
- Runs a search on the computers present in the network neighborhood and informs if the user is currently logged on

```
G:\Windows_Forensics\Tools\psloggedon>psloggedon

PsLoggedOn v1.31 - Logon Session Displayer
Copyright (C) 1999-2003 Mark Russinovich
Sysinternals - www.sysinternals.com

Users logged on locally:
  4/15/2005 12:41:08 AM      SYSTEM5\Mahendran

No one is logged on via resource shares.
```

Investigating Windows File Slack



File Slack

- The space existing at the end of the file or the last cluster.
- Contains data from computer's memory.
- Identifies network logon names, passwords and other sensitive information associated with computer.

- File slacks can be gathered from a hard disk drive or a floppy diskette by using *Encase Forensic edition* tool
- Examiner connects to target computer and selects media
- Bit-level copy of the original media is created
- It is checked again by generating its hash value
- Investigation using keyword searches, hash analysis, file signature analysis, and Enscripts present in *Encase* tool

Examining File Systems

Run dir /o:d under c:/%systemroot%/system32> in DOS prompt

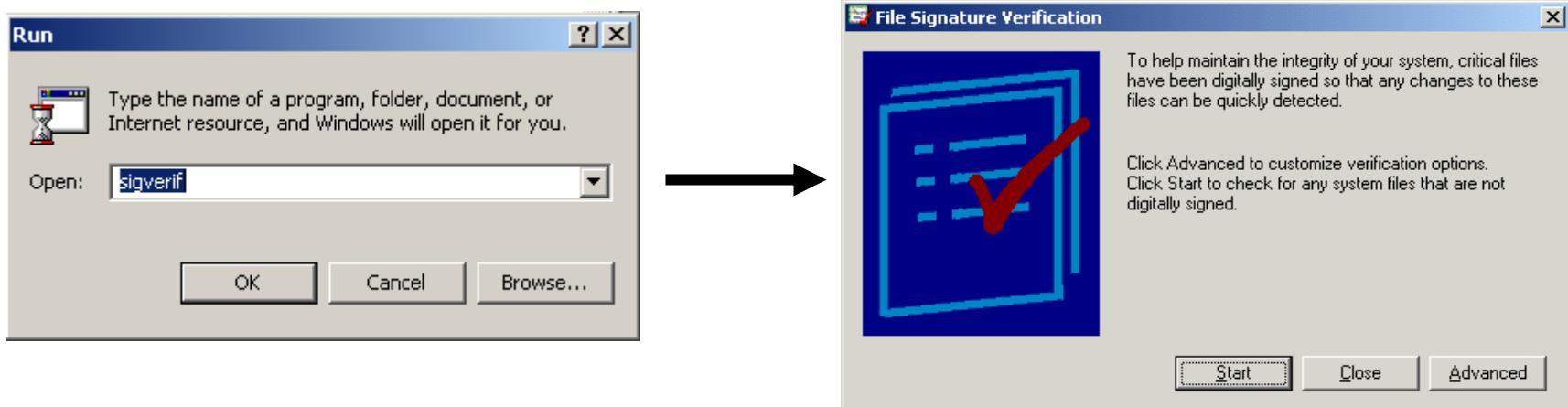
- Enables the investigator to examine
 - The time and date of the installation of the operating system
 - The service packs, patches, and sub-directories that automatically update themselves very often
 - For example: drivers etc
- Importance should be given to recently dated files



```
01/26/2005 04:22a          198,424 vspubapi.dll
01/26/2005 04:22a          71,448 vsregexp.dll
01/26/2005 04:22a          354,064 vsutil.dll
01/26/2005 04:23a          100,112 vsxml.dll
01/26/2005 04:23a          75,536 zlcomm.dll
01/26/2005 04:23a          67,352 zlcommdb.dll
01/27/2005 03:35p          2,806,272 MSHTML.DLL
02/08/2005 03:33p          75 LuResult.txt
02/10/2005 10:01p          328,128 gcTypLibA.tlb
02/10/2005 10:03p          212,240 RICHTX32.OCX
02/10/2005 10:32p          81,120 hashlib.dll
02/10/2005 10:32p          119,520 GCCollection.dll
02/10/2005 10:32p          130,272 gcUnCompress.dll
02/23/2005 12:55p          10,752 gcmd5query.dll
03/03/2005 12:54a          32,768 asteriskie.exe
03/03/2005 09:32p          <DIR> URTTemp
03/03/2005 09:32p          <DIR> wbem
03/03/2005 09:32p          <DIR> mui
03/03/2005 09:34p          371,750 PerfStringBackup.INI
03/03/2005 09:34p          50,808 perfcb009.dat
03/03/2005 09:34p          369,124 perfh009.dat
03/03/2005 10:01p          <DIR> DirectX
03/13/2005 05:06p          20,480 HQtKeysH@k.DLL
03/16/2005 11:24p          <DIR> appmgmt
03/16/2005 11:24p          <DIR> drivers
03/23/2005 10:04a          <DIR> NtmsData
03/28/2005 11:41a          100,352 dfrg.nsc
04/09/2005 07:24p          442,368 Clock - EC-Council Clock.scr
04/10/2005 04:06p          <DIR> ZoneLabs
04/12/2005 08:20p          <DIR> ..
04/12/2005 08:20p          <DIR> ..
```

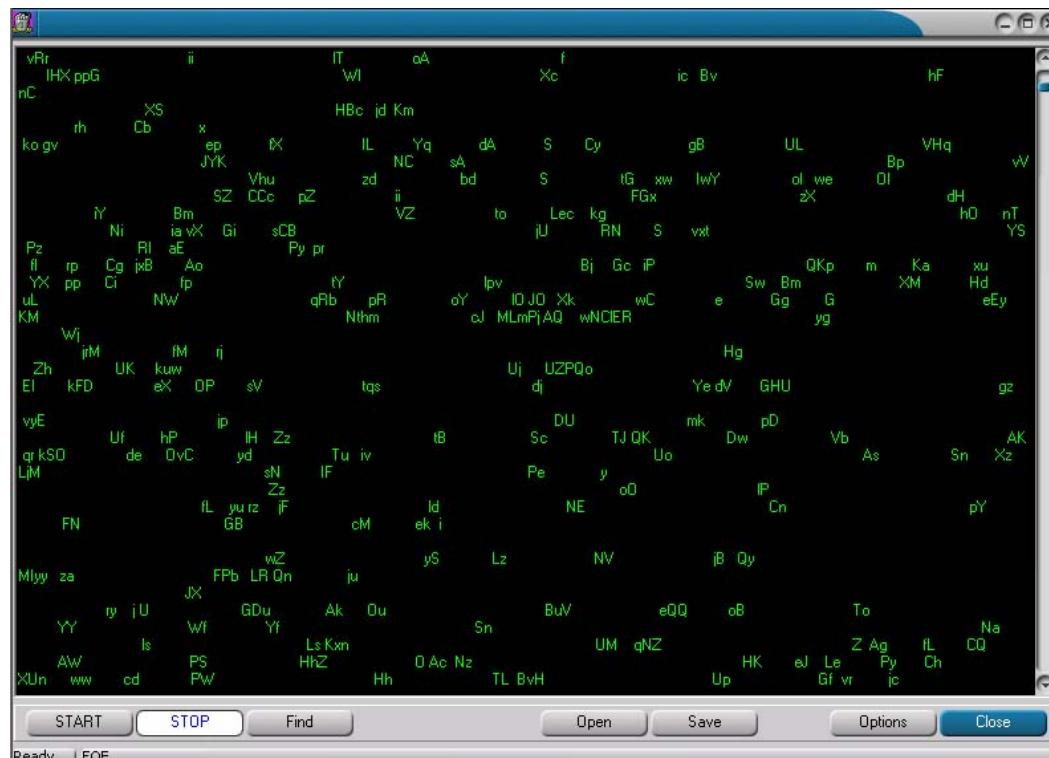
Built-in Tool: Sigverif

- A program that displays all the unsigned drivers and related files in the computer
- A signed file indicates the authenticity and quality associated to a file from its manufacturer
- Any unsigned files can indicate presence of infected driver files placed by hackers
- Most of the driver files are signed by the operating system manufacturer such as Microsoft
- Helps in finding the unsigned files present in the system



Word Extractor

- Hacking tool that interprets human words from machine language
- Helps in many ways like finding a cheat in a game, finding hidden text or passwords in a file (exe, bin, dll), etc...



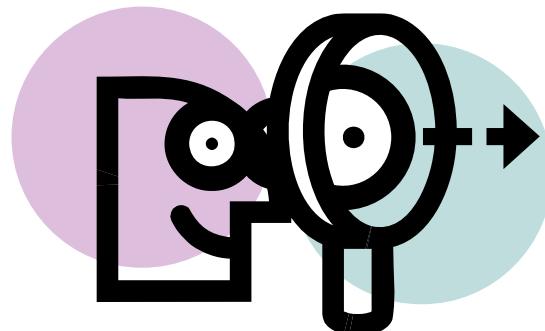
Checking Registry

① HKEY_LOCAL_MACHINE

- \Software\Microsoft\Windows\CurrentVersion\Run
- \Software\Microsoft\Windows\CurrentVersion\RunOnce
- \Software\Microsoft\Windows\CurrentVersion\RunOnceEx
- \Software\Microsoft\Windows\CurrentVersion\RunServices
- \Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
- \Software\Microsoft\WindowsNT\CurrentVersion\Winlogon

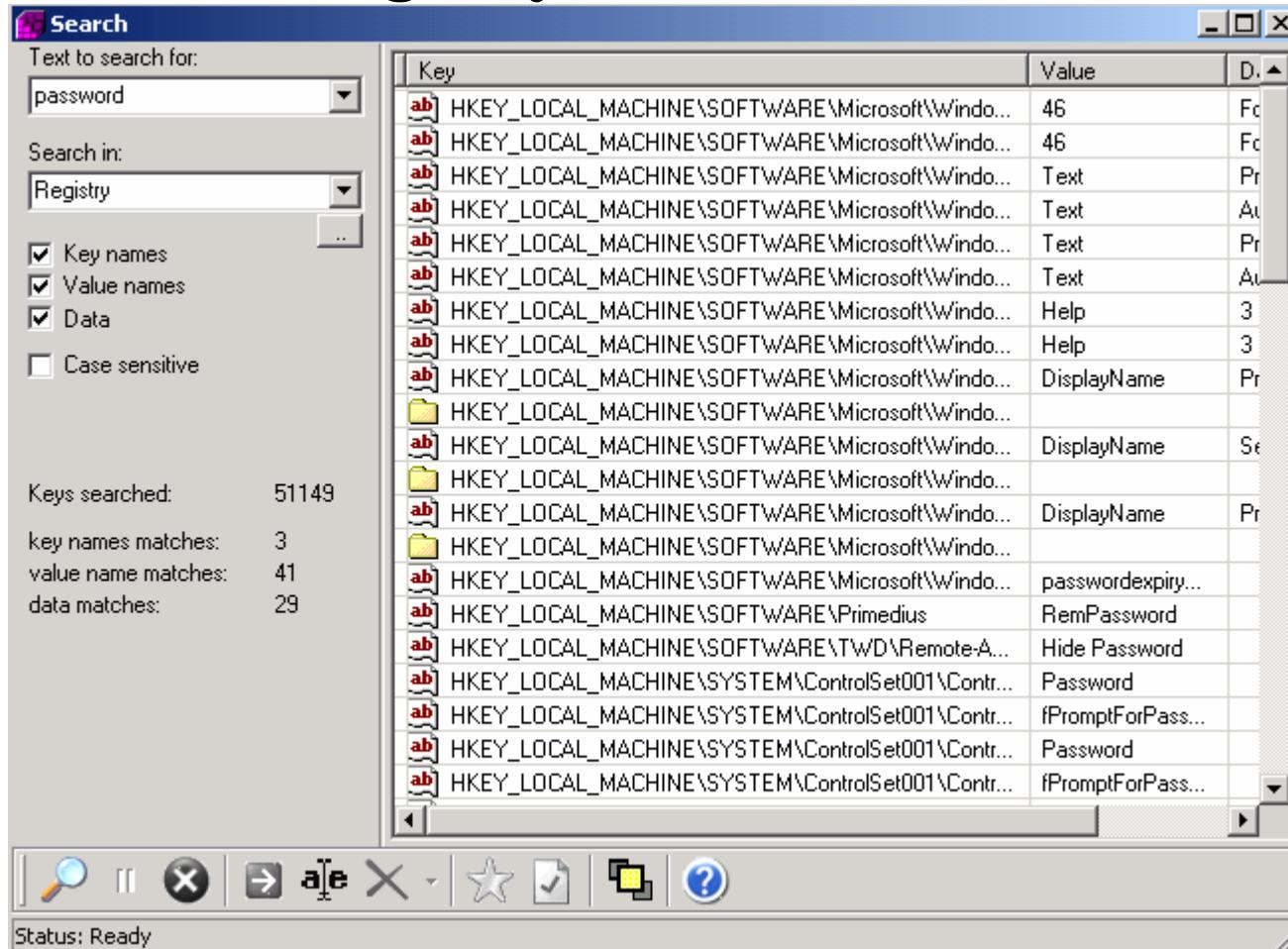
② Same for

- HKEY_CURRENT_USER
- HKEY_USERS\.DEFAULT



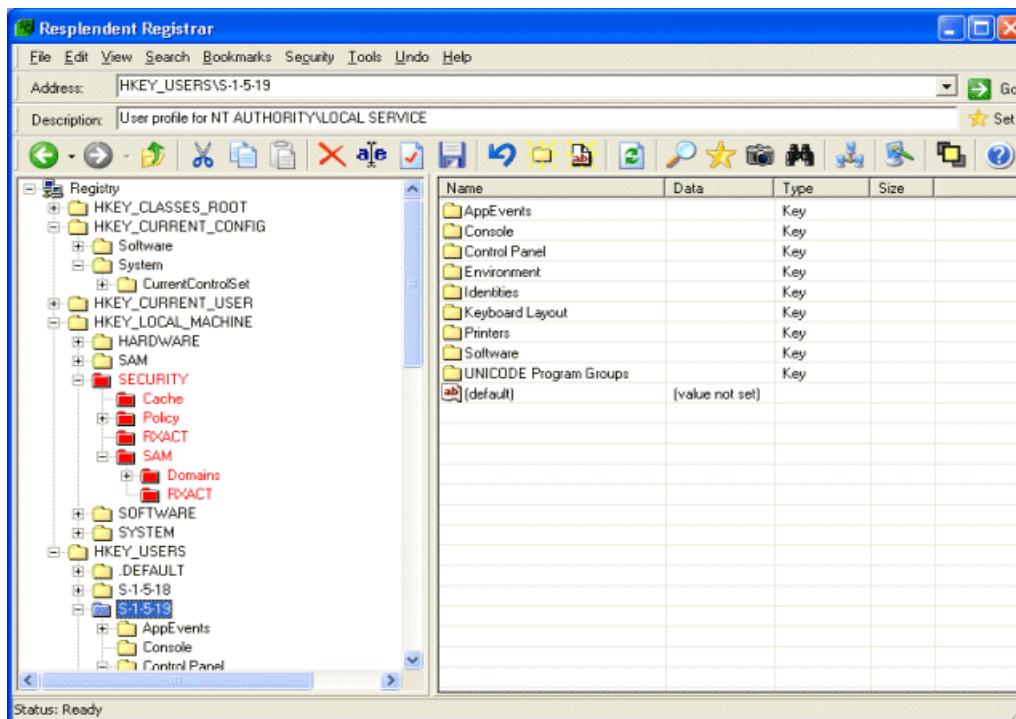
Reglite.exe

① Searches Registry



Tool: Resplendent Registrar 3.30

- Controls system configuration
- Reliable registry backup
- Repair broken Windows configurations
- Remote access to systems on a network

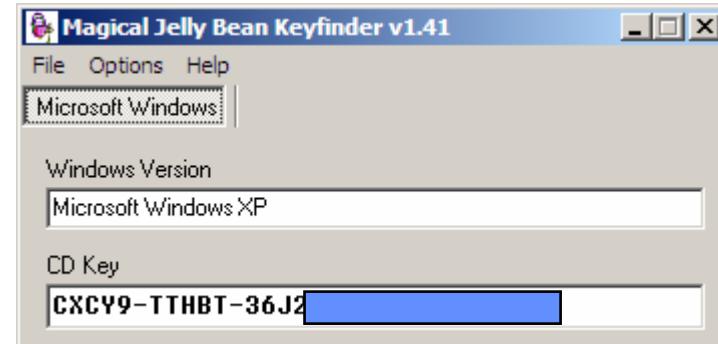


Microsoft Security ID

- Microsoft Security IDs are available in Windows Registry
- For accessing IDs, process is as follows:
 - Go to Registry Editor and view:
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList`
 - Present under the ProfileList key

Windows CD-KEY Revealer

- This program reveals CD-KEY of a Windows operating system
- Helps in investigating the ownership license of the OS software
- Download this tool from
<http://www.eccouncil.org/cehtools/win-cdkey.zip>

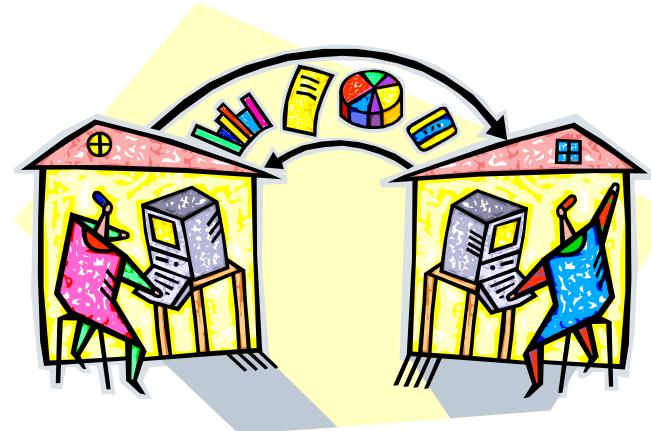


Note: This slide is not in your courseware

Importance of Memory Dump

- ◎ Memory dump refers to copying data from one place to another without formatting
- ◎ Used to diagnose bugs
- ◎ Helps in analyzing memory contents during program failure
- ◎ The memory dumps contains information in binary, octal or hexadecimal forms
- ◎ Memory dump information can be checked using dumpchk.exe

- ◎ A memory dump file records all information that made a computer to stop abruptly
- ◎ Windows keeps a list of all the small memory dump files in the %SystemRoot%/Minidump folder



Manual Memory Dumping in Windows 2000

- Right-click My Computer, and click Properties
- Advanced tab -> Startup and Recovery
- Select Complete memory dump and ensure that a valid dump file location is entered
- Connect the Null modem cable to the server's serial port
- Editing boot.ini file
 - Copy the typical boot up entry and add it at the end of the boot.ini file
 - Add and mark the following description as Debug boot
 - /debug /debugport=com1 /baudrate=57600
- Click Debug boot after rebooting the system

Memory Dumping in Windows XP and Pmdump

In Windows XP

- By default, stores information to Pagefile.sys on the system root drive
- Enables offline analysis tools
- Contains small memory dump which uses upto 64 kb space.
- Stored in %systemroot%/Minidump folder

PMDump

- A tool that dumps the memory contents of processor to a file without stopping the process
- Stands for Post Mortem Dump
- The dump information is saved on some secondary storage medium like magnetic tape or disk
- Supports Windows 2000/XP/NT

System State Backup

- Useful for forensic analysis of a Windows system
- Windows backup or registry backup will not suffice
- A full system state backup stores the following:
 - Active Directory
 - The boot files.
 - The COM+ class registration database.
 - The Registry
 - The system volume
 - The IIS metabase.



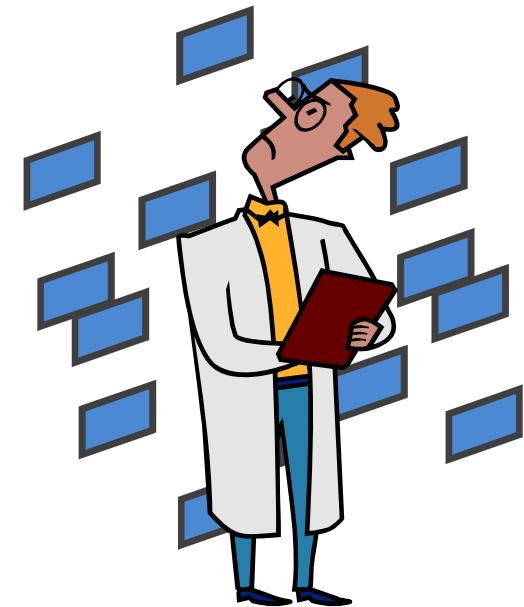
How to Create a System State Backup?

- **Start -> Programs -> Accessories -> System Tools -> Backup.**
- In **Backup** tab, check the **System State** box
- Select the **Schedule Job** tab and click **Add Job** button
- Click **Yes** and choose media options
 - Media type,
 - Location and
 - Backup name.
- Click **Next** and recheck that **Normal** option is selected, then click **Next**
- In the case of backing-up to disk, there will not be a need for verifying data.
Click **Next**
- Choose whether you want to append to or replace any existing backups. Click **Next**
- Schedule the backup accordingly. Click **Next**
- Set the account under which the backup should be run.
- Click **Finish**

Investigating Internet Traces

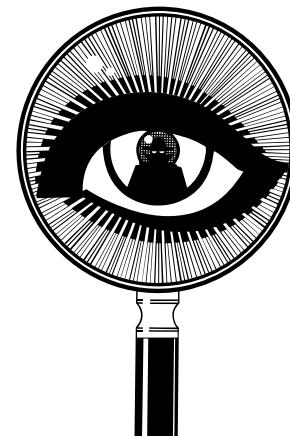
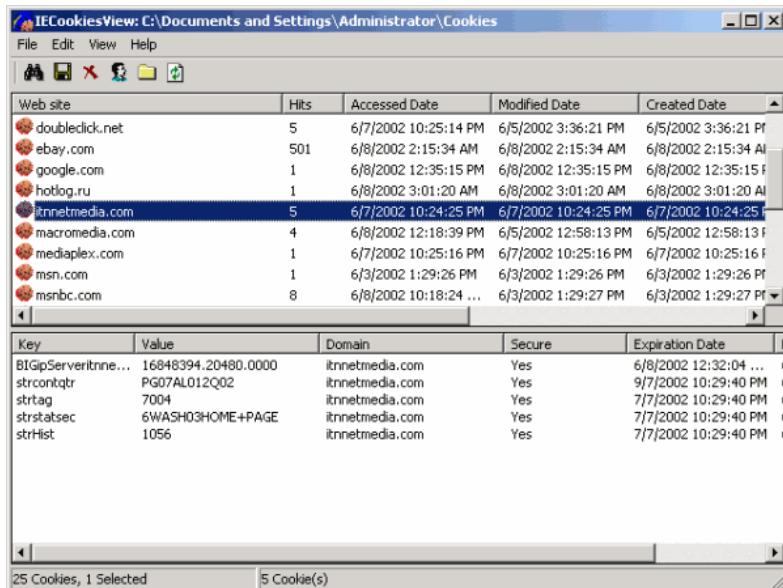
① Internet Explorer investigations

- **Cookies**
 - **Windows 2000/XP**
 - <c:\Documents and settings\%username%\Cookies>
 - **Windows 95/98/ME**
 - <c:\Windows\Cookies>
- **History**
- **Temporary Internet files**



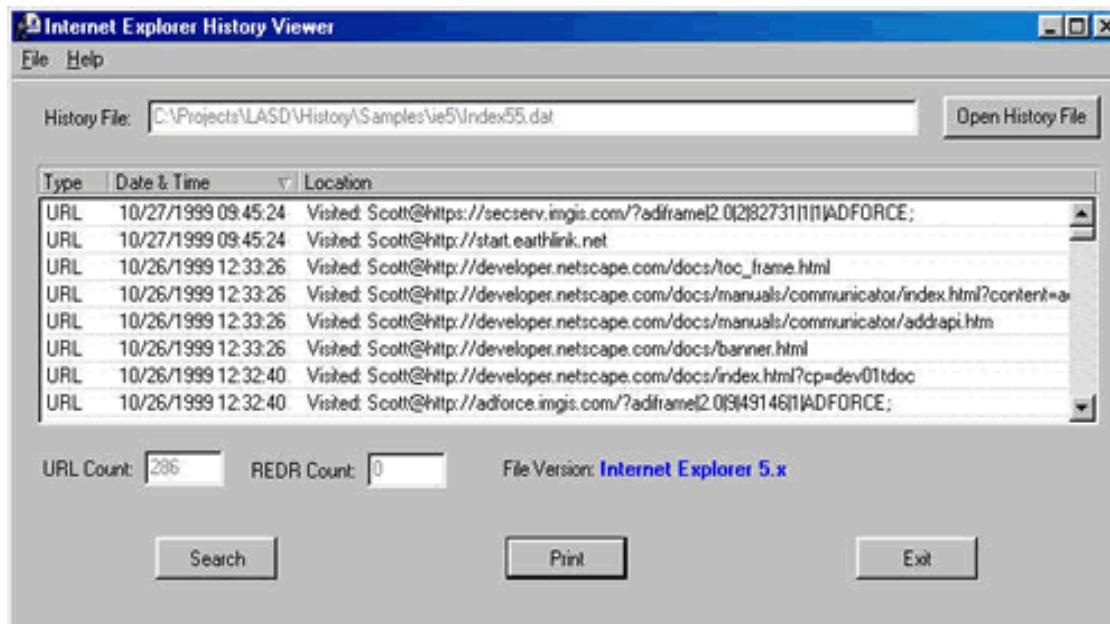
Tool - IECookiesView

- Displays details of all cookies stored on the computer
- View the contents of each cookie as well as save the cookies to a readable text file
- Also enables the user to view references to deleted cookies



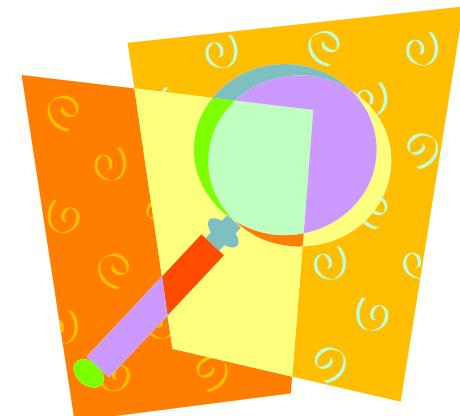
Tool - IE History Viewer

- It parses and prints the history of visited URLs
- Reads the NFO and INFO2 files from recycle bins of the Windows and also from the Netscape cache file "fat.db" and Netscape history file "Netscape.hst"



Forensic Tool: Cache Monitor

- Offers real time view of current state cache
- Offers an interface to modify data
- Also does the following:
 - Verify the configuration of dynamic caches.
 - Verify the cache policies
 - Monitor cache statistics
 - Monitors data flowing through the caches.
 - Data in the edge cache
 - View data offloaded to the disk
 - Manage the data in the cache

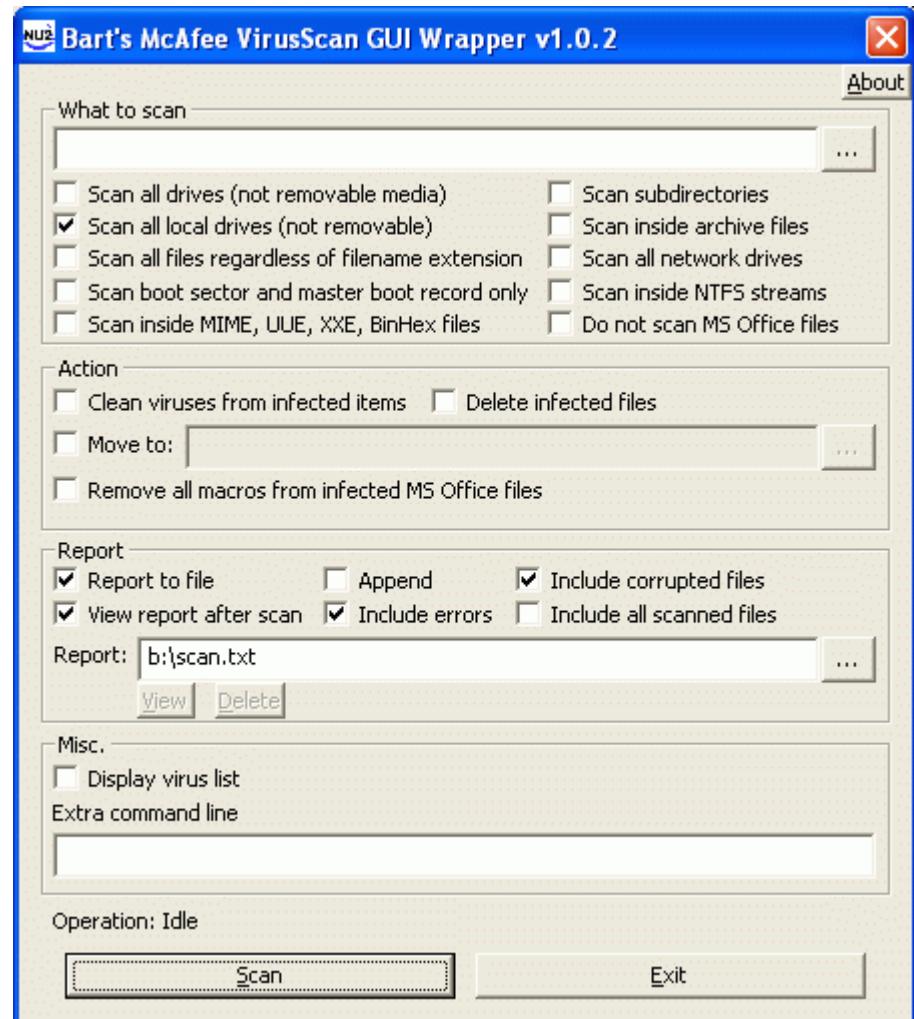
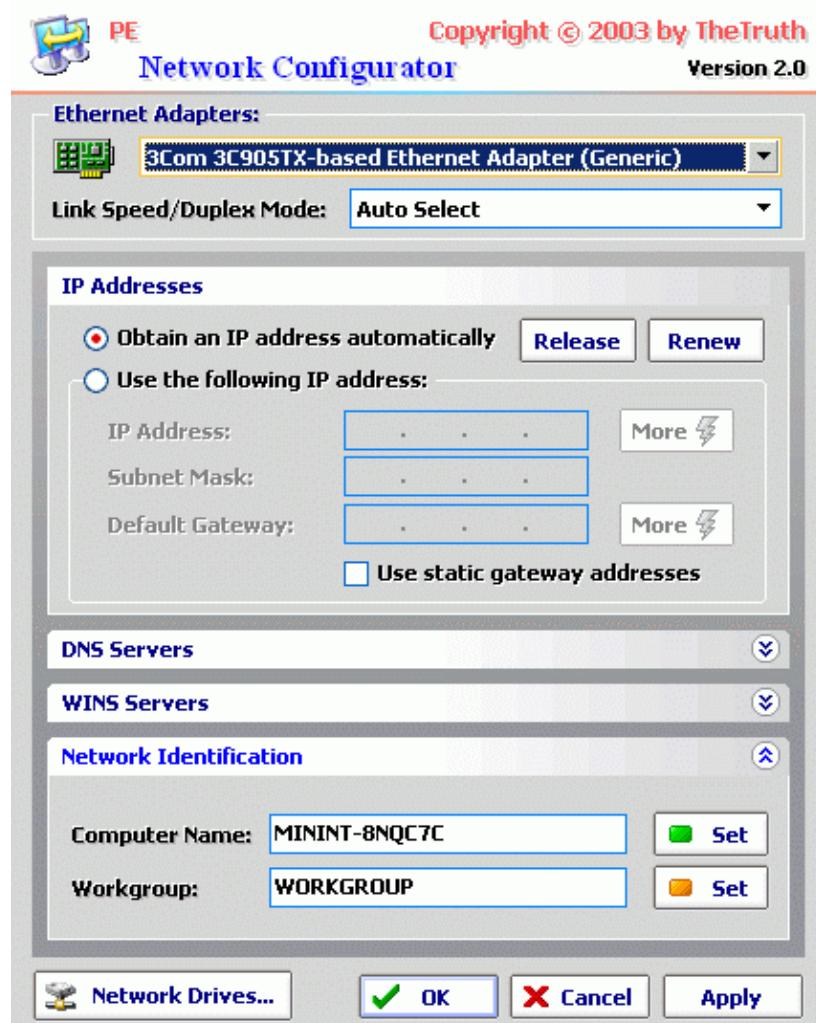


Action	Options	Entry #	Include strays	Include Cookies	File Path	Status	Local File	Size	Last Access	Last Modified	Last Sync'd	Flags
		98	<input checked="" type="checkbox"/>		ail/images/tearoff_icon.gif		C:\Documents ...	4096	2005/04/14 23:54:48	2005/03/25 9:13:34	2005/04/14 23:54:50	41
		143		<input checked="" type="checkbox"/>	ail/images/chevron.gif		C:\Documents ...	4096	2005/04/14 23:54:48	2005/03/25 9:13:33	2005/04/14 23:54:50	41
		25			http://www.gmail.google.com/gmail/images/opentriangle.gif		C:\Documents ...	4096	2005/04/14 23:54:48	2005/03/25 9:13:33	2005/04/14 23:54:48	41
		106			http://www.foundstone.com/images/tbl3body_divline1.gif		C:\Documents ...	4096	2005/04/14 23:54:47	2003/02/25 9:31:28	2005/04/14 23:54:52	41
		8			http://www.foundstone.com/images/tbl1ftr_start2.gif		C:\Documents ...	4096	2005/04/14 23:54:47	2003/02/25 9:31:27	2005/04/14 23:54:52	41
		129			http://www.foundstone.com/images/tbl1ftr_fill.gif		C:\Documents ...	4096	2005/04/14 23:54:47	2004/07/16 20:45:01	2005/04/14 23:54:52	41
		47			http://www.foundstone.com/images/bullet_2.gif		C:\Documents ...	4096	2005/04/14 23:54:47	2003/02/25 9:31:26	2005/04/14 23:54:52	41
		152			http://www.foundstone.com/images/tbl2hdr_midfill.gif		C:\Documents ...	4096	2005/04/14 23:54:47	2003/02/25 9:31:28	2005/04/14 23:54:50	41

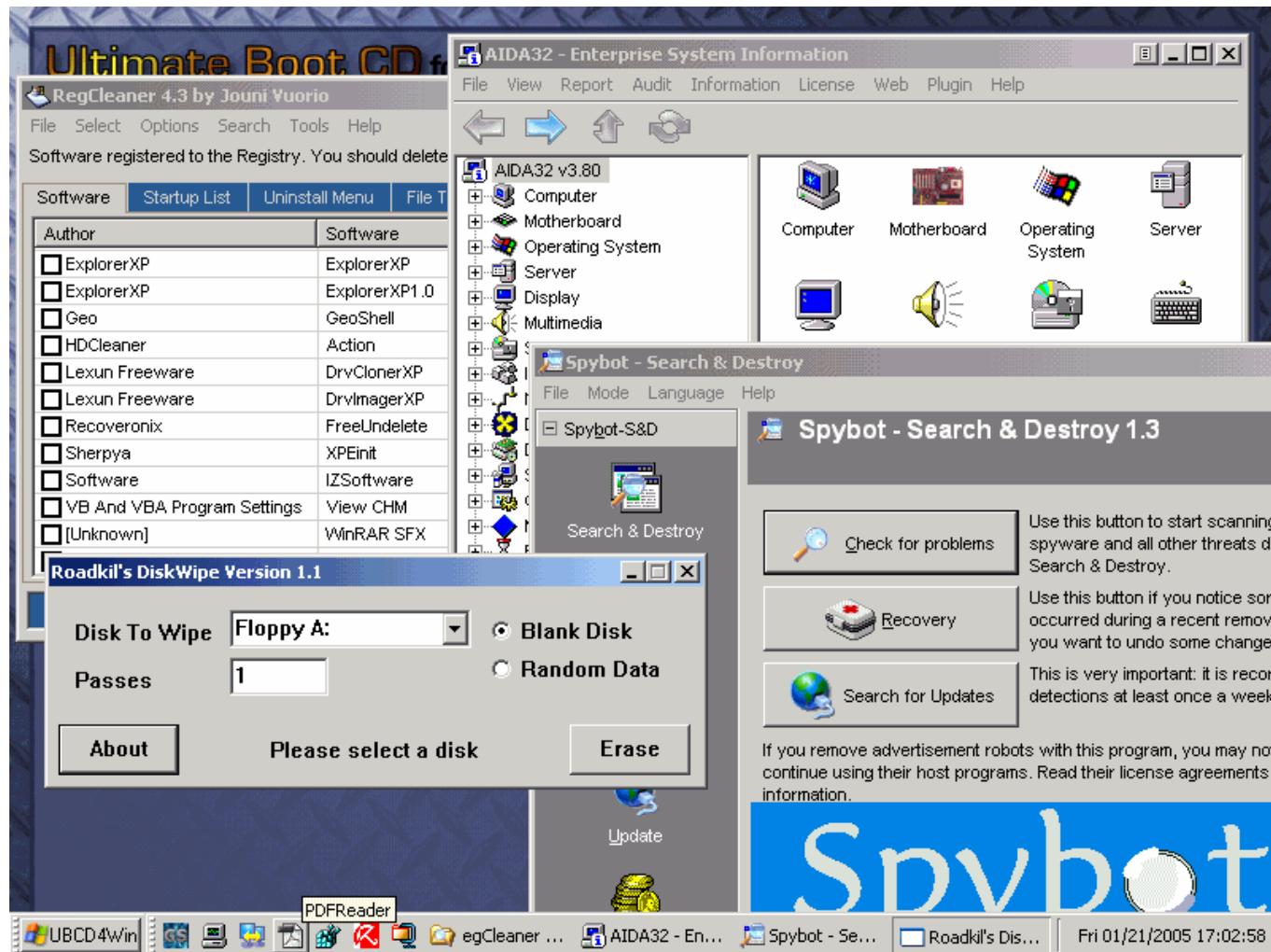
CD-ROM Bootable Windows XP

- ⦿ Following are the methods of creating Bootable CD-ROM for Windows XP:
 - Bart PE (Bart Preinstalled Environment)
 - Provide a complete Win32 environment with network support
 - Rescuing files to a network share, virus scan etc
 - Ultimate Boot CD
 - Provide shared internet access .
 - Can Modify NTFS volumes,
 - Recover deleted files,
 - Create new NTFS volumes, scanning viruses etc.

Bart PE Screenshot



Ultimate Boot CD-ROM



List of Tools in UB CD-ROM

AntiVirus Tools

AVPersonal	6.30.0.17	Great full featured freeware AntiVirus solution
McAfee Stinger	2.3.9	Scans for a limited number of viruses
Trend Micro SysClean	varies	Scan your system for viruses

Applications

FireFox NEW	1.0.2	Internet Browser
PDF Reader	1.2 0201	PDF viewer
Popcorn	1.73	Email Client
Scribe	1.87	Email Client
UltraReader NEW	1.01	File reader, supports many formats

CD Burning Applications

DeepBurner		Allows you to burn CD's in the BPE environment.
Express Burn	1.07	CD Burning software
SmallCD	1.12	CD Burning software

Disk Tools

-Backup/Cloning

Disk Copy	N/A	Floppy disk copier
Disk Image	1.15	Creates and restores images of disks to files
DrvImagerXP	2.0	Lexun utility. No support on their new website and development has ceased. Please use at your own risk.
DriveClonerXP	2.1	Lexun utility. No support on their new website and development has ceased. Please use at your own risk.
ImgMaker	1.1	

-Defrag

DefragNT	1.9	Hard disk defragmenter
Dirms	1.2.20	Comand Line utility to defragment your entire drive

List of Tools in UB CD-ROM

-Diagnostic

Bst5	5.1.4	Bart's Stuff test. Small Win32 application for long time heavily stress testing storage devices. Supports testing at file and device levels.
chkdsk	N/A	
DskChkup	1.1	Allows you to monitor the SMART attributes of a hard drive
Disk Check	1.0.57	Utility to check disks for errors and benchmarking
HDTune	2.1	Hard disk utility that will: Benchmark, Error scan, display temperature, SMART health information and provide other hard drive information
MaxBlast NEW	4.0	Maxtor MaxBlast for Win. Sorry, still trying to get it to work properly.
WinDLG	1.02	Western Digital HDD diagnostic software for Windows

-Partition

MbrFix	1.0.0.4	Fix or create Master boot record
MBRWiz	1.52	Master Boot Record Wizard
TestDisk	5.3	Tool to check and undelete partitions

-Security

Drive Erase	1.02	Permanently erases data from hard disks, removable media, partitions, files and folders.
Disk Wipe	1.1	Securely wipes data from discs
Eraser	5.7	Completely remove sensitive data from your hard drive by overwriting it several times with carefully selected patterns
HD Cleaner	2.36	Safely removes Web cookies, Web history, recent documents history, any hidden user traces and more

List of Tools in UB CD-ROM

-Compression		
IZArc	3.4.1.6	Popular freeware compression tool.
-Explorers		
a43	2.31	File management
Agent Ransack	1.73	File search
ExplorerXP	1.04	File management
WinDir Stat	1.1	Disk usage statistics viewer and cleanup tool.
-Recovery		
Copy Handler	1.28	Can't get this to work properly in BPE, still working on it-- small tool designed for copy/move files and folders between different storage medias
DBXtract	4.5	Repairs PST files for Outlook express
Disk Investigator	1.31	Display the true drive contents by bypassing the operating system and directly reading the raw drive sectors. View and search raw directories, files, clusters, and system sectors. Verify the effectiveness of file and disk wiping programs. Undelete previously deleted files
Fab's AutoBackup	1.0.2	Backup and restore personal settings like emails, documents, internet browser bookmarks
File Recovery	3.0	Data recovery for damaged files and erased partitions
Floppy Repair	1.0	Eliminates bad sectors of Floppy disk surface, does not hide bad sectors in the file system, as Scandisk like utilities, it really restores them
Free Undelete	1.0	Data recovery program for deleted files
Handy Recovery NEW	1.0	Designed to restore files accidentally deleted from hard disks and floppy drives
SectorSpyXP	2.01	Lexun utility. No support on their new website and development has ceased. Please use at your own risk.
Recovery Manager	1.0	Backup & Restore, Duplicate, Recover files accidentally deleted or from corrupted media, and Format Digital Flash Media
Restoration	2.5.14	File Recovery, restore files that have been deleted from the Recycle Bin
UnChk	3	Recover CHK files
Unstop Copier	1.9	Recovers files from disks with physical damage
Linux Tools		
Explore2fs	1.00	Allows exploration of Linux partitions in the Windows environment
R-Linux	1.0	Recovery utility for the Ext2FS file system
Malware Tools		
AdAware	1.05 SE	Scans remote hard drives for spyware, etc.
CWShredder		
EzPCFix	??	Helpful tool when trying to remove viruses, spyware, other troublesome advertising programs, and malware from your computer.
Hijack This	1.99	General browser hijacker detector and remover
..

List of Tools in UB CD-ROM

Network Tools

Cisco		Cisco VPN Client. Still working on this. Further steps are necessary to complete plugin.
FileZilla	2.2.1.2c	FTP Client
IPScan	2.21	Fast IP scanner for Windows
NetStumbler	0.4	Find wireless networks
nwdskpe		Novell's NetWare Client to access NetWare servers by IP/IPX
Putty	.58	Implementation of Telnet and SSH for Win32 and Unix platforms, along with an xterm terminal emulator
Real VNC Server	4.0	Remote control software which allows you to view and interact with one computer
ShowTraf	1.4.1	Show Traffic, Monitors network traffic
Tight VNC Viewer	1.2.9	Remote control software package
UltraVNC	1 RC18	Remotely control a computer over any TCP/IP connection
VNC Neighborhood	1.1.8	VNC server TCP scanner, uses Microsoft Windows Networking features to locate computers in Microsoft Windows domains and workgroups

Password Tools

cmos	4.3	Find your CMOS password and/or replace it
InsidePro	1.0	Passwords recovery, encryption and cryptography
KeyFinderPE	1.41	Will find your Windows installation key, the included version works in PE
PasswordPro	1.3	MD5, MD4, MySQL, SHA-1 hashes password recovery, password keeper, password generator, hash generator, dictionary generator, etc
Sala Password Renew	1.0 RC2	(re)set the passwords of any user that has a valid local account, create a new local user with administrator rights, and set administrator rights to existing user on your NT system

Registry Tools

Erunt	1.1h	Emergency Recovery Utility -Registry backup and restore
RegBrows	1.2.2	Browses local/remote system registry using a specified account
RegCleaner	4.3	Remove obsolete registry entries from software that you may have deleted
RegEditPE	0.9c	Registry Editor for PE, SourceForge project
RegResWiz	1.04	Accesses restore points on a system to restore registry to a previous point
XSP	6.6	X-Setup Pro PE version; Windows tweaker, allows you to change many Windows settings

List of Tools in UB CD-ROM

Shell Features

ASPI	N/A	CD Support
AutoRamSizer	1.9	Adjusts size by the amount of RAM installed on the system
AutoRun	N/A	BPE functionality
atapi_824146	N/A	XP Patch
BartPE	5.1.4	small win32 application for long term heavy stress testing storage devices at the file and device level
BGInfo	4.05	System information
dcomlaunch	N/A	Launch DComLaunch service first -for SP2
Dialup		Ability to use your modem, you will need to create a modem driver plugin for your particular model. Email me for support, I will try to help
DosPE	1.0.6	DOS 16-bit support
GeoShell	N/A	Adds more "XP" feel, enhanced startbutton, quicklaunch, taskbar, etc.
keyboard		Keyboard mapper
MMC NEW	1.2	Microsoft Management Console
mstsc	N/A	Remote desktop client
nu2menu		Menu system
onscrkb	N/A	On Screen Keyboard tool
peinst		HD installation tool for PE
penetcfg		PE Network Configurator
PeLoader		Removes several restrictions set in Bart's PE such as 6 app.'s & 24hr limit
PPOE2k3		PPPOE dialup network support for Win 2k3
PPOEXP		PPPOE dialup network support for XP
ramdisk NEW		Creates a RAM drive in the PE environment , Bart's new version included in his latest BETA
sermouse		Serial mouse support
UnxUtils		GNU utilities for Win32
USB	1.0	My USB plugin, tested on a few simple devices. Not completely plug and play but I'm working on it.
VBdlls	5.0&6.0	Visual Basic DLL's, makes these runtime dll's available in PE
ViewChmHlp	N/A	My help and CHM file plugin, adds support so these files can be viewed
WSHSupport		Windows scripting host support which allows VBScript and JScript to run

Summary

- File Slack identifies network logon names, passwords and other sensitive information associated with computer
- The investigator must look for renamed files, changed extensions and file attributes as they can be used to hide data
- Sigverif is a built-in Windows program that displays all the unsigned drivers and related files in the computer
- Memory dump refers to copying data from one place to another without formatting
- System state backup is useful for forensic analysis of a Windows system

Computer Hacking Forensic Investigator



Module VIII

Linux and Macintosh Boot processes

Introduction

Macintosh is a personal computer introduced in the mid-80's that proved to be an alternative of IBM PC. Macintosh has great role to play in making the graphical user interface popular. Apple computers developed Macintosh.

Unix and Linux are the other important operating systems, which are widely accepted by the industry community for the development of new applications and performing networking tasks.

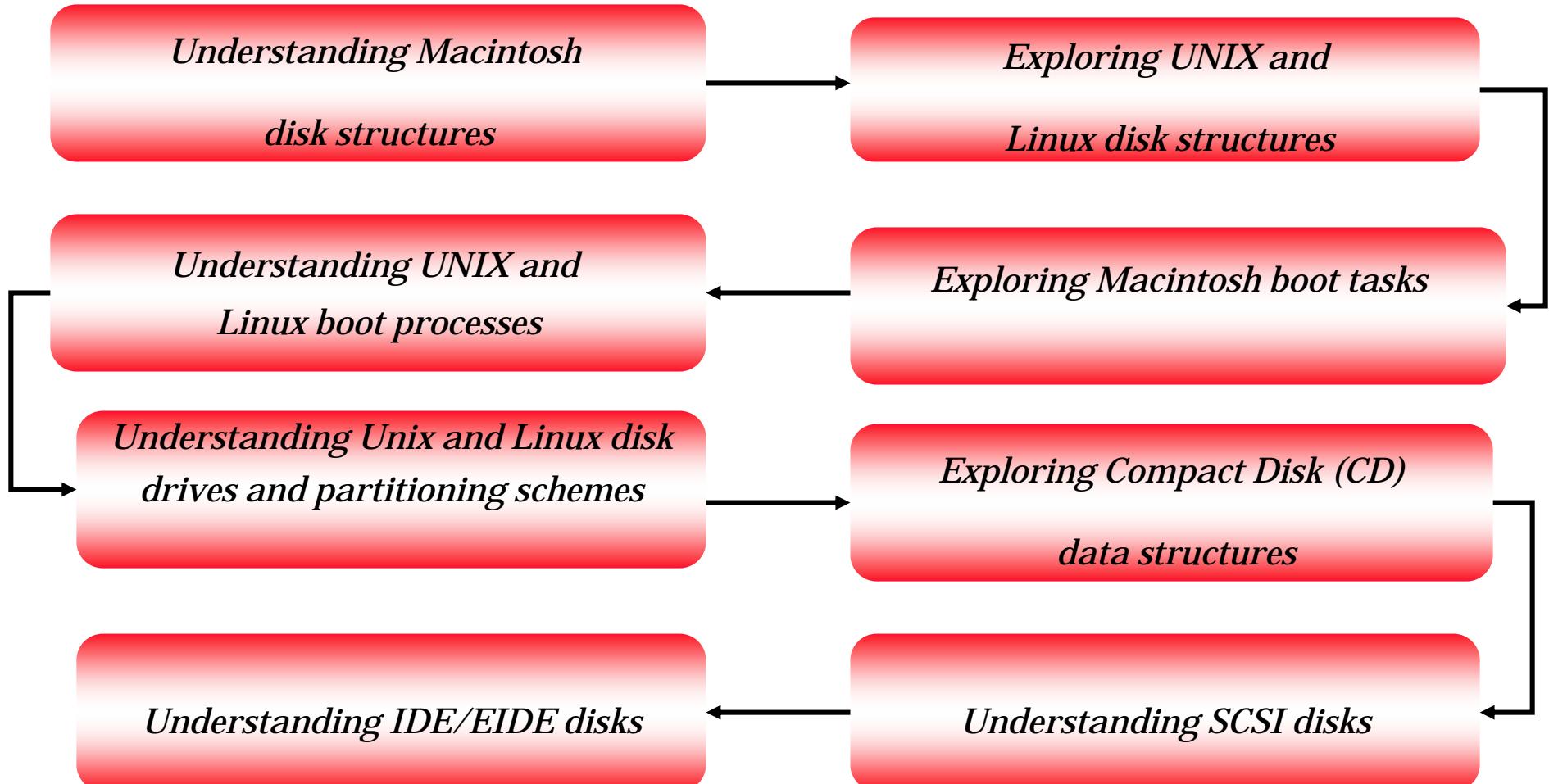
Unix has embedded TCP/IP in it, which gives it the advantage to be used as the server managing operating system.



Module Objective

- Understanding Macintosh disk structures
- Exploring UNIX and Linux disk structures
- Exploring Macintosh boot tasks
- Understanding UNIX and Linux boot processes
- Understanding Unix and Linux disk drives and partitioning schemes
- Exploring Compact Disk (CD) data structures
- Understanding SCSI disks
- Understanding IDE/EIDE disks

Module Flow



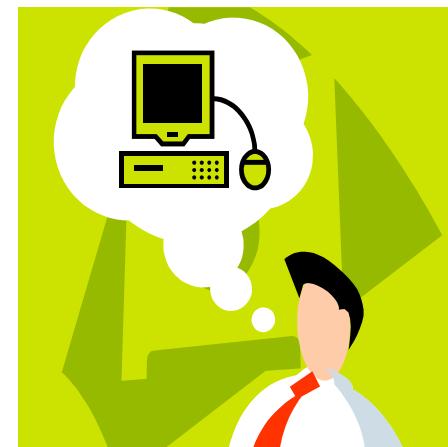
UNIX Overview

- UNIX is a multitasking and multiprogramming operating system that has in-built TCP/IP
- It utilizes a hierarchical file system
- The Unix shell is a simple user process and is also appropriate for programming
- It supports regular expressions suitable for complex searching



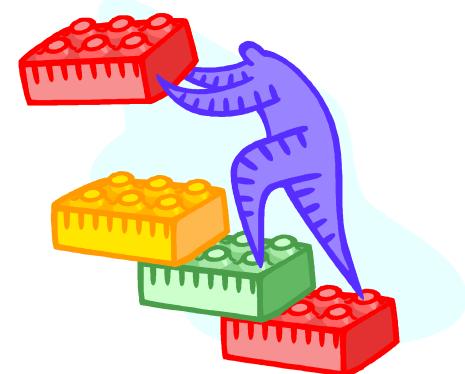
Linux Overview

- Linux is an Open Source implementation of UNIX triggered by Linus Torvalds
- It runs on platforms like Intel, Sparc®, PowerPC, and Alpha Processors
- Architecture of Linux like LNA creates a more reliable system
- Linux is easy to customize and update rapidly
- Linux can run on handheld devices (mobile phones, PDA's) and embedded systems to clusters of hundreds of servers

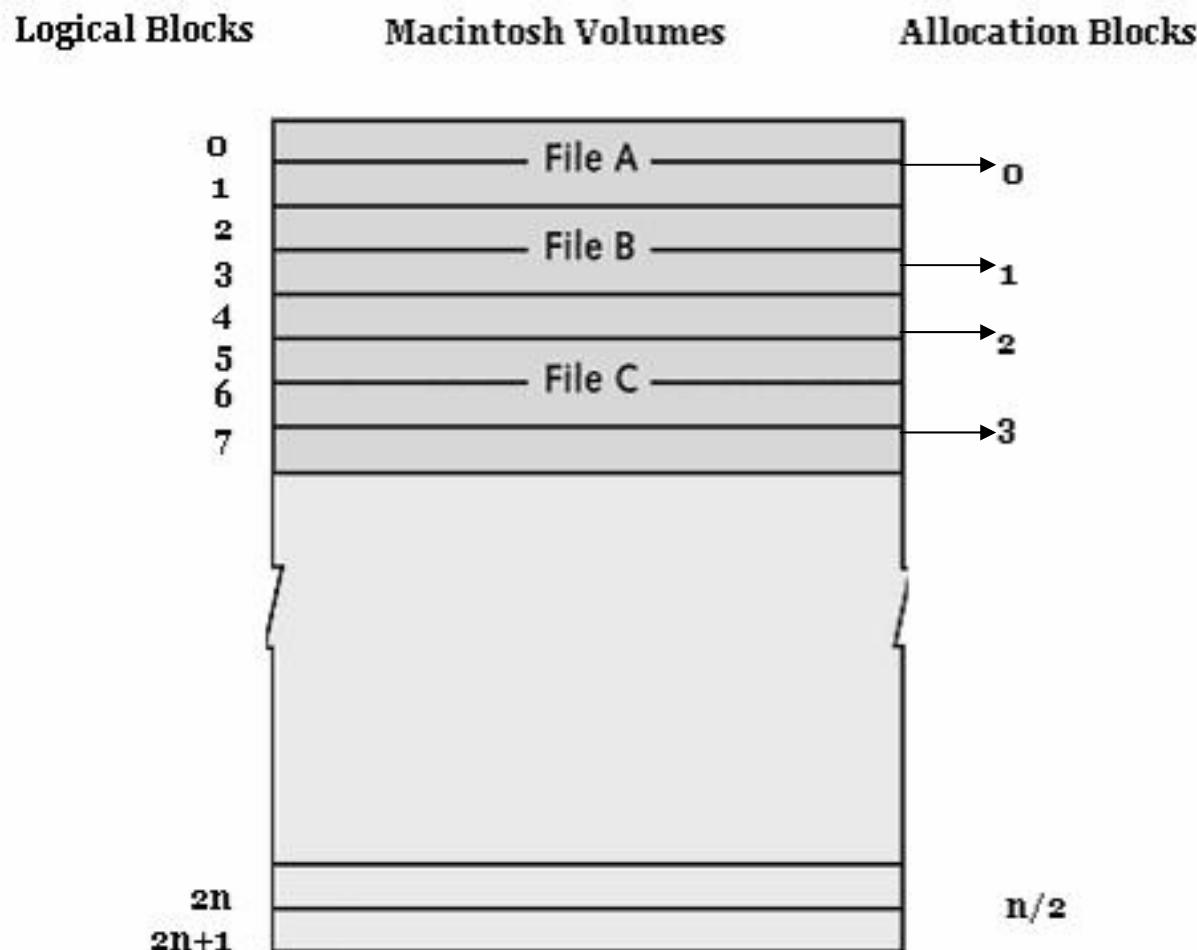


Understanding Volumes -I

- ◎ **Volume** –A volume is any storage media meant for storing files
- ◎ **Allocation block** – It contains logical blocks in which the data stored in the hard disk is preserved
- ◎ **Logical block** – It is the collection of data that cannot exceed 512 bytes
- ◎ **Logical EOF** – It is the number of bytes containing data
- ◎ **Physical EOF** – It is the number of allocation blocks allotted to the file



Understanding Volumes -II



Exploring Unix/Linux Disk Data Structures

Unix System Files

OS	System Files	Purpose
AIX	/etc(exports	Configuration files
	/etc/filesystems	Static file system information
	/etc/utmp	Current logon information
	/var/admn/wtmp /etc/security/lastlog	Logon history information
	/etc/security/failedlogin	Failed logon information
HP-UX	/etc/utmp	Currents logon information
	/var/adm/wtmp /var/adm/wtmpx	Logon history information
	/var/adm/btmp	Failed logon information
	/etc/fstab	Static file system information
	/etc/checklist	Static file system information (version 9.x)
LINUX	/etc(exports	Configuration files
	syslog	System log files
	/etc(exports	Configuration files
	/etc/fstab	Other relevant files
	/var/log/lastlog /var/log/wtmp	Logon history information
	/var/run/utmp	Currents logon information

Understanding Unix/linux Boot Process

- ROM loads instructions
- Instruction code verifies hardware
- Boot device and kernel are sited
- Kernel is implemented and identifies devices
- Kernel loads processes and detects the root directory, swap file, and dump file
- Information such as time zone, hostname, network services, and partitions are set



Understanding Linux Loader

- LILO is the famous boot loader for Linux
- It allows booting of multiple operating systems
- It allows the user to make choice between various kernel configurations and versions
- LILO is a two-stage boot loader:
 - I stage: It loads Linux into memory
 - II stage: It boots the Linux operating system



Linux Boot Process Steps

- Step 1: The Boot Manager
- Step 2: init
- Step 2.1: /etc/inittab
- Step 3: Services
- Step 4: More inittab

Step 1: The Boot Manager

- ◉ Boot manager is a small program that resides mostly on the MBR
- ◉ Displays a menu letting user to choose what operating system (if more than one OS) to boot.
- ◉ LILO is the common boot loader in Linux

Step 2: init

- Boot loader passes control to /sbin/init
- Linux init will then read a file called /etc/inittab
- Runlevel
 - A runlevel is a state for the system. Usually 0 , 1 , 2 , 3 , 4 , 5 , 6 and S
 - example, pass init=/bin/sh to the kernel, and then a plain shell would be used.

Step 2.1: /etc/inittab

```
1:2345:respawn:/sbin/mingetty tty1
```

- They have 4 fields, separated with colons
- **id**
 - This has no real meaning, but should be different for each line, can be one to four characters
- **runlevels**
 - For example, 2345 means this line applies to runlevels 2,3,4 and 5.
- **action**
 - what this line does
- **process**
 - a command to be executed.

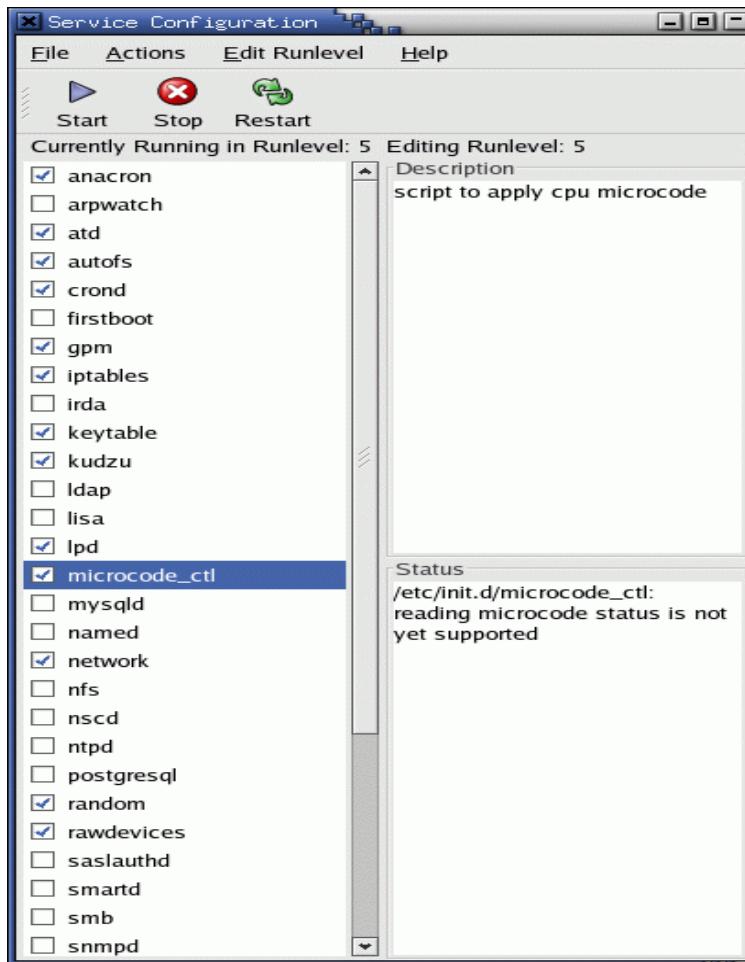
runlevels

The runlevels used by RHS are:

```
#      0 - halt (Do NOT set initdefault to this)
#      1 - Single user mode
#      2 - Multiuser, without NFS (The same as 3, if
#           you do not have networking)
#      3 - Full multiuser mode
#      4 - unused
#      5 - X11
#      6 - reboot (Do NOT set initdefault to this)
```

Step 3: Services

- Services are specified here /etc/init.d/ or /etc/rc.d/init.d



Understanding Permission Modes

- Linux and Unix allows high level security by allowing the owner of a file to provide access permissions to a file
- *Chmod* – It is a command available with Linux and Unix, which is used to grant read, write and execute permissions to users
- For example ls-1executes the following:

-rwxr--r--	1	root	root	1024	Mar 27	09:45	my doc
lrwxrwxrwx	1	root	root	1024	Apr 13	09:45	text
drwxr-xr--	1	root	root	1024	May 18	09:45	star

Unix and Linux Disk Drives and Partitioning Schemes

- Disk partition can be done by creating divider between various areas on the disk
- The major reason behind partitioning is to separate system files from user file
- Partition is done during installation of operating system
- In Linux disk partition is created using *cfdisk* program

Mac OS X

- Mac OS X is based on BSD Darwin engine
- MAC OS X uses HFS+ file system
- Mac OS X has nothing like the /etc/init.d directory. Instead, it finds its startup items in either /System/Library/Startup Items (for system startup items) or /Library/StartupItems (for locally-installed startup items)

File or Directory	Description
.DS_Store	This file contains Finder settings.
.Trashes	This directory contains files that have been dragged to the Trash.
.vol/	This directory maps HFS+ file IDs to files.
Applications/	This directory holds all your Mac OS X applications. Check out its Utilities/ subdirectory for lots of fun stuff!
Desktop DB, Desktop DF	The Classic Mac OS desktop database.
Desktop Folder/	The Mac OS 9 desktop folder.
Developer/	Apple's Developer Tools and documentation. Only available if you have installed the Developer Tools.
Library/	Support files for locally installed applications, among other things.
Network/	Network-mounted Application, Library, and Users directories, as well as a Servers directory.
Shared Items/	Use by Mac OS 9 to share items between users.
System Folder/	The Mac OS 9 System Folder.
System/	Contains support files for the system and system applications, among other things.
Temporary Items/	Temporary files used by Mac OS 9.
TheVolumeSettingsFolder/	This directory keeps track of details such as open windows and desktop printers.
Trash/	Mac OS 9 trash folder.
Users/	Home directories.
VM Storage	Mac OS 9 virtual memory file.
Volumes/	Contains all mounted filesystems.
automount/	This directory handles static NFS mounts.
bin/	Contains essential system binaries.
cores/	If core dumps are enabled (with tcsh's limit and bash/sh's ulimit commands), they will be created in this directory as core.pid.
dev/	This directory contains files that represent various devices.
etc/	This directory contains system configuration files.
lost+found	This directory stores orphaned files discovered by fsck.
mach	This is a symbolic link to the /mach.sym file.
mach.sym	Kernel symbols.
mach_kernel	The Darwin kernel.
private/	Contains the tmp, var, etc, and cores directories.
sbin/	Executables for system administration and configuration.
tmp/	Temporary files.
usr/	This directory contains BSD Unix applications and support files.
var/	This directory contains frequently modified files such as log files.

Mac OS X Hidden Files

- In Unix a file can be made invisible by prefixing its name with a ., as in /.vol
- HFS+ (a file system used my Mac OS) files and directories have a hidden attributes that can be set using SetFile command
- `SetFile -a V SomeFile.`

Booting Mac OS X

- ◎ Booting in Mac OS X depends on three steps
 - Mac's Open Firmware
 - Bootloader
 - Boot up sequence
- ◎ Open Firmware can be started by pressing cmd-opt-O-F
- ◎ Bootloader can load kernels from various filesystems

1. The following command prints the device tree:

```
0 > dev / ls
ff880d90: /cpus
ff881068:  /PowerPC,750@0
ff881488:  /l2-cache
ff882148:  /chosen
ff882388:  /memory@0
ff882650:  /openprom
ff882828:  /client-services
...
More [<space>,<cr>,q,a] ? _
```

2. The following command gives you information about installed RAM:

```
0 > dev /memory .properties ok
name          memory
device_type   memory
reg           00000000 10000000
              10000000 10000000
slot-names    00000003
              SODIMM0/J25LOWER
              SODIMM1/J25UPPER
...
dimm-types   DDR SDRAM
              DDR SDRAM
dimm-speeds  PC2700U-25330
              PC2700U-25330
...
```

Screenshot

① Directory Listing

```
0 > dir hd:\

      Size/          GMT
      bytes        date       time
      6148        12/25/ 3    4:25:25
      156         9/12/ 3    20:41:59
      589824       12/25/ 3   6:45: 6
      ...
      .DS_Store
      .hidden
      .hotfiles.btree
```

② Boot from TFTP Server

```
boot enet:<server IP>,<file>,<my IP>;<subnet>;<gateway IP>
```

Mac OS X Boot Options

- Command-S Boot into Single User Mode
- Command-V Boot using "Verbose" mode (shows all kernel and startup console messages)
- X Reset startup disk selection and boot into Mac OS X Server
- Shift Boot into "Safe Boot" mode, which runs Disk First Aid. A reboot will be required afterward.
- Option Boot into Open Firmware to select a boot device
- Command-Option-Shift-Delete Bypass internal harddrive on boot
- T Boot into Firewire target disk mode
- C Boot from the internal optical drive
- N Start from the Network (NetBoot)
- Command-Option-P-R Reset Parameter RAM (PRAM) and non-volatile RAM (NVRAM)
- (mouse button) Eject (internal) removable media

The Mac OS X Boot Process

- Mac OS X uses boot loader to perform the boot process.
- Follows various steps.
 - Starts the OpenFirmware which Looks for a boot device
 - Open Firmware loads 'tbxi' (BootX) file from partition
 - It executes BootX which,
 - Reads root partition from nvram
 - Loads mach kernel from the device
 - Copies Mac OS X device drivers from partition into memory
 - Disables all address translations
 - Starts Mac OS X mach kernel
 - Mach kernel begins its boot process
 - Mac OS X desktop is loaded

Installing Mac OS X on Windows XP

- Set path for prom_driver_graphic.
- Start and click install.
- Can customize the installation.
- Virtual machines like PearPC is used to install Mac OS X on Windows XP.
- PearPC is a way to get the OS X running in very less time span.
- <http://pearpc.sourceforge.net>

PearPC

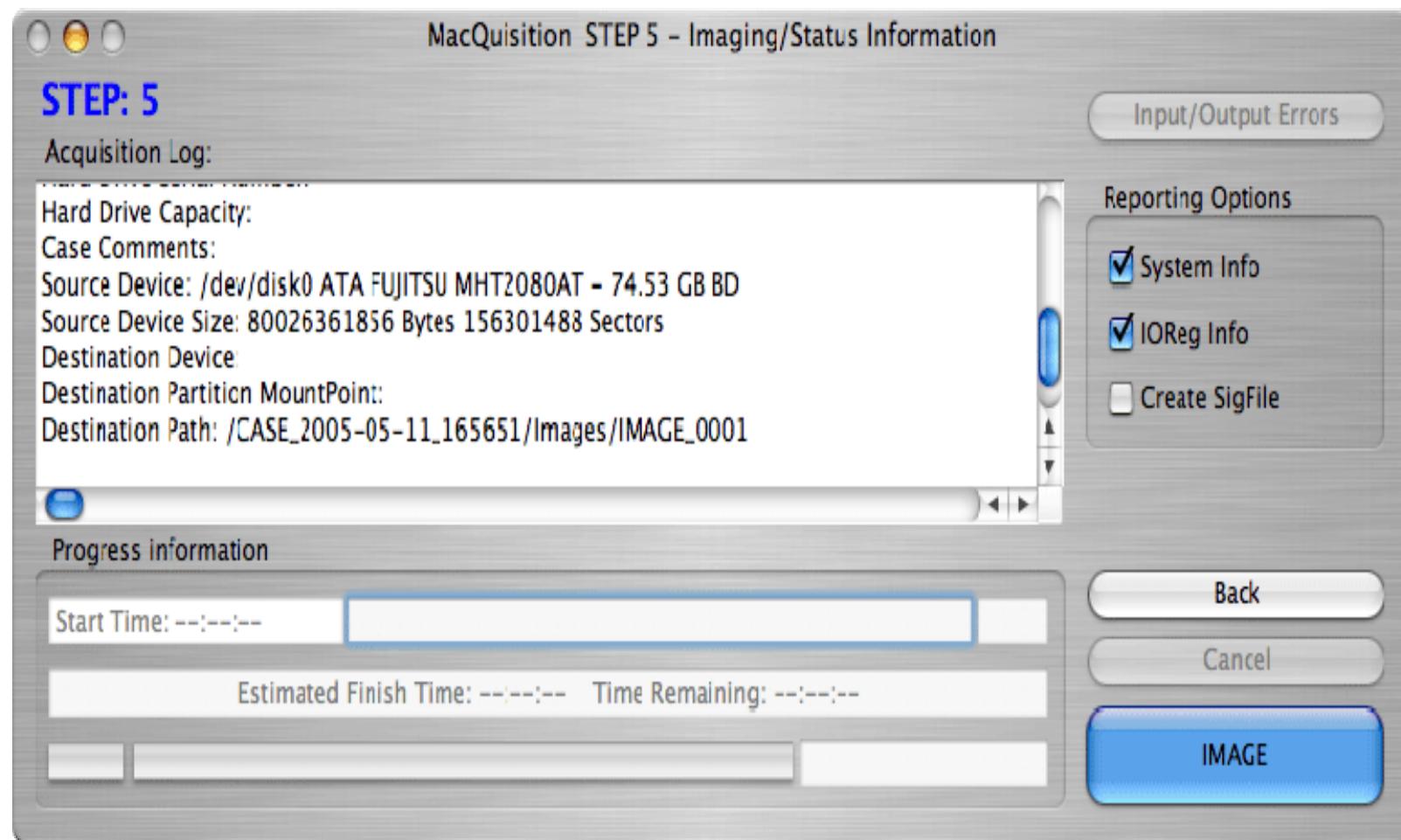
- ⦿ Capable of running most PowerPC OS.
- ⦿ Behave as a client on some operating system.
- ⦿ Limitations:
 - Performs well on small architectures.
 - Inaccurate timings.



MacQuisition Boot CD

- Forensic acquisition tool utilized to image Mac suspect drives using the suspects own system safely and easily .
- Features:
 - Identify the suspected device(s).
 - Configure the image of destination location directly over the network.
 - Can use Command line also.
 - Log case, exhibit and evidence tracking numbers and notes.
 - Generate MD5 hashes automatically.
 - Hash and block size customization with extension naming.
 - <http://www.blackbagtech.com>

MacQuisition



Summary

- Macintosh popularized the graphical user interface
- Mac OS X implements a boot sequence that prepares the system for operation
- Linux and Unix allows high level security by allowing the owner of a file to provide access permissions to a file
- The Linux file structure consists of meta-data and data. Meta-data includes items such as the user ID and group ID
- CDs and DVDs are optical media utilized for storing huge amounts of data
- SCSI connectors are used for a genre of peripheral devices



Computer Hacking Forensic Investigator

Module IX
Linux Forensics

Module Objective

- Use of Linux as a Forensic Tool
- Recognizing Partitions in Linux
- Overview of File System in Linux
- Linux Boot Sequence
- Linux forensics tools – Primer
- Case study – Extracting evidence from a floppy disk using Linux
- Challenges in disk forensics with Linux
- Case study – Extracting evidence from a hard disk using Linux

Use of Linux as a Forensics Tool

○ Why use Linux for Forensics?

- Greater Control
 - Treats every device as a file
 - Does not need a separate write blocker
- Flexibility
 - can be booted from a CD
 - can recognize several file systems
- Power
 - Distributions like F.I.R.E and Sleuth make Linux a forensic tool in itself.

Recognizing Partitions in Linux

- If a standard IDE disk is being used, it will be referred to as "hdx"
- The "x" is replaced with an "a" if the disk is connected to the primary IDE controller as master and a "b" if the disk is connected to the primary IDE controller as a slave device.
- Similarly, the IDE disks connected to the secondary IDE controller as master and slave will be referred to as "hdc" and “hdd” respectively

File System in Linux

```
/  
|_ bin  
| |_ <files> ls, chmod, sort, date, cp, dd  
|_ boot  
| |_ <files> vmlinuz, system.map  
|_ dev  
| |_ <devices> hd*, tty*, sd*, fd*, cdrom  
|_ etc  
| |_ X11  
| |_ <files> XF86Config, X  
| |_ <files> lilo.conf, fstab, inittab,  
modules.conf  
|_ home  
| |_ default user  
| |_ <files> .bashrc, .bash_profile,  
personal files  
| |_ other users
```

```
|_ mnt  
| |_ cdrom  
| |_ floppy  
| |_ other external file system mount  
points  
|_ root  
| |_ <root user's home directory>  
|_ sbin  
| |_ <files> shutdown, cfdisk, fdisk,  
insmod  
|_ usr  
| |_ local  
| |_ lib  
| |_ man  
|_ var  
| |_ log
```

On most Linux distributions, the basic directory structure is organized in the same manner.

Linux Boot Sequence

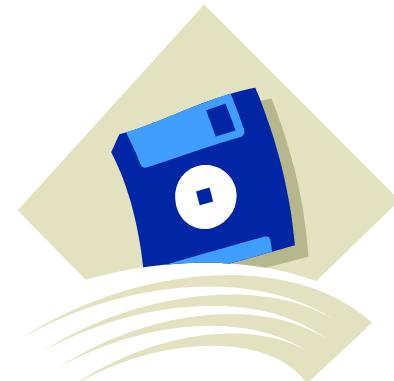
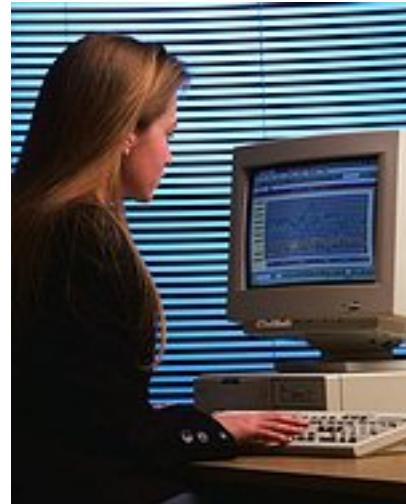
- The first step in the boot up sequence for Linux is loading the kernel. The kernel image is usually contained in the */boot* directory.
- Details of the boot loader can be gained from LILO or GRUB using more */etc/lilo.conf* or more */etc/grub.conf*
- The next step is initialization where runlevel and startup scripts are initialized and terminal process controlled.
- The file that controls the initialization is file */etc/inittab* and */sbin/init* begins the process.

Linux Forensics

- Linux has a number of simple utilities that make imaging and basic analysis of suspect disks and drives easier. These include
 - **dd** -command used to copy from an input file or device to an output file or device.
 - **sfdisk** and **fdisk** -used to determine the disk structure.
 - **grep** -search files for instances of an expression or pattern.
 - The **loop device** -allows user to mount an image without having to rewrite the image to a disk.
 - **md5sum** and **sha1sum** -create and store an MD5 or SHA hash of a file or list of files (including devices).
 - **file** -reads file header information in an attempt to ascertain its type, regardless of name or extension.
 - **xxd** - command line hexdump tool.
 - **ghex** and **khexedit** -the Gnome and KDE (X Window interfaces) hex editors.

Case Example

- ⦿ Ms. Angry had filed a lawsuit against GoodCompany Inc for sexual harassment by one of its senior director's Mr. Suspect.
- ⦿ She has submitted a floppy as evidence of Mr. Suspect's advances.
- ⦿ She has also ascertained that Mr. Suspect used to send her explicit material through floppy disks marked as legitimate work.
- ⦿ Mr. Investigator has been called to investigate the case by GoodCompany Inc
- ⦿ How do you think he should proceed with the evidence?



Step-by-step approach to Case 1 (a)

1. Document all processes.
 - a. Begin with creating a directory where all forensic activities can be done. */mkdir evidence*
 - b. It is desirable to create a special mount point for all physical subject disk analysis *mkdir /mnt/investigation*
2. Determine the disk structure
 - a. Create an image of the disk using the simple bit streaming command dd. *dd if=/dev/fd0 of=image.suspectdisk*
 - b. Change the read-write permissions of the image to read-only using chmod. *Chmod 444 image.suspectdisk*

Step-by-step approach to Case 1 (b)

3. Mount the restored imaged working copy and analyze the contents. *mount -t vfat -o ro,noexec /dev/fd0 /mnt/investigations*
 - a. Another option is to mount a point within the image file using the *loop* interface rather than mounting the contents to another location. *mount -t vfat -o ro,noexec,loop image.suspectdisk /mnt/investigations*
4. Verify the integrity of the data on the imaged file by checking the file hash. *md5sum /evidence/md5.image.suspectfile* or *shasum -c /evidence/SHA.image.suspectfile*

Step-by-step approach to Case 1 (c)

5. Use the ls command to view the contents of the disk. *ls -alR* to list all files including hidden files and list the directories recursively.
6. Make a list of all files along with access times.
ls -laiRtu > /evidence/suspectfiles.list
7. Search for likely evidence using grep. *grep -i xxx suspectfiles.list*
8. List unknown file extensions and changed file appearances. *file changedfile*
 - a. Files can be viewed using *strings, cat, more* or *less*

Step-by-step approach to Case 1 (d)

9. Certain keywords can be searched for from the entire file list. *cat /evidence/ suspectfiles.list / grep blackmailword*
 - a. A systematic approach to searching for keywords would be to create a keywords list. E.g. save it as */evidence/keywordlist.txt*.
 - b. Grep the files for the keywords and save it to a file. *grep -aibf keywordlist.txt image.suspectdisk > results.txt*
 - c. View the results. *Cat results.txt*
 - d. To analyze the files at each offset use the hexdump tool. *xxd -s (offset) image.suspectdisk / less*

Case 2

⦿ Mr. Bad has been accused of hoarding illegal material of questionable moral content on his company network systems.

⦿ Mr. Investigator has been called upon to examine the suspect hard disk and unearth evidence related to the said illegal material.

⦿ How do you think Mr. Investigator should proceed in extracting and preserving the evidence?



Challenges in disk forensics with Linux

- Linux cannot identify the last sector on hard drives with an odd number of sectors
- Most Linux tools are complicated and prefer to be used at the command line
- Devices can be written to even if they are not mounted
- Bugs in the open source tools can be used to question the credibility of the tool for forensics use.
- Forensic and Incident Response Environment (F.I.R.E) by William Salusky provides a good tool set

Step-by-step approach to Case 2 (a)

1. Note down the model information from the hard disk label /manufacturer's Web site, also note size and total number of sectors on the drive.
2. Wipe and format a image disk drive using the ext3 file system (> 3x evidence size). Fill the disk with zeros and ensure that the contents are matched. *dcfldd if=/dev/zero of=/dev/hda bs=4096 conv=noerror, sync*
3. Partition the disk and reboot. *fdisk /dev/hda*
4. Format with the ext3 file system. *mkfs –t ext3 /dev/image.disk*

Step-by-step approach to Case 2 (b)

5. Prepare the disk for imaging.
 - a. Mount the freshly prepared read-write image disk. `mount /dev/hda /mnt/image.disk`
 - b. Create a directory for all documentation and analysis. `mkdir /mnt/image.disk/case_no`
 - c. Create a sub-directory to hold the evidence image. `mkdir /mnt/image.disk/case_no/evidence_no`
 - d. Document details of the investigation in a text file including investigator's details, case background details, investigation dates etc.
 - e. Document details of the disk media including investigator name and organization; case number; media evidence number; date and time imaging was done; make, model, and serial number of computer; IP and system hostname; make, model, and serial number of HD; source of HD and scope of investigation.

Step-by-step approach to Case 2 (c)

6. Image the disk.
 - a. Connect both original evidence drive and drive to be imaged to the Imaging System.
 - b. Verify all jumper settings – Master / Slave
 - c. Make sure that the imaging system will boot only from CD by checking the BIOS settings
 - d. Image the disk using *dd*
dd if=/dev/hdx of=image.disk conv=noerror,sync
This will allow dd to try to ignore any errors (*conv=noerror*) and synchronize the output (*sync*) with the original
7. Check for accuracy by comparing md5sum
8. Mount the disk and extract evidence. Images can be carved using *dd* or the hex dump tool *xxd*.

Popular Linux Tools

- Sleuthkit - written by Brian Carrier and maintained at <http://www.sleuthkit.org>.
- Autopsy – HTML front-end for sleuthkit
- SMART - by ASR Data, is a commercial GUI forensic tool for Linux
- Penguin Sleuth - Knoppix based linux distribution with a forensic flavor
- White Glove Linux –by Dr. Fred Cohen
- F.I.R.E - Forensic and Incident Response Environment by William Salusky

Summary

- ◉ Linux imparts greater control, flexibility and power as a forensics tool
- ◉ Linux has a number of simple utilities that make imaging and basic analysis of suspect disks and drives easier
- ◉ NASA's loopback driver is a kernel module that can be used to associate an entire disk image with a single loop device
- ◉ There are several popular Linux tool kits that provide GUI as well for convenience.



Computer Hacking Forensic Investigator

Module X

Data Acquisition and Duplication

Scenario

Allen a forensic investigator was hired by a bank to investigate employee fraud. The bank has four 30 GB machines on the Local Area Network. One of the machines was used to transfer client account information.

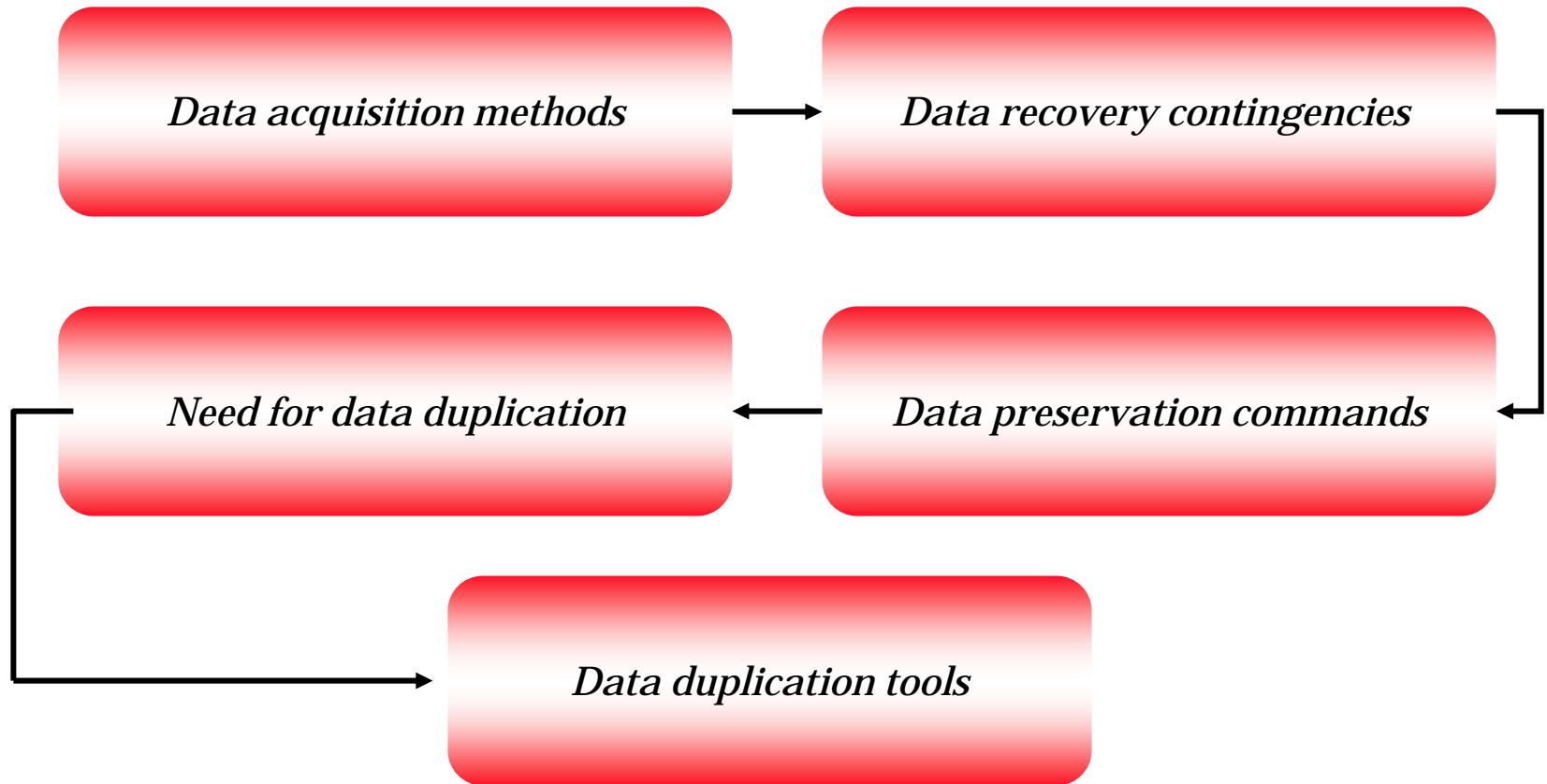
Allen makes two copies of the data from each of the computers and discovers that the computer used by the employee was booby trapped. He recovers the data by using the SafeBack tool.



Module Objective

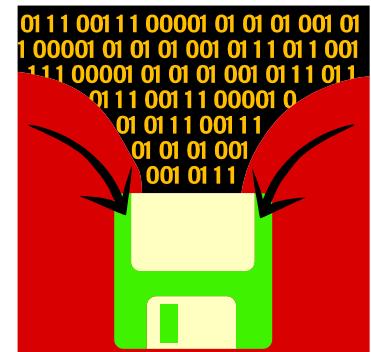
- ◉ Determining the best data acquisition methods
- ◉ Understanding data recovery contingencies
- ◉ Data preservation commands
- ◉ The need for data duplication
- ◉ Data duplication tools

Module Flow



Determining the Best Acquisition Methods

- Forensic investigators acquire digital evidence using the following methods
 - Creating a bit-stream disk-to-image file
 - Making a bit-stream disk-to-disk copy
 - Creating a sparse data copy of a folder or file



Data Recovery Contingencies

- ◉ Investigators must make contingency plans when data acquisition failure occurs
- ◉ To preserve digital evidence investigators need to create a duplicate copy of the evidence files
- ◉ In case the original data recovered is corrupted investigators can make use of the second copy
- ◉ Use of at least two data acquisition tools are preferred to create copy of evidence incase the investigator's preferred tool does not properly recover data



MS-DOS Data Acquisition Tools

- In the past software tools developed for forensics investigation were created for MS-DOS
- Investigators still make use of these tools as they are commercially available and easy to use
- Advantages of MS-DOS acquisition tools

- Fit in a forensic boot disk
- Require fewer resources to make bit-stream files
- User friendly



MS-DOS Data Acquisition Tool: DriveSpy

- DriveSpy enables the investigator to direct data from one particular sector range to another sector
- DriveSpy provides two methods in accessing disk sector ranges:
 - Defining the absolute starting sector after a comma and the total number of sectors to be read on the drive
 - Listing the absolute starting and ending sectors



DriveSpy Data Manipulation Commands

- ⦿ There are two commands in DriveSpy that is used for Data Manipulation:

- The “*SaveSect*” command-

- Used to copy particular sectors on a disk to a file
 - It copies the sectors as a bit-stream image so that the file is a duplicate of the original sectors

- The “*WriteSect*” command-

- Used to regenerate the information acquired through the SaveSect command



DriveSpy Data Preservation Commands

- The data preservation commands in the DriveSpy application are:

- The “*SavePart*” command-

- Used to create an image file of the specified disk partition of the suspect's drive

- The “*WritePart*” command-

- Counterpart of the “*SavePart*” command

- Used to recreate the saved partition image file that is created with the “*SavePart*” command



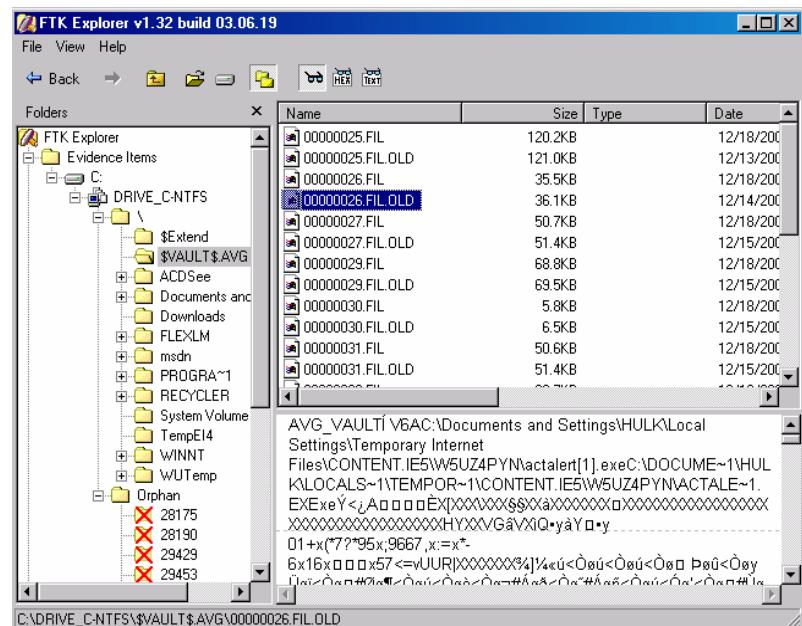
Using Windows Data Acquisition Tools

- Windows data acquisition tools allow the investigator to easily acquire evidence from a disk with the help of removable media such as USB storage devices
- These tools also can use Firewire to connect hard disks to the forensic lab systems
- Data acquisition tools in Windows cannot acquire data from the host protected area of the disk

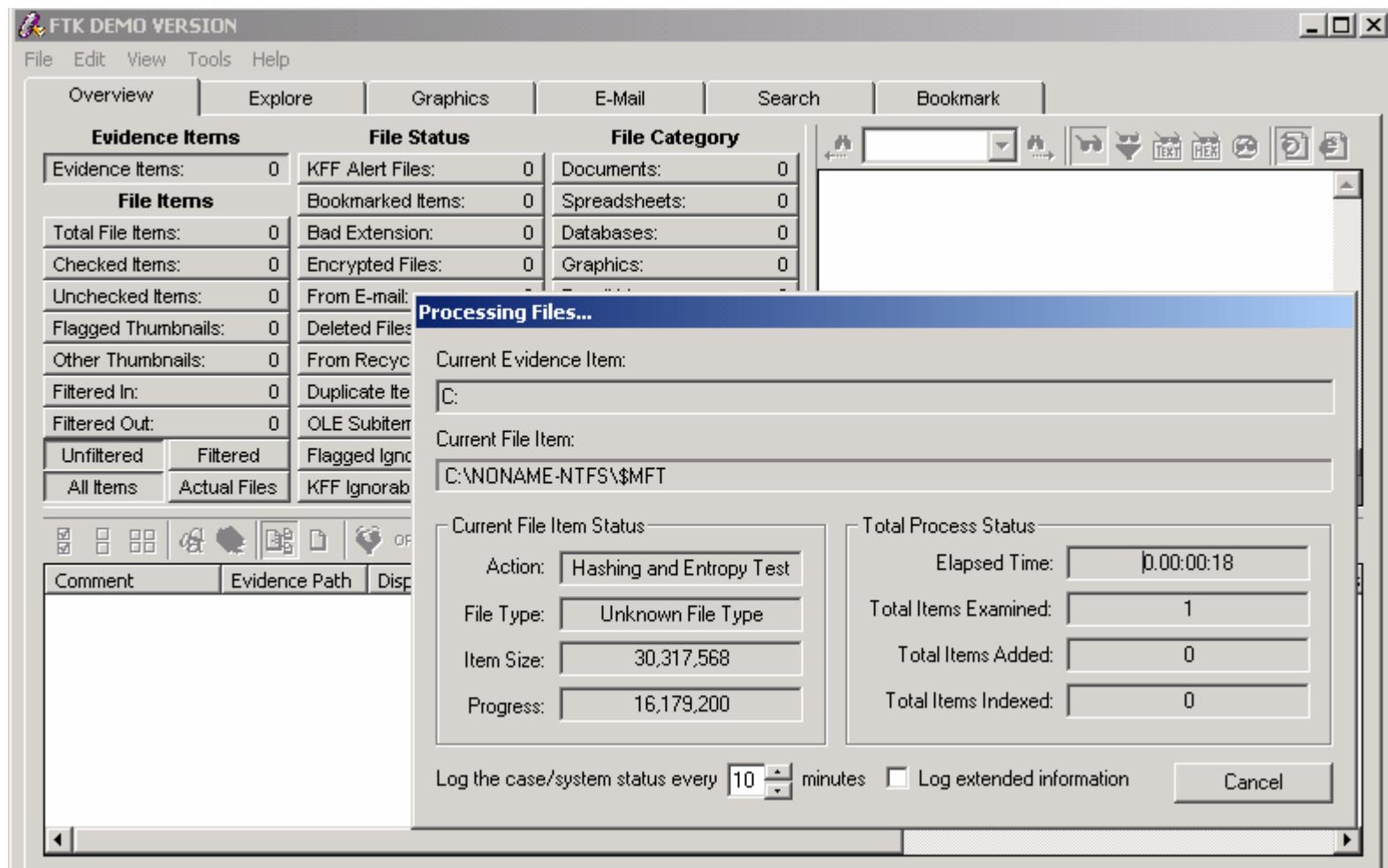


Data Acquisition Tool: AccessData FTK Explorer

- FTK Explorer acquires data that can help the investigator understand how other forensic tools in Windows work
- This tool was first designed to examine disks and bit-stream disk-to-image files created by using other forensic software
- FTK Explorer can make bit-stream disk-to-image copies of evidence disks
- This tool allows the investigator to acquire the evidence disk from a logical partition level or a physical drive level



FTK



Acquiring Data on Linux

- Forensic Investigators use the built-in Linux command “**dd**” to copy data from a disk drive
- This command can make a bit-stream disk-to-disk file, disk-to-image file, block-to-block copy/ block-to-file copy
- The “**dd**” command can copy data from any disk that Linux can mount and access
- Other forensic tools such as AccessData FTK and Ilook can read dd image files

Dd.Exe (Windows XP Version)

- Works on Windows platform
- Detects unauthorized dialers
- User friendly program
- Command Syntax

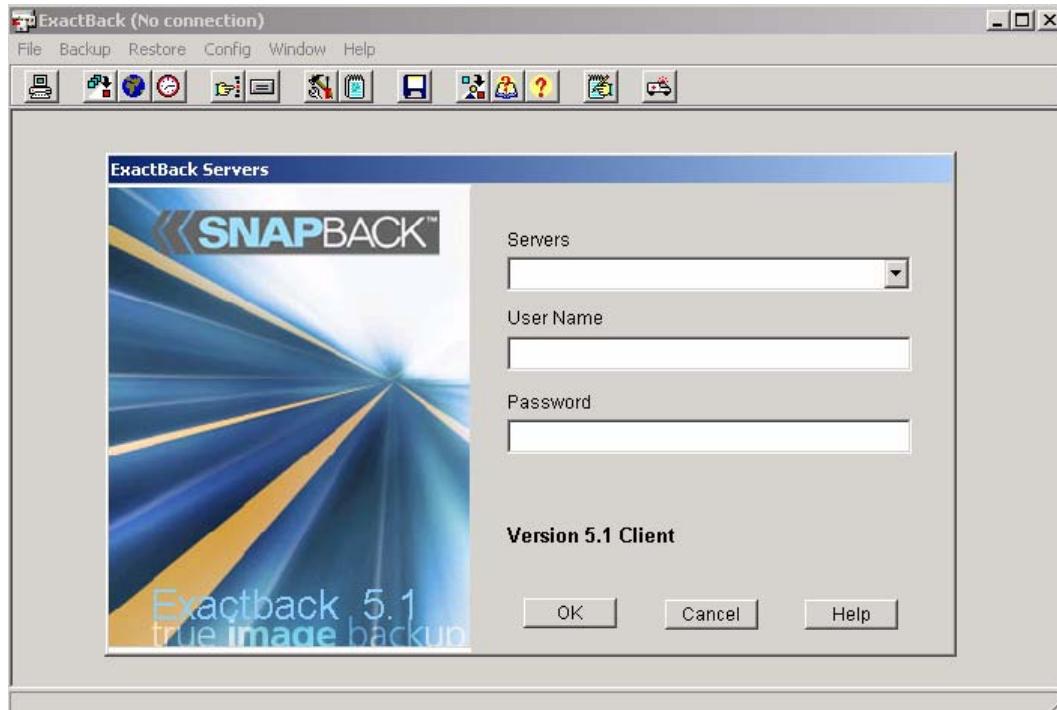
```
dd.exe if=\\.\\PhysicalDrive0
of=d:\\images\\PhysicalDrive0.
img --md5sum --verifymd5 --
md5out=d:\\images\\PhysicalDri
ve0.img.md5
```



Data Acquisition Tool: Snapback Exact

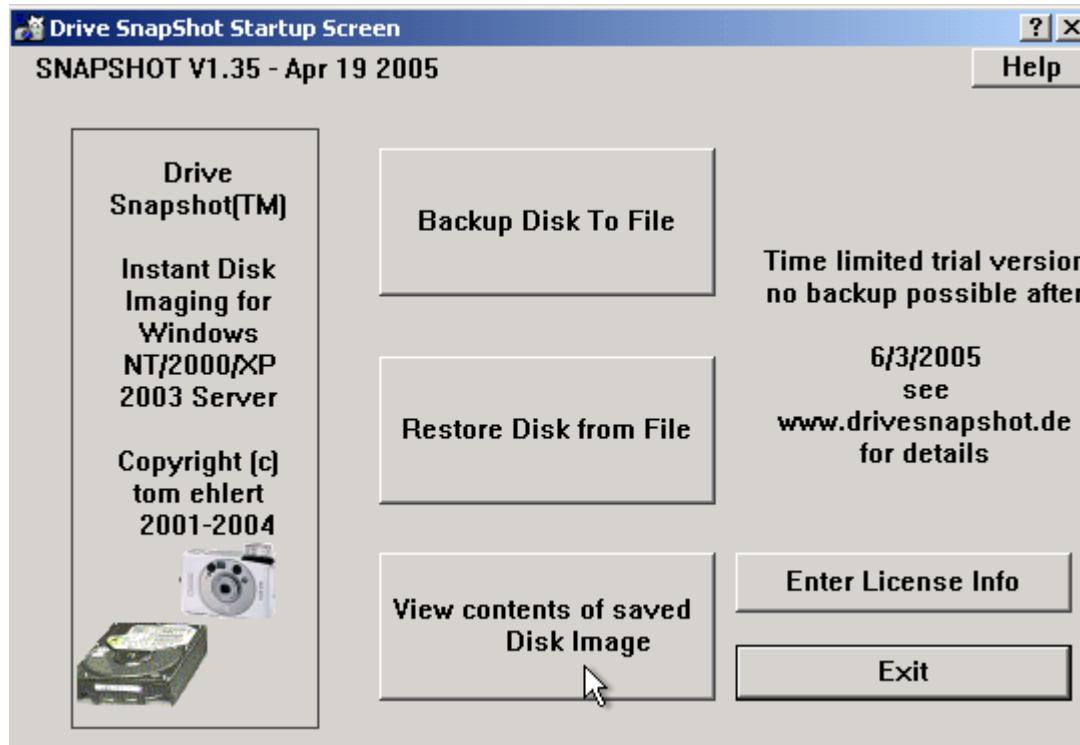
- o Server based backup program for Windows server
- o Copies byte by byte images of the server hard drives to the tape
- o Keep tracks of records
- o Important features are:

- Full open file management
- Remote administration
- Backup scheduling



Snapshot

Data acquisition tool



DatArrest

- Supports the tools for Forensic Data Seizure
- Works on all IBM compatible systems
- Recovers the deleted data
- User interface tool
- Any removable drives can back up through DatArrest

Data Acquisition Tool: SafeBack

- SafeBack is also a MS-DOS data acquisition tool and can perform a CRC-32 calculation for each sector copied to ensure data integrity
- SafeBack creates a log file of all transactions it performs
- Functions:
 - Creates disk-to-image files
 - Copies data from a source disk to an image on a tape drive
 - Copies data from a partition to an image file
 - Compresses acquired files to reduce the volume save-set sizes

Data Acquisition Tool: Encase

- ◉ The Encase tool delivers advanced features for computer forensics and investigations
- ◉ It is the primary data acquisition tool that is used by forensic investigators
- ◉ Provides tools to conduct investigations with accuracy and efficiency
- ◉ Data can be acquired by:
 - Disk to disk
 - Disk to network server drive
 - Parallel port with a laplink cable to the forensics workstation's disk drive

Encase

File Edit View Tools Help

New Open Save Print Add Device Search Refresh Show Excluded Show Deleted Delete View Email Email/Internet Search To Filter Display

Cases

Table Report Gallery Timeline Disk Code

	Name	From	To	Subject	Created	Sent
1	Re: If you love your daughter	billyray150@hotmail.com	Chaser1191@aol.com	Re: If you love your daughter		06/03/02 11:47:39AM
2	Re: Your Daughters Safety Depends on This!!!	billyray150@hotmail.com	Chaser1191@aol.com	Re: Your Daughters Safety Depends or		06/03/02 10:33:32AM
3	Delivery Status Notification (Failure)	postmaster@guidancesoftware.com	Chaser1191@aol.com	Delivery Status Notification (Failure)		06/03/02 09:17:30AM
4	Delivery Status Notification (Failure)	postmaster@guidancesoftware.com	Chaser1191@aol.com	Delivery Status Notification (Failure)		06/03/02 09:17:30AM
5	Returned mail: User unknown	MAILER-DAEMON@aol.com	Chaser1191@aol.com	Returned mail: User unknown		05/14/02 10:09:32AM
6	Criminal Defense Lawyers - California Crimina...	billyray150b@netscape.net	chaser1191@aol.com	Criminal Defense Lawyers - California C		05/23/02 07:09:31AM
7	Welcome to My Calendar	AOLMyCalendar@aol.com	chaser1191@aol.com	Welcome to My Calendar		04/18/02 01:11:51PM
8	Re: Next few days	billyray150@hotmail.com	Chaser1191@aol.com	Re: Next few days		04/03/02 08:35:03AM
9	Re: you gotta see this one	billyray150@hotmail.com	Chaser1191@aol.com	Re: you gotta see this one		04/03/02 08:29:34AM
10	Re: Time Test	billyray150@hotmail.com	Chaser1191@aol.com	Re: Time Test		04/03/02 08:28:39AM
11	Re: (no subject)	billyray150@hotmail.com	Chaser1191@aol.com	Re: (no subject)		04/03/02 08:27:47AM
12	Re: xdrive	billyray150@hotmail.com	Chaser1191@aol.com	Re: xdrive		04/03/02 08:26:55AM
13	Re: Instant Messaging	billyray150@hotmail.com	Chaser1191@aol.com	Re: Instant Messaging		04/03/02 08:25:59AM
14	Re: http://www.xdrive.com/page.cfm?name...	billyray150@hotmail.com	Chaser1191@aol.com	Re: http://www.xdrive.com/page.cfm?		04/03/02 08:25:10AM
15	Re: (no subject)	billyray150@hotmail.com	Chaser1191@aol.com	Re: (no subject)		04/03/02 08:23:52AM
16	Delivery Status Notification (Failure)	postmaster@guidancesoftware.com	Chaser1191@aol.com	Delivery Status Notification (Failure)		06/03/02 09:17:30AM
17	Re: Instant Messaging	billyray150@hotmail.com	Chaser1191@aol.com	Re: Instant Messaging		04/03/02 08:25:59AM
18	Re: xdrive	billyray150@hotmail.com	Chaser1191@aol.com	Re: xdrive		04/03/02 08:26:55AM
19	Delivery Status Notification (Failure)	postmaster@guidancesoftware.com	Chaser1191@aol.com	Delivery Status Notification (Failure)		06/03/02 09:17:30AM
20	Re: Your Daughters Safety Depends on This!!!	billyray150@hotmail.com	Chaser1191@aol.com	Re: Your Daughters Safety Depends or		06/03/02 10:33:32AM
21	Welcome to My Calendar	AOLMyCalendar@aol.com	chaser1191@aol.com	Welcome to My Calendar		04/18/02 01:11:51PM
22	Re: Next few days	billyray150@hotmail.com	Chaser1191@aol.com	Re: Next few days		04/03/02 08:35:03AM
23	Re: you gotta see this one	billyray150@hotmail.com	Chaser1191@aol.com	Re: you gotta see this one		04/03/02 08:29:34AM
24	Re: Time Test	billyray150@hotmail.com	Chaser1191@aol.com	Re: Time Test		04/03/02 08:28:39AM
25	Re: (no subject)	billyray150@hotmail.com	Chaser1191@aol.com	Re: (no subject)		04/03/02 08:27:47AM

Text Hex Report Console Details Lock 12932/62665

Attachments: NO
From: billyray150@hotmail.com
To: Chaser1191@aol.com
Subject: Re: xdrive

Case 1|Hunter XP\Program Files\America Online 7.0\organize\chaser1191\AOL Personal Filing Cabinet\Chaser1191\Mail\Incoming/Saved Mail\Re: xdrive (chaser1191: PS 29323 LS 29323 CL 29323 SO 000 FO 0 LE 0)

EnScripts Filters Conditions Email Filter Condition To Filter

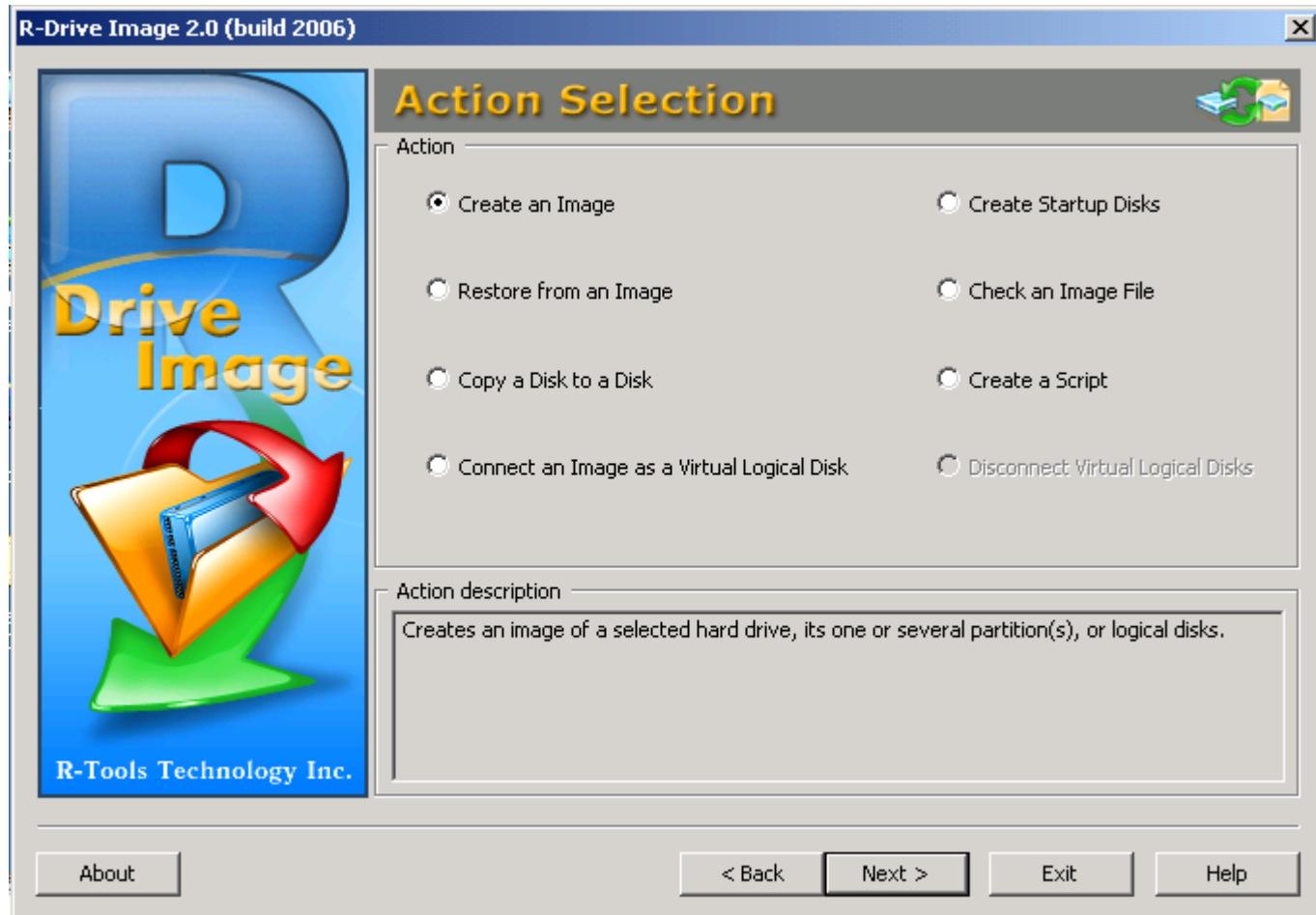
Need for Data Duplication

- ◉ Investigators need to worry about destructive devices that can be planted in the system by the owner. Evidence can be destroyed if the investigator is not careful
- ◉ Data fragments can be overwritten and data stored in the Windows swap file can be altered or destroyed
- ◉ Data duplication is essential for the proper preservation of digital evidence

Data Duplication Tool: R-drive Image

- R-Drive Image is an important tool that provides disk image files creation for backup or duplication purposes
- Disk image file contains exact, byte-by-byte copy of a hard drive, partition or logical disk
- R-Drive can create partitions with various compression levels freely without stopping Windows OS
- These drive image files can then be stored in a variety of places, including various removable media such as CD-R(W) or DVD-R(W) , Iomega Zip or Jazz disks

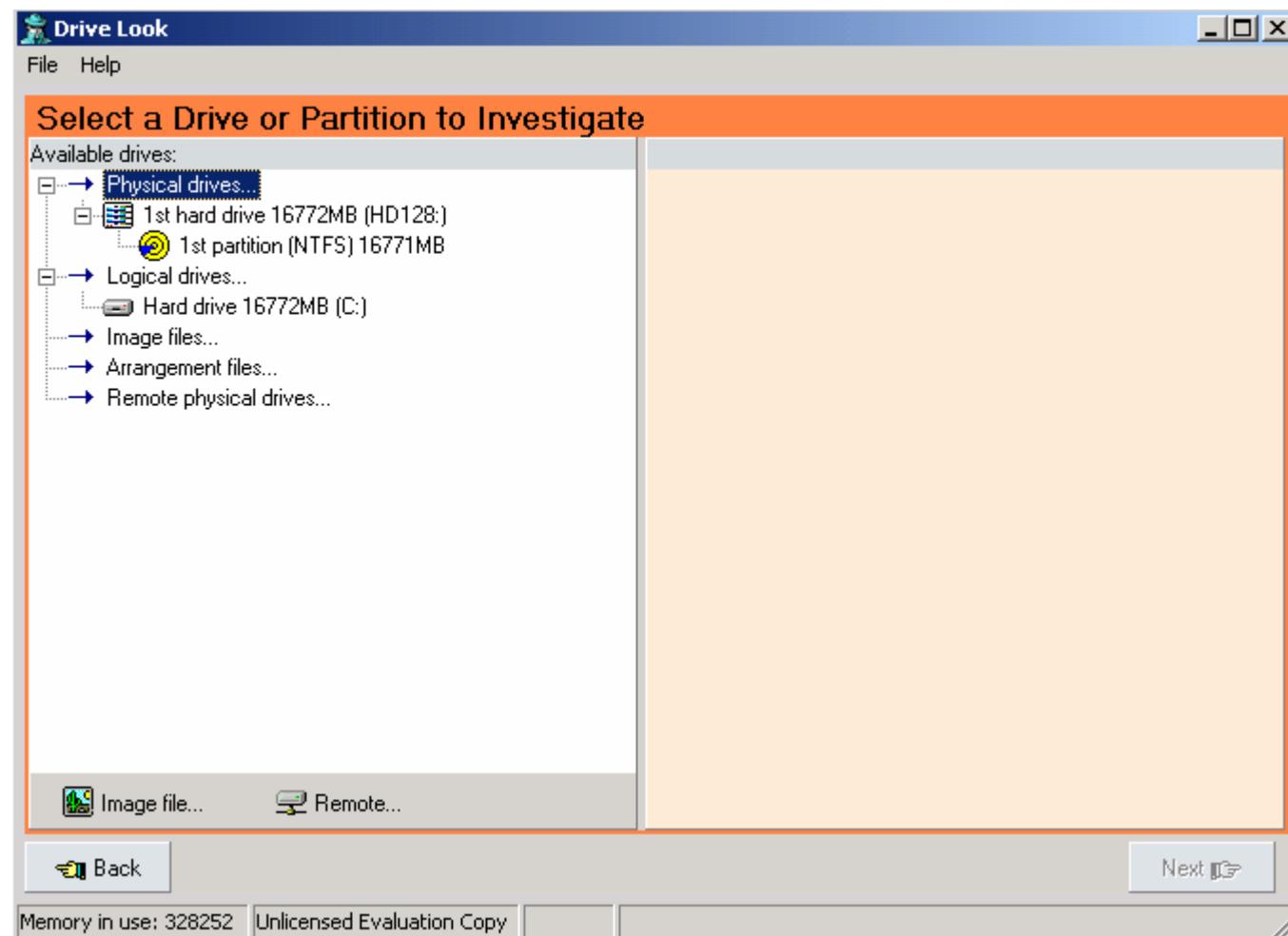
R-drive Image



Data Duplication Tool: DriveLook

- ◉ The DriveLook Tool has the following features:
 - Indexes the hard drive for the text that was written to it
 - Searches through a list of all words stored on the drive
 - View the location of words in the disk editor
 - Switches between different views
 - Uses image file as input
 - Access remote drives through serial cable or TCP/IP

Drivelook



Data Duplication Tool: DiskExplorer

- DiskExplorer aides examiners to investigate any drive and recover data
- Two versions of DiskExplorer exist:
 - DiskExplorer for FAT
 - Disk Explorer for NTFS
- The tool also has provisions to navigate through the drive by jumping to:
 - Partition table
 - Boot record
 - Master file table
 - Root directory

Diskexplorer

Runtime's DiskExplorer for NTFS

File Goto Link Edit View Tools Help

Sector Partition table

x00000000 Valid Partition Table										
Entry No	System	Boot	Starting Cylinder	Head	Sector	Ending Cylinder	Head	Sector	Relative Start Sector	Total Sectors
1	NTFS	Yes	x000	x01	x01	x3FF	xFE	x3F	x0000003F	x01FFD5E9
			0	1	1	1023	254	63	63	33543657
2	Free	No	x000	x00	x00	x000	x00	x00	x00000000	x00000000
			0	0	0	0	0	0	0	0
3	Free	No	x000	x00	x00	x000	x00	x00	x00000000	x00000000
			0	0	0	0	0	0	0	0
4	Free	No	x000	x00	x00	x000	x00	x00	x00000000	x00000000
			0	0	0	0	0	0	0	0
x00000001 Invalid Partition Table										
Entry No	System	Boot	Starting Cylinder	Head	Sector	Ending Cylinder	Head	Sector	Relative Start Sector	Total Sectors
1	Free	No	x000	x00	x00	x000	x00	x00	x00000000	x00000000
			0	0	0	0	0	0	0	0
2	Free	No	x000	x00	x00	x000	x00	x00	x00000000	x00000000
			0	0	0	0	0	0	0	0
3	Free	No	x000	x00	x00	x000	x00	x00	x00000000	x00000000
			0	0	0	0	0	0	0	0
4	Free	No	x000	x00	x00	x000	x00	x00	x00000000	x00000000
			0	0	0	0	0	0	0	0

(Sector:Offset)=x00000000:x1C2 (0:450) Selection=x00000000:x1C2-x00000000:x1C2

Drive: HD128: (1st hard drive), 33543720 (x01FFD628) sectors Sectors 0-33,543,719

Path: HD128:

Volume: No volume mounted Region: NONE

Memory in use: 442248 View: R/O Unlicensed Evaluation Copy

Summary

- ◉ Investigators can acquire data in three ways: creating a bit-stream, disk-to-image file, making a bit-stream disk-to-disk copy, or creating a sparse data copy of a specific folder path or file
- ◉ The “SavePart” command retrieves information about the partition space in the hard disk
- ◉ The “dd” command in Linux can make bit-stream disk-to-disk copy and disk-to-image file copy
- ◉ Lossless compression is an acceptable method for computer forensics because it does not change the data
- ◉ Lossy compression alters the data, leading to loss of data



Computer Hacking Forensic Investigator

Module XIX Recovering Deleted Files

Scenario

Susan runs a home business developing images and sound for the advertising business. She accidentally deleted a file containing client information.

All her efforts to recover the deleted file were in vain.

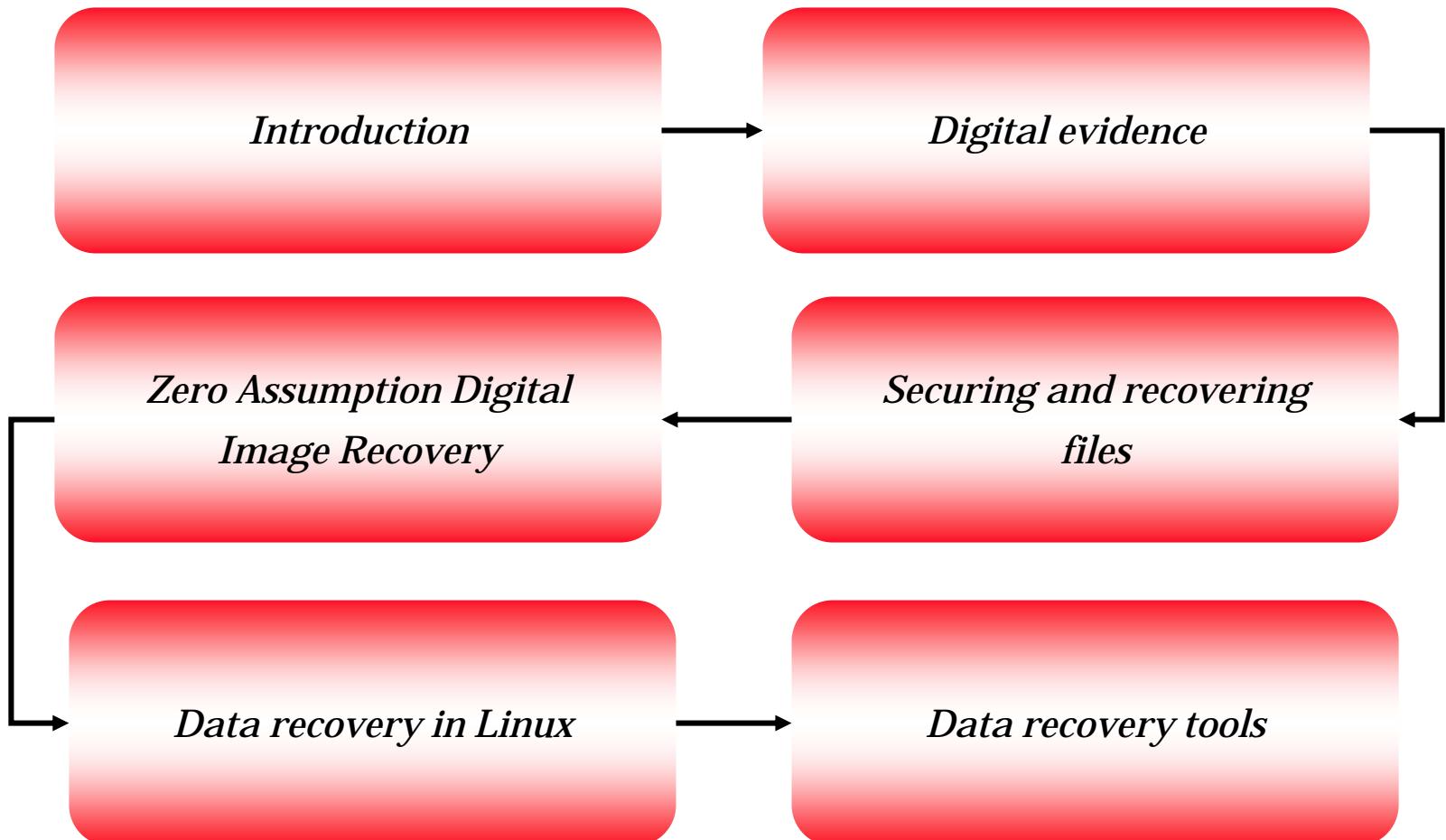
An investigator was hired by to recover the deleted files. The Investigator determined that the drive did not suffer any mechanical failure and was a software related problem. By using the Restorer 2000 application he was able to recover all of the deleted files.



Module Objective

- Introduction to recovering image files
- Digital evidence
- Securing and recovering deleted files
- Zero Assumption Digital Image Recovery
- Data recovery in Linux
- Data recovery tools

Module Flow



Introduction

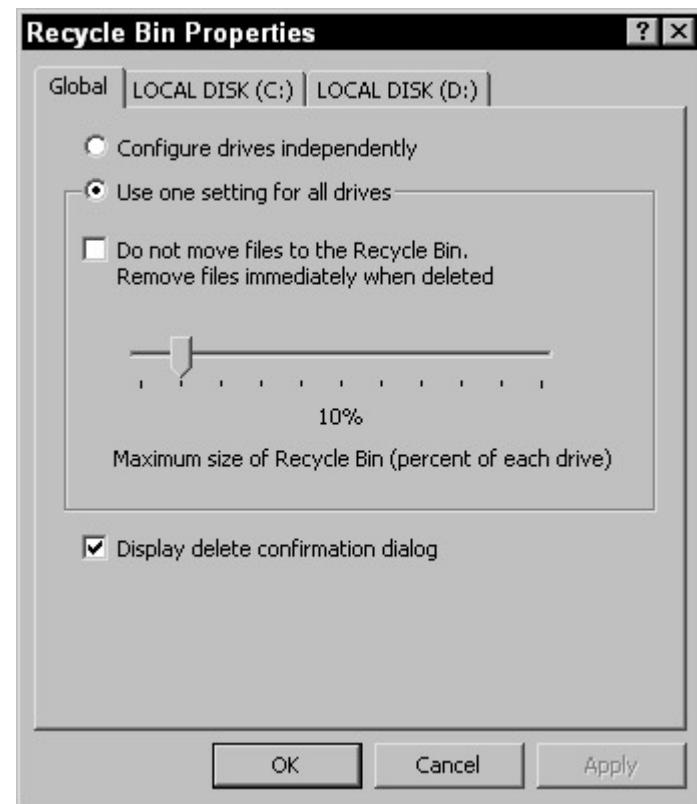
- Recovery of deleted files is the process by which the investigator evaluates and extracts deleted files from a media and returns it in an intact format
- What happens when a file is deleted?

- The first letter of a file name is replaced by a hex byte code E5h
- Corresponding clusters in FAT marked unused
- Index field in MFT marked with special code NTFS
- The Data in the File system is not erased



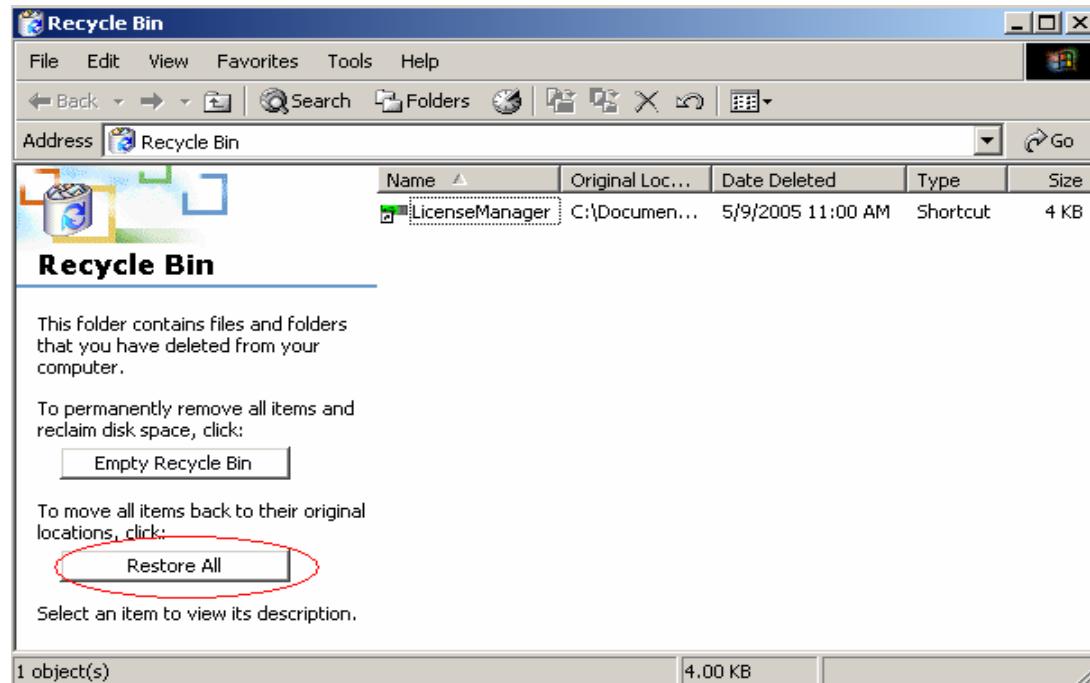
Digital Evidence

- ◎ When files are deleted the deleted file is sent to the Recycle Bin
- ◎ After the Recycle Bin is emptied the data still remains in its original location on the hard drive for a period of time
- ◎ The data will disappear only when the operating system is overwritten from the original location where the file was stored
- ◎ The “index” application in Windows locates the data that has been destroyed



Recycle Bin in Windows

- The main objective of the Recycle Bin is to allow users to retrieve files that have been deleted by them
- When a file is deleted it is sent to the Recycle Bin where it remains until the Recycle Bin is emptied
- The *Restore All* button of the recycle bin restores the data to its original location.
- Once data is deleted from removable media such as floppy disks these files are not stored in the Recycle Bin



Recycle Hidden Folder

- This folder contains files deleted from My Computer, Windows Explorer, and some Windows applications
- The Windows OS keeps track of any files sent by the user to the Recycle Bin by generating temporary Info files
- When a file or folder is deleted the complete path, including the original file name, is stored in a special hidden file called “Info” in the Recycled folder
- The deleted file is renamed, using the following syntax:

D<original drive letter of file><#>. <original extension>

Recycle folder

```
C:\> C:\WINDOWS\System32\cmd.exe
Directory of D:\RECYCLER
01/07/2005  03:54 PM    <DIR> .
01/07/2005  03:54 PM    <DIR> ..
05/18/2005  02:28 PM    <DIR> S-1-5-21-2275786481-1800536561-533452318-500
05/21/2005  06:00 AM    <DIR> S-1-5-21-3020190987-1822439336-4113303836-1005
          0 File(s)          0 bytes
          4 Dir(s)  1,362,382,848 bytes free

D:\RECYCLER>dir/h
Invalid switch - "h".

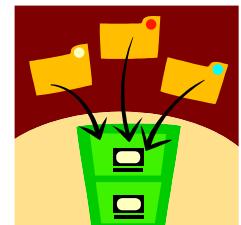
D:\RECYCLER>cd S-1-5-21-2275786481-1800536561-533452318-500
D:\RECYCLER\S-1-5-21-2275786481-1800536561-533452318-500>dir
  Volume in drive D has no label.
  Volume Serial Number is 3761-1CB9

Directory of D:\RECYCLER\S-1-5-21-2275786481-1800536561-533452318-500
01/07/2005  03:13 PM    176,594 Dd1
01/07/2005  03:26 PM    <DIR> Dd2
03/27/2005  07:24 AM    <DIR> Dd3
03/30/2005  01:02 AM    31,195,136 Dd4
03/30/2005  01:19 AM    262,144 Dd5
03/27/2005  12:31 PM    524,288 Dd6
          4 File(s)    32,158,162 bytes
          2 Dir(s)  1,362,382,848 bytes free

D:\RECYCLER\S-1-5-21-2275786481-1800536561-533452318-500>notepad Dd5
D:\RECYCLER\S-1-5-21-2275786481-1800536561-533452318-500>
```

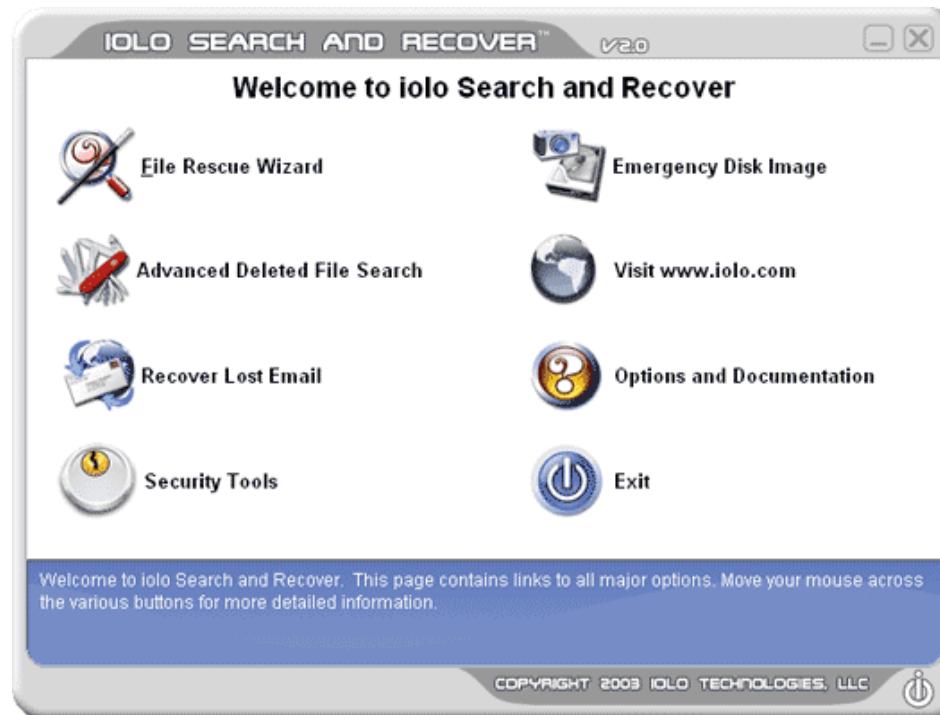
How to Undelete a File?

- The procedure principally involves finding the data on the raw partition device and making it visible again to the operating system
- There are basically two ways of doing this:
 - Modify the existing file system such that the deleted inodes have their `deleted' flag removed
 - Find out where the data lies in the partition and write it out into a new file on another file system



Tool: Search and Recover

- It allows the investigator to quickly recover deleted or destroyed files, folders, songs, pictures, videos, programs, critical system components, web pages, and email messages in Microsoft Outlook and Outlook Express, Netscape, and Eudora
- It works with any hard drive or floppy drive, any drive format, and can even recover deleted items from digital cameras, MP3 players, USB flash drives, and other portable devices



Tool: Zero Assumption Digital Image Recovery

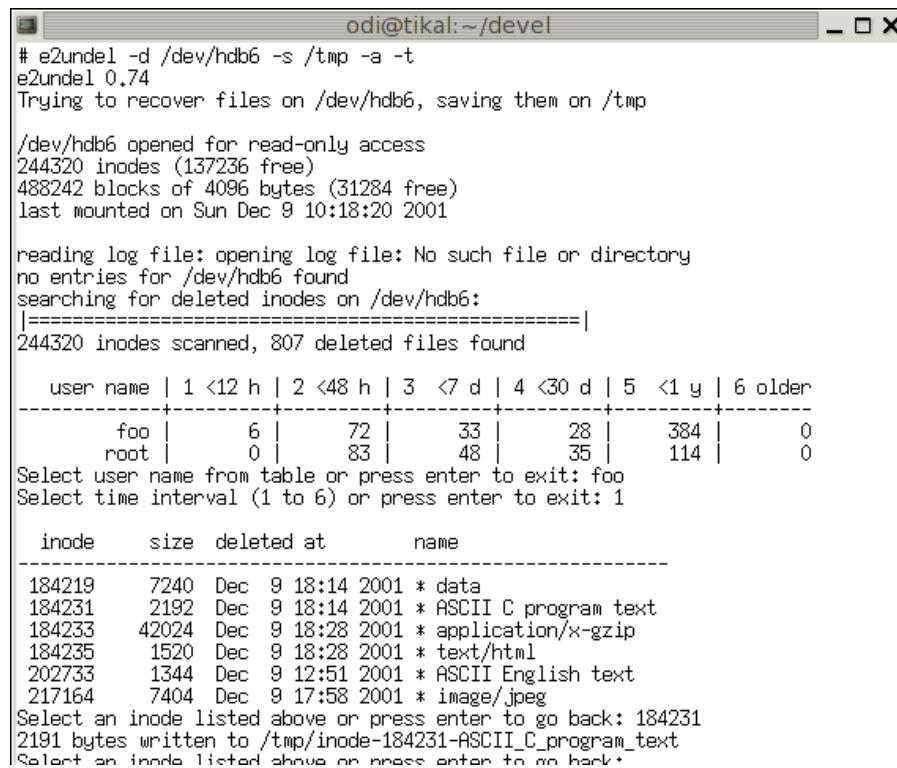
- It is a free data recovery tool that works with digital images
- Digital photographs that are deleted from a digital camera can be retrieved using this tool
- It supports media such as CompactFlash, MemoryStick, SmartMedia etc that can be accessed through an Operating System
- Version 1.2 supports the following format:
 - GIF
 - JPEG
 - TIFF
 - CRW - Canon RAW data
 - MOV - QuickTime movie
 - WAV - Waveform audio

Data Recovery in Linux

- In Linux, files that are deleted using `/bin/rm` remain on the disk
- The second extended file system (ext2) file system is commonly used in most of Linux systems
- The design of the ext2 filesystem is such that data can be hidden shows several places where data can be hidden
- Run a process that keeps the file open and then remove the file
- The file contents are still on disk and the space will not be reclaimed by other programs
- It is worthwhile to note that if an executable erases itself, its contents can be retrieved from /proc memory image: command "`cp /proc/$PID/exe /tmp/file`" creates a copy of a file in /tmp

Data Recovery Tool: E2undel

- e2Undel is an interactive console tool that recovers the data of deleted files in Linux.
- This tool does not manipulate internal ext2 structure and require only read access to the file system.
- e2Undel contains a library that allows the investigator to recover deleted files by their names.



The screenshot shows a terminal window titled "odi@tikal:~/devel". The command "# e2undel -d /dev/hdb6 -s /tmp -a -t" is run, followed by "e2undel 0.74". It then attempts to recover files from /dev/hdb6 and save them to /tmp. The log indicates 244320 inodes (137236 free) and 488242 blocks of 4096 bytes (31284 free), last mounted on Sun Dec 9 10:18:20 2001. It reads a log file and finds no entries for /dev/hdb6, then searches for deleted inodes on /dev/hdb6. A summary table shows 244320 inodes scanned, with 807 deleted files found. The user is prompted to select a user name (foo) and a time interval (1 to 6). Finally, a list of deleted files is displayed, including inode numbers, sizes, times, and names. The user is prompted to select an inode or press enter to go back.

```
# e2undel -d /dev/hdb6 -s /tmp -a -t
e2undel 0.74
Trying to recover files on /dev/hdb6, saving them on /tmp
/dev/hdb6 opened for read-only access
244320 inodes (137236 free)
488242 blocks of 4096 bytes (31284 free)
last mounted on Sun Dec 9 10:18:20 2001

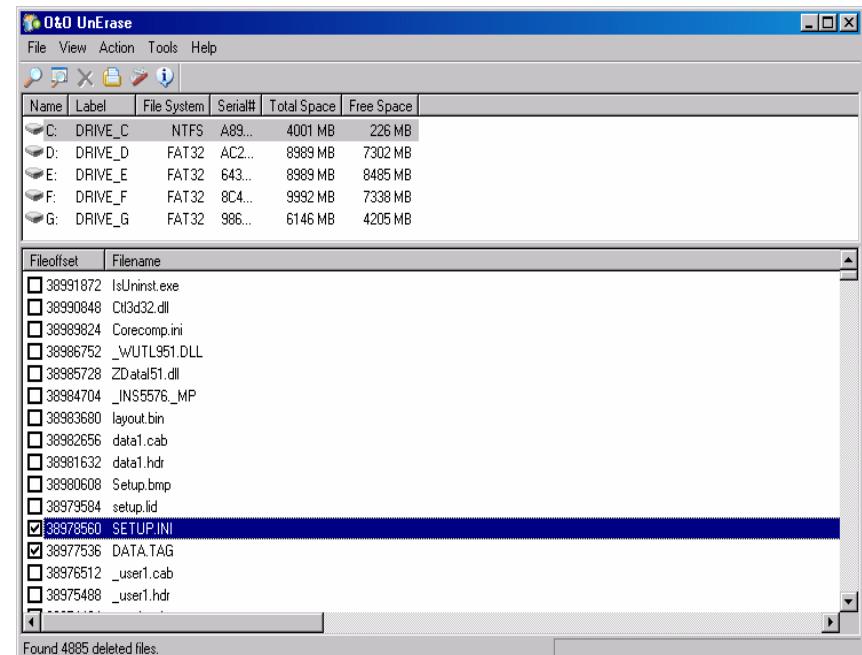
reading log file: opening log file: No such file or directory
no entries for /dev/hdb6 found
searching for deleted inodes on /dev/hdb6:
|=====
244320 inodes scanned, 807 deleted files found

user name | 1 <12 h | 2 <48 h | 3 <7 d | 4 <30 d | 5 <1 y | 6 older
+-----+-----+-----+-----+-----+-----+
    foo |      6 |     72 |     33 |     28 |   384 |     0
    root |      0 |     83 |     48 |     35 |   114 |     0
Select user name from table or press enter to exit: foo
Select time interval (1 to 6) or press enter to exit: 1

inode    size  deleted at        name
-----+-----+-----+-----+-----+
184219    7240 Dec  9 18:14 2001 * data
184231    2192 Dec  9 18:14 2001 * ASCII C program text
184233    42024 Dec  9 18:28 2001 * application/x-gzip
184235    1520 Dec  9 18:28 2001 * text/html
202733    1344 Dec  9 12:51 2001 * ASCII English text
217164    7404 Dec  9 17:58 2001 * image/jpeg
Select an inode listed above or press enter to go back: 184231
2191 bytes written to /tmp/inode-184231-ASCII_C_program_text
Select an inode listed above or press enter to go back:
```

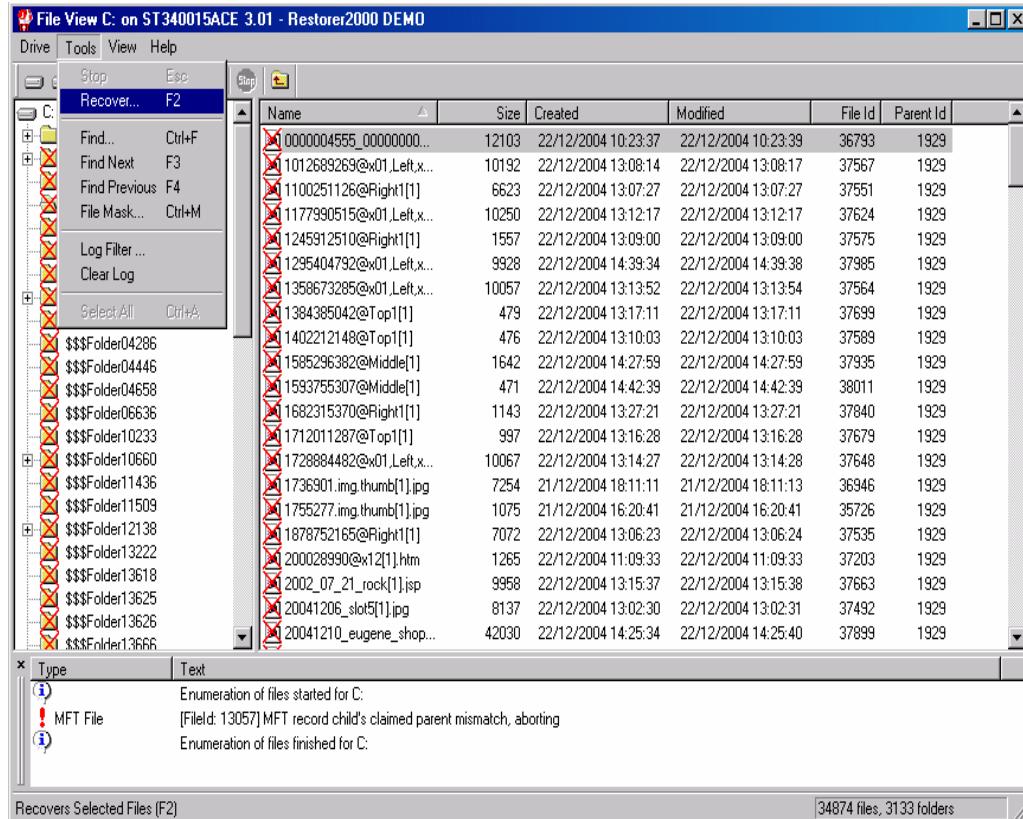
Data Recovery Tool: O&O Unerase

- O&O Unerase recovers deleted files with the help of an algorithm which enables more files to be recovered at a time
- O&O Unerase can also recover important documents such as digital photography, exe program files etc



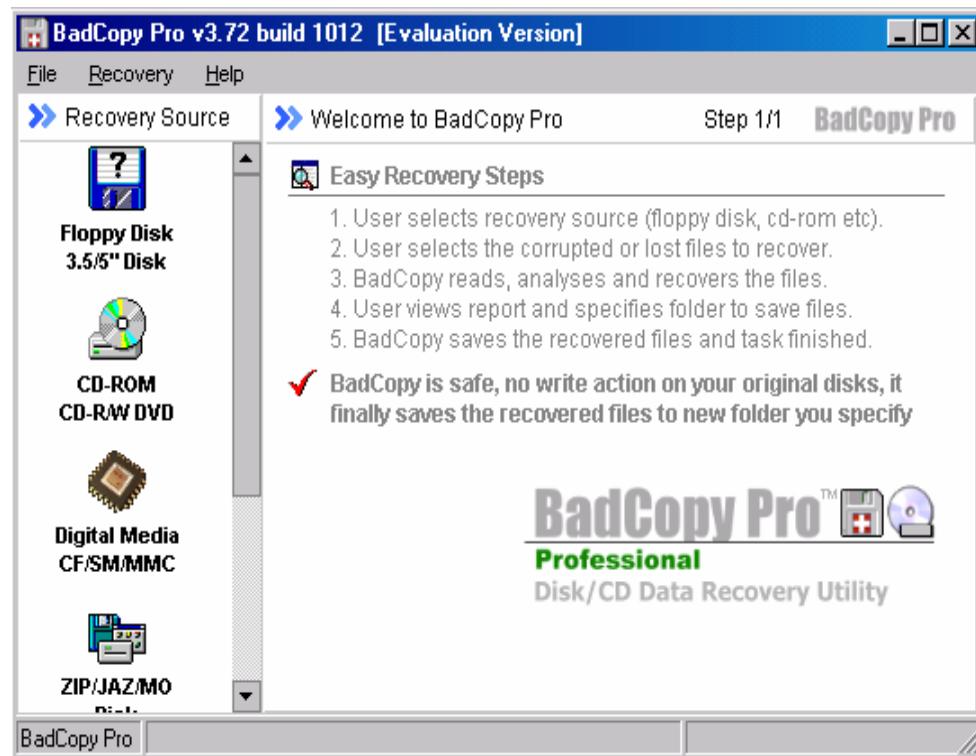
Data Recovery Tool: Restorer 2000

- It supports windows 95/98/ME/NT/2000/XP platform
- It allows the investigator to:
 - Undelete files
 - Unerase files
 - Unformat files
 - Restore and recover data from NTFS and FAT partitions



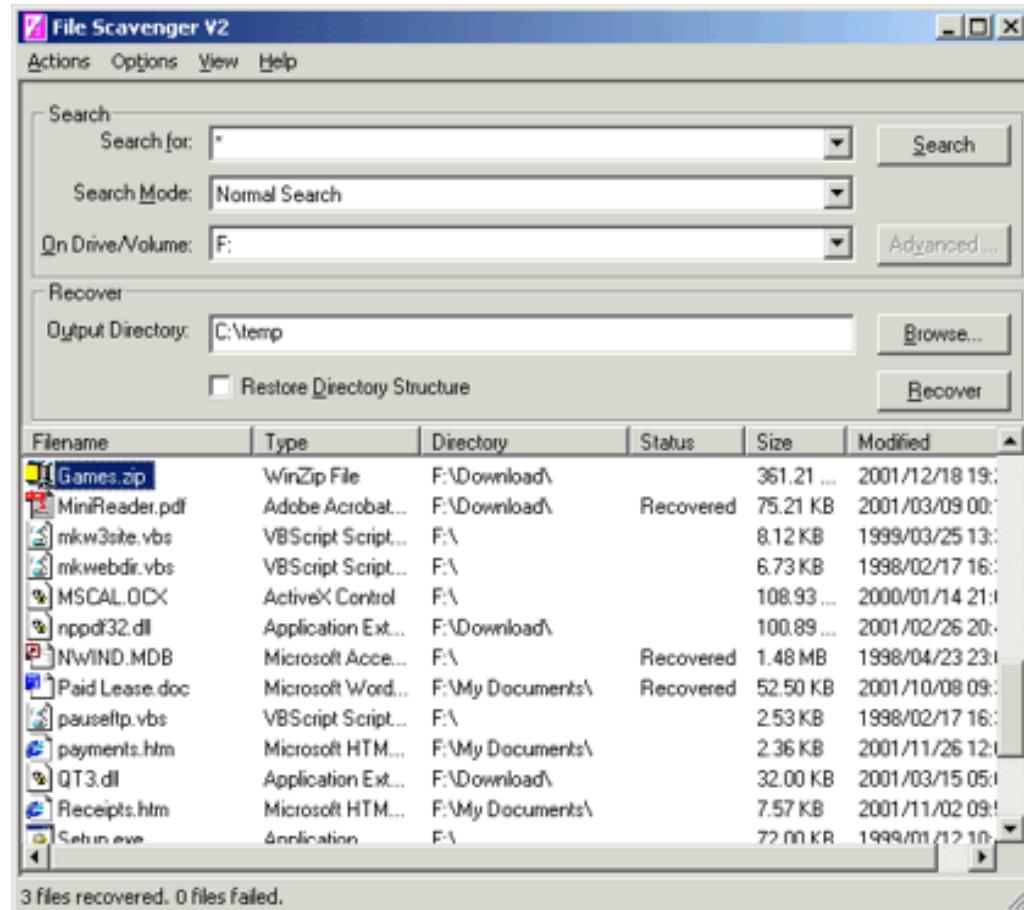
Data Recovery Tool: Badcopy Pro

- BadCopy Pro is one tool that is valuable to forensic investigators with regard to removable storage mediums
- It does not write data to the original disk but to a location specified by the user
- BadCopy Pro recovers files from floppy disks, CD-ROMs, CD-R/Ws, digital media, zip disks and other storage media
- BadCopy Pro can recover corrupted or lost data



Data Recovery Tool: File Scavenger

- ◉ File Scavenger can recover files that have been accidentally deleted
- ◉ This would include files that have been removed from :
 - Recycle Bin
 - DOS shell
 - Network drive
 - Windows Explorer
- ◉ File Scavenger supports both basic and dynamic disks, NTFS compression, and Unicode filenames



Data Recovery Tool: Mycroft V3

The MyCrost tool used by investigators has the following features:

- It sorts out the suspect computers from a given pool before copying the data
- Searches unallocated sectors in the disk to map the given information in order to identify stolen computers
- Searches for references to specific types of crimes on the suspect systems
- Conducts the first high-speed search to test the search attributes

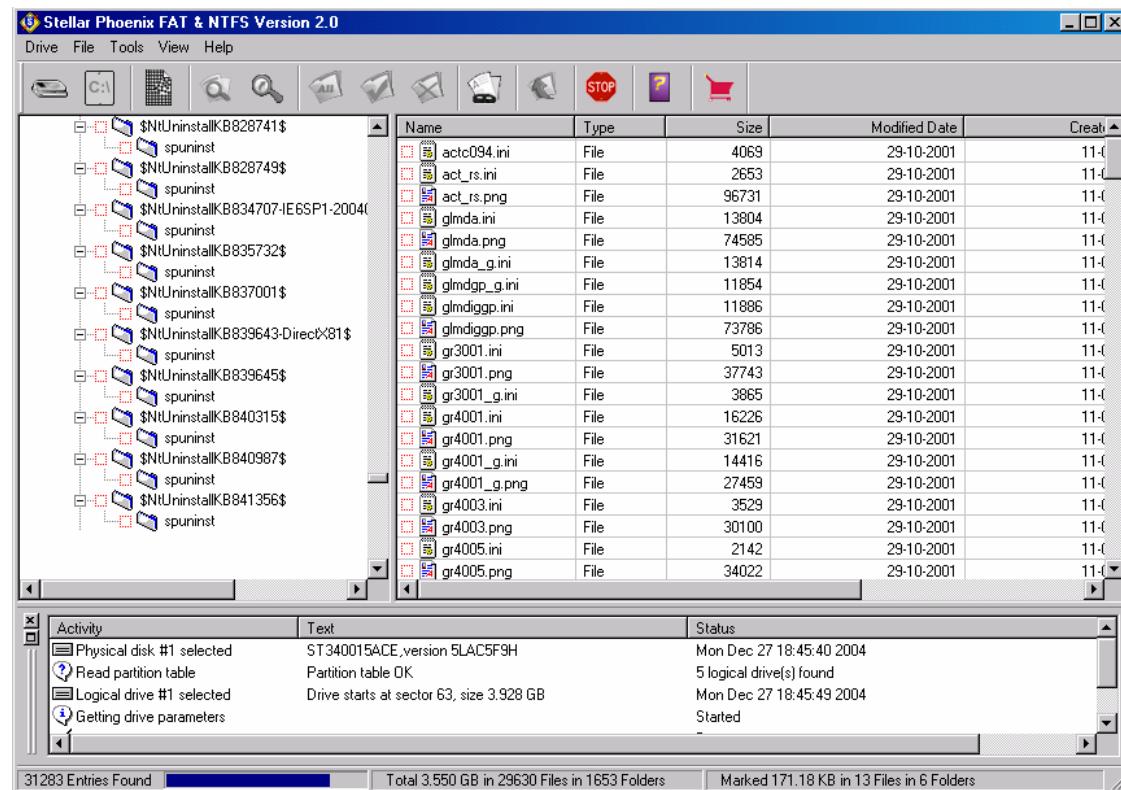


Data Recovery Tool: PC Parachute

- PC ParaChute automatically protects and recovers data stored on any Intel-based PC on a network without user intervention
- It can recover a system that crashes back into fully functioning condition without re-installing the operating system, patches, configuration, etc.
- It recovers the systems to its last state before the incident
- It supports Windows, Solaris Intel, BSDI, Linux, Novell, UnixWare, and SCO platforms

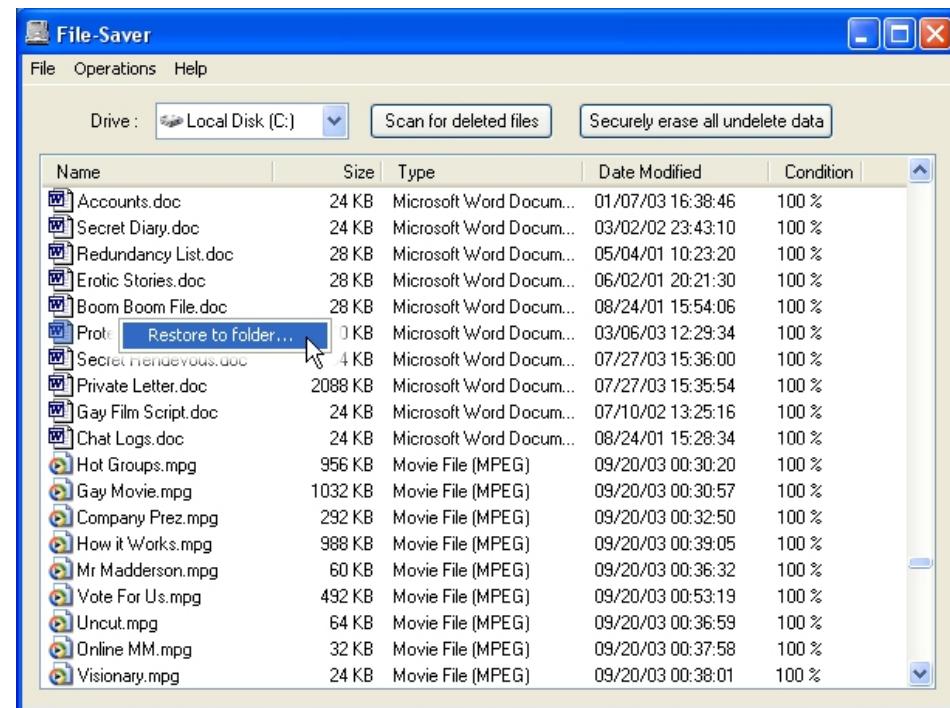
Data Recovery Tool: Stellar Phoenix

- Stellar Phoenix is a non-destructive and read-only software
- This tool is user friendly and is equipped with a automated wizard which helps in recovering files
- Has different versions for different file systems
- The investigator walks through the wizard in 3 easy steps:
 1. Evaluate
 2. Analysis
 3. Recover



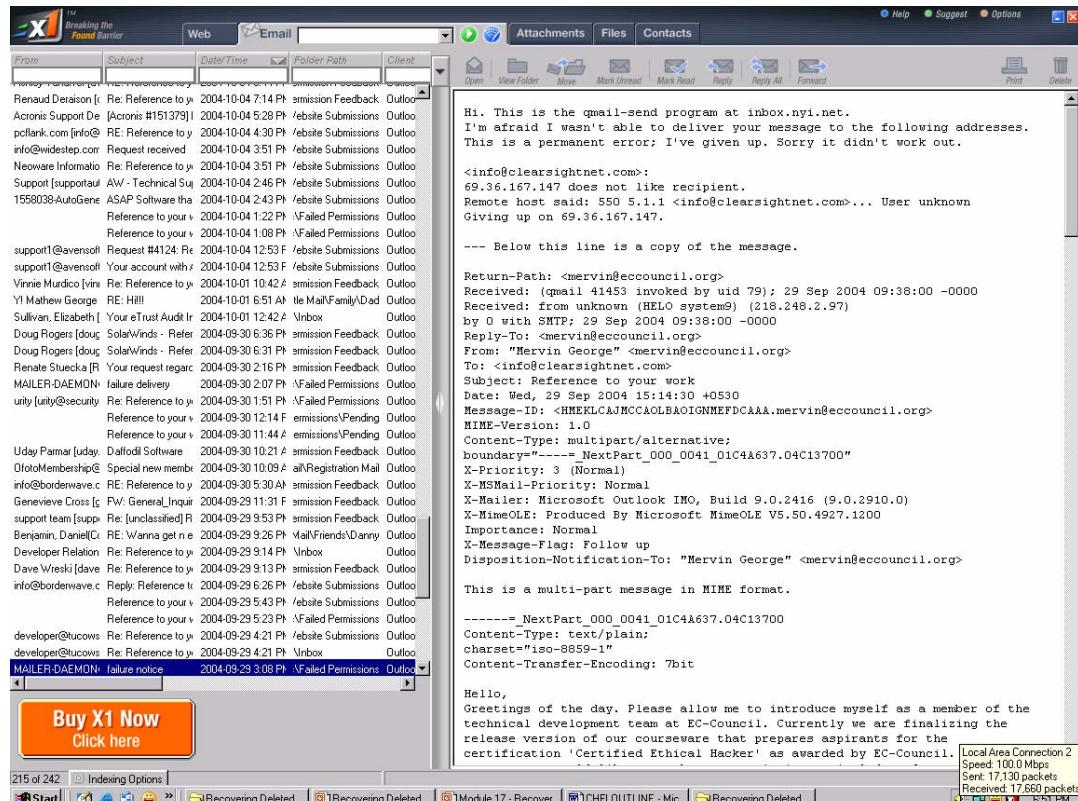
Data Recovery Tool: FileSaver

- The FileSaver tool is an undelete application that works by searching for bits of data that can be recovered and pieced together to form the original file.
- FileSaver restores as many files from as many drives as possible.



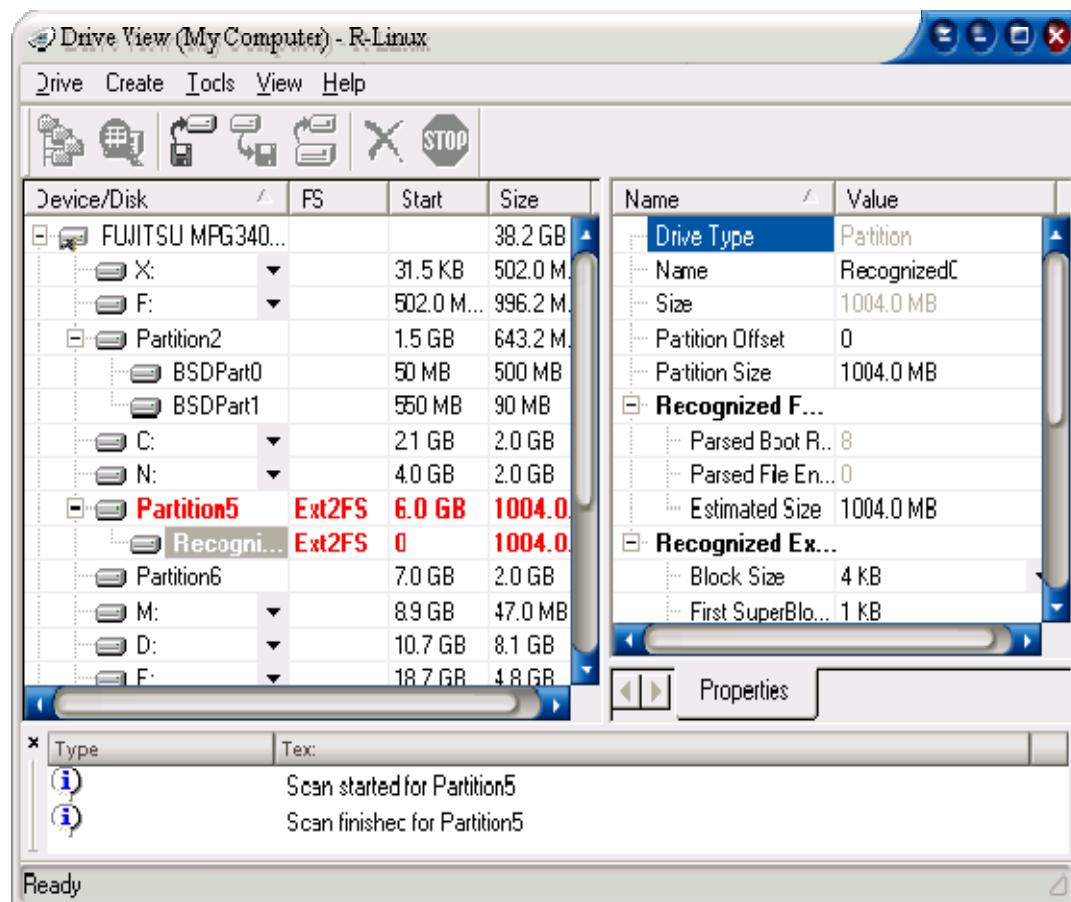
Data Recovery Tool: Virtual Lab

- Virtual Lab recovers files from Jaz, Zip disk and other removable drive formats and digital camera media.
- It recovers files from disks that are not recognized by the operating system
- It recovers deleted files, and damaged partitions



Data Recovery Tool: R-linux

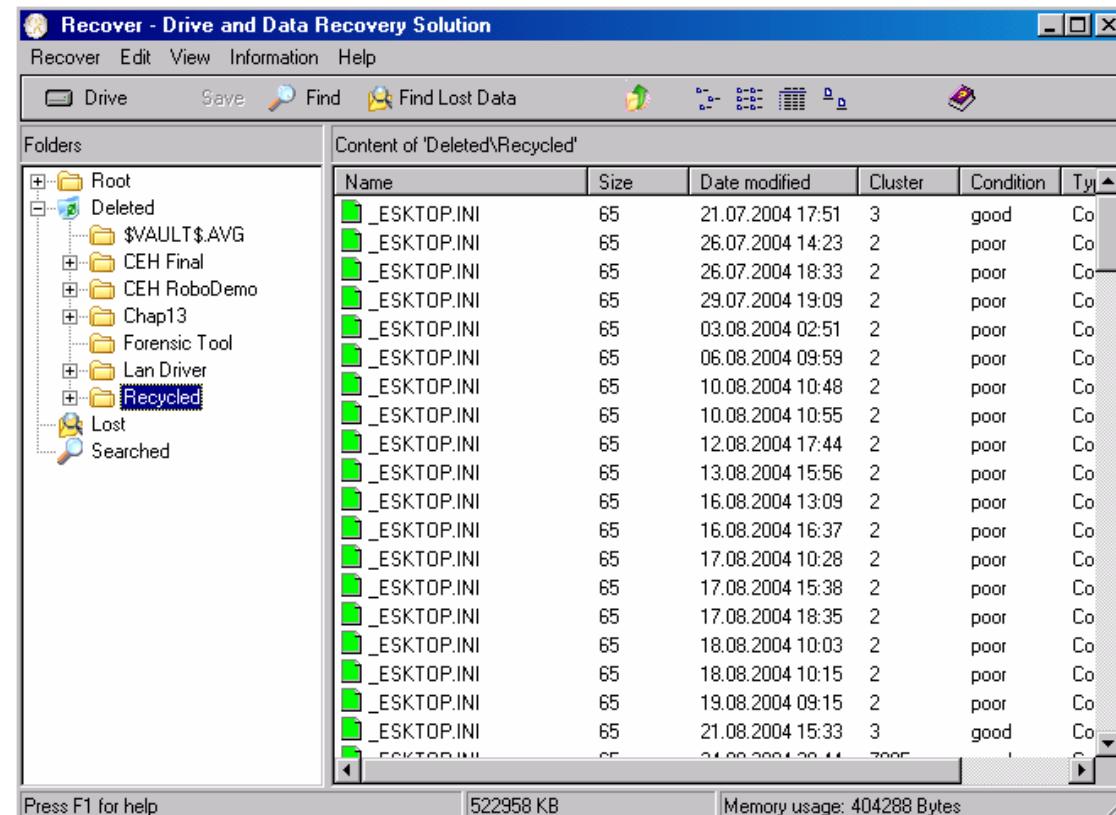
- R-Linux recovers files from existing logical disks even when file records are lost
- R-Linux is a file recovery utility for the Ext2FS file system used in Linux OS and several Unix versions
- R-Linux uses unique IntelligentScan technology and a flexible parameter setting that makes recovery faster



Data recovery tool: Drive and Data Recovery

- The Drive and Data Recovery tool helps forensic investigators in undeleteing and recovering important files such as:

- Word/Excel documents
- Database files
- Mp3 and Mpegs



Data recovery tool: active@ UNERASER - DATA recovery

- <http://www.uneraser.com>
- **Active@ UNERASER - DATA Recovery** is a compact and powerful undelete utility that can recover deleted files and folders on FAT12, FAT16, FAT32 and NTFS systems
- It can even restore files from **deleted** and **reformatted** partitions
- It is not necessary to install the utility on your system's hard drive, as it fits on a **boot floppy disk**, removing the possibility of overwriting data which you want to recover

Active@ UNERASER - DATA Recovery

Drives

Floppy A:
HDD 80h
└→ Logical C:
└→ Unallocated

HDD 81h
└→ Unallocated

HDD 82h
└→ Unallocated

Found: 9.99 Gb - FAT32

Logical drive ?:

Drive's first sector: 63
Total number of sectors: 20964762
Size: 9.99 Gb
File system: FAT32 (LBA)

BOOT info: OEM identifier: MSWIN4.1
Bytes per sector: 512
Sectors per cluster: 16
Reserved sectors: 32
Number of FATs: 2
Root entries: not used
Sectors per one FAT: 10232
Sectors per track: not used
Number of heads: 255
Hidden sectors: 63
Number of sectors: 20964762
Serial number: 18E4-3A77
Volume label: BACKUP
System ID: FAT32

DG.TXT (restored)

904

44	34	50	20	4C	6F	61	64	69	[000CB7D4] Loading Device = C:\W
63	65	20	30	20	43	3A	5C	57	IN98\HIMEM.SYS..
0000-0050	49	4E	39	38	5C	48	49	40	[000CB7D5] LoadS
0000-0060	58	30	30	30	43	42	37	44	ccess = C:\W
0000-0070	6E	67	20	44	65	76	69	63	IN98\HIMEM.SYS..
0000-0080	49	4E	39	38	5C	44	42	40	[000CB7D5] Load
0000-0090	00	0A	5B	30	30	30	43	42	ng Device = C:\W
0000-00A0	64	53	75	63	63	65	73	73	IN98\DBLBUFF.SYS..
0000-00B0	5C	57	49	4E	39	38	5C	44	[000CB7D5] Loa
0000-00C0	59	53	00	0A	5B	30	30	43	dSuccess = C:\
0000-00D0	6F	61	64	69	6E	67	20	44	WIN98\DBLBUFF.S
0000-00E0	43	3A	5C	57	49	4E	39	38	YS..[000CB7D5] L
0000-00F0	53	59	53	00	0A	5B	30	30	oadDevice = C:\WIN98\IFSHLP.
0000-0100	4C	6F	61	64	53	75	63	63	SYS..[000CB7D4]
0000-0110	20	43	3A	5C	57	49	4E	39	LoadSuccess = C:\WIN98\IFSHLP.
0000-0120	2E	53	59	53	00	0A	5B	30	.SYS..[000CB7FB]V

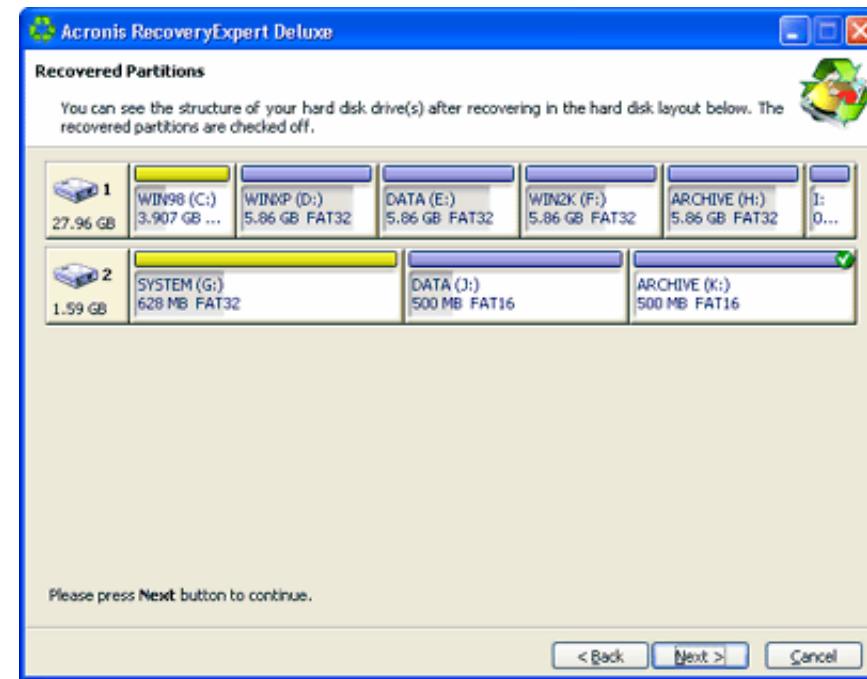
↑, ↓, Home, End - scroll PgUp, PgDn - prev/next Ctrl+G - go to Tab - view

Active@ UNERASER Version 1.0 <PRO>

2002 (C) Active Data Recovery Software Inc http://www.uneraser.com

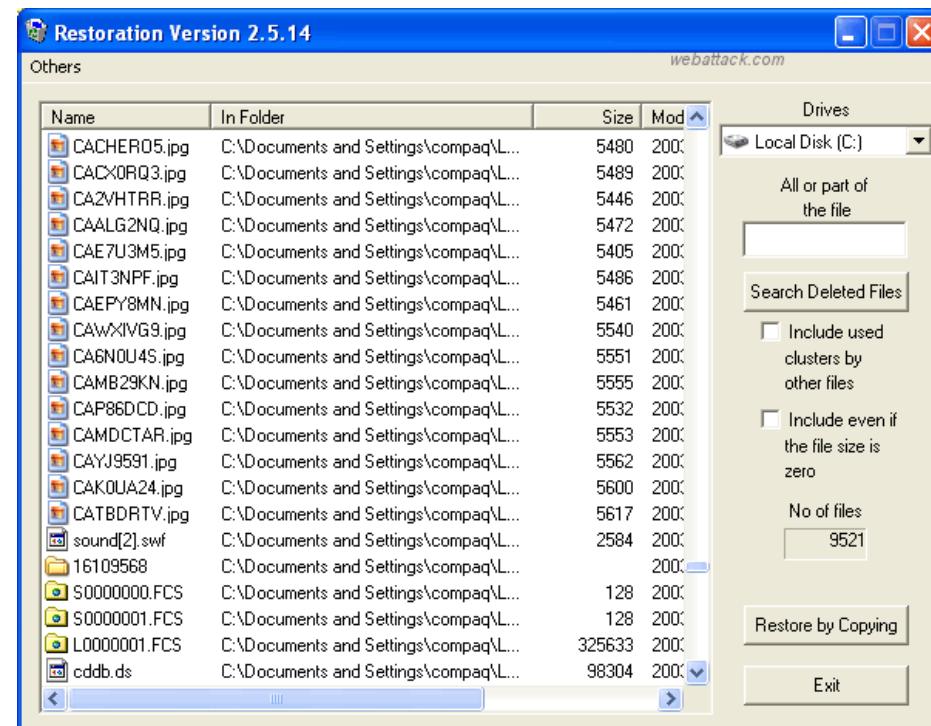
Data recovery tool: Acronis Recovery Expert

- Acronis Recovery Expert protects data by recovering hard disk partitions, if damaged or lost by any reason
- It allows user to recover data in two modes:
 - Automatic recovery
 - Manual recovery
- It supports disks with capacity greater than 180 Gb
- It has unique feature of working independently from bootable CDs or diskettes that recovers partitions even if the operating system fails to boot



Data Recovery Tool: Restoration

- Restoration is an easy to use tool designed to recover files deleted from Windows as well as recycle bin
- It is a standalone program that runs from floppy disk eliminating the need of installation
- It works with FAT as wells as NTFS



Data Recovery Tool: PC Inspector File Recovery

- PC Inspector File Recovery supports FAT and NTFS filesystems and recovers deleted files with original date and time stamp
- It can recover files without header entry and can restore them to network drive
- This data recovery program scans drive and automatically add recovered files to Explorer Style navigation tree

The screenshot shows the PC Inspector File Recovery application window. The menu bar includes Object, Edt, View, Info, Tools, and Help. The toolbar contains icons for Open, Save, Find, and others. The main window has two panes: a left pane titled 'Folders' showing a navigation tree with nodes like Root, Deleted, MFT 28, MFT 471, MFT 5215, MFT 5216, MFT 6145, MFT 8080, MFT 8605, MyDocuments, RECYCLER, SQLServerData, Lost, and Searched; and a right pane titled 'Content of 'Deleted'\MFT 5216'' showing a detailed list of recovered files. The list includes columns for Name, Size, Date modified, MFT entry, Condition, and Type. The files listed are mostly small images (GIF, JPEG) and a few text documents (HTML, Text Document). The status bar at the bottom says 'Press F1 for help.'

Name	Size	Date modified	MFT entry	Condition	Type
lbalQ01C216BC7B661...	326	20.06.1999 18:24	9125	good	GIF Image
lbalM01C216BC7B661...	327	20.06.1999 18:24	9126	good	GIF Image
lbalI01C216BC7B661...	110	05.09.1999 13:33	9123	good	GIF Image
lbalZ01C216BC7B661...	100	20.06.1999 18:24	9124	good	GIF Image
trbook01C216BC790...	14102	23.11.1998 03:00	8935	good	CGI File
btop01C216BC7B4616...	6155	21.03.1999 17:54	9057	good	GIF Image
lbalR01C216BC7B881...	335	20.06.1999 18:24	9127	good	GIF Image
blackpixel01C216BC7B...	799	21.09.1998 03:42	9056	good	GIF Image
side2001_H01C216BC7...	4855	09.11.1998 03:00	9157	good	GIF Image
index_file_1.txt01C216...	1	29.11.2001 21:49	8983	good	PAGECOUNT File
index_file_help.txt01C2...	1	29.11.2001 21:49	8985	good	PAGECOUNT File
index01C216BC79651...	51	29.11.2001 21:49	8981	good	HTML Document
index_file_101C216BC7...	7273	29.11.2001 21:49	8982	good	Text Document
auth_token01C216BC7...	43	29.11.2001 21:49	8978	good	Text Document
indexbg01C216BC7B82...	37941	01.09.2001 22:03	9120	good	GIF Image
goldword01C216BC7B...	5025	21.09.1999 20:23	9112	good	GIF Image
arrow_right01C216BC7B...	370	04.11.1998 14:49	9041	good	GIF Image
do_not_rename_pl_to_e...	0	29.11.2001 21:50	8961	good	Text Document
clearlog01C216BC7B5...	8862	21.07.1999 06:42	9079	good	GIF Image
engineilog01C216BC7B...	5787	21.09.1999 23:05	9088	good	GIF Image
dolphin01C216BC7B631...	274	24.09.1999 12:45	9087	good	GIF Image
NewFiles0000000.dat	194	18.06.2002 04:07	9190	good	DAT File

Summary

- Deleting files and formatting the hard drive does not get rid of the data on the drive
- Forensic evidence can be found in the Recycle Bin and files that have been deleted from the system
- The design of the ext2 filesystem in Linux shows several places where data can be hidden
- Files or folders deleted from floppy disks, Zip disks, or network servers are not stored in the Recycle Bin



Computer Hacking Forensics Investigator

Module XII Image Files Forensics

Scenario

Target Software systems has completed an expensive marketing and customer service analysis. The company plans to advertise for the latest product, which is to be released. However the company suspects that an employee might have given their sensitive marketing data to a competitor.

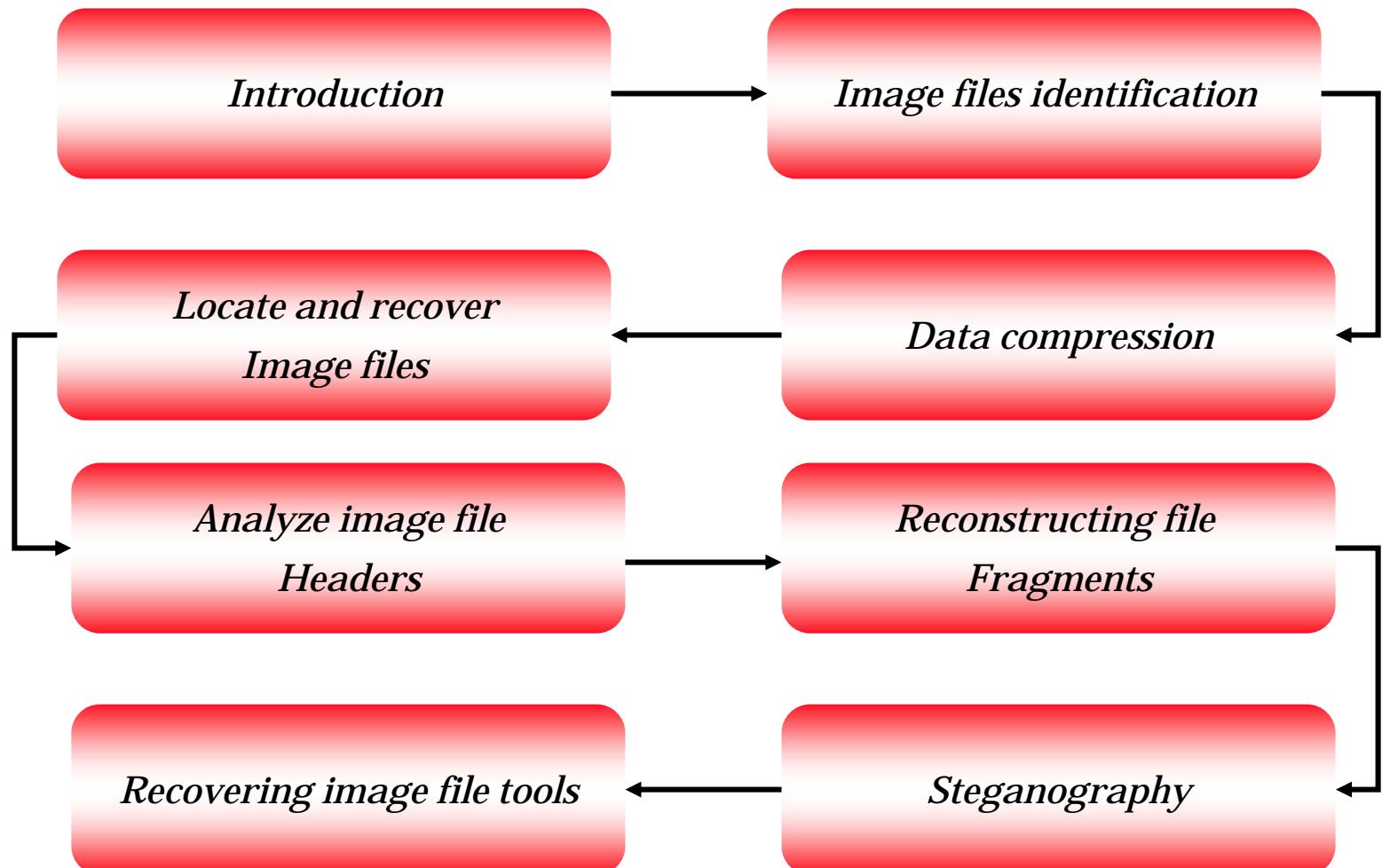
A floppy disc was found containing proprietary company data regarding key clients hidden in an image file headers. Exhaustive investigation resulted in evidence found in fragments of a JPEG file header.



Module Objectives

- Introduction to image files
- Recognize image files
- Understand data compression
- Locate and recover image files
- Analyze image file headers
- Reconstructing file fragments
- Understanding steganography in image files
- Tools for viewing images

Module Flow



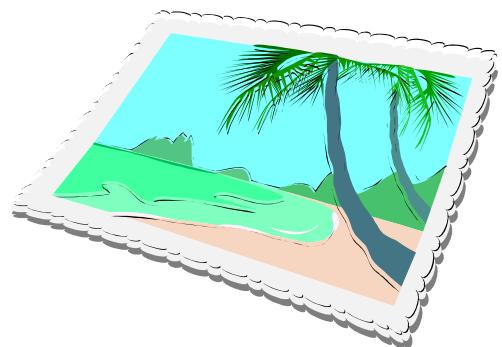
Introduction to Image Files

- Image file formats can be:
 - A black and white Image
 - A grayscale Image
 - A color image
 - Indexed Color image
- All image formats differ between ease of use, size of the file, and the quality of reproduction



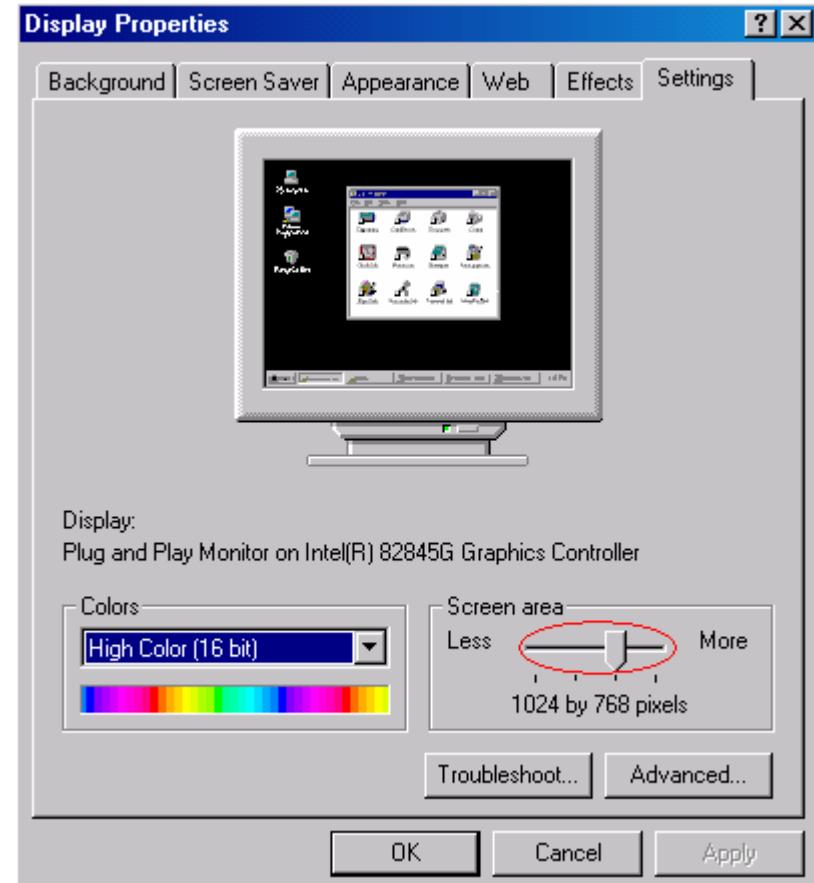
Recognizing an Image File

- Pixels: are small dots used to create images
- Bitmap Images: A representation of a graphics image in a grid-type format
- Metafiles: Combination of bitmap and vector images
- Vector Images: An image based on mathematical equations



Recognizing an Image File

The circled area in this screen shot shows the resolution of the screen by pixels



Understanding Bitmap and Vector Images

Bitmap Images

- Bitmap images can be made in the following applications:
 - Photoshop
 - MS Paint
 - Image Ready
 - Paintshop Pro
- Continuous tone photos

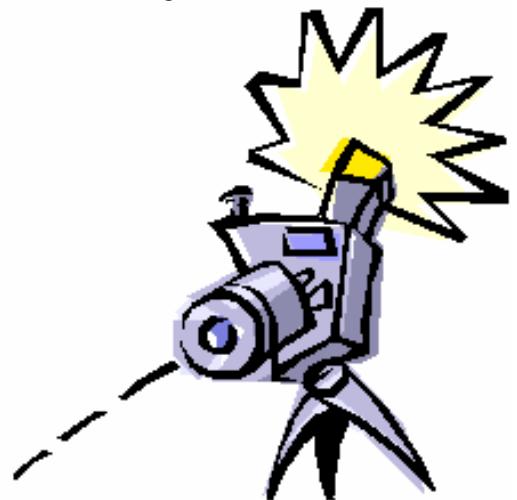
Vector Images

- Uses geometric equations
- Higher quality image than a bitmap
- Useful for rendering types and shapes



Metafile Graphics

- ◉ Metafiles combine raster and vector graphics.
- ◉ Metafiles have similar features of both bitmap and vector images.
- ◉ When metafiles are enlarged it results in a loss of resolution giving the image a shady appearance.



Understanding Image File Formats

File Format	File Extension	Icon Appearance in ACDSee
Graphics Interchange Format	.gif	 Sample
Joint Photographic Experts Group	.jpg	 Sample
Tagged Image File Format	.tif	 Sample
Windows Bitmap	.bmp	 Sample
JPEG 2000	.jp2	 Sample
Portable Network Graphics	.png	 Sample

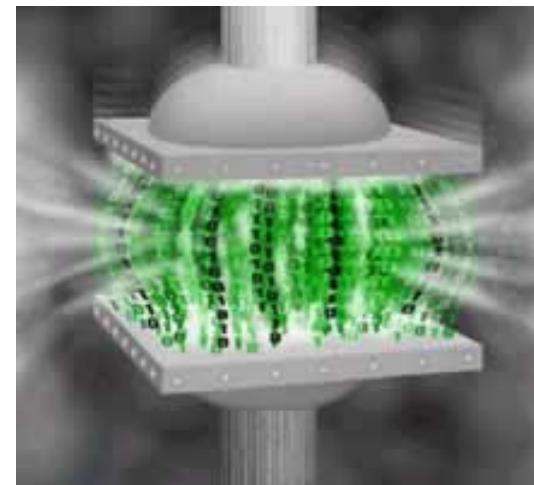
File types

⦿ Different types of files

- Graphics file format
 - .gif/.jpg/.jpeg/.jfif
- Text file format
 - .txt/.htm/.html
- Audio file format
 - .au/.uLaw/.MuLaw/.aiff
 - .mp3/.ra/.wav/.wma
- Video file format
 - .avi/.mov/.movie
 - .mpg/.mpeg/.qt/.ram
- Document file format
 - .doc/.pdf/.ps
- Compress file format
 - .z/.zip/.sit/.gzip/.gz

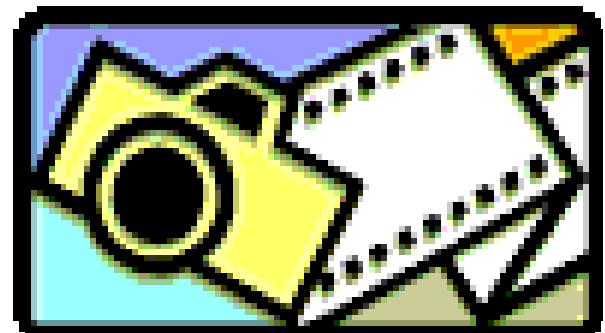
Understanding Data Compression

- **Data compression:** is done by using a complex algorithm used to reduce the size of a file
- **Vector quantization:** A form of vector image that uses an algorithm similar to rounding up decimal values to eliminate unnecessary data



Understanding Lossless and Lossy Compression

- GIF and PNG image file formats reduce the file size by using lossless compression
- Lossless compression saves file space by using algorithms to represent data contained in the file
- Lossy compression compresses data permanently removing information contained in the file



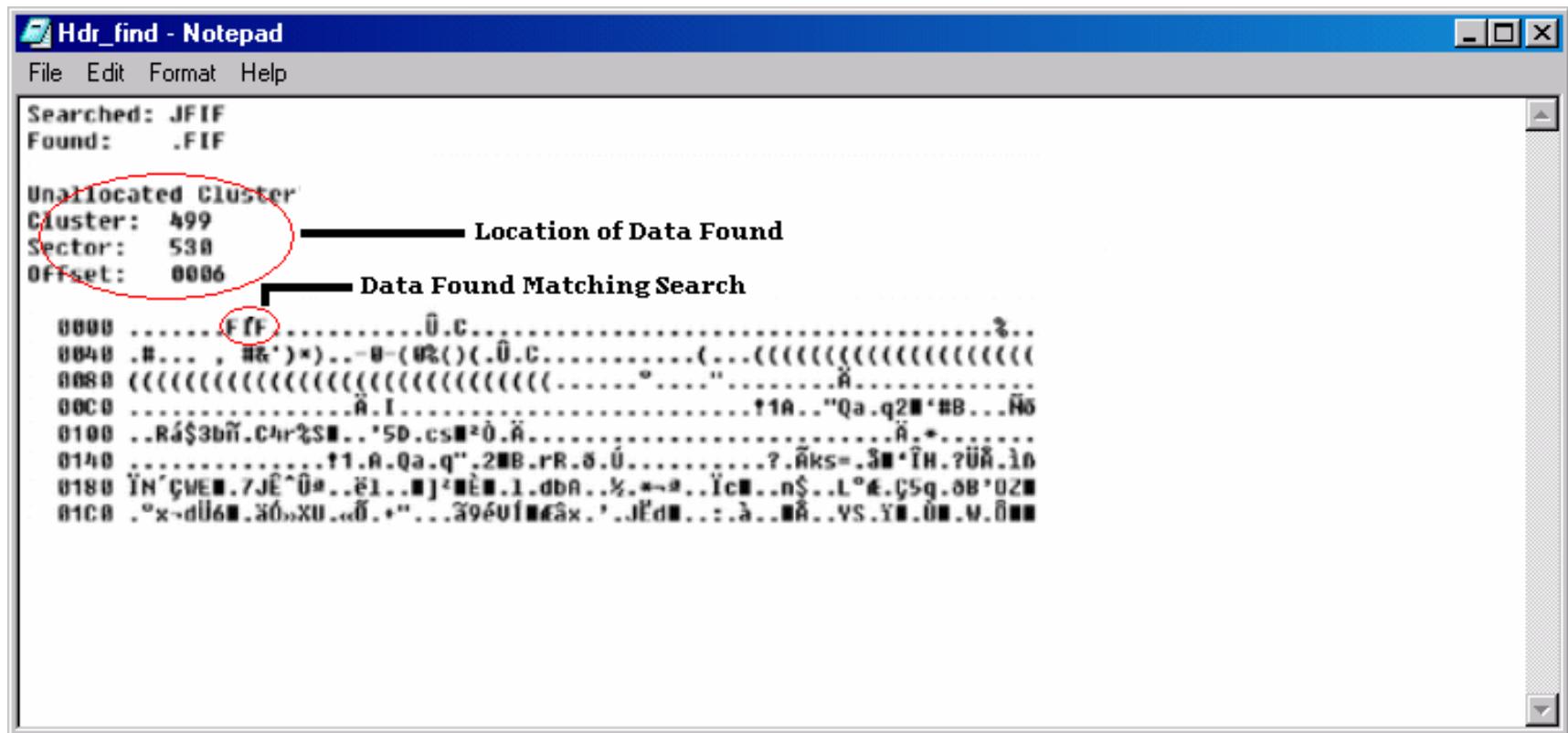
Locating and Recovering Image Files

Carving: The process of removing an item from a group of items

Salvaging: Another term for carving. It is the process of removing an item from a group of them



Locating and Recovering Image Files



The screenshot above shows the location of the clusters where the data has been found and the data found with the matching search.

Repairing Damaged Headers

- Investigators recover data remnants from free space
- This data would be similar to headers from common image files
- Header data that is partly overwritten can be used to repair damaged headers
- The HEX Workshop application can be used to repair damaged headers by the process of comparison
- Jpeg files would include letters “JFIF” after hexadecimal values

Example:

Jpeg file have a hexadecimal value of : FF D8 FF E0 00 10



Reconstructing File Fragments

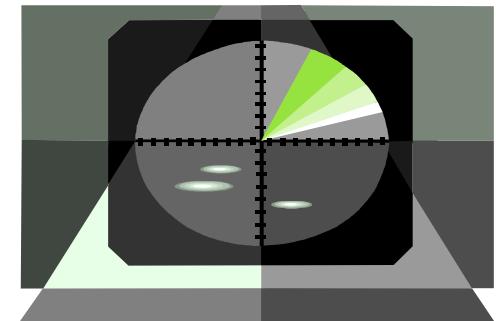
- Corruption of data prevents investigators from reconstructing file fragments for image files
- Data corruption can be:
 - Accidental
 - Intentional
- File fragments can be reconstructed by examining a suspect disk with the help of the DriveSpy application
- Investigators can build the case based on the data reconstructed



Identifying Unknown File Formats

To understand unknown image file formats one should know about non-standard file formats:

- Targa (.tga)
- Raster Transfer Language (.rtl)
- Photoshop (.psd)
- Illustrator (.ai)
- Freehand (.h9)
- Scalable vector graphics (.svg)
- Paintbrush (.pcx)



Analyzing Image File Headers

- Investigators analyze image file headers when new file extensions are present that forensic tools cannot recognize
- File Headers are accessed with the help of a hexadecimal editor such as the Hex Workshop
- Hexadecimal values present in the header can be used to define a file type



Picture Viewer: Ifran View

IfranView is an image viewing program that supports many unknown file formats including

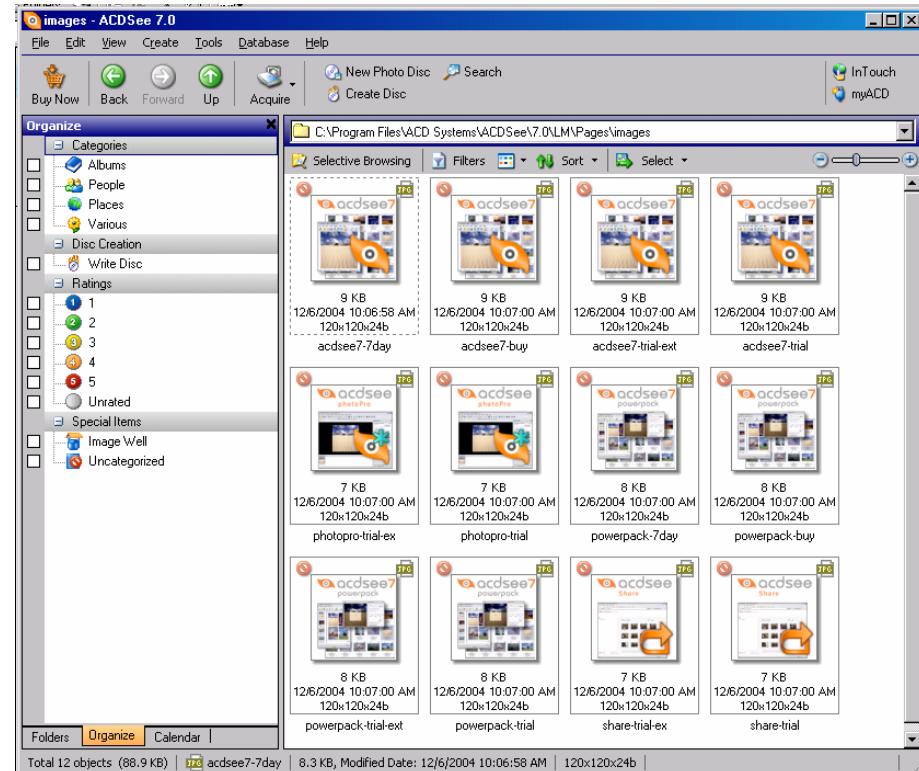
- Targa (.tga)
- Illustrator (.ai)
- Scalable vector graphics (.svg)
- FlashPix (fpx)



Picture Viewer: Acdsee

ACDSee is an image viewing program that enables investigators to

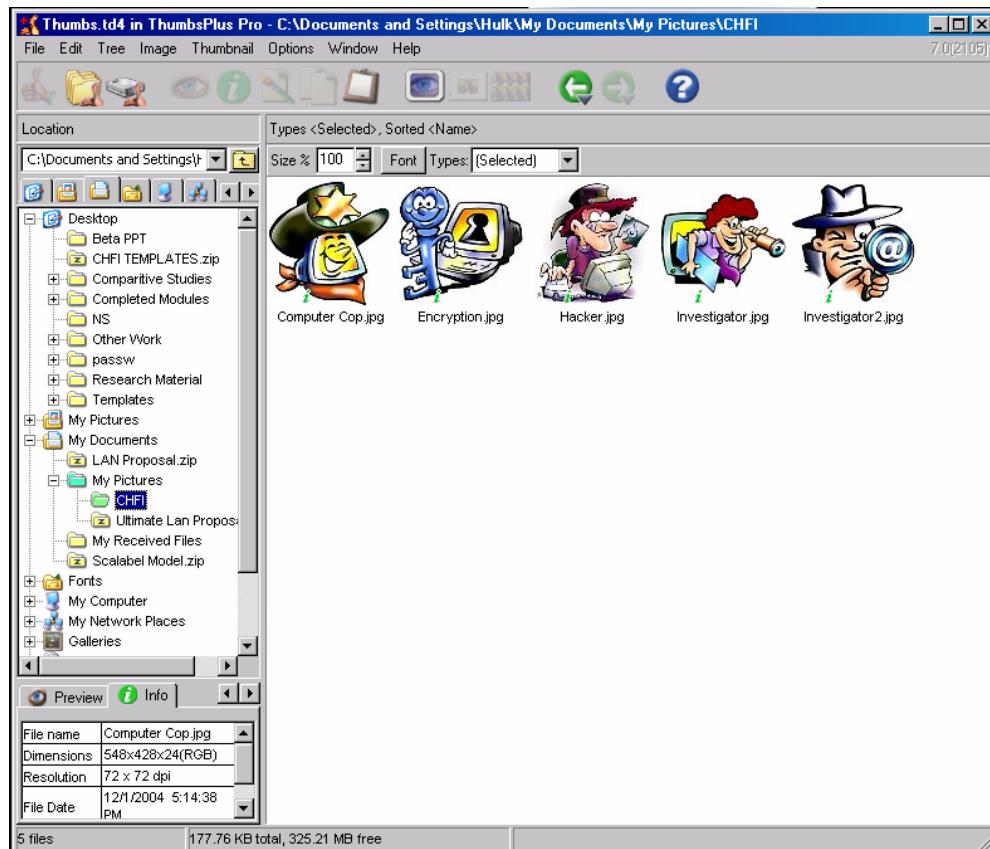
- Find images
- View images
- Manage image files on the drive
- Search and view unknown file formats



Picture Viewer: Thumbsplus

ThumbsPlus is an image viewing program that enables investigators to

- View images from a drive database
- View files other than images such as audio and multimedia files
- Catalog image files for future reference



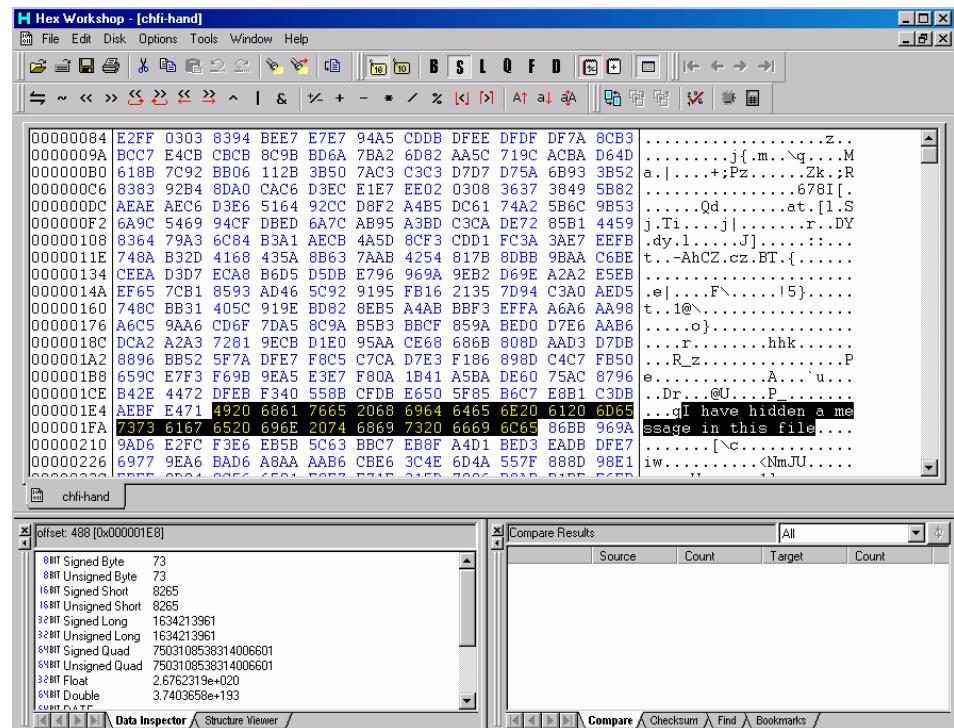
Steganography in Image Files

- ◉ Two files need to hide a message within an image file
 - The file containing the image into which the message is supposed to be put in
 - The file containing the message itself
- ◉ There are 3 methods to hide messages in images, they include:
 - Least Significant Bit
 - Filtering and Masking
 - Algorithms and Transformation



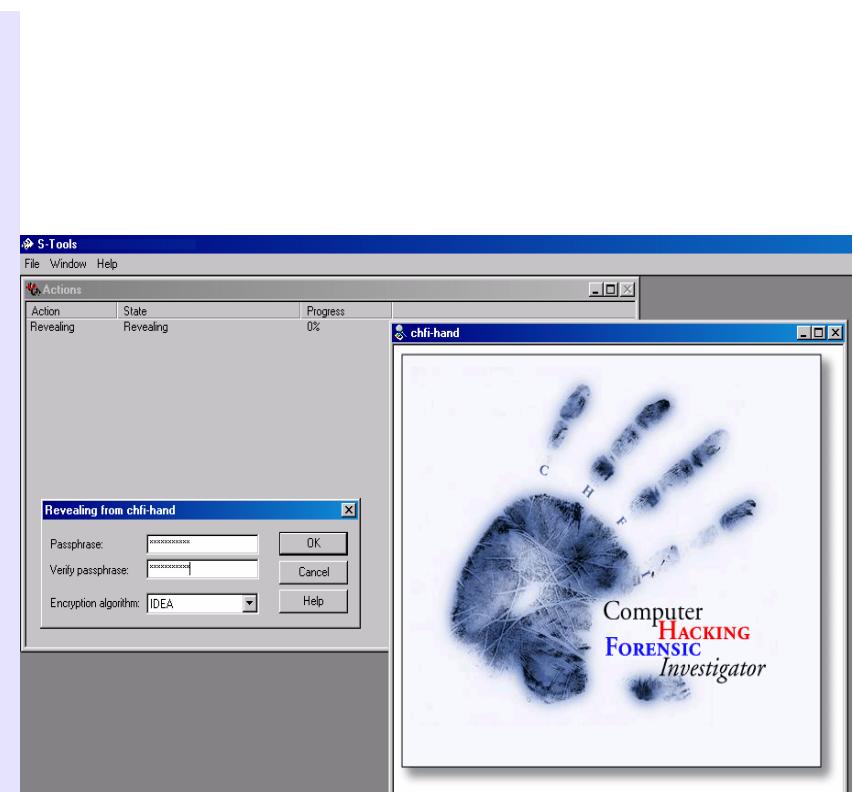
Steganalysis Tool: Hex Workshop

- The Hex Workshop application can detect and write messages on to a file
- Investigators use the Hex Workshop tool to reconstruct damaged file headers



Steganalysis Tool: S-tools

- S-Tools can hide and detect files hidden in BMP, GIF and WAV files
- Investigators have the advantage of multi-threaded operation
- Investigators can hide/reveal operations simultaneously without fear of interference to the work environment



Identifying Copyright Issues With Graphics

- Section 106 of the 1976 Copyright Act generally gives the owner of copyright the exclusive right to do and to authorize others to do the following:
 - To perform the work publicly
 - To display the copyright work publicly
 - In the case of sound recordings, to perform the work publicly by means of a digital audio transmission
 - To reproduce the work in copies or phonorecords
 - To prepare derivative works based upon the work
 - To distribute copies or phonorecords of the work to the public by sale or other transfer of ownership, or by rental, lease, or lending

Identifying Copyright Issues With Graphics (Contd..)

Copyrightable works include the following:

- Literary works
- Musical works; including any accompanying words
- Dramatic works; including any accompanying music
- Pantomimes and choreographic works
- Pictorial, graphic, and sculptural works.
- Motion pictures and other audiovisual works.
- Sound recordings
- Architectural works



Summary

- The standard image file formats include Jpeg, GIF, BMP, TAG and EPS
- Data Compression is done by using a complex algorithm to reduce the size of a file
- Lossy compression compresses data permanently removing information contained in the file
- Image files have a unique file header value. Common image header values have residual data from partially overwritten headers in file slack



Computer Hacking Forensics Investigator

Module XVII Steganography

Scenario

Daniel works as a marketing executive for a reputed firm. However Daniel is not happy with his job and desires an increase in his income. He decides to sell information regarding a list of clients of the firm to a rival marketing agency.

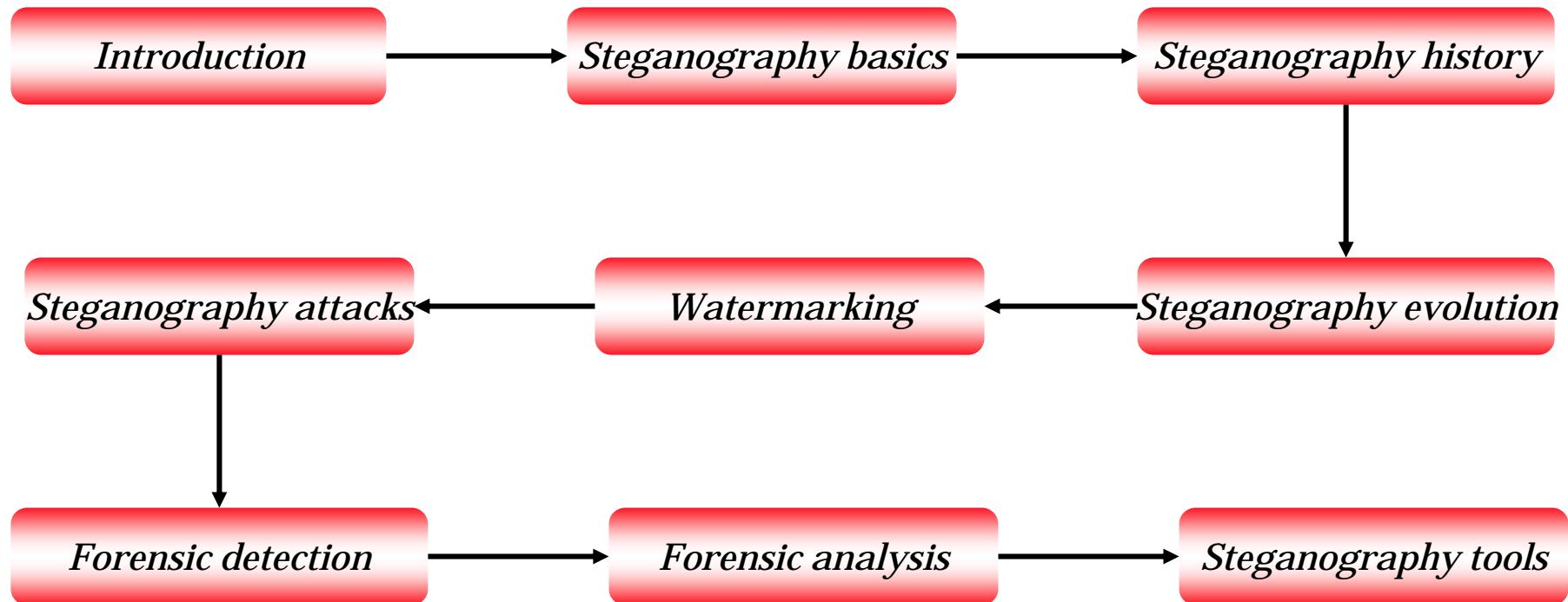
He makes use of the steganography tool “Steganos” to hide the list of clients in a word file and embeds it into a harmless image file and emails it to the rival firm.



Module Objective

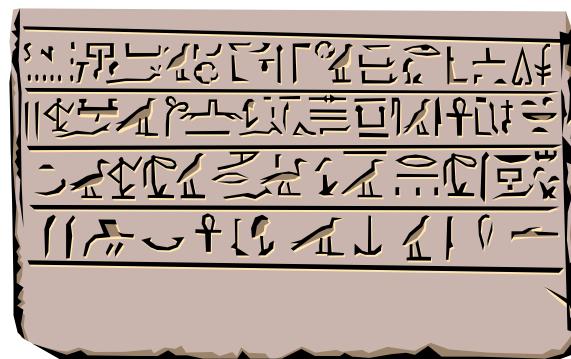
- Introduction to steganography
- Understanding the basics of steganography
- Reviewing the early history of steganography
- Reviewing the evolution of steganography
- Understanding watermarking
- Forensic detection and analysis
- Steganography tools

Module Flow



Introduction

- Steganography is defined as “*The art and science of hiding information by embedding messages within other, seemingly harmless messages*”
- Steganography involves placing a hidden message in some transport medium.
- The meaning is derived from two Greek words mainly “*Stegos*” which means secret and “*Graphie*” which means writing



Important Terms in Stego-forensics

- What are Microdots?
- The concept of Null Ciphers
- The uses of Anamorphosis
- What is Invisible Ink?
- The Spread Spectrum
- The News Paper code
- The Jargon code
- The concept of Cardano' Grille



Background Information to Image Steganography

- Image file properties relates to how digital images vary in terms of their resolution, width, and height
- Four image file compressions commonly used in stegnography are:

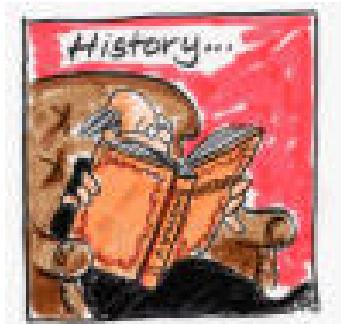
- GIF- Graphic Interface Format
- BMP- A Microsoft standard image
- JPEG- Joint Photographic Experts
- TIFF- Tag Image File Format



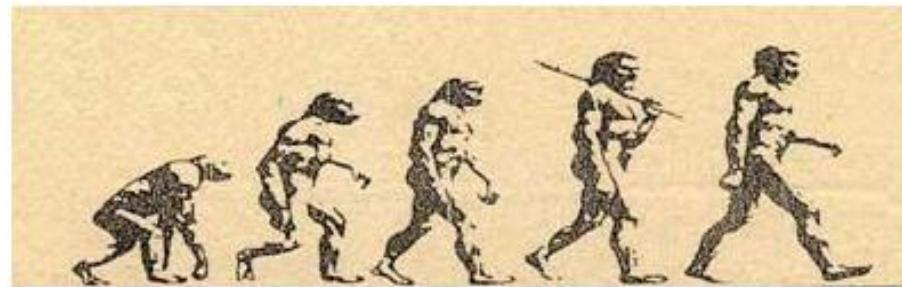
Steganography History

Steganography in its earliest form has been used by:

- ◉ The Greeks
- ◉ The Egyptians
- ◉ The Chinese
- ◉ The United States during World War II and Vietnam



Evolution of Steganography

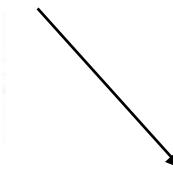
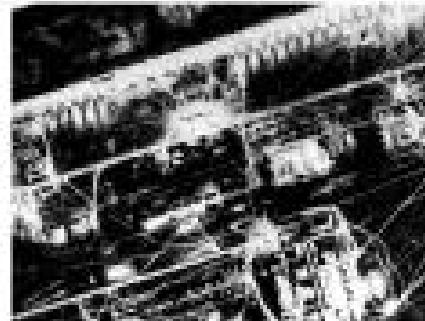


- Steganography comes in different forms:
 - Hidden information in Text Files
 - Hidden information in Image Files
 - Hidden information in Audio Files
 - Hidden information in DNA
- Least Significant Bit Insertion in image files
- Masking and filtering in image files
- Algorithms in image files

Steps for Hiding Information in Steganography

- ◎ Stenographic methodology

- Choosing the image in which to hide the vital information
- Need for the secret message which is to be hidden
- Insertion of the message into an image file



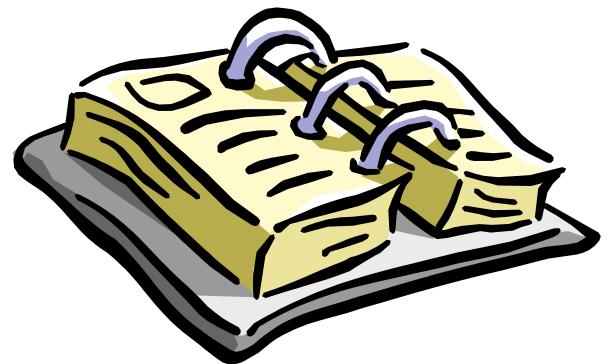
Six Categories of Steganography in Forensics

- Substitution system techniques
- Transformation domain techniques
- Spread spectrum techniques
- Statistical method techniques
- Distortion techniques
- Cover generation techniques



Types of Steganography

- Linguistic steganography
- Open code steganography
- Masking
- Null ciphers
- Cues
- Music
- Jargon code
- Newspaper code
- Grilles



What Is Watermarking?

- ⦿ During the manufacture of paper the wet fiber is subjected to high pressure to expel the moisture
- ⦿ If the press' mold has a slight pattern, this pattern leaves an imprint, a *watermark*, in the paper, best viewed under transmitted light
- ⦿ *Digital watermarks* are imperceptible or barely perceptible transformations of digital data; often the digital data set is a digital multimedia object



Classification of Watermarking

- The fragile watermark is one of the watermarking methods for authentication that has a low robustness toward modifications
- A fragile watermark is supposed to break
- A robust watermark is almost exactly the opposite of a fragile watermark
- A robust watermark can be either visible or invisible, depending on purpose

Types of Watermarks

○ **Visible watermarks:**

- A visible watermark is robust.
- Though not part of the foundation image, the watermark's presence is clearly noticeable and often very difficult to remove

○ **Invisible watermarks:**

- An invisible watermark's purpose is to identify ownership or verify the integrity of an image or piece of information.
- An invisible watermark is imperceptible, but can be extracted via computational methods

Steganographic Detection

- Statistical tests
 - StegDetect
 - StegBreak
- Dictionary attacks on steganographic system
- Visible noise
- Appended spaces and “Invisible” characters
- TCP/IP packet capture



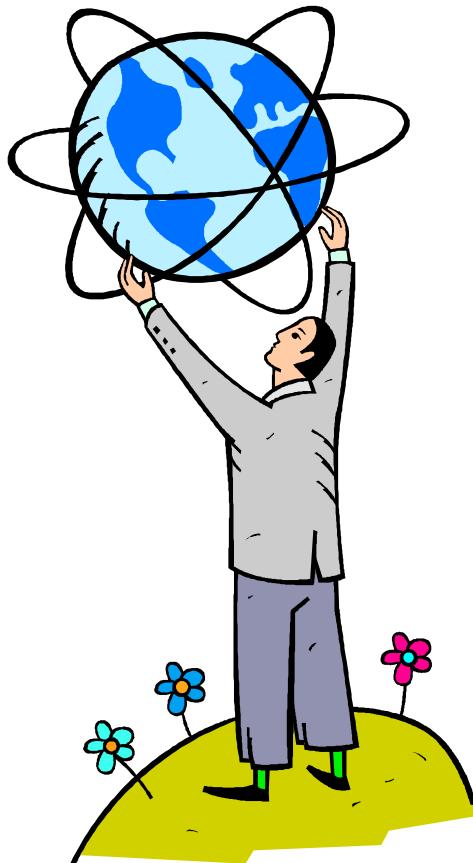
Steganographic Attacks

- Stego-only attack
- Known-cover attack
- Known-message attack
- Chosen-stego attack
- Chosen-message attack
- Disabling or active attack
- Watermark attack



Real World Uses of Steganography

- Medical records
- Workplace communication
- Digital music
- Terrorism
- Cinema industry



Steganography in the Future

- Legitimate uses of steganography in the future

- Protection of Property, Real and Intellectual
- Individuals or organization using steganographic carriers for personal or private information



Unethical Use of Steganography

- Criminal communications
- Fraud
- Hacking
- Electronic payments
- Gambling and pornography
- Harassment
- Intellectual property offenses
- Viruses



Hiding Information in Text Files

"Unencrypted message can be hidden within innocent sounding messages" Neil F Johnson

We explore new steganographic and cryptographic algorithms and techniques throughout the world to produce wide variety and security in the electronic web called the Internet. (S0)

A word-shifting algorithm (an algorithm that alters the spacing between words) is then applied to the above text to obtain:

We explore new steganographic and cryptographic algorithms and techniques throughout the world to produce wide variety and security in the electronic web called the Internet. (S1)

An example of how information can be hidden in text files.

Hiding Information in Image Files

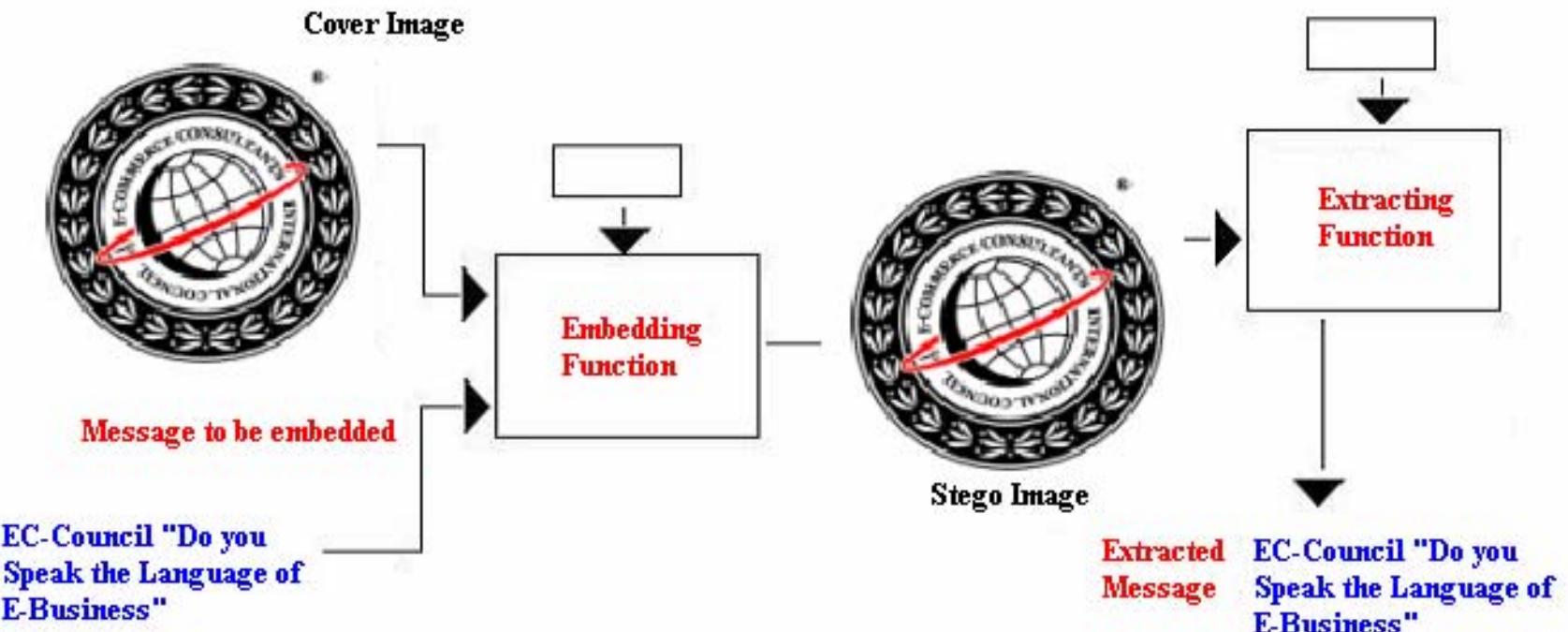
⦿ Two files are required to hide a message within an image file.

- The file containing the image into which the message is supposed to be put in
- The file containing the message itself

⦿ There are 3 methods to hide messages in images, they include:

- Least Significant Bit
- Filtering and Masking
- Algorithms and Transformation

Process of Hiding Information in Image Files



Least Significant Bit

① Disadvantages of LSB Insertion:

- As can be inferred from the example with the 8 bit pixel, applying LSB insertions can alter the color constituents of the pixel
- This could lead to noticeable differences from the cover image to the image, thus alerting observers of the existence of steganography

② Advantages of LSB Insertion:

- It is quick and easy
- There has been steganography software developed which work around LSB color alterations via palette manipulation
- LSB insertion also works well with gray-scale images

Simplified Example with a 24 bit pixel:

1 pixel:

(00100111 11101001 11001000)

Insert 101:

(00100111 11101000 11001001)
red green blue

Simplified Example with an 8 bit pixel:

1 pixel:

(00 01 10 11)
white red green blue

Insert 0011:

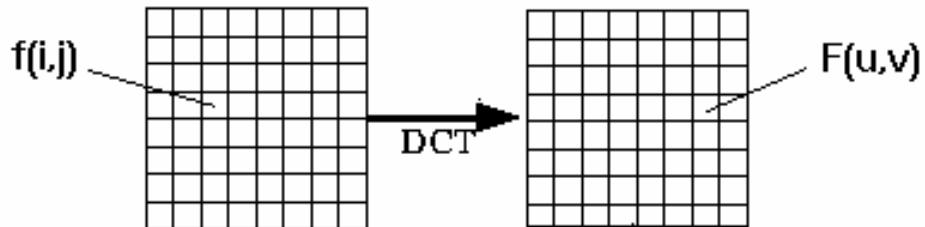
(00 00 11 11)
white white blue blue

Masking and Filtering

- ◉ Masking is one of the main techniques of digital watermarking
- ◉ Watermarking techniques can be applied to images without fear of their destruction
- ◉ They can thereby not be removed by cropping



Algorithms and Transformation



The DCT function:

$$F(u, v) = \frac{\Lambda(u)\Lambda(v)}{4} \sum_{i=0}^7 \sum_{j=0}^7 \cos \frac{(2i+1) \cdot u\pi}{16} \cdot \cos \frac{(2j+1) \cdot v\pi}{16} \cdot f(i, j)$$

$$\Lambda(\xi) = \begin{cases} \frac{1}{\sqrt{2}} & \text{for } \xi = 0 \\ 1 & \text{otherwise} \end{cases}$$

Another steganography method is to hide data in mathematical functions that are in compression algorithms.

Hiding Information in Audio Files

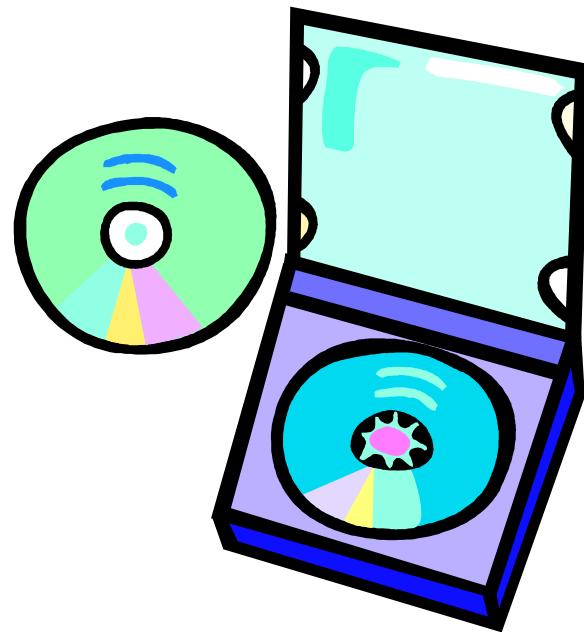
⦿ Hiding messages in audio can be done in three ways:

- Low-bit encoding
- Phase coding
- Spread spectrum
- Echo data hiding



Low-bit Encoding in Audio Files

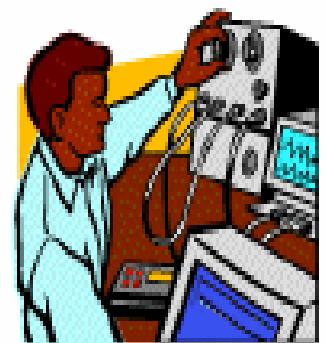
- Low bit Encoding is a type of audio steganography, which is similar to Least Bit Insertion method done through Image Files
- Binary Data can be stored in the least important audio files
- The channel capacity is 1 kilo byte per second per kilohertz



Phase Coding

Phase coding is described as the phase in which an initial audio segment is replaced by a reference phase that represents the data. The method is clearly described below:

- The original sound sequence is shortened into short segments
- A DFT (Discrete Fourier Transform) is applied to each segment to create a matrix of the phase and magnitude.
- The phase difference between each adjacent segment is calculated
- For all other segments, new phase frames are created
- The new phase and original magnitude are combined to get a new segment
- The new segments are concatenated to create the encoded output



Spread Spectrum

- The encoded data is spread across as much of the frequency spectrum
- Spread Spectrum can be clearly illustrated by using Direct Sequence Spread Spectrum (DSSS)
- Unlike phase coding, DSSS does introduce some random noise to the signal



Echo Data Hiding

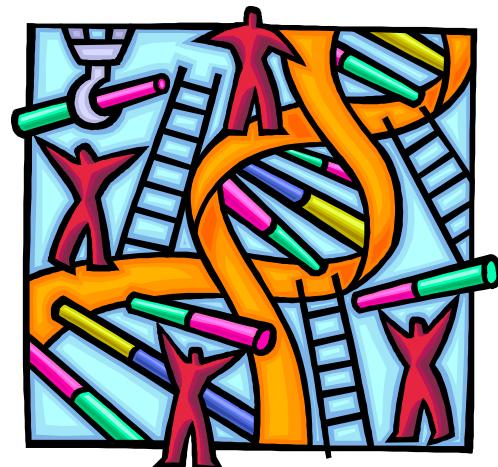
- An echo is introduced to the original signal
- Three properties of this Echo can then be varied to hide data

- Initial Amplitude
- Decay Rate
- Offset



Hiding Information in DNA

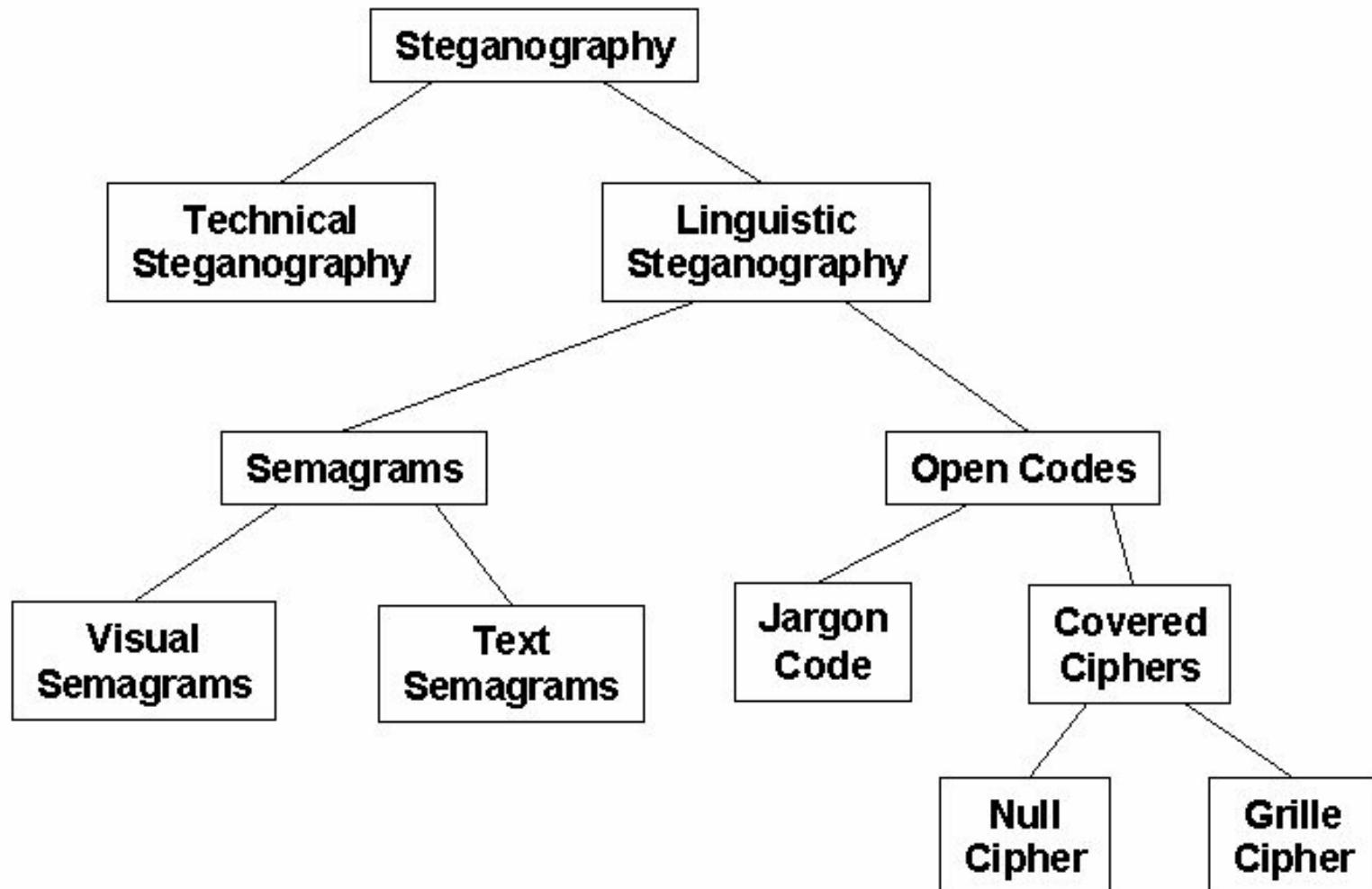
- In the near future biological data, such as DNA may be a viable medium for hidden messages
- This could be particularly useful for "invisible" watermarking that biotech companies could use to prevent the unauthorized usage of their work
- The technological ability to do this has already been demonstrated, three researchers in New York successfully hid a secret message in a DNA sequence and sent it across the country



TEMPEST

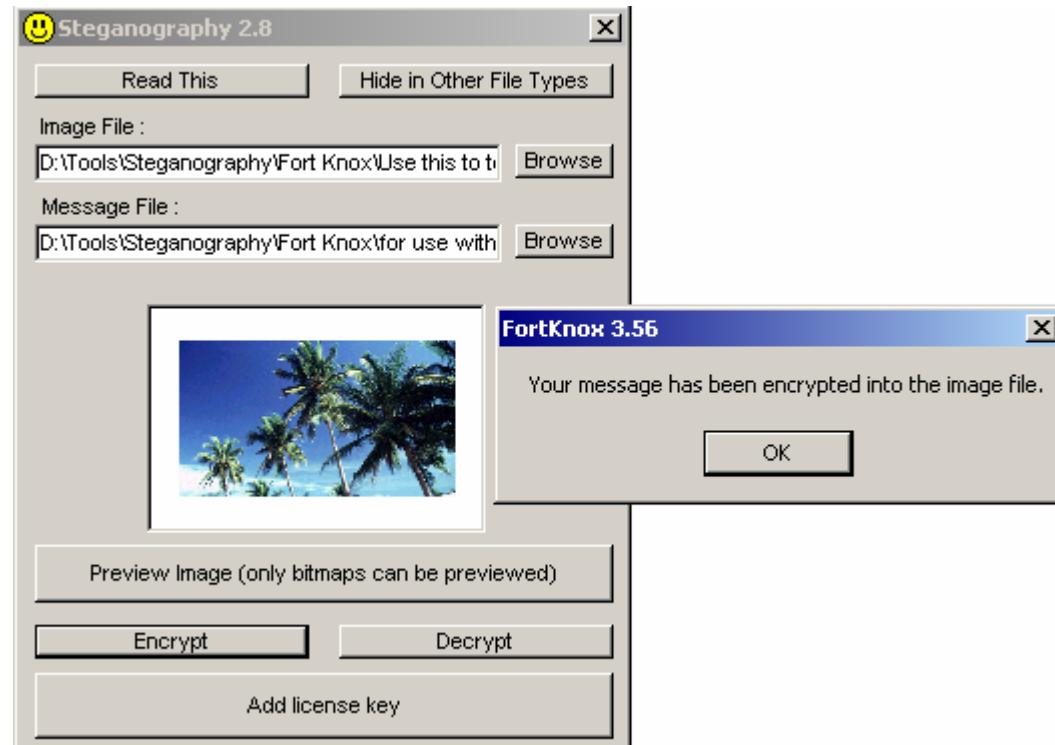
- ◉ TEMPEST = Transient Electromagnetic pulse surveillance technology
- ◉ The term refers to US government evaluated and endorsed equipment that is immune to tempest like attacks
- ◉ Weakness of cryptographic methods is that every bit of the encrypted data has to be viewed in its unencrypted form at least twice
- ◉ When using a tempest like attack it has the ability to obtain the data in unencrypted form during any one of these instances

The Steganography Tree



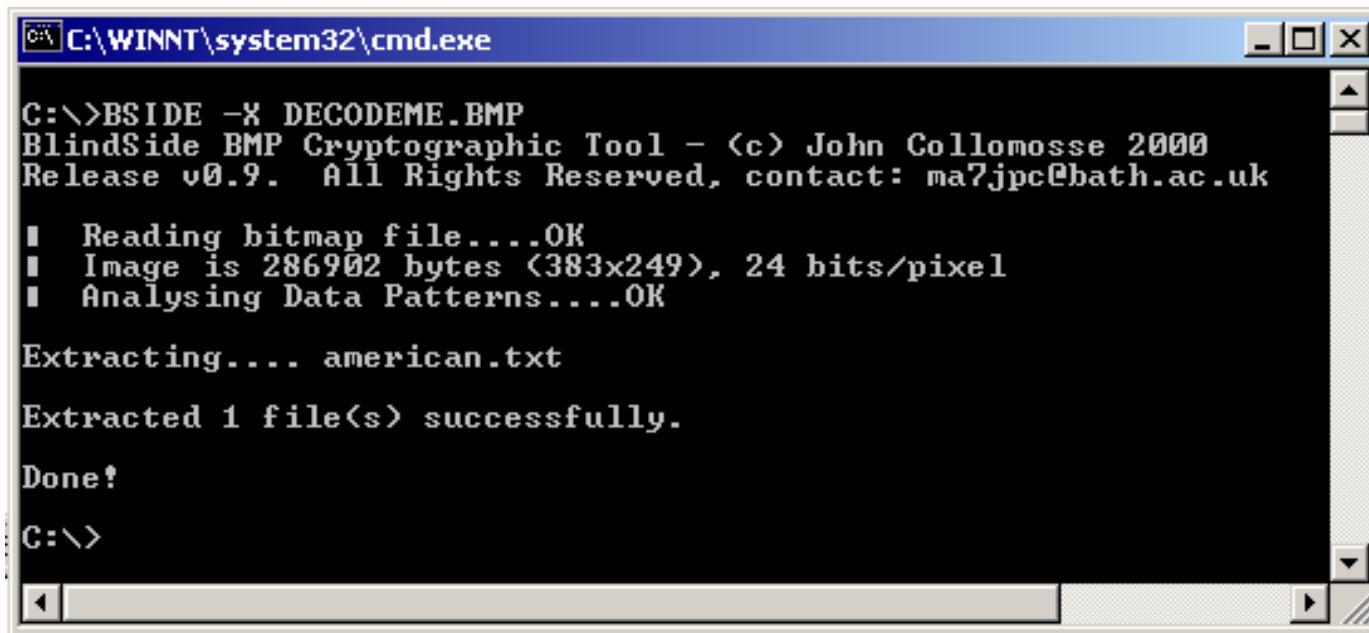
Steganography Tool: Fort Knox

- Supports Windows 95/98/Me/XP/NT/2000/2003
- Uses MD5, Blowfish, CryptAPI algorithms
- Some features that Fort Knox supports are:
 - Password protection lock
 - hiding, securing files and folders
 - Logon password masking



Steganography Tool: Blindsight

- Blindsight can hide files of any file type within a windows bitmap image
- It uses a steganographic technique supplemented with a cryptographic algorithm



C:\>BSIDE -X DECODEME.BMP
BlindSide BMP Cryptographic Tool - (c) John Collomosse 2000
Release v0.9. All Rights Reserved, contact: ma7jpc@bath.ac.uk
■ Reading bitmap file....OK
■ Image is 286902 bytes (383x249), 24 bits/pixel
■ Analysing Data Patterns....OK

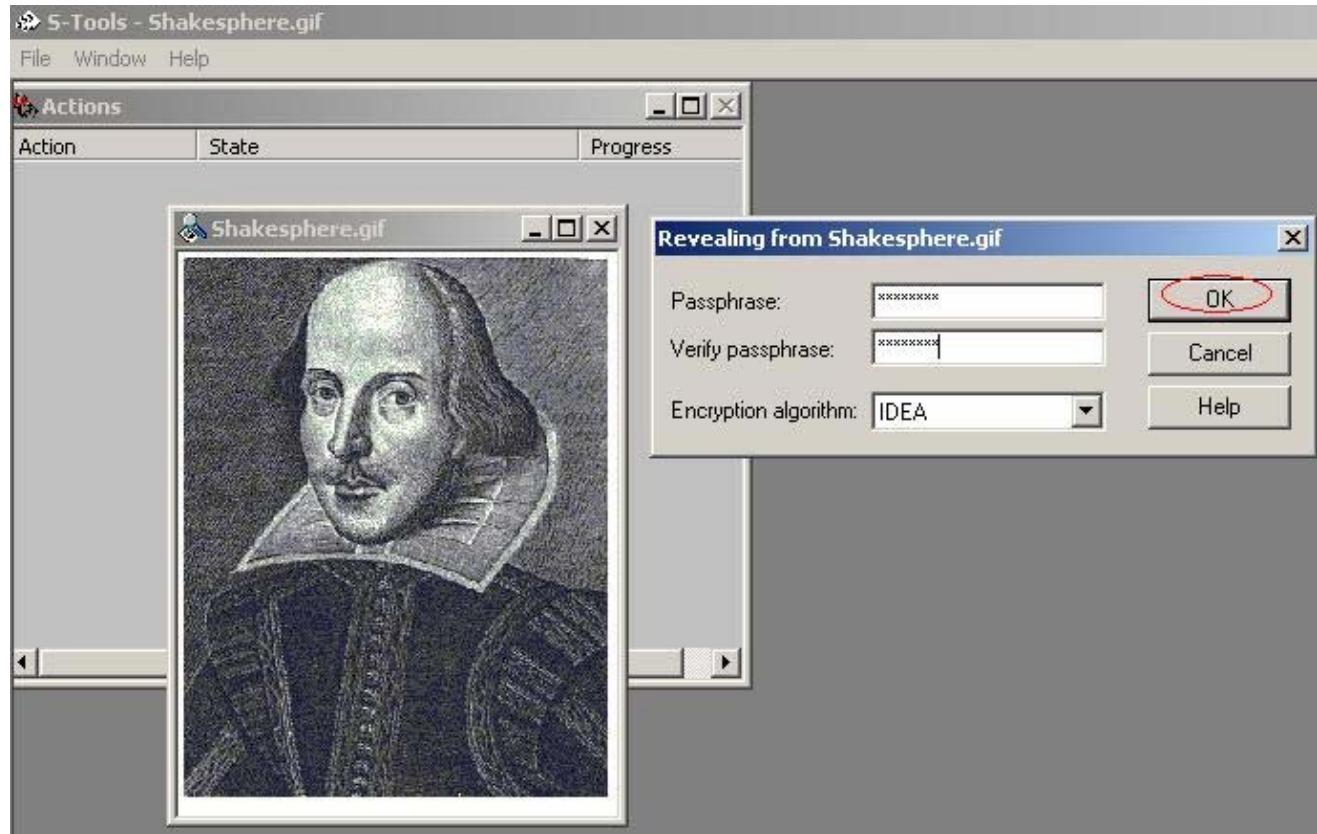
Extracting.... american.txt

Extracted 1 file(s) successfully.

Done!
C:\>

Steganography Tool: S- Tools

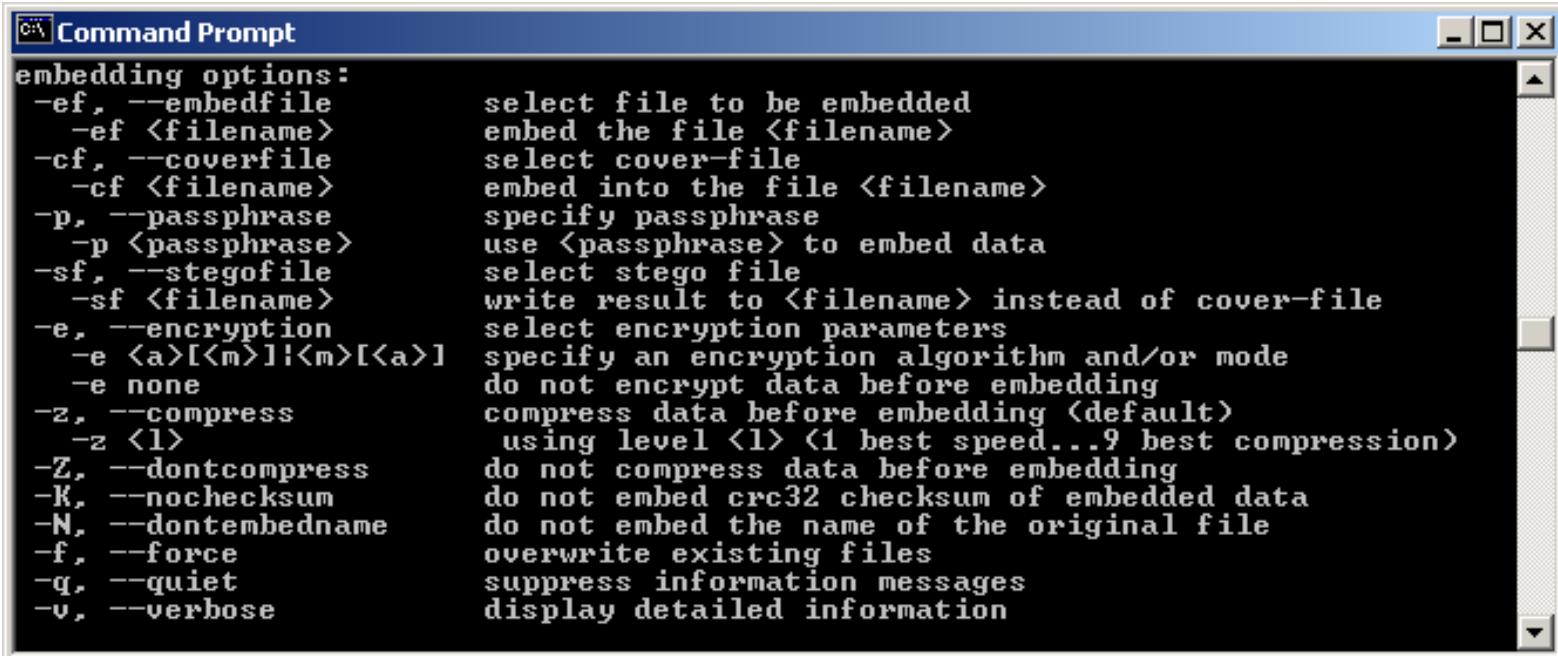
- Ability to hide multiple applications in a single object



Steganography Tool: Steghide

- Following are the features of this tool:

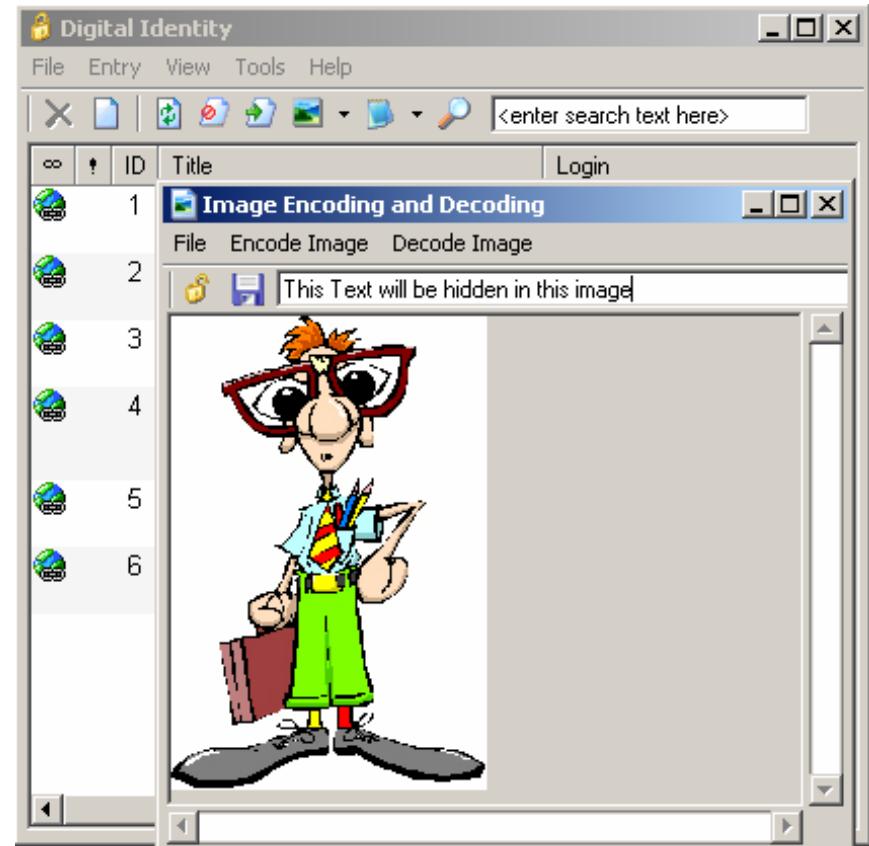
- Compression of the embedded data
- Encryption of the embedded information
- Automatic integrity checking using a checksum



```
Command Prompt
embedding options:
-ef, --embedfile      select file to be embedded
-ef <filename>       embed the file <filename>
-cf, --coverfile     select cover-file
-cf <filename>       embed into the file <filename>
-p, --passphrase     specify passphrase
-p <passphrase>     use <passphrase> to embed data
-sf, --stegofile     select stego file
-sf <filename>       write result to <filename> instead of cover-file
-e, --encryption     select encryption parameters
-e <a>[<m>][<m>][<a>] specify an encryption algorithm and/or mode
-e none              do not encrypt data before embedding
-z, --compress        compress data before embedding (default)
-z <l>               using level <l> (1 best speed...9 best compression)
-Z, --dontcompress   do not compress data before embedding
-k, --nochecksum     do not embed crc32 checksum of embedded data
-N, --dontembedname  do not embed the name of the original file
-f, --force           overwrite existing files
-q, --quiet           suppress information messages
-v, --verbose         display detailed information
```

Steganography Tool: Digital Identity

- It is a secure password and file management system
- It has a master password recovery system that allows the user to encode an image with the main password file



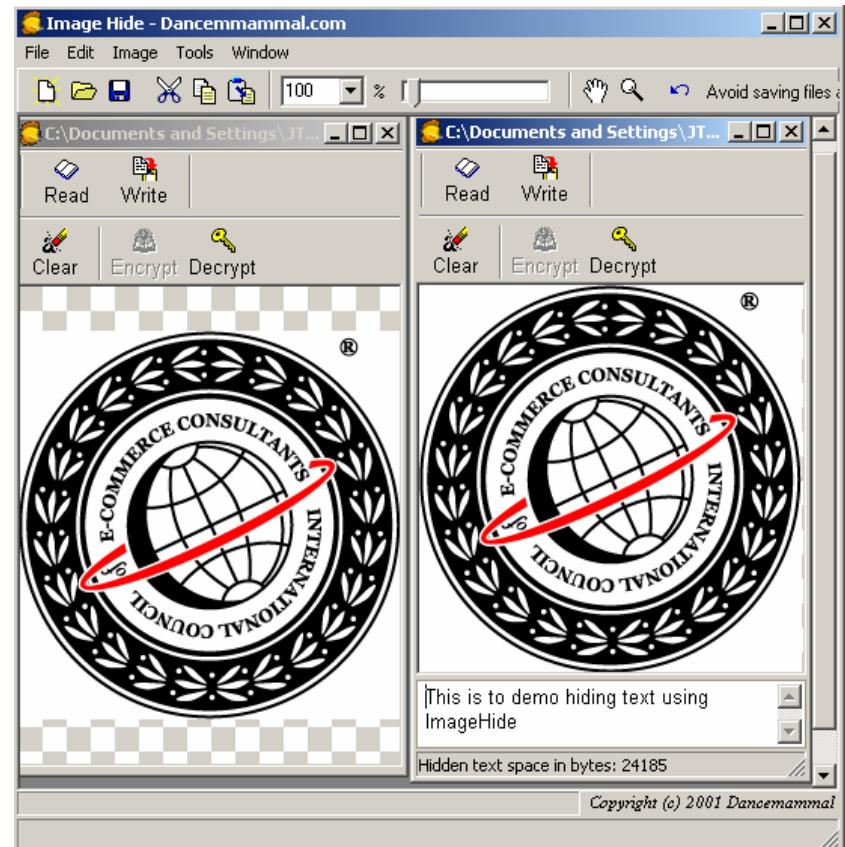
Steganography Tool: Stegowatch

- On the basis of mathematical model, the detector is able to determine if steganography is either detected, suspected or is it a clear image

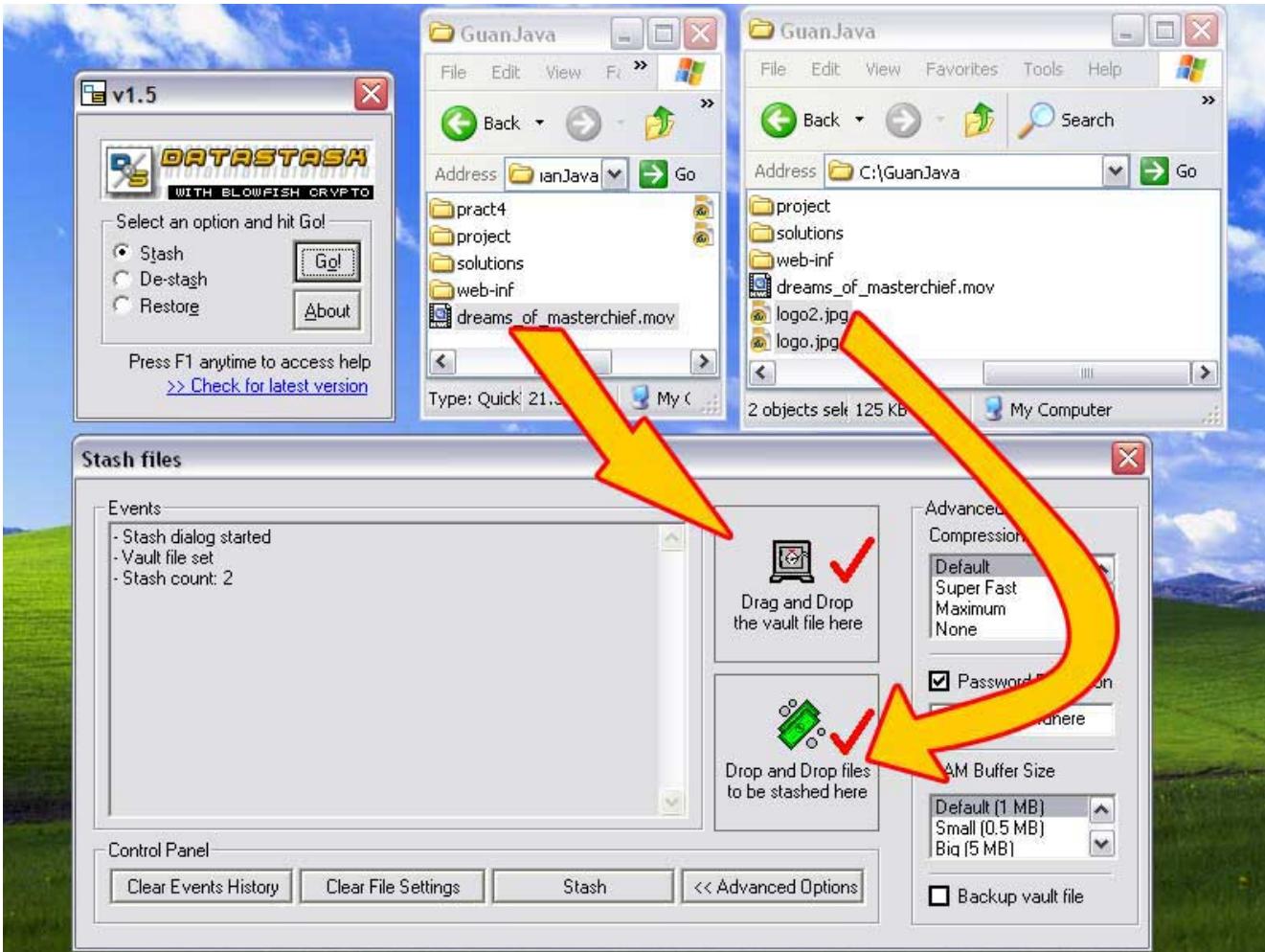


Tool : Image Hide

- ImageHide is a steganography program which hides loads of text in images
- Does simple encryption and decryption of data
- Even after adding bytes of data, there will not be any increase in image size
- Image looks the same to normal paint packages
- Loads and saves to files and gets past all the mail sniffers



Data Stash



Tool: Mp3Stego

◎<http://www.techtv.com>

- ◎MP3Stego will hide information in MP3 files during the compression process
- ◎The data is first compressed, encrypted and then hidden in the MP3 bit stream

```
C:\WINDOWS\System32\cmd.exe

Z:\Development\MP3Stego>encode -E hidden_text.txt -P pass svega.wav svega_stego.mp3
MP3StegoEncoder 1.1.15
See README file for copyright info
Microsoft RIFF, WAVE audio, PCM, mono 44100Hz 16bit, Length: 0: 0:20
MPEG-I layer III, mono Psychoacoustic Model: AT&T
Bitrate=128 kbps De-emphasis: none CRC: off
Encoding "svega.wav" to "svega_stego.mp3"
Hiding "hidden_text.txt"
[Frame 791 of 791] <100.00%> Finished in 0: 0: 6

Z:\Development\MP3Stego>decode -X -P pass svega_stego.mp3
MP3StegoEncoder 1.1.15
See README file for copyright info
Input file = 'svega_stego.mp3' output file = 'svega_stego.mp3.pcm'
Will attempt to extract hidden information. Output: svega_stego.mp3.txt
the bit stream file svega_stego.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=3, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=single-ch, sblim=32, jsbd=32, ch=1
[Frame 791] Avg slots/frame = 417.434; b/smp = 2.90; br = 127.839 kbps
Decoding of "svega_stego.mp3" is finished
The decoded PCM output file name is "svega_stego.mp3.pcm"

Z:\Development\MP3Stego>
```

Tool: Snow.exe

- <http://www.darkside.com.au/snow/>
- Snow is a whitespace steganography program and is used to conceal messages in ASCII text by appending whitespace to the end of lines
- Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. If the built in encryption is used, the message cannot be read even if it is detected

To Encode the Message to a file — myfile.doc

```
snow -m "Swiss bank a/c: 3453434" -p "password-123" myfile.doc  
myfile2.doc.
```

To extract the message, the command would be

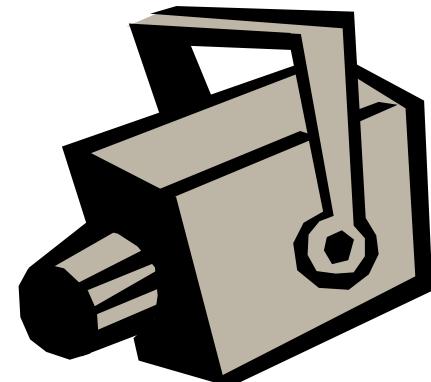
```
snow -p "password-123" myfile2.doc
```

Tool: Camera/Shy

- <http://www.netiq.com/support/sa/camerashyinfo.asp>
- Camera/Shy works with Windows and Internet Explorer and lets users share censored or sensitive information buried within an ordinary gif image
- The program lets users encrypt text with a click of the mouse and bury the text in an image. The files can be password protected for further security
- Viewers who open the pages with the Camera/Shy browser tool can then decrypt the embedded text on the fly by double-clicking on the image and supplying a password

Steganography Detection

- ◎ <http://www.outguess.org/download.php>
- ◎ Stegdetect is an automated tool for detecting steganographic content in images
- ◎ It is capable of detecting different steganographic methods to embed hidden information in JPEG images
- ◎ Stegbreak is used to launch dictionary attacks against Jsteg-Shell, JPHide and OutGuess 0.13b



Summary

- Steganography is the art of hidden or covered writing
- Steganography involves placing hidden messages in some transport medium
- Digital watermarks are imperceptible or barely perceptible transformations of digital data; often the digital data set is a digital multimedia object
- Weakness of cryptographic methods is that every bit of the encrypted data has to be viewed in its unencrypted form at least twice



Computer Hacking Forensic Investigator

Module XIV Computer Forensic Tools

Module Objective

- Dump tools
 - Ds2dump
 - Choasreader
- Slack space & data recovery tools
 - DriveSpy
 - Ontrack
- Hard disk write protection tools
 - Pdblock
 - Write-blocker
 - NoWrite
 - DriveDock
- Permanent deletion of files
 - PDWipe
- File integrity checkers
 - HashKeeper
- Disk imaging tools
 - Image
 - SnapBack DataArrest
 - IXimager
- Partition managers
 - Part
 - Explore2fs

Module Objective

- Linux/UNIX tools

- Ltools
- Mtools
- TCT
- TCTUTILs

- Password recovery tool

- @stake

- Internet History Viewer

- ASRData

- Ftimes

- Oxygen phone manager

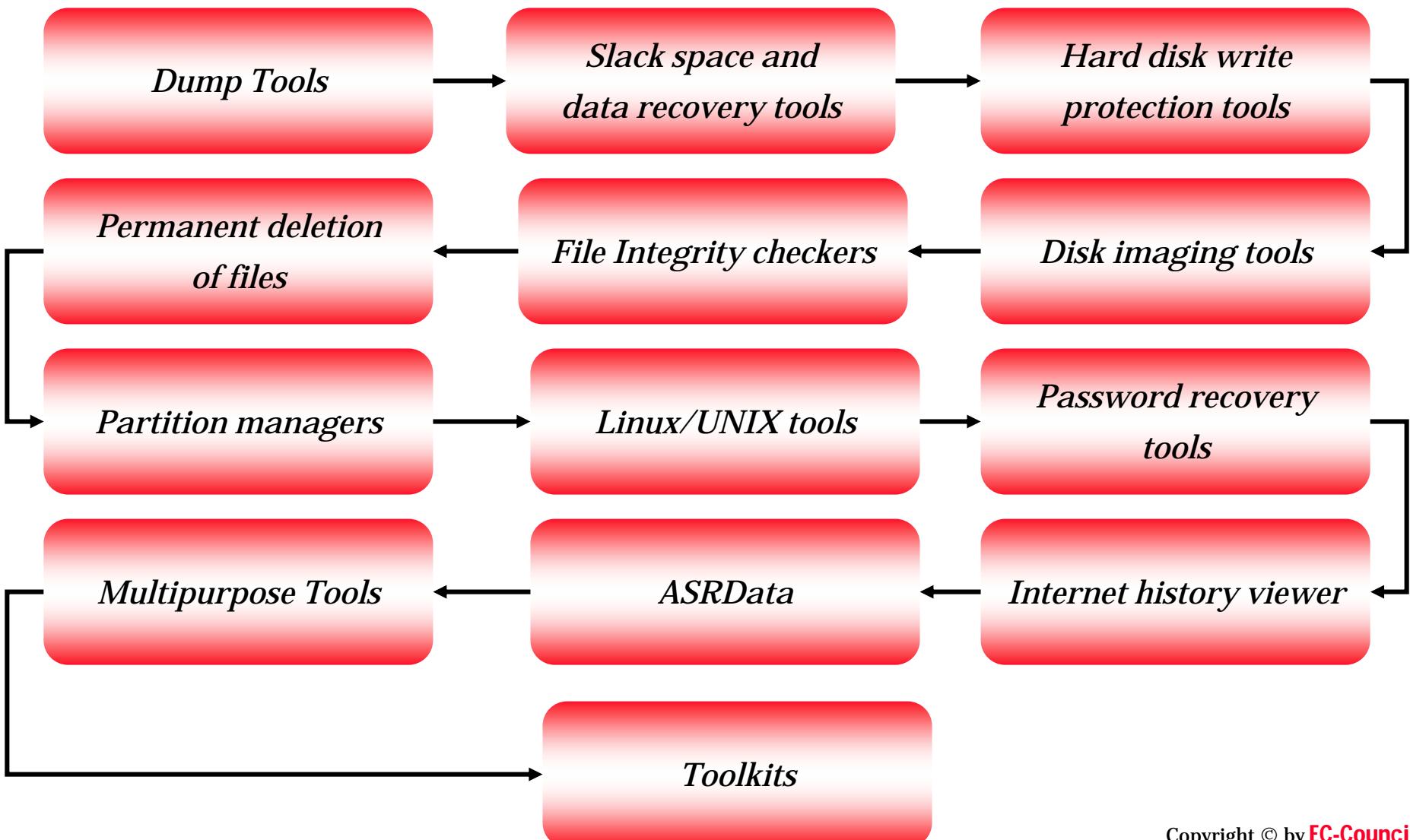
- Multipurpose tools

- ByteBack
- Maresware
- BIA Protect Tools
- LC-Technology Software
- WinHex specialist editor
- ProDiscover DFT

- Toolkits

- NTI-Tools
- DataLifter
- R-Tools

Module Flow



Dump Tool: DS2DUMP

- A software to recover unallocated space, or create a bit-stream dump
- DS2DUMP must be run from real-mode DOS. This includes the "Restart in MS-DOS Mode" option when choosing Start>Shutdown from the Taskbar
- DS2DUMP extracts unallocated clusters from FAT12/16/32 file systems
- DS2DUMP can dump an entire physical drive to several allocated bit-stream files

Dump Tool: Chaosreader

- Used trace TCP/UDP sessions and capture the application data
- Data captured from tcpdump or snoop logs
- It creates html index files and links all the session details
- Few the quick commands that are used are

Chaosreader [-ae hikqr vx A H I R T U X Y] [-D dir]

Chaosreader [-b port[,...]] [-B port[,...]]

Chaosreader [-j IPAddr[,...]] [-J IPAddr[,...]]

Slack Space & Data Recovery Tools: Drivespy

- ④ A Forensic DOS shell
- ④ Programmed to imitate and expand the potential of DOS for forensic purposes
- ④ Uses its own commands included with common DOS commands
- ④ This tool can process
 - Hard drives with capacity of more than 8.4 GB
 - Floppy drives and other removable drives
 - FAT12/16/16x/32/32x partitions
 - Hidden DOS partitions

Slack Space & Data Recovery Tools: Ontrack

- Retrieves lost, remote or deleted data and entire partitions
- The user can start, stop or resume the recovery process
- The user can select an FTP location to copy the recovered files and folders
- Allows the user to filter and sort the recovered files according to date, name, time, status and size
- It does the following functions for recovering data
 - Scans the media for data that is lost or remote to access
 - The user can select copy the recovered files and folders to another specified location

Hard Disk Write Protection Tools: Pdblock

① PDBlock

- Write protects hard disks on a system and prevents write requests to particular hard disks on a system
- Has an option to select specific write protected hard drives
- Safeguard any particular drive accessed from the system through Interrupt 13 or the MS/IBM Interrupt 13 extensions

② Write-blocker

- Prevents data from being written to a hard disk during investigations
- Allows ample access to the forensic examiner to download, examine and investigate the data present in a system



Hard Disk Write Protection Tools: Nowrite & Firewire Drivedock

○ NoWrite

- It is a hardware device which does not allow writing on to the hard drive
- It supports drives with huge capacity
- Supports Windows, DOS, Linux and other known operating systems



○ FireWire DriveDock

- Wiebetech's DriveDock is a forensic tool for investigators who want to swap the hard drive or test it
- It is compatible with Mac and Windows operating systems
- It is the FireWire to IDE bridge that write protects the hard drive



Permanent Deletion of Files:pdwipe

- ◉ PDWipe (Physical Drive Wipe) is capable of wiping large hard drives with capacity greater than 8.4 Gb in a matter of time
- ◉ PDWipe's wiping technology is based on DriveSpy
- ◉ PDWipe has three basic modes of operation

- Command line interactive
- Command line confirmation
- Batch file operation

Disk Imaging Tools: Image & IXimager

○ Image

- It is a standalone utility to generate physical replicas of floppy disks
- It generates highly compressed or "flat" images for forensic analysis
- Processing of large numbers of diskettes is supported and automated by cyclic imaging and restoration processes

○ IXimager

- Captures and analyzes images created from hard drives and other external storage media
- It is compatible with Windows XP Service Pack 1, Windows 2000 Service Pack 4 and Windows 2003 Server

Disk Imaging Tools: Snapback Datarrest

- This software has a user friendly interface backed by powerful operation to create mirror images of variety of operating systems
- Performs fast and successful back-up and restoration.
- SnapBack DatArrest is compatible with all IBM-compatible computers containing any OS
- If a DOS floppy is booted, data can be seized quickly, accurately, and completely
- It gathers every bit from the hard drive

Partition Managers: PART & Explore2fs

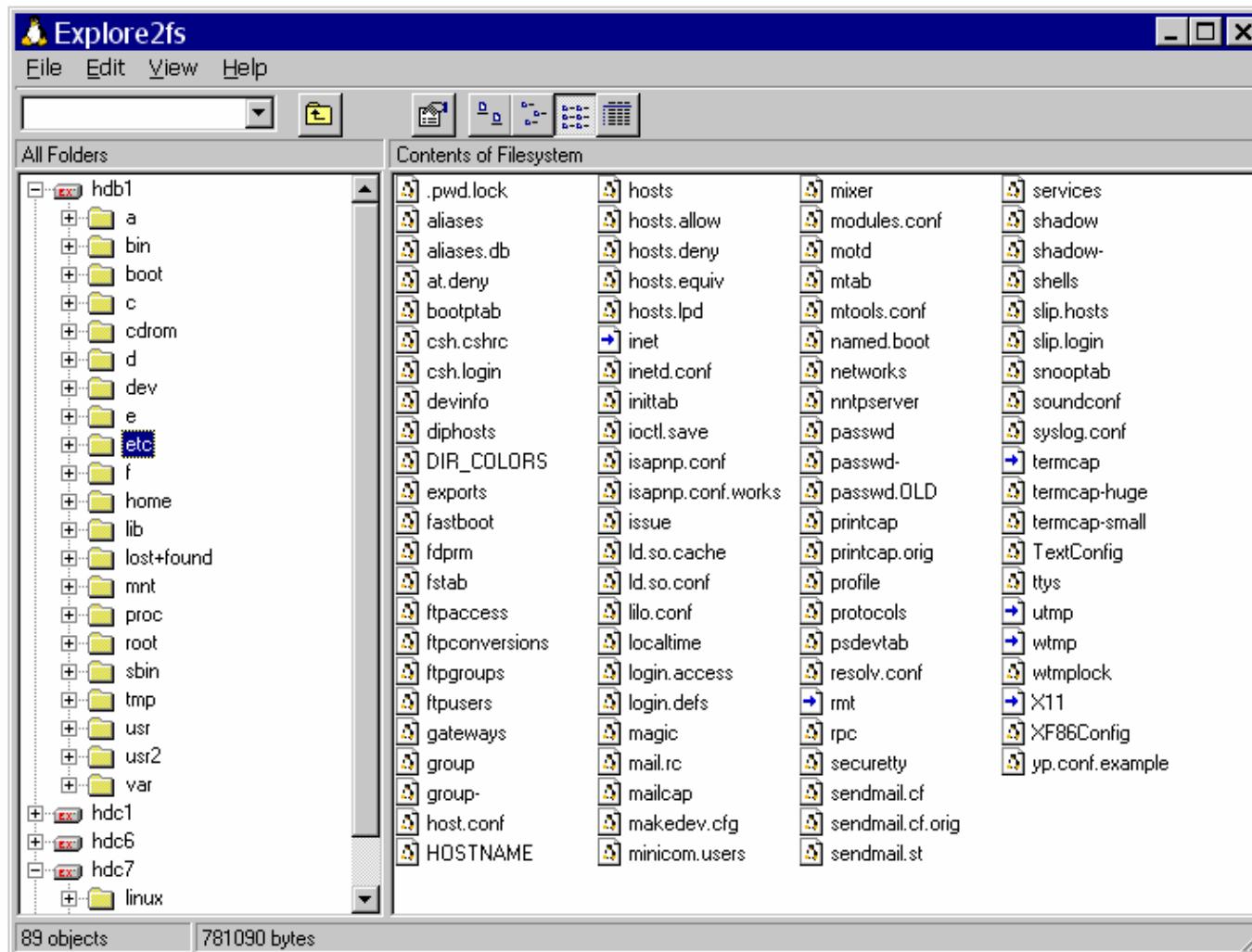
◦ PART

- It displays important information about all the partitions present in a hard disk
- It performs switching bootable partitions, and hides and unhide DOS partitions
- It identifies the available partitions and file format for the disks/drives of a compromised system

◦ Explore2fs

- The Native IO feature of Explore2fs cures partitions undetected by NT users
- This access is not available from the Win32 subsystem
- Explore2fs bypasses Win32 and interface directly with the Native API

Screenshot - Explore2fs



Linux/unix Tools: Ltools and Mtools

⦿ Ltools

- Accesses Linux files from Windows 9x and Windows NT
- A set of command line tools for reading and writing Linux ReiserFS, ext2, and ext3 file systems
- Has Java and .NET based GUI, an Explorer-like interface in a Web browser, providing remote access to file systems
- Used in DOS environment to repair Linux , if the Linux system does not boot

⦿ Mtools

- Allows MS-DOS files to be manipulated by Unix systems
- Reads , writes and moves files of MS-DOS file system (floppy disk)
- Floppies can be changed without unmounting and mounting

Linux/unix Tools: TCT and Tctutils

- The Coroners Toolkit(TCT) developed by Dan Farmer and Wietse Venema is a collection of programs developed for forensics investigation on UNIX systems
- TCTUTILS is a collection of utilities that adds additional functionality to The Coroners Toolkit (TCT)
- Supports the following operating systems
 - FreeBSD2-4.*
 - OpenBSD2.*
 - BSD/OS2-3.*
 - SunOS4-5.*
 - Linux2.*

Password Recovery Tool: @Stake

- LC™ 5 is the password auditing and recovery application
- @stake LC5 which is the current version of @stake reduces security risk by helping administrators to
 - Remove vulnerabilities caused due to weak or easily guessed passwords
 - Recover Windows and Unix account passwords if lost
 - Has pre-computed password tables containing huge amount of passwords

Screenshot of @Stakelc5

The screenshot shows a Microsoft Internet Explorer window displaying the @Stake LCE - Corporate Audit software. The main window is titled "Run Report" and displays a table of user accounts with their details and audit status. The table includes columns for Domain, User Name, Password, Password Age (days), Password Score, Locked Out, Disabled, Expired, Never Expires, Audit Time, and Method. Most users have a password score of Fci and are listed as "Never Expires". The audit time for most users is 0d 0h 0m 0s, indicating they were cracked using a dictionary attack.

Domain	User Name	Password	Password Age (days)	Password Score	Locked Out	Disabled	Expired	Never Expires	Audit Time	Method
lce	Administrator	c	0	Fci					0d 0h 0m 0s	Dictionary
lce	charles	ca	0	Fci					0d 0h 1m 12s	Precomputed Hash
lce	sergo	cacao	0	Fci					0d 0h 1m 28s	Precomputed Hash
lce	nacho	zzzz	0	Fci					0d 0h 1m 30s	Precomputed Hash
lce	hrcd	crackpot	0	Fci					0d 0h 0m 0s	Dictionary
lce	tonny	zzzz	0	Fci					0d 0h 0m 57s	Precomputed Hash
lce	ken	mmmm	0	Fci					0d 0h 0m 57s	Precomputed Hash
lce	jonth	cac	0	Fci					0d 0h 0m 0s	Dictionary
lce	amr	caca	0	Fci					0d 0h 2m 38s	Precomputed Hash
lce	kathy	cacaoa	0	Fci					0d 0h 0m 0s	Dictionary
lce	toxas	VochChava	0	Fci					0d 0h 0m 1s	Dictionary
lce	hector	z	0	Fci					0d 0h 0m 1s	Dictionary
lce	zmo	zz	0	Fci					0d 0h 0m 39s	Precomputed Hash
lce	theresa	zzz	0	Fci					0d 0h 1m 38s	Precomputed Hash
lce	wilhelm	impunity	0	Fci					0d 0h 0m 1s	Dictionary
lce	cezar	zzzzz	0	Fci					0d 0h 0m 11s	Precomputed Hash
lce	Administrator	Administrator	0	Fci					0d 0h 0m 1s	Dictionary
lce	ray	m	0	Fci					0d 0h 0m 1s	Dictionary
lce	Guest	* missing *	0	Fci						
lce	vlad	mm	0	Fci					0d 0h 1m 38s	Precomputed Hash
lce	octavo	mmm	0	Fci					0d 0h 0m 19s	Precomputed Hash
lce	thomas	mmmmmm	0	Fci					0d 0h 0m 51s	Precomputed Hash
lce	DaveKlez	ca	0	Fci					0d 0h 1m 12s	Precomputed Hash
lce	nto	cac	0	Fci					0d 0h 0m 0s	Dictionary

Below the table, a log window shows the audit progress:

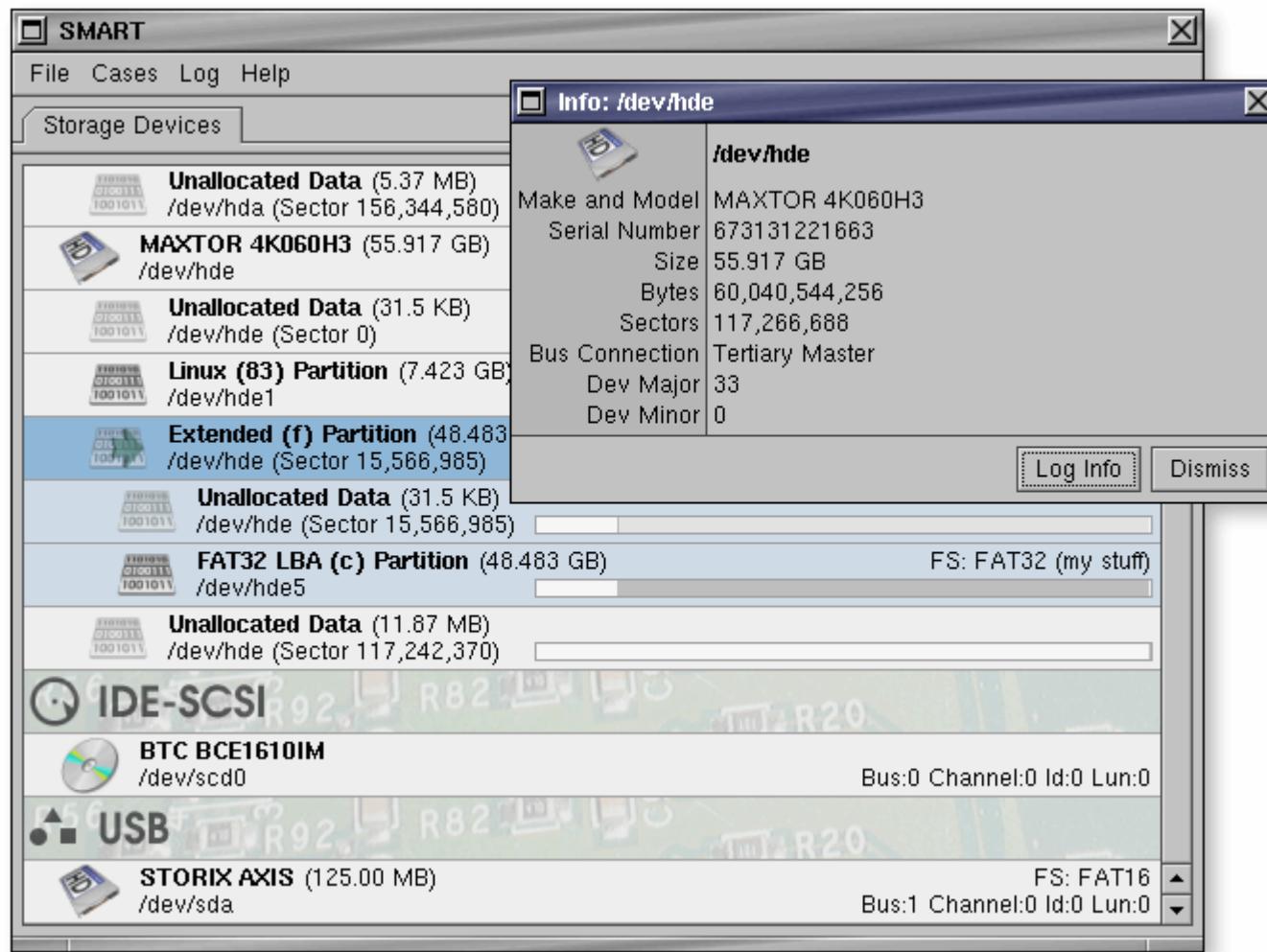
```
11:14:51 14/11/14 *E:41 11 Cracked password for 'mke' with Precomputed Hashes
06/13/2004 *E:43 36 Cracked password for 'mke' with Precomputed Hashes
11:14:51 14/11/14 *E:44 4* Cracked password for 'thomas' with Precomputed Hashes
06/13/2004 *E:43 13 Cracked password for 'mke' with Precomputed Hashes
05/17/2004 *E:43 47 Cracked password for 'mke' with Precomputed Hashes
06/13/2004 *E:43 17 Cracked password for 'mke' with Precomputed Hashes
06/13/2004 *E:44 43 Cracked password for 'mke' with Precomputed Hashes
06/13/2004 *E:44 44 Auditing session completed.
```

The interface includes a sidebar with cracking metrics and a summary section. The summary shows a total of 25 successful hashes, 20 cracked, and 100.00% completion. A legend at the bottom indicates the types of attacks used: User Info, Dictionary, Hybrid, Precomputed, and Brute Force.

Asrdata

- ◉ ASR developed forensic Tool SMART for Linux
- ◉ The features of SMART allow it to be used in many scenarios, including
 - on-site or remote preview of a target system
 - post mortem analysis of a dead systems and providing baselines
 - testing and verification of other forensic programs
 - conversion of proprietary "evidence file" formats

SMART Screenshot



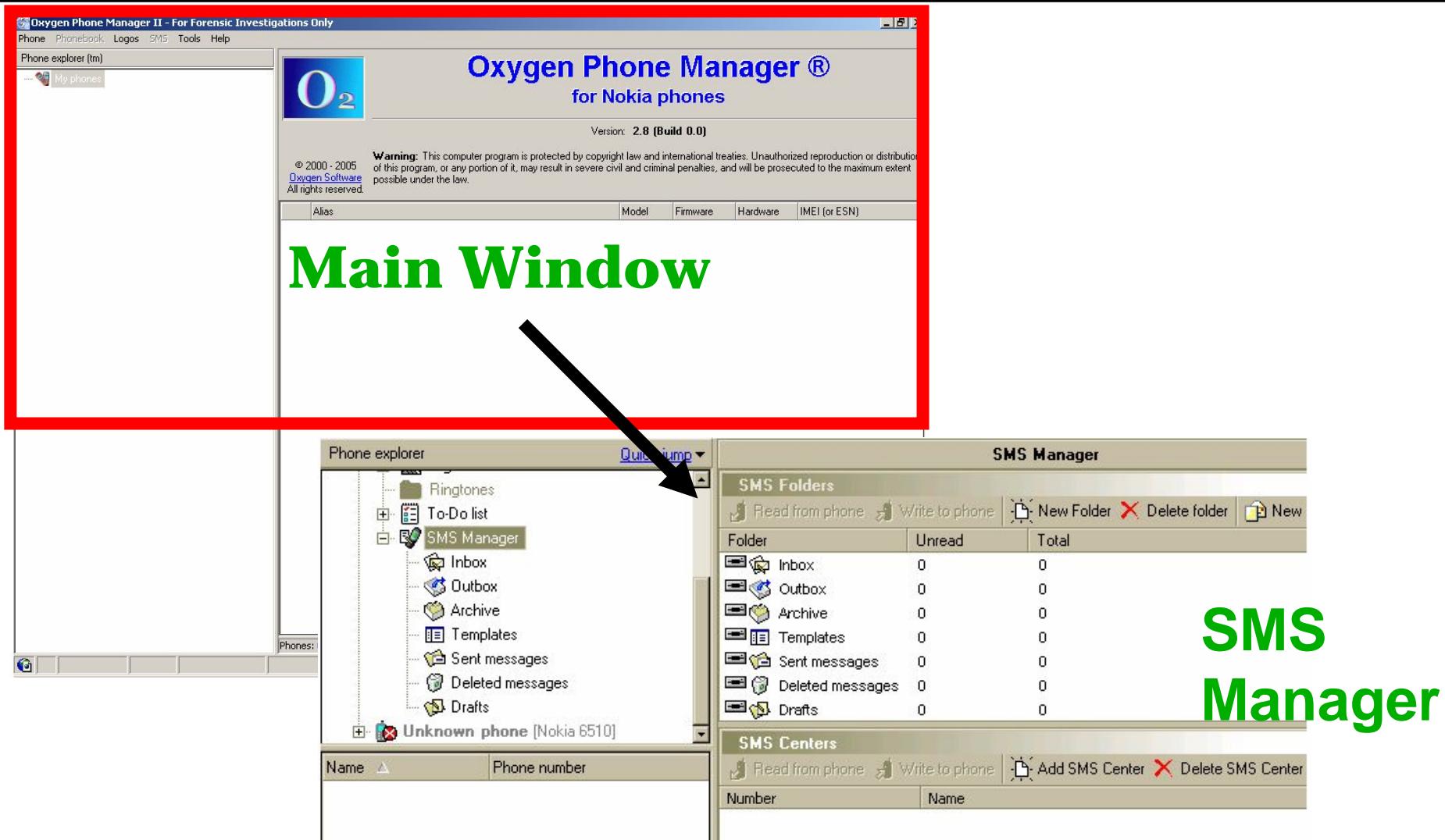
Ftime

- ◉ Ftime is a evidence collection and system baselining tool
- ◉ It gathers the information regarding the specified directories and files
- ◉ It is created to log four types of information: configuration settings , progress indicators, metrics and errors
- ◉ It can be used on any operating systems
 - Workbench
 - Client-server

Oxygen Phone Manager

- It supports all the models of Nokia mobile phone
- Supported connection types: InfraRed; Bluetooth; and various USB
- Backup and restore all information from mobile phone
- Highly customizable imports
- Export of phonebook to all the popular formats.
- Supports three storage types: SIM card, phone memory and disk

Oxygen Phone Manager



**SMS
Manager**

Multipurpose Tools: Byte Back & Biaprotect

① ByteBack

- It is a professional data recovery and computer investigative utility with the following functionality
 - Cloning / Imaging
 - Automated File Recovery
 - Rebuild Partitions and Boot Records
 - Media Wipe: Overwrites every sector of a drive

① BIAProtect

- BIA stands for Business Intelligence Associates
- It is an organization indulged in the fields of law, computer forensics and software programming
- It has various hardware and software (tools) for computer forensics

Multipurpose Tools: Maresware

- ⦿ It is used in computer forensics for following purposes

- discovery of "hidden" files(such as NTFS Alternate Data Streams)
- for incident response purposes and timelines
- file key word searching and comparing and file formatting and verification
- drive wiping for information privacy and security
- keyboard locking and diskette imaging
- documentation of all steps and procedures

Multipurpose Tools: LC Technologies Software

⦿ It has following software/tools

- *Photorecovery*: Designed to recover images, movies, and sound files from all types of digital media
- *File RecoveryPro*: Scans and finds lost partitions, boot sectors and other file system components
- *FILEExtinguisher*: This tools completely removes a data from disks to avoid passing private/secret information
- *SanDiskRescuePRO*: It recovers all kinds of data from the hard disk
- *Data Recovery kit*: It allows fast, safe, and reliable file recovery with Windows environment
- *Intelli-SMART*: This is a software used for reporting

Multipurpose Tools: Winhex Specialist Edition

- It is a hexadecimal editor, which helps in recovering data, low-level data processing
- It is used in the field of computer forensics and IT security
- Salient features

- RAM and disk editor
- A data interpreter, which recognizes 20 types of data
- Templates to repair partition table/boot sector
- Helps in copying disks
- Has programming API and scripting interface

Multipurpose Tools: Prodiscover DFT

- *ProDiscoverForensics*: finds all the data on a computer disk while protecting evidence during reports creation
- Some of the important features

- Creates bit-stream copy of disk to be analyzed
- Previews all files, hidden/deleted or metadata
- Searches files or entire disk including slack space, HPA section, and ADS
- Reads and writes images in the UNIX dd format
- Ensures data integrity by generating and recording MD5 or SHA1 hashes

Toolkits: NTI Tools

◎ Some of the important NTI tools

- *AnaDisk*: A floppy diskette analysis tool for security reviews and to identify data storage pattern anomalies
- *DiskScrub*: A utility that is used to securely destroy computer data on a disk drive
- *GetSlack*: Captures data stored in the file slack associated with all of the files on a target computer hard disk drive
- *NTA Stealth*: Determines the past Internet-based computer usage of a specific computer system
- *SafeBack 3.0*: Hard disk's bit-stream backup software

Toolkits: R-Tools-I

- R-Tools Technology Inc. is the provider of forensic utilities for Windows OS family
- It has following set of tools
 - R-Studio: An undelete and data recovery software recovering files
 - R-Undelete: It is a file undelete solution for Windows and Linux systems
 - R-Drive Image: A disk image file contains the exact, byte-by-byte copy of a hard drive, partition or logical disks
 - R-Firewall: It protects a computers present in a local network and/or to the Internet against any intrusions

Toolkits: R-Tools-II

- R-guard: used for access right control, encryption and audit
- R-mail: R-Mail recovers damaged *.dbx files and the messages are recovered in the .eml format and can be imported into Outlook Express mail bases
- R-word: R-Word is a tool designed to recover corrupted Microsoft Word documents
- R-Wipe&Clean: It deletes private records of user's on-line and off-line activities, such as temporary internet files, history, cookies, passwords, swap files, etc
- R-Linux: It is a free file recovery utility for the Ext2FS file system used in the Linux OS and several Unix versions

Toolkits: Datalifter

- ◉ DataLifter is a forensics toolkit built by StepaNNet Communications Inc
- ◉ It has a set of 10 tool kits that helps in forensics investigations
- ◉ There are two versions of DataLifter: DataLifter v2.0 and DataLifter.Net Bonus Tools
- ◉ The utilities that are grouped together along with DataLifter v2.0 includes Active reports, Disk2File, File extraction, Image linker, Internet history, File signature generator, Email retriever, Ping/Trace route/WHOIS, Recycle Bin history, Screen capture

Toolkits: Accessdata

- ⦿ These are the set of programs for computer forensic purposes
 - *Password Recovery Toolkit*: The Password Recovery Toolkit recovers passwords from well-known applications
 - *Distributed network attack*: Recovery of lost passwords for MS Office 97/2000 products like Word and Excel and pdf file decryption feature
 - *Registry viewer*: Registry Viewer views independent registry files and generate reports
 - *Wipe drive*: It is used to overwrite and remove all the data present in a computer

LC Technology International Hardware

- It is the developer of data recovery, digital media recovery, and digital photo recovery software
- It has two computer forensic hardware: data recovery and other forensic tools
- The DRAC 2000 was developed to make the investigation and recovery of "digital artifacts" easy and straight forward

Screenshot of Forensic Hardware



DRAC 2000



DRAC 1000



P-DRAC



Mini-DRAC

Image MASter Solo and Fastbloc

○ **Image MASter Solo:**

- It is a hard drive duplicator for workstation cloning.
- It can load any operating system and application software including: Windows95/98, NT, SCO, Unix, OS/2, and Mac OS



○ **FastBloc:**

- It is a data acquisition software, which connects through an IDE channel. Does not require SCSI controller cards or SCSI drivers
- The common IDE write-blocked architecture allows data from any IDE hard drive to be gathered safely in Windows OS



RMON2 Tracing Tools and MCI DoStracker

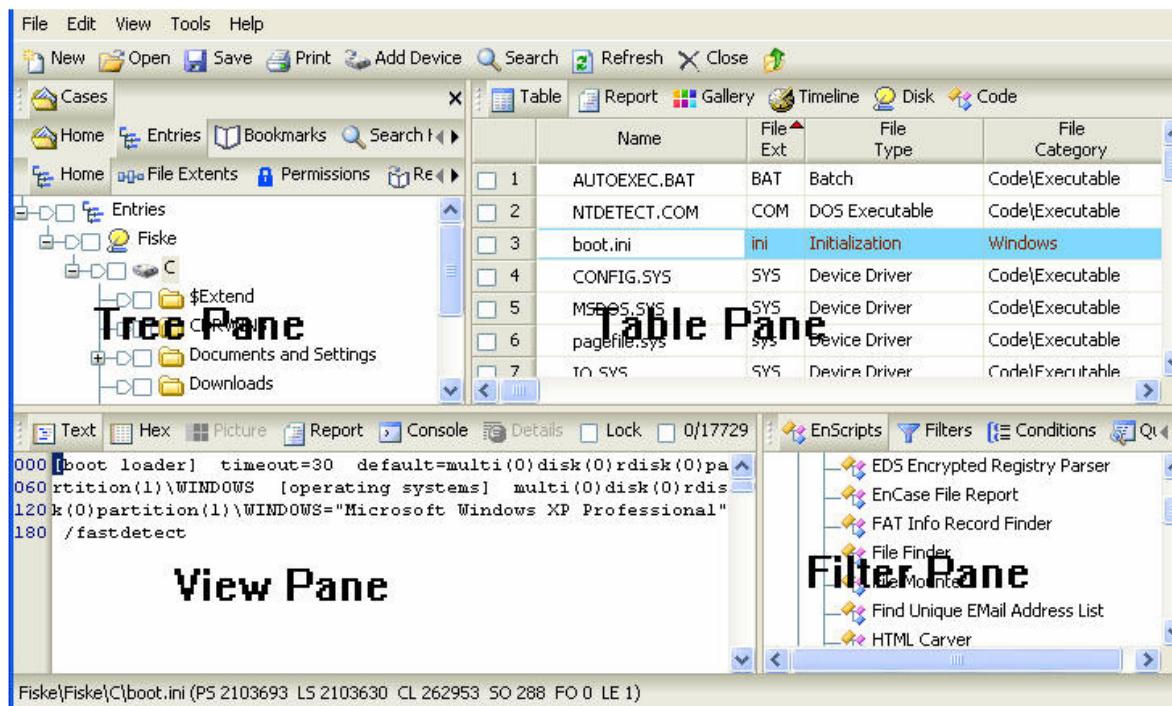
◎ RMON2 tracing tools:

- It requires some compatible devices to perform tracing
- Looks for evidence of remote/unrecognized conversations performed within the victim's perimeter
- By moving “outwards” a step at a time, the source of the attack is determined

◎ MCI DoSTracker:

- Traces source forged packets from the victim's location to its source while tracing backwards.
- Deploys access control list in debug mode for victim IP.
- Clears victim subnet cache and looks for forged packets by comparing to route table.
- Spawns separate process to log into next hop router and continue.

Encase



- Forensic data and analysis program
- Performs computer related investigations
- Data can be exported to various file formats
- Supports Windows 95/NT

Summary

- ◉ DS2Dump is used to recover unallocated space, or create a bit-stream dump
- ◉ Data recovery plays a crucial role during investigations. The tool, Ontrack, is used for data recovery
- ◉ Hard disks must be write protected to safeguard integrity of data
- ◉ Ltools, Mtools, TCT and TCTutils are Linux/UNIX based forensic tools
- ◉ Tools that perform various different functions are known as Multi-purpose tools



Computer Hacking Forensic Investigator

Module XV

Application password
crackers

Scenario

Kristy, a research associate with a drug manufacturing company is not happy about the yearly appraisal. She plans to leave her job and in between that she gets an exciting offer from competitor. She was asked to provide specifications of a famous drug and in return they are ready to give her good amount of money. Kristy stole the specification, zipped, password protected the file and sent it as an email attachment to the competitor.

In her company all mails are checked by the system administrator. He opened the attachment and found the specification. Kristy was fired for breaching company policy.

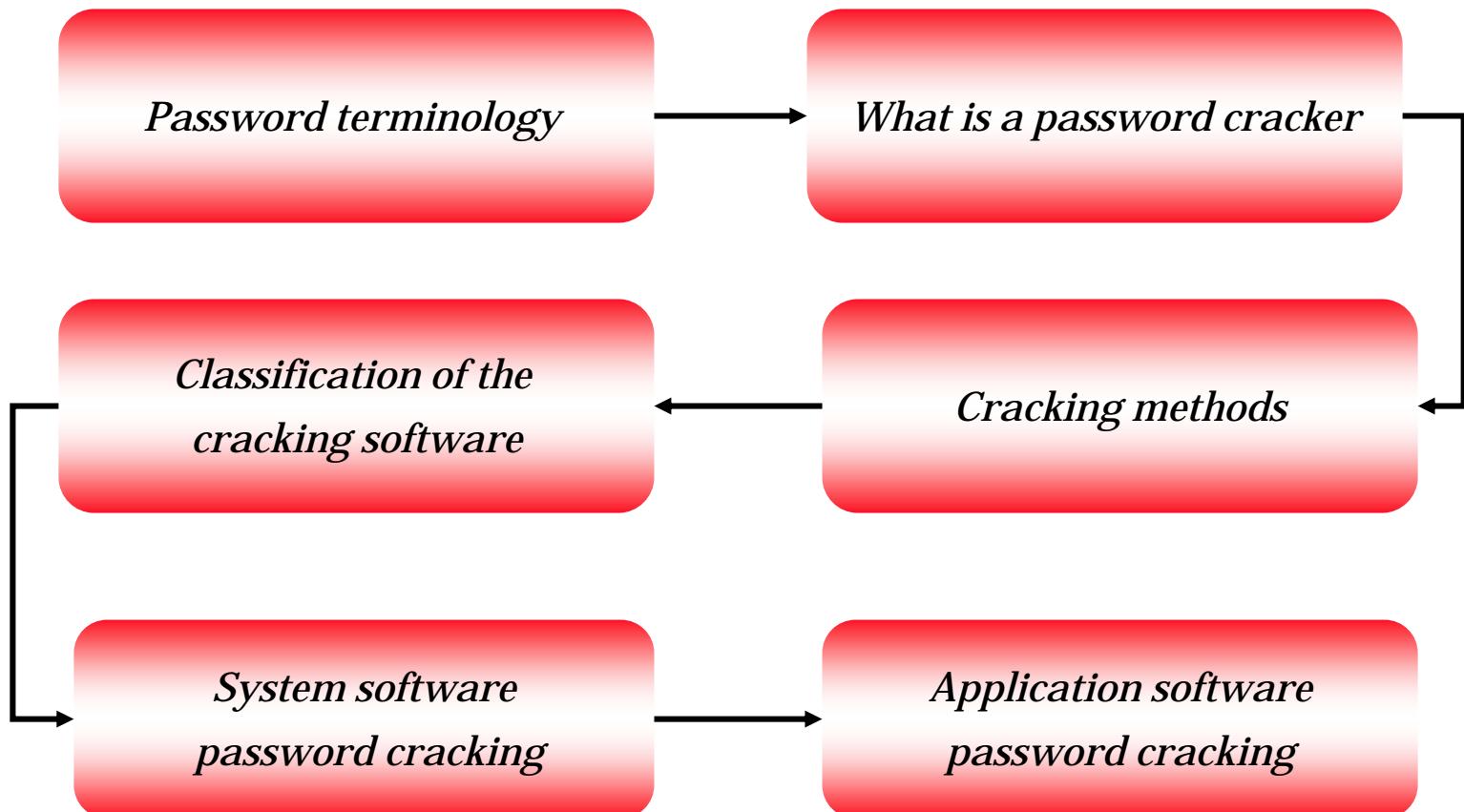
Now the question arises - how the system administrator opened the password protected attachment?



Module Objective

- Password- terminology
- What is a password cracker?
- Various cracking methods
- Classification of cracking softwares
- System software password cracking
- Application software password cracking

Module Flow



Password - Terminology

- ◎ *A secret series of characters that enables a user to access a file, computer, or a program* (www.webopedia.com)
- ◎ Contains an unique string of characters used to restrict access to computers and sensitive files
- ◎ Passwords are of the following types

- Passwords that contain only letters
- Passwords that contain only numbers
- Passwords that contain only special characters
- Passwords that contain letters and numbers
- Passwords that contain only letters and special characters
- Passwords that contain only special characters and numbers
- Passwords that contain letters, special characters and numbers



What Is a Password Cracker?

- ◉ According to the Maximum Security definition “A password cracker is any program that can decrypt passwords or otherwise disable password protection”
- ◉ A password cracker may also be able to identify encrypted passwords. After retrieving the password from the computer's memory, the program may be able to decrypt it
- ◉ Cracking a key means an attempt to recover the key's value
- ◉ Cracking cipher text means an attempt to recover the corresponding plaintext

How Does A Password Cracker Work?

- The wordlist is sent through the encryption process, generally one word at a time
- Rules are applied to the word and, after each such application, the word is again compared to the target password (which is also encrypted)
- If no match occurs, the next word is sent through the process
- In the final stage, if a match occurs, the password is then deemed *cracked*. The plain-text word is then piped to a file

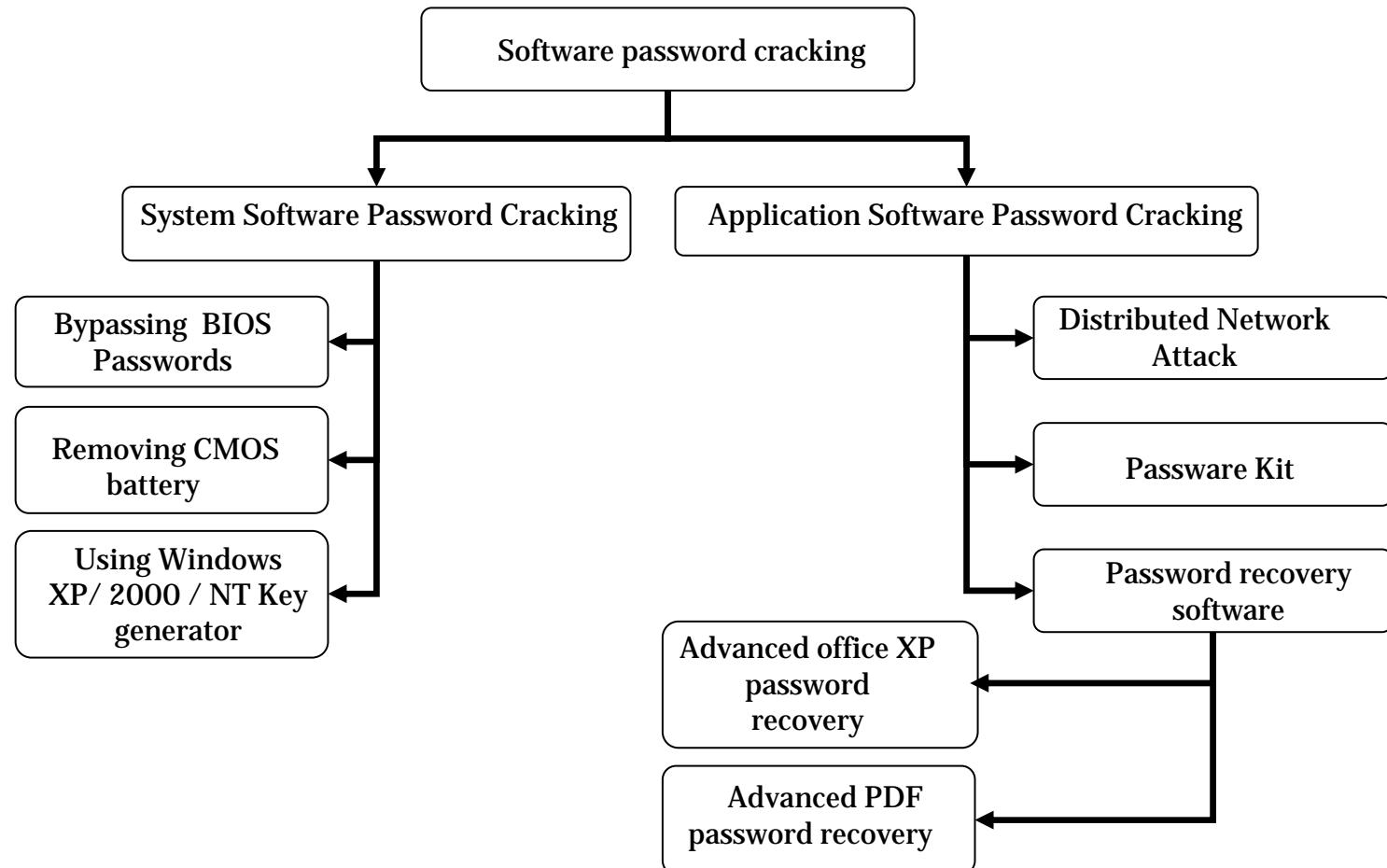


Various Password Cracking Methods

- Brute force attack
- Dictionary attack
- Syllable attack
- Rule-based attack
- Distributed network attack
- Password Guessing



Classification of Cracking Software



System Level Password Cracking

- System software password cracking is defined as

“Cracking passwords of operating system and other utilities that enable the computer to function”

- Following are ways by which, one can access a system

- Bypassing BIOS Passwords
- By removing the CMOS Battery
- Using Windows XP / 2000 / NT Key generator



System Level Password Cracking- I

⦿ Following methods are used to bypass BIOS Passwords

- *Using a manufacturer's backdoor password to access the BIOS*

Few passwords are

ALFAROME	ALLy	aLLy	_award
AWARD PW	AWKWARD	awkward	BIOSTAR

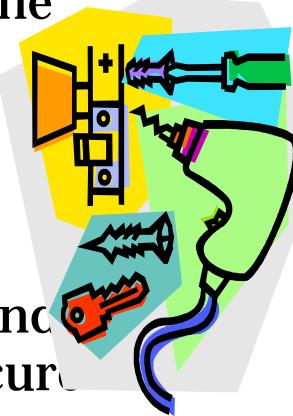
- *Using password cracking tools such as*

- CMOS password recovery tools 3.1
- !BIOS
- RemPass
- KILLCMOS

System Level Password Cracking- II

① Removing the CMOS Battery

- The CMOS settings on most systems are buffered by a small battery that is attached to the motherboard
- Unplug the PC and remove the battery for 10-15 minutes; the CMOS gets reset



② Using Windows XP/2000/NT Key generator

- **Windows XP / 2000 / NT Key** is a program to reset Windows XP / 2000 / NT security if the administrator password, secure boot password or key disk is lost

Application Password Cracking

- ◉ Tools used as application password cracking
 - Password Recovery software
 - Advanced PDF Password Recovery
 - Advanced office XP Password Recovery
 - Distributed Network Attack by AccessData
 - Accent Password Extractor
 - Passware kit

Application Software Password Cracker

① Password recovery software

- **Advanced office XP password cracker**

“Advanced Office XP Password Recovery (or AOXPPR for short) is a program to recover the lost or forgotten passwords to the files/documents created in the following applications (all versions up to 2002/XP)”

- *Advanced PDF Password Recovery*

It is a tool to recover protected Adobe Acrobat PDF files, which have "owner" password set, preventing the file from editing, printing, selecting text and graphics or adding/changed annotations and form fields (in any combination)

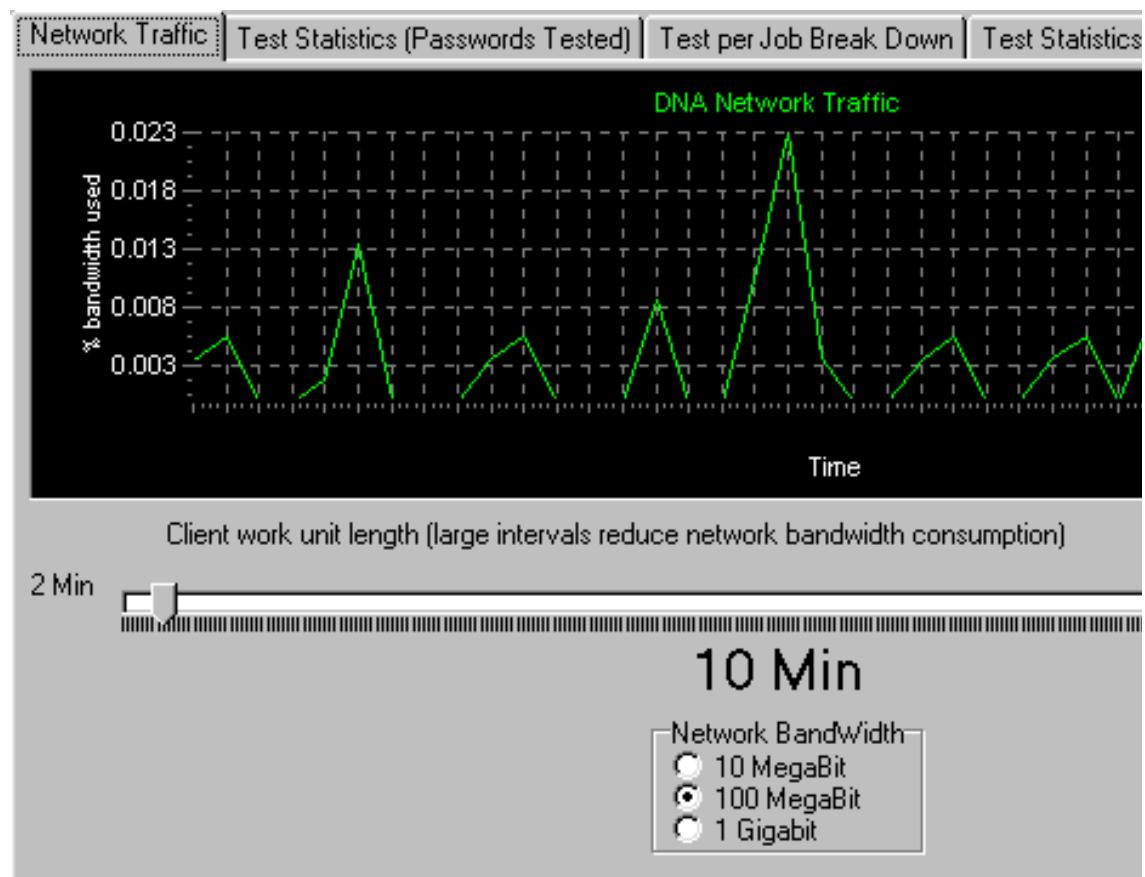


Distributed Network Attack-I

- The DNA Manager is installed in a central location where machines running DNA Client can access it over the network
- DNA Manager coordinates the attack, assigning small portions of the key search to machines distributed throughout the network
- DNA Client will run in the background, consuming only unused processor time
- The program uses the combined processing capabilities of all the attached clients to perform an exhaustive key search on Office '97 and Office 2000 encrypted documents in order to decrypt the file

Distributed Network Attack-II

Time estimated



Microsoft Word/Excel (One machine would require 56 days maximum)

DNA Configuration	Maximum Time	Average
5 Client Network	11 days	5 ½ days
10 Client Network	5 ½ days	2 ¾ days
25 Client Network	2 ½ days	1 ¼ days
50 Client Network	1 ¼ days	½ days
100 Client Network	12 hours	6 hours
1,000 Client Network	1 hour 12 minutes	36 minutes

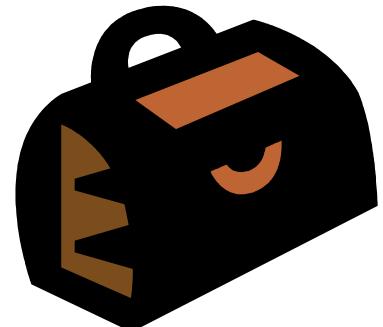
Adobe Acrobat PDF (One machine would require 40 days maximum)

DNA Configuration	Maximum Time	Average
5 Client Network	8 days	4 days
10 Client Network	4 days	2 days
25 Client Network	1 ½ days	20 hours
50 Client Network	20 hours	10 hours
100 Client Network	10 hours	5 hours
1,000 Client Network	1 hour	30 minutes

Note: These calculations are based on 500 MHz, Intel® machines.

Passware Kit

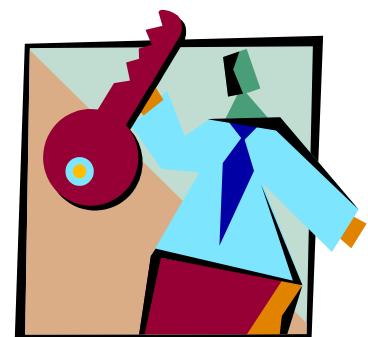
- Passware kit combines over 25 password recovery programs in one single package
- Passware kit can crack passwords from the following applications



Office	Excel	Word
Windows XP/2000/NT	Access	Outlook
Outlook Express	Exchange	WinZip PKZip ZIP
WinRAR RAR	VBA Visual Basic modules	Internet Explorer
FileMaker	Acrobat	Quicken
QuickBooks	Lotus 1-2-3	Lotus Notes
Lotus Organizer	Lotus WordPro	Quattro Pro
Backup	Project	MYOB
Peachtree	Paradox	ACT!
Mail	Schedule+	Money
WordPerfect		

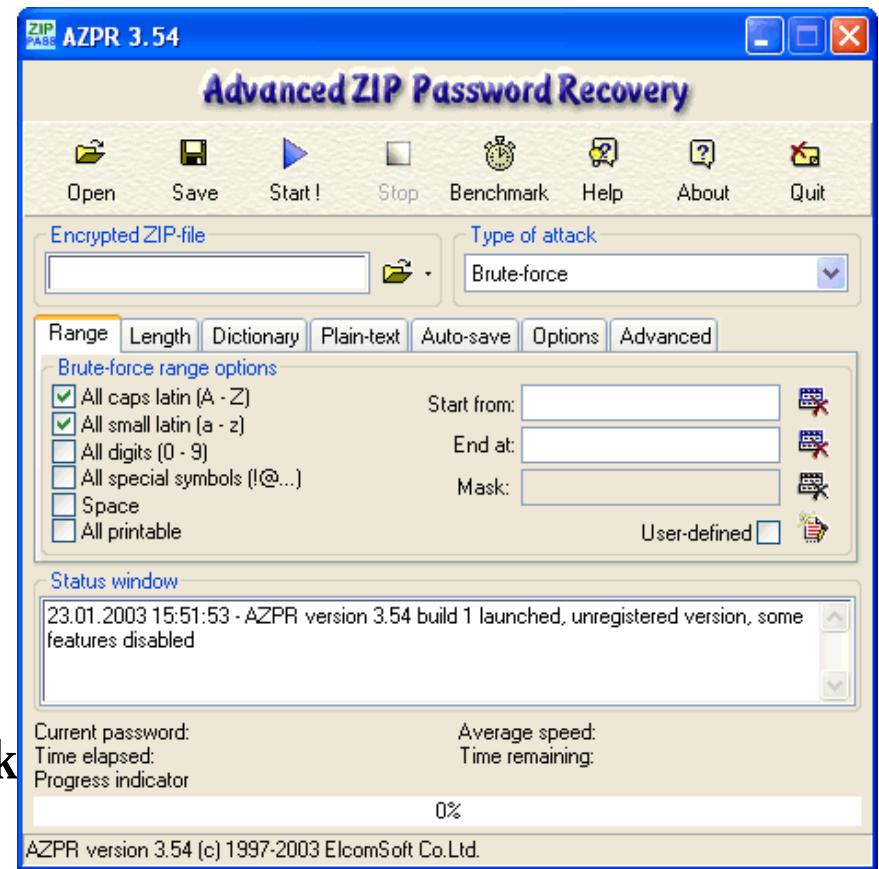
Accent Keyword Extractor

- ◉ Accent Keyword Extractor uses dictionary attack method
- ◉ The program loads a page from the Internet, extracts all unique words found on that page and adds them to the dictionary
- ◉ Then it follows all links found on the page and extracts words from the linked pages as well



Advanced Zip Password Recovery

- This program is utilized to crack password protected zip files
- Available methods for cracking are brute force attack, dictionary attack, and plaintext attack
- This utility can be customized according to password length, character set and more
- Supports self-extracting archives
- It is very fast and effective but works only with archives containing only one encrypted file



Default Password Database

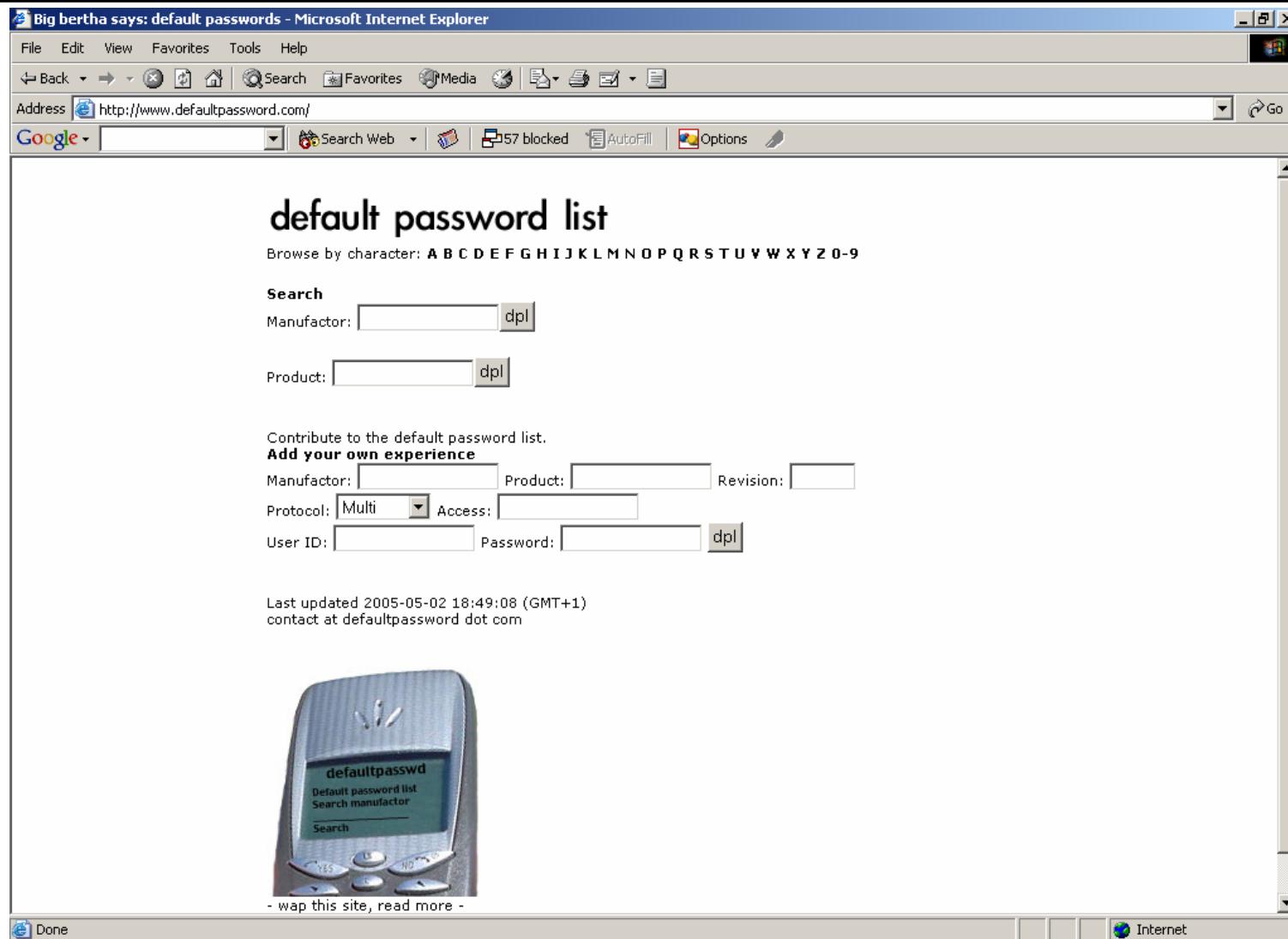
- Default password database provides
 - list of vendors, and certain information related to respective product such as protocols used, user names, passwords, access and validation of passwords
- Below listed are the few default password database
 - <http://phenoelit.darklab.org/>
 - <http://www.defaultpassword.com/>
 - <http://www.cirt.net/cgi-bin/passwd.pl>

<http://phenoelit.darklab.org/>

The screenshot shows a Microsoft Internet Explorer window with the title "Default Password List - Submit - Microsoft Internet Explorer". The address bar contains the URL "http://phenoelit.darklab.org/cgi-bin/display.pl?SUBF=list&SORT=1". The main content is titled "Default Password List" and includes a search bar and a "Submit Query" button. Below is a table listing default passwords for various 3COM products.

INDEX	Manufactor	Product	Revision	Protocol	User ID	Password
1	3COM	CoreBuilder	7000/6000/3500/2500	Telnet	debug	synnet
2	3COM	CoreBuilder	7000/6000/3500/2500	Telnet	tech	tech
3	3COM	HiPerARC	v4.1.x	Telnet	adm	(none)
4	3COM	LANplex	2500	Telnet	debug	synnet
5	3COM	LANplex	2500	Telnet	tech	tech
6	3COM	LinkSwitch	2000/2700	Telnet	tech	tech
7	3COM	NetBuilder		SNMP		ANYCON
8	3COM	NetBuilder		SNMP		ILMI
9	3COM	Office Connect ISDN Routers	5x0	Telnet	n/a	PASSWOR
10	3COM	SuperStack II Switch	2200	Telnet	debug	synnet

<http://www.defaultpassword.com/>



http://www.cirt.net/cgi-bin/passwd.pl

The screenshot shows a Microsoft Internet Explorer window displaying the CIRT.net website. The address bar shows the URL <http://www.cirt.net/cgi-bin/passwd.pl>. The main content area features the CIRT.net logo and the tagline "Suspicion Breeds Confidence". On the left, there is a sidebar with several menu items under categories: Data, Code, Advisories, and Misc. The "Data" category includes links for Default Passwords, Default Wireless SSIDs, Default Port List, and Scnru Security Search. The "Code" category includes links for Nikto Web Scanner, Nessus Plugins, SETI-Web, and More... The "Advisories" category includes links for Cyclades Console Connect, Cyclades Info Disclosure, Cyclades Priv Escalation, MySQL Eventum Backdoor, MySQL Eventum XSS, EW FileManager Retrieval, cPanel File Retrieval, and cPanel XSS, along with a More... link. The "Misc" category includes links for Latest News, Press, Links/Amigos, Donate, and Nikto Loot!. The central content area is titled "Default Passwords" and describes it as "Default IDs and Passwords in Vendor Products". It features a search bar for "Search Default Passwords" and buttons for "Search Passwords", "CSV Export", and "Add/Update DB". Below this, a list of 279 vendors and 1413 passwords is displayed, with the first few entries being 360 Systems, Acer, Adtech, AirLink Plus, Alcatel, Allot, Amtron, APC, Asante, and A....

Password Cracking Tools List

- Access PassView:
 - reveals the database password of every password-protected mdb file
- AIM-Recover:
 - recover AOL instant messenger passwords
- Asterisk Logger:
 - reveal the passwords stored behind the asterisks
- Basic Authentication:
 - verifies the user name, password and other details
- Brutus:
 - remote password cracker
- Crackit!:
 - recovers Word/Excel password for opening by brute-force attack
- DeBat:
 - recovers passwords for e-mail program
- Dialupass:
 - enumerates all Dial-Up entries on your computer and reveals their logon details
- Enterprise Manager PassView:
 - enumerates all servers registered in your Enterprise Manager, and reveals the login details stored in the system

Password Cracking Tools List

◎ Magical Jelly Bean Keyfinder:

- retrieves your Product Key (cd key) used to install windows and MS Office from the registry

◎ Mail PassView:

- displays the details of email accounts

◎ Messenger Key:

- recovers passwords for Mirabilis ICQ UINs

◎ MessenPass:

- reveals the passwords for some of the instant messengers

◎ Netscape Passwords:

- reveal the stored POP3 server and web site password

◎ Outlooker:

- displays information about all email accounts from Outlook Express

◎ PasswordsPro:

- MD5 hashes password recovery

◎ PCAnywhere PassView:

- reveals the passwords stored in PCAnywhere items

◎ Protected Storage View:

- reveals the passwords stored on your computer by Internet Explorer, Outlook Express and POP3 accounts of MS-Outlook

Password Cracking Tools List

- Getkey for Zip:

- recover the lost or forgotten passwords for password-encrypted zip files

- GetPass:

- decrypts Cisco IOS Passwords

- Keyfinder PE:

- extract the installation key for 2000/XP

- Lepton's Crack:

- password cracking engine and development laboratory

- RockXP:

- retrieve and change XP key

- Share Password Checker:

- obtains the passwords on the network

- Win 9x PassView:

- reveals the passwords stored on computer by Windows 95/98 operating system

- Xpass:

- reveals the passwords stored behind the asterisks

Summary

- Password is a secret series of characters created to secure important files from unauthorized access
- Cracking is a way to escalate security of the program or a system
- Various cracking methods like brute force, dictionary attack, syllable attack, rule-based attack, distributed network attack and guessing are used
- Password cracking software are classified into system software password cracking and application software password cracking



Computer Hacking Forensic Investigator

Module XVI
Investigating Logs

Scenario

Xsecurity.com receives several reports from customers about unauthorized orders on their accounts.

They suspect that someone has compromised their web-based ordering system so they gather the log files from several different IIS web servers.

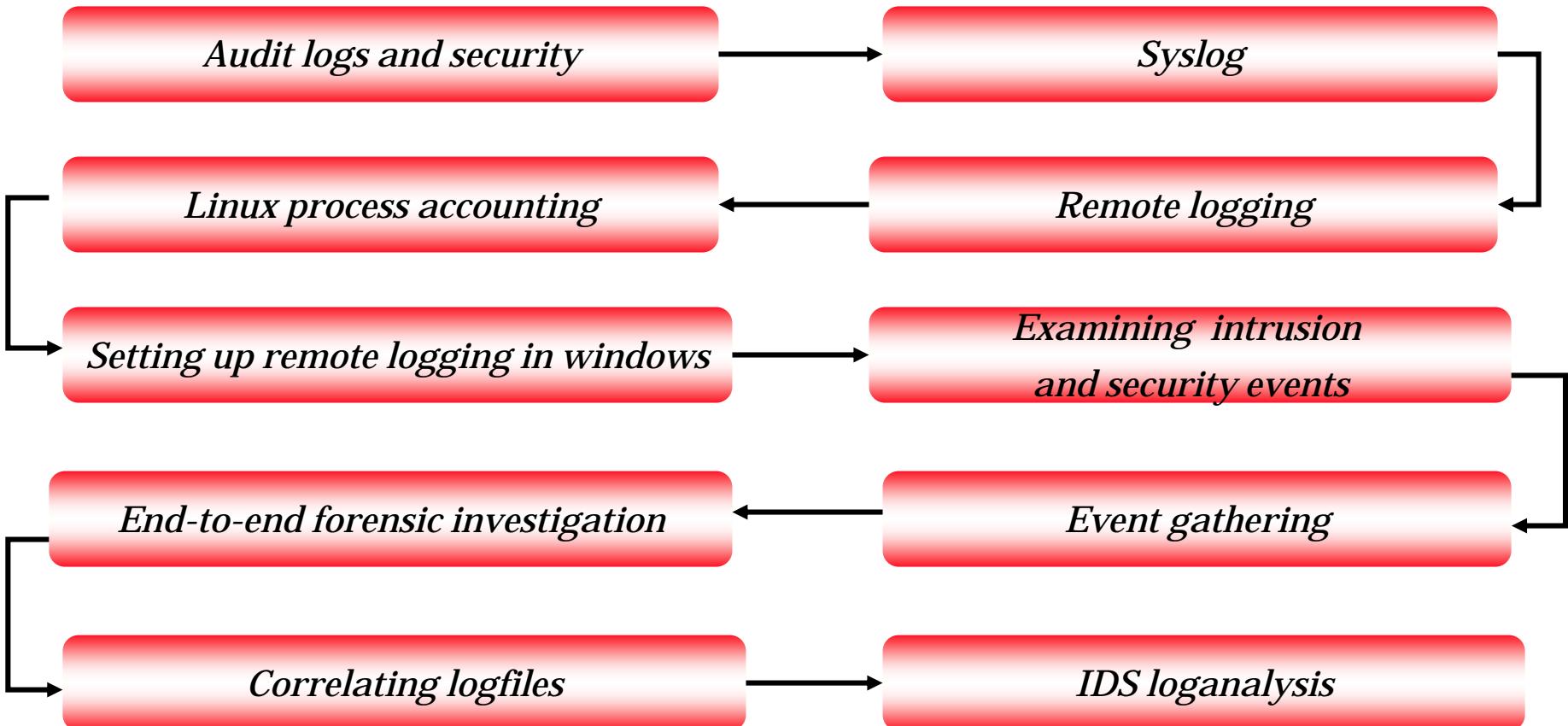
Searching for activity from log files, IP addresses in the log files turns up with nothing. Tracking down the flaw and IP addresses used by the suspect seems impossible.



Module Objective

- ◉ Audit logs and security
- ◉ Syslog
- ◉ Remote logging
- ◉ Linux process accounting
- ◉ Setting up remote logging in windows
- ◉ Examining intrusion and security events
- ◉ Event gathering
- ◉ End-to-end forensic investigation
- ◉ Correlating logfiles
- ◉ IDS loganalysis

Module Flow



Audit Logs and Security

- Audit data provide the critical information after break-in
- Make the audit secure to prevent the attacker from altering the audit log data
- An audit policy defines the types of security events
- Configure the logfile to record maximum amount of data



Audit Incidents

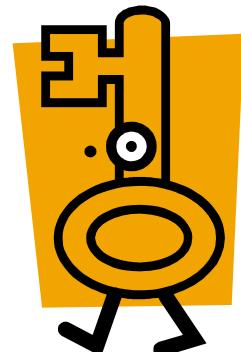
- Audit events can be split into two categories:

- **Success events**

- A success event indicates successful access gained by the user

- **Failure events**

- A failure event indicates the unsuccessful attempt made to gain access to a resource



Syslog

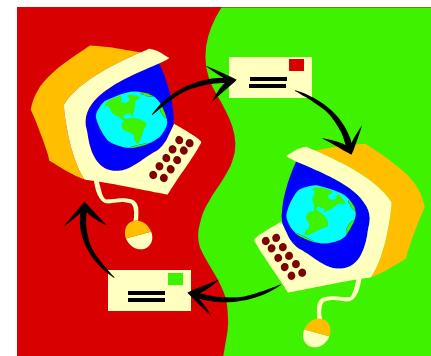
- Syslog is the heart of Linux logging
- Syslog is controlled through the configuration file `/etc/syslog.conf`
- To log all messages to a file, replace the selector and action fields with the wildcard *:
`*.* /var/log/syslog`
- Configure syslog to log all authorize messages with a priority of lower or higher to the `/var/log/syslog`



Remote Logging

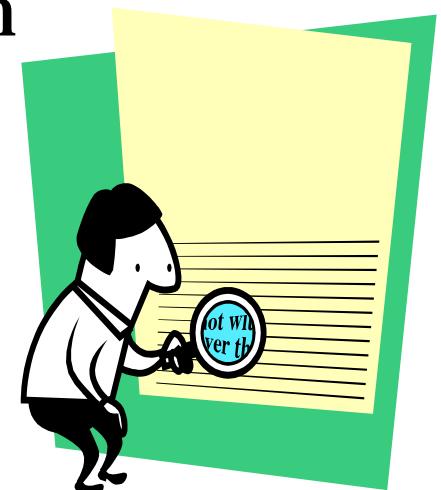
- Create a central syslog server that accepts incoming syslog messages
- Configure to listen on UDP port **514**
- Run *syslogd* with **-r** option
- Configure other servers to log their message to this server
- Modify the action field in the **syslog.conf** file as below

Auth.* @10.0.0.2



Linux Process Accounting

- Process accounting tracks the commands that each user executes
- The **process tracking logfile** is found at */var/adm*, */var/log* or */usr/adm*
- The **tracked files** can be viewed with *lastcomm* command
- Enable process tracking by *accton* command or the startup (*/usr/lib/acct/startup*)



Configuring Windows Logging

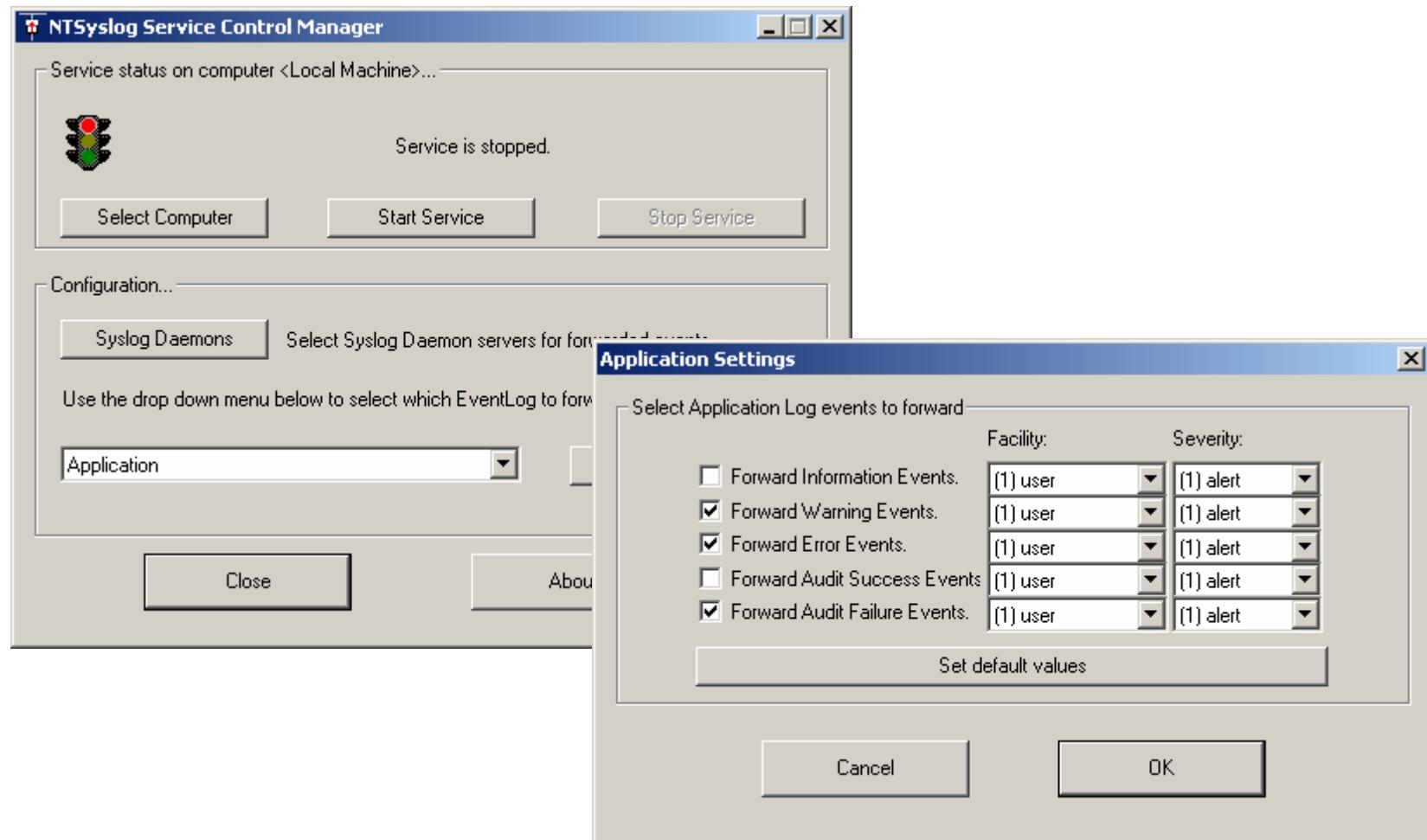
Local Security Settings			
Action	View		
Tree	Policy	Local Setting	Effective Setting
	Audit account logon events	Success, Failure	Success, Failure
	Audit account management	Success, Failure	Success, Failure
	Audit directory service access	Success, Failure	Success, Failure
	Audit logon events	Success, Failure	Success, Failure
	Audit object access	Success, Failure	Success, Failure
	Audit policy change	Success, Failure	Success, Failure
	Audit privilege use	Success, Failure	Success, Failure
	Audit process tracking	Success, Failure	Success, Failure
	Audit system events	Success, Failure	Success, Failure

Setting up Remote Logging in Windows

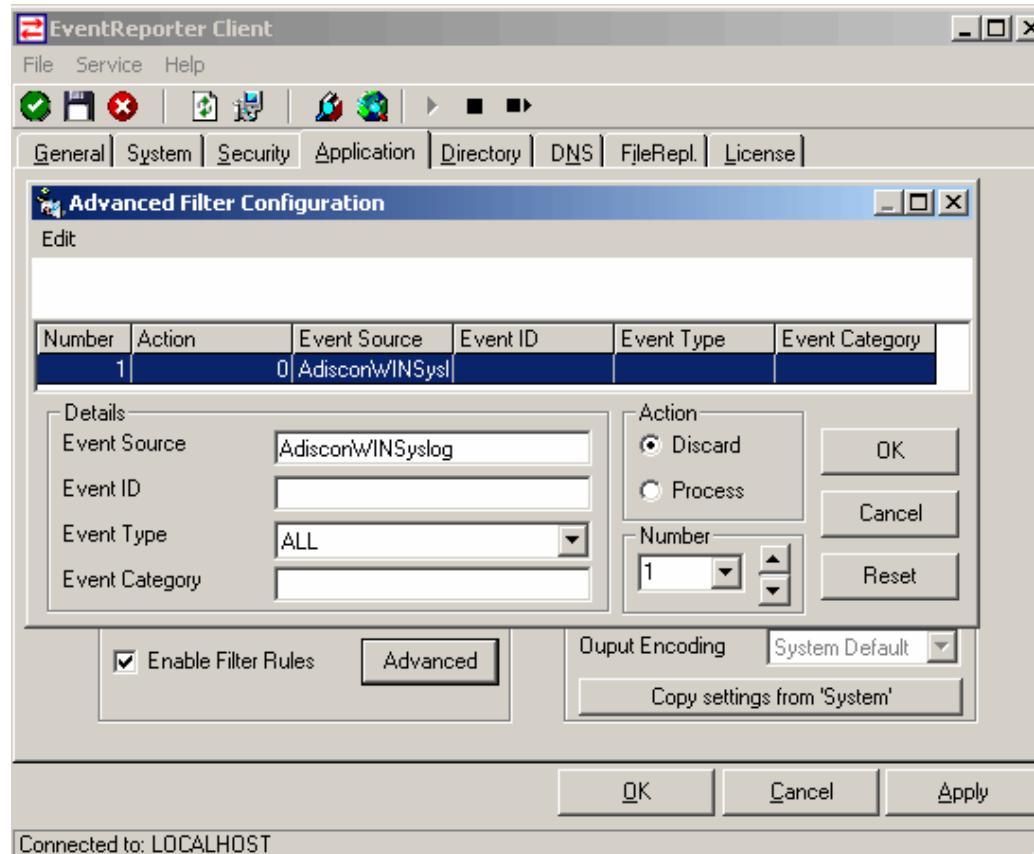
- Deleting `c:\winnt\system32\config*.evt` could erase the event-tracking logs
- Windows does not support remote logging unlike Linux
- NTSyslog enable remote logging in Windows



Ntsyslog



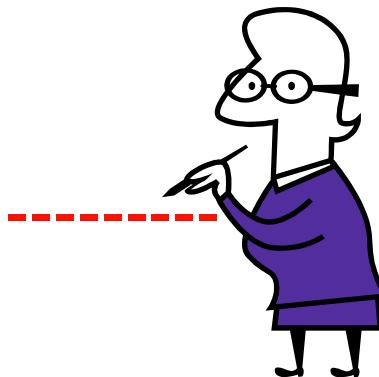
Eventreporter



- Centralized logging tool for Windows
- Automatically monitors the event logs
- Detects system hardware and software failures

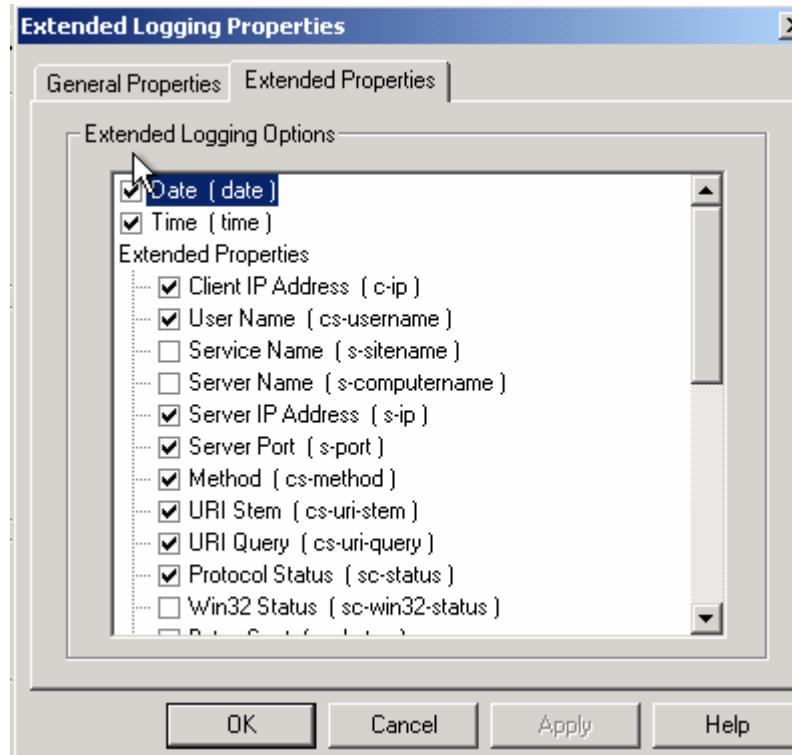
Application Logs

- Log messages to a file that only the administrator can access
- Log messages to a secure remote log host
- Log as much useful information as possible
- Log IP addresses rather than NetBIOS or domain names



Extended Logging in IIS Server

- Enable extended logging in IIS Servers



Examining Intrusion and Security Events

- Monitoring for intrusion and security events includes both passive and active tasks
- Inspection of log files reveal the intrusion or attack made to the system by attacker
- Intrusions detected after the attack are known as passive intrusion detection
- Many intrusions are detected as soon as the attack takes place; such intrusions come under active intrusion detection



Significance of Synchronized Time

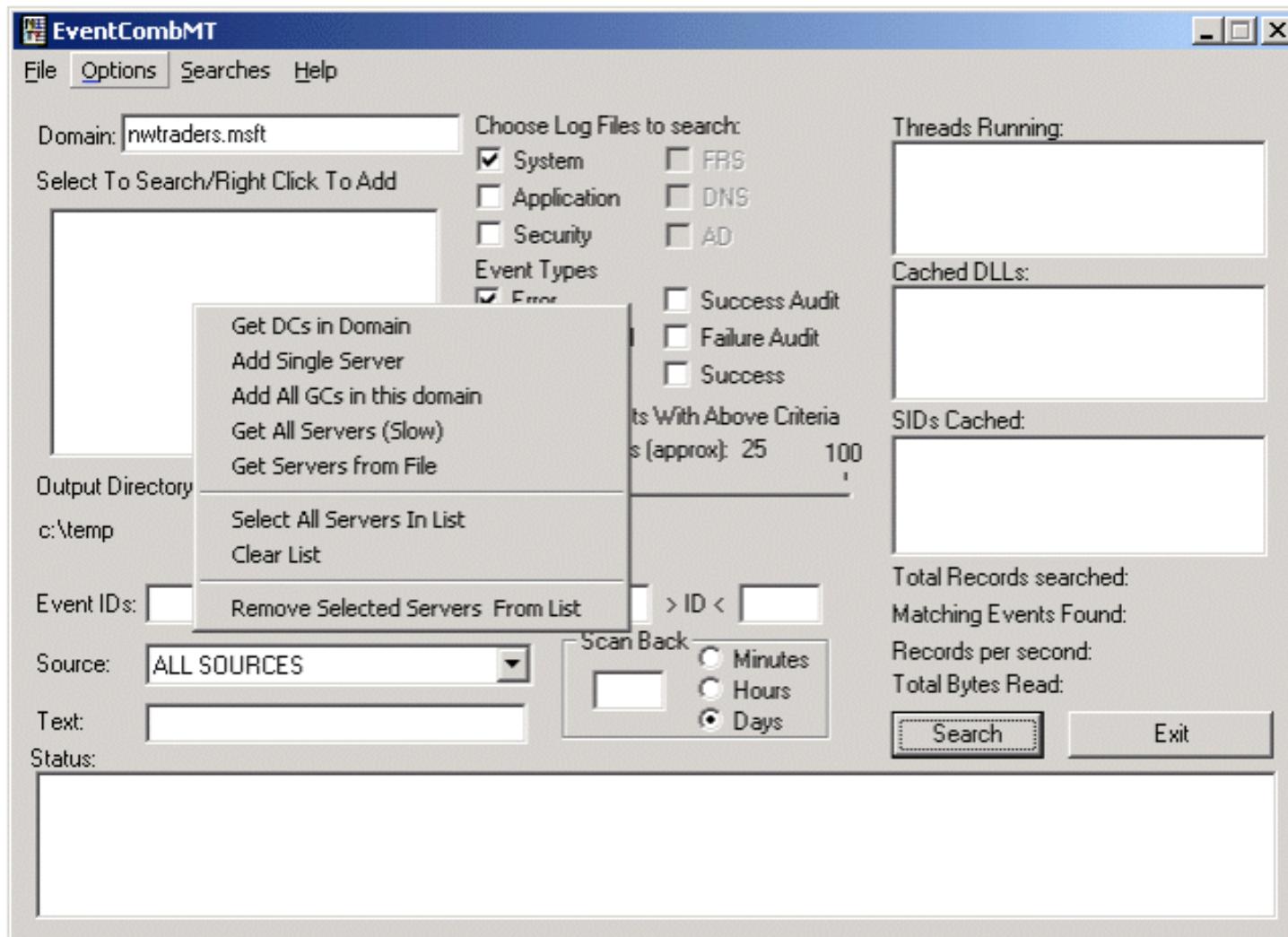
- Synchronize the computers' clocks
- Makes reconstruction and reviewing of the attack easy
- Without synchronized time, determination of relationship between events become difficult



Event Gathering

- ◉ Motive behind auditing is to identify the actions taken by the intruder
- ◉ To understand the extent of any attack, coordinating and consolidating information from many computers is must
- ◉ Importing of log utilities into a database can make it easy to coordinate the information from multiple logs
- ◉ Dump Event Log serve the purpose as it export any of the event logs to delimited text from the command line

Eventcombmt



Writing Scripts

- Scripts can be written that collect event log information from remote computers and store it in a central location
- By using scripting, one can choose when to run the scripts using Scheduled Tasks and what actions to take once the event log is successfully copied to the central location



Event Gathering Tools

- **Event Log Monitor** — automates a variety of the administrative functions required for monitoring and managing event logs, log files, SNMP traps and syslog messages
- **Event Archiver** — makes it easy to backup and clear event logs automatically on remote machines
- **LogCaster** — has centralized management console which monitor and manage system availability and performance around the clock

Forensic Tool: Fwanalog

- ◉ fwanalog is a shell script
- ◉ It parses and summarizes firewall log files
- ◉ Analog is used for creating the reports



End-to End Forensic Investigation

- **The end-to-end concept** - trails the whole incident – how the attack begins, which are the intermediate devices through which it pass and who was the victim
- **Location of evidence** - logs, firewall, internetworking devices and files
- **Pitfalls of network evidence collection** - Evidence can be lost in few seconds during log analysis because logs change rapidly
- **Event analysis** - picking out the useful information from various sources and correlating them

Correlating Log Files

Case Study: Log Analysis of Red Hat Linux 6.2 Server

```
=====
Nov 08 00 06:25:53      2836 .a. -r-xr-xr-x root      root      /t/usr/bin/uptime
Nov 08 00 06:26:15          0 m.c -rw-r--r-- root      root      /t/etc/hosts.deny
Nov 08 00 06:26:51      1024 .a. drwxr-xr-x root      root      /t/etc/rc.d/init.d
Nov 08 00 06:29:27      63728 .a. -rwxr-xr-x root      root      /t/usr/bin/ftp
Nov 08 00 06:33:42      1024 .a. drwx----- daemon    daemon   /t/var/spool/at
Nov 08 00 06:45:18          161 .a. -rw-r--r-- root      root      /t/etc/hosts.allow
                           0 .a. -rw-r--r-- root      root      /t/etc/hosts.deny
Nov 08 00 06:45:19          63 .a. -rw-r--r-- root      root      /t/etc/issue.net
Nov 08 00 06:45:24      1504 .a. -rw-r--r-- root      root      /t/etc/security/console.perms
Nov 08 00 06:51:37  2129920 m.. -rw-r--r-- drosen    drosen   <honeypot.hda8.dd-dead-8133>
=====
```

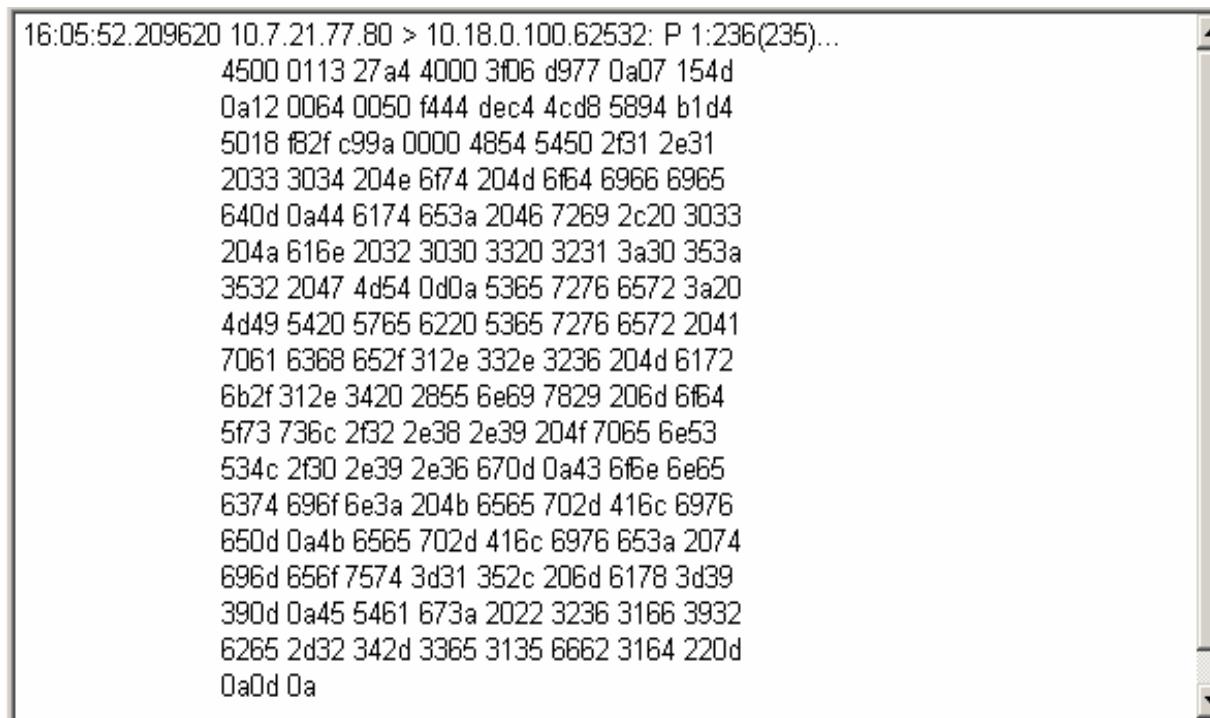
Code is discussed below in the notes

For more information:

<http://honeynet.org/challenge/results/dittrich/evidence.txt>

Investigating Tcpdump

- ◉ Tcpdump is a program which is used for monitoring the network traffic



A screenshot of a terminal window displaying network traffic captured by Tcpdump. The output shows several lines of hex and ASCII data, indicating a single TCP connection between two hosts. The connection ID (P) is 1:236(235), and the sequence numbers range from 4500 to 6265.

```
16:05:52.209620 10.7.21.77.80 > 10.18.0.100.62532: P 1:236(235)...
4500 0113 27a4 4000 3f06 d977 0a07 154d
0a12 0064 0050 f444 dec4 4cd8 5894 b1d4
5018 f82f c99a 0000 4854 5450 2f31 2e31
2033 3034 204e 6f74 204d 6f64 6966 6965
640d 0a44 6174 653a 2046 7269 2c20 3033
204a 616e 2032 3030 3320 3231 3a30 353a
3532 2047 4d54 0d0a 5365 7276 6572 3a20
4d49 5420 5765 6220 5365 7276 6572 2041
7061 6368 652f 312e 332e 3236 204d 6172
6b2f 312e 3420 2855 6e69 7829 206d 6f64
5f73 736c 2f32 2e38 2e39 204f 7065 6e53
534c 2f30 2e39 2e36 670d 0a43 6f6e 6e65
6374 696f 6e3a 204b 6565 702d 416c 6976
650d 0a4b 6565 702d 416c 6976 653a 2074
696d 656f 7574 3d31 352c 206d 6178 3d39
390d 0a45 5461 673a 2022 3236 3166 3932
6265 2d32 342d 3365 3135 6662 3164 220d
0a0d 0a
```

IDS Loganalyais:realsecure

- ◉ RealSecure monitors the security events and also make changes to the system in real-time
- ◉ It is comprised following elements:
 - Network Sensors – monitors traffic
 - OS Sensors – monitors the server
 - Console – defines the policies

IDS Loganalysis :SNORT

- Snort is an open source network intrusion detection system capable of performing real-time traffic analysis, and packet logging of IP networks
- It can perform protocol analysis, content searching/matching
- Used to detect a variety of attacks and probes, such as: buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts

Summary

- Audit data provide the critical information after the break-in
- An audit policy defines the types of security events
- Monitoring for intrusion and security events includes both passive and active tasks
- Log analysis and correlation is collecting the useful information from the logs and correlating them to get the whole picture



Computer Hacking Forensic Investigator

Investigating Network Traffic
Module XVII

Scenario

Jessica was missing from her home for a week. She left a note for her father mentioning that she was going to meet her school friend. Few weeks later Jessica's dead body was found near a dumping ground.

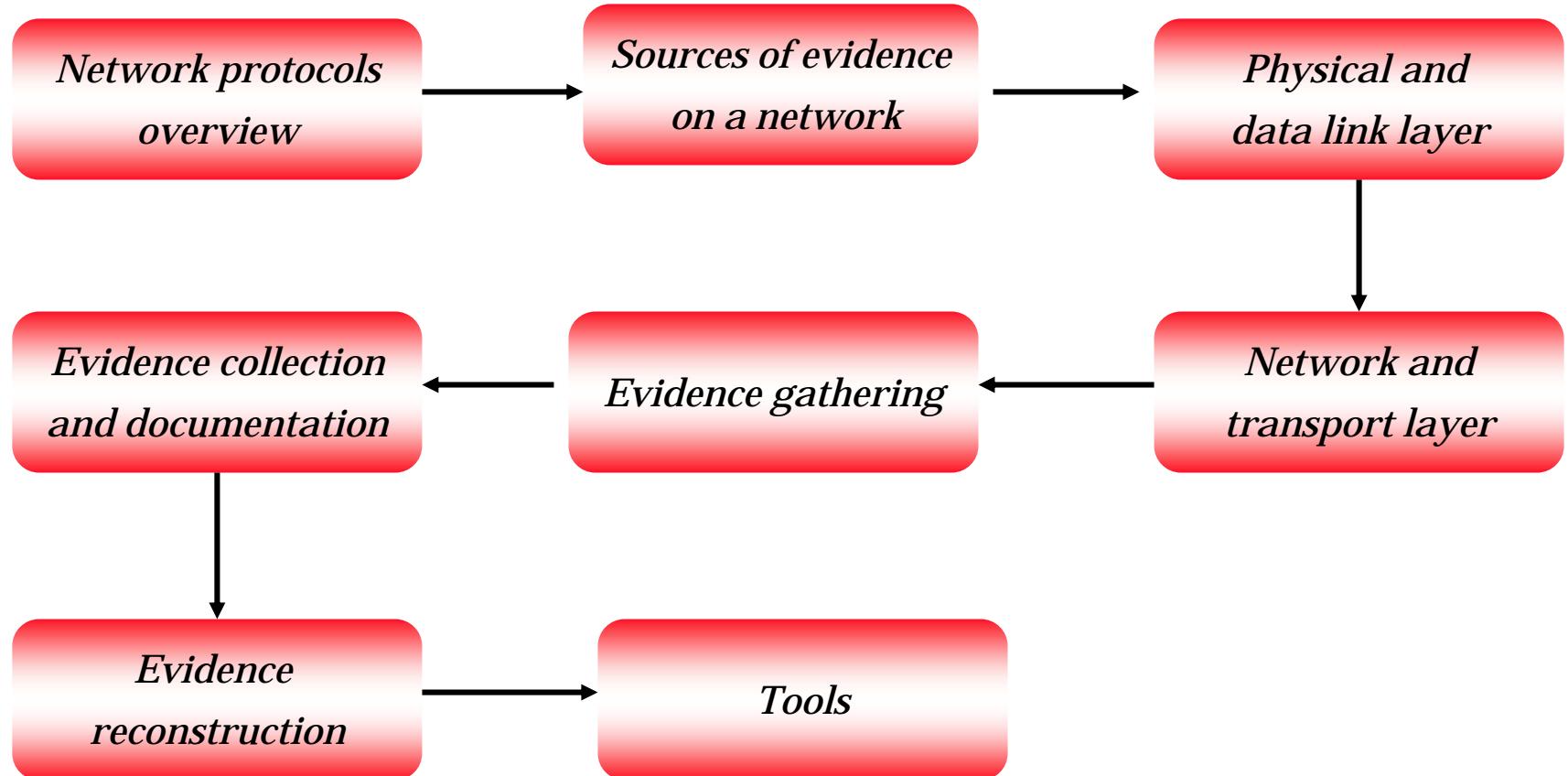
Investigators were called in to reveal the mystery that surrounded Jessica's death. Preliminary investigation of Jessica's computer and logs revealed some facts which helped the cops trace the killer.



Module Objective

- Overview of network protocols
- Sources of evidence on a network
- Physical and data-link layer of the OSI model
- Evidence gathering at the physical and data link layer
- Network and transport layer of the OSI model
- Evidence gathering at the network and transport layer
- Evidence collection and documentation on a network
- Gathering evidence on a network
- Documenting the gathered evidence on a network
- Evidence reconstruction for investigation
- Tools

Module Flow



Overview of Network Protocols

Layers

Protocols

Application layer

HTTP, SMTP, NNTP

Presentation layer

**TELNET, FTP, SNMP,
TFTP**

Session layer

Transport layer

UDP, TCP

Network layer

ARP, RARP, ICMP,IGMP, IP

Data-link layer

PPP, SLIP

Sources of Evidence on a Network

⦿ Following are the few sources on a network where the digital evidence resides:

- IDS logs
- Router logs
- Firewall logs
- Switch logs
- Application Server logs



Overview of Physical and Data-link Layer of the OSI Model

○ Physical layer:

- It helps in transmitting data bits over a physical channel
- It has a set of predefined rules that physical devices and interfaces on a network have to follow for data transmission to take place

○ Data-link layer:

- The data-link layer is responsible for communication between computers that are nearby
- It controls error in transmission by adding a trailer to the end of the data frame

Evidence Gathering at the Physical Layer

- Sniffers , which put NICs in promiscuous mode are used to collect digital evidence at the physical layer
- SPANned ports, hardware taps help sniffing in a switched network
- Sniffers collect traffic from the network and transport layers other than the physical and data-link layer.
- Investigators should configure sniffers for the size of frames to be captured
- The default size of frame that some sniffers capture is 68 bytes of Ethernet frame
- It is advisable to configure sniffers to collect Ethernet frames of size 65535 bytes

Evidence Gathering at the Physical Layer

- The de facto standard of saving the gathered data from the network is in a tcpdump file with “*.dump” extension
- Following is the command for saving the captured data packets using Windump as a sniffer:

C:\Windump -w filename.dmp

The packets are stored in the C drive with the filename. The packets can be analyzed by using a notepad

C:\Windump -w filename.dmp -s 65535

The above command can be used to specify the size of the Ethernet packet to be captured

Tool: Windump

- WinDump is the porting to the Windows platform of tcpdump, the most used network sniffer/analyzer for UNIX
- Given below is the output obtained from Windump

```
20:50:00.037087 IP (tos 0x0, ttl 128, id 2572, len 46)  192.168.2.24.1036 >
64.12.24.42.5190: P [tcp sum ok] 157351:157357(6) ack 2475757024 win 8767 (DF)
```

The above entry can be deciphered as:

timestamp → 20:50:00.037087

IP [protocol header] → tos 0x0, ttl 128, id 2572, len 46

source IP:port → 192.168.2.24.1036

destination IP:port → 64.12.24.42.5190:

P [push flag] [tcp sum ok] → 157351:157357

[sequence numbers] (6) [bytes of data]

acknowledgement and sequence number → ack 2475757024

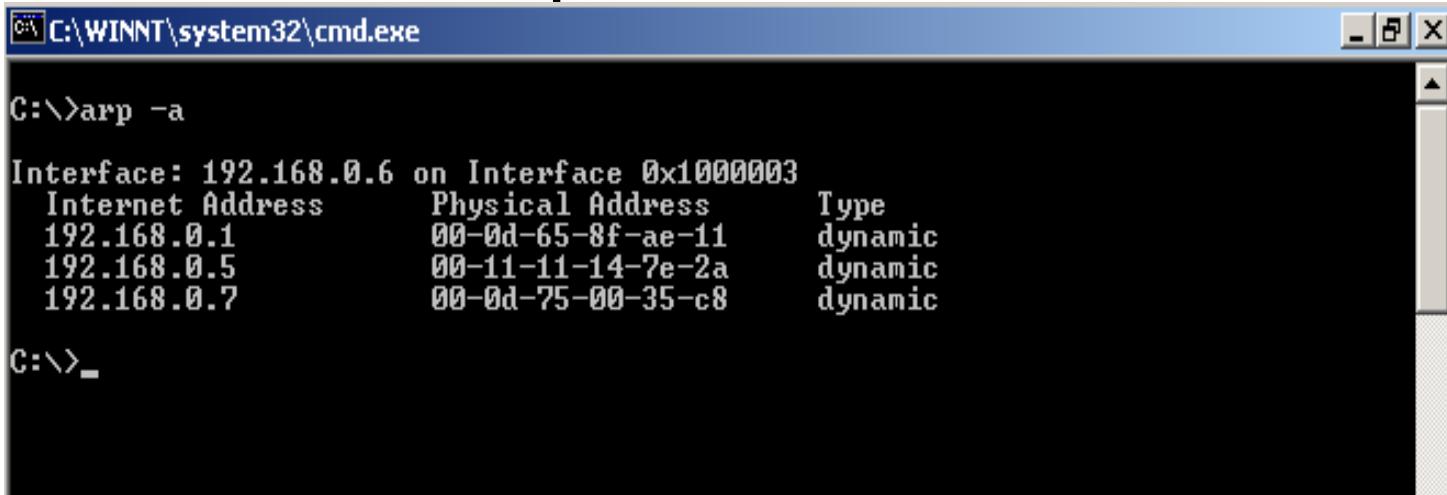
window size (DF) [don't fragment set] → win 8767

Tool: Windump

```
C:\WINNT\System32\cmd.exe - windump -n -vv
C:\>windump -n -vv
windump: listening on \Device\NPF_{F036ABE8-53D7-4C7B-B2E4-082BEF4D72D8}
19:56:53.427131 IP <tos 0x88, ttl 106, id 58655, len 108> 68.193.110.230.5000 >
192.168.2.162.5000: udp 80
19:56:53.493683 IP <tos 0x88, ttl 106, id 58656, len 108> 68.193.110.230.5000 >
192.168.2.162.5000: udp 80
19:56:53.506094 IP <tos 0x88, ttl 43, id 46880, len 40> 64.4.26.250.80 > 192.168
.2.69.2446: . [tcp sum ok] 894239202:894239202(0) ack 4229117801 win 17520
19:56:53.506528 IP <tos 0x88, ttl 43, id 46881, len 510> 64.4.26.250.80 > 192.16
8.2.69.2446: P 894239202:894239672(470) ack 4229117801 win 17520
19:56:53.508241 IP <tos 0x88, ttl 43, id 46882, len 576> 64.4.26.250.80 > 192.16
8.2.69.2446: . 894239672:894240208(536) ack 4229117801 win 17520
19:56:53.508465 IP <tos 0x0, ttl 128, id 19205, len 40> 192.168.2.69.2446 > 64.4
.26.250.80: . [tcp sum ok] 4229117801:4229117801(0) ack 894240208 win 16514 (DF)
19:56:53.508602 IP <tos 0x88, ttl 43, id 46883, len 106> 64.4.26.250.80 > 192.16
8.2.69.2446: . 894240208:894240274(66) ack 4229117801 win 17520
19:56:53.527161 IP <tos 0x88, ttl 107, id 30218, len 1500> 68.58.11.235.2824 > 1
92.168.2.69.2443: . 47592813:47594273(1460) ack 4228398193 win 8359 (DF)
19:56:53.538245 IP <tos 0x88, ttl 106, id 58657, len 108> 68.193.110.230.5000 >
192.168.2.162.5000: udp 80
19:56:53.580115 IP <tos 0x88, ttl 243, id 39962, len 40> 202.87.41.115.80 > 192.
168.2.129.2549: F [tcp sum ok] 3461109112:3461109112(0) ack 6724698 win 8760 (DF)
>
```

Evidence Gathering at the Data-link Layer

- MAC address , a part of the data-link layer is associated with the hardware of a computer
- The ARP table of a router comes handy for investigating network attacks as the table contains IP addresses associated with the respective MAC addresses
- ARP table can be seen using the given command in Windows OS c:\arp -a



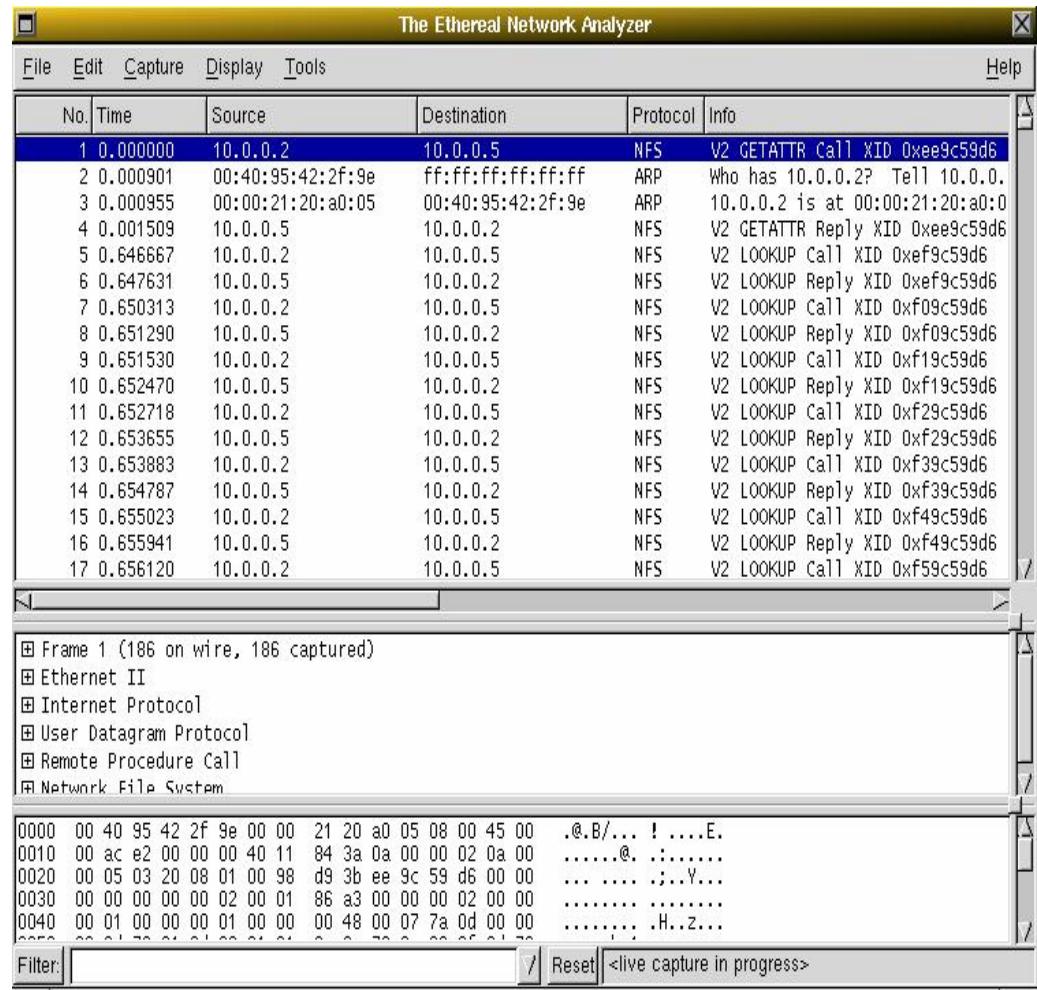
```
C:\WINNT\system32\cmd.exe
C:\>arp -a
Interface: 192.168.0.6 on Interface 0x10000003
  Internet Address      Physical Address      Type
  192.168.0.1            00-0d-65-8f-ae-11    dynamic
  192.168.0.5            00-11-11-14-7e-2a    dynamic
  192.168.0.7            00-0d-75-00-35-c8    dynamic
C:\>_
```

Evidence Gathering at the Data-link Layer

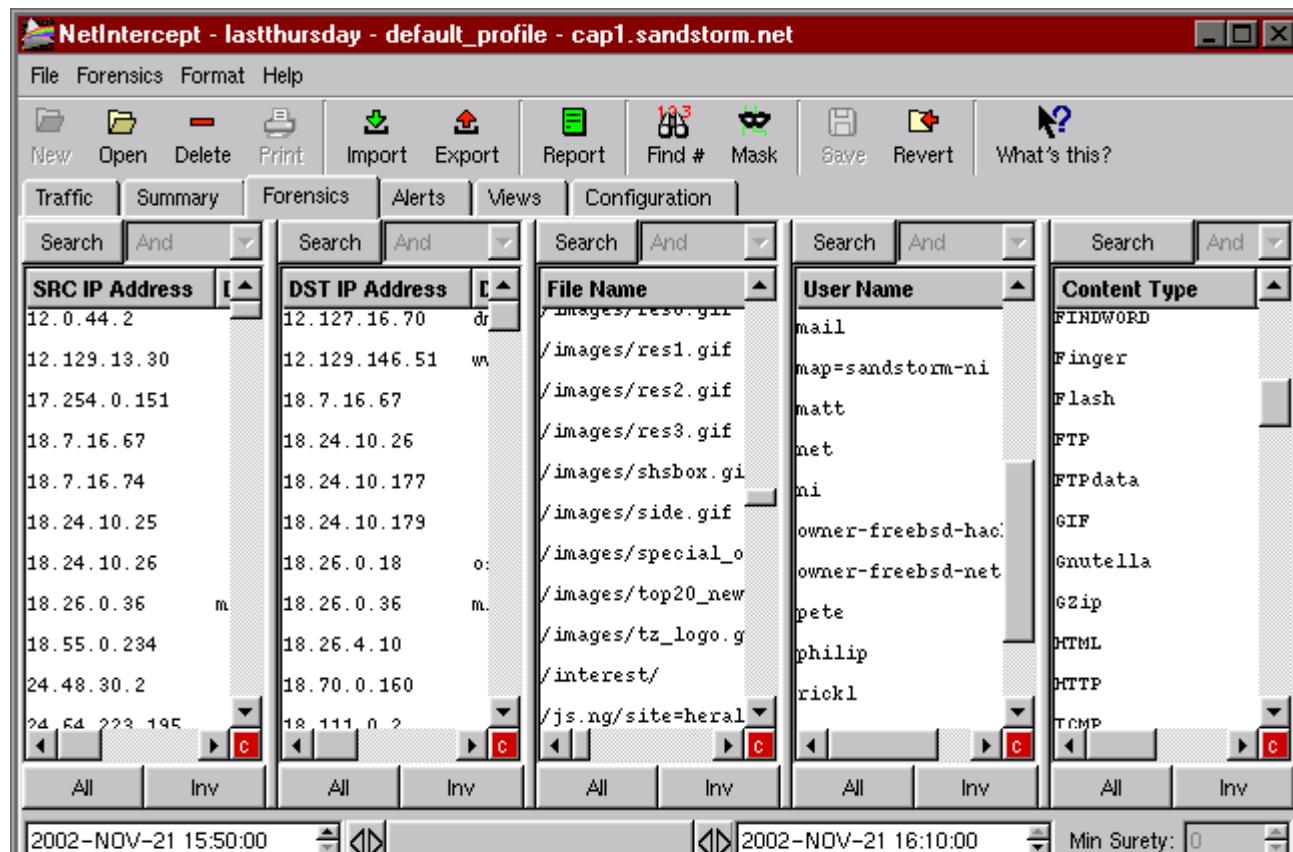
- The DHCP database also provides as a means for determining the MAC addresses associated with the computer in custody
- The DHCP server maintains a list of recent queries along with the MAC address and IP address
- Documentation of ARP table is done by the following:
 - Photographing the computer screen
 - Screenshot of the table is taken and saved on the disk
 - The HyperTerminal logging facility is used

Tool: Ethereal

- Ethereal is a network protocol analyzer for UNIX and Windows
- It allows the user to examine data from a live network or from a capture file on a disk
- The user can interactively browse the captured data, viewing summary and detailed information of each packet captured



Tool: NetIntercept



It is a sniffing tool that studies external break-in attempts, watch for misuse of confidential data, display the contents of an unencrypted remote login or a web session , categorize or sort traffic by dozens of attributes , search traffic by criteria such as email headers, web sites, and file names etc

Overview of Network and Transport Layer of the OSI Model

○ Network layer:

- It is responsible for sending information from the source to a destined address across various links
- The network layer adds logical addresses of the sender and receiver to the header of the data packet

○ Transport layer:

- The transport layer ensures that the whole message sent by the source has reached its destination and is in order
- It oversees the error control and flow control in between the transmission

Evidence Gathering at the Network and Transport Layer-(I)

○ Authentication logs:

- Shows accounts related to a particular event
- The IP address of the authenticated user gets stored in this log file

○ Application logs:

- Application logging is meant for the storage of auditing information, which includes information produced by application activity
- Web server logs help identify the system which was used as a means to commit the crime
- Only administrator has the privilege to access these log files

Evidence Gathering at the Network and Transport Layer- (II)

○ Operating System logs:

- It maintains log of events such as errors, system reboot, shutdown, security policy changes, user and group management
- But before enable logging one should bear in mind: what to log otherwise, it can result in over-collection of data making it difficult to trace the critical event

○ Network device logs:

- Network devices such as router and firewalls are configured to send a copy of their logs to remote server as the memory for these devices is low
- The logs from network devices can be used as evidence for particular investigation on that network

Gathering Evidence on a Network

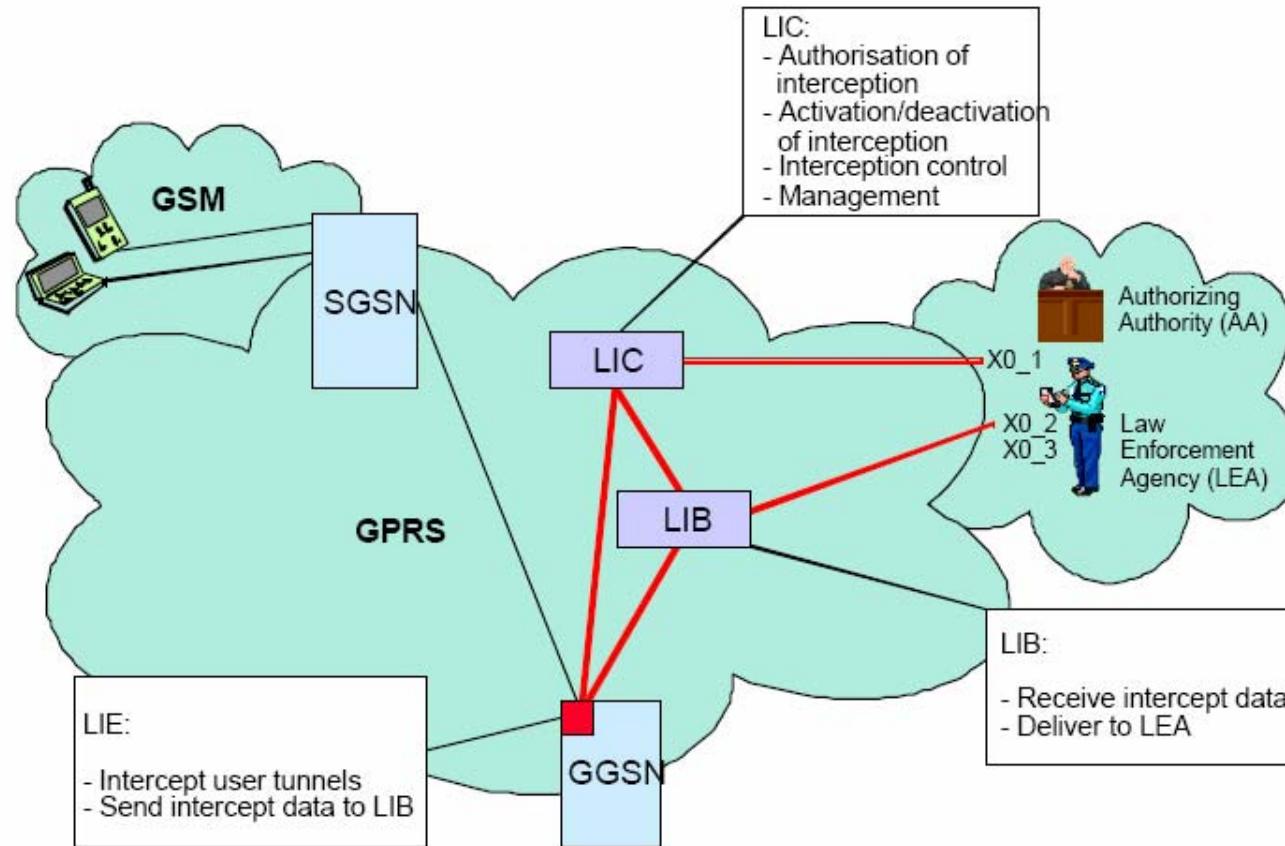
- IDS can be configured to capture network traffic when an alert is generated
- Examination results of networking devices such as routers, firewalls etc , can be recorded through a serial cable using Windows HyperTerminal program or by Script on UNIX
- If the amount of information to be captured is huge, then it is advised to record the onscreen event using a video camera or a relative software program

GPRS Network Sniffer : Nokia LIG

- ① The Nokia LIG is fabricated at the same standard platform as followed by Gateway GPRS Support Node (GGSN)
- ① Provides precise solution for constructing the GPRS interception system
- ① The architecture of implementation comprises of:
 - Lawful Interception Controller (LIC)
 - Lawful Interception Browser (LIB)
 - Lawful Interception Extension (LIE)



GPRS Network Sniffer : Nokia LIG



NetWitness

- The primary focus of NetWitness is on expanding efficiency of gathered information
- Enables organization to recognize and respond to the network activity promptly
- Presents data at application layer that remove the necessity of low level packet inspection

Screenshot: NetWitness Reader

The screenshot shows the NetWitness Reader interface. The left pane displays a hierarchical tree view of network objects, including Collection, Action, Address, Alert, Alias, Content, Port, Properties, Protocol, Resource, Service, and Size. The Address node is expanded, showing various IP addresses and their counts. The main pane displays a list of sessions with columns for Time, Service, Size, and Events. One session is selected, showing detailed information. The session details pane shows the following:

Session ID: 100-1-703177 **View Type:** Mail

10.1.15.44 : 207.46.248.16 : 119
NOTE: This session is marked as incomplete and may not display properly

Message Headers:

From:	"Eric Perlin [MS]" <ericperl@microsoft.com>
Newsgroups:	microsoft.public.platformsdk.security
Subject:	Re: Smart cards
Date:	Fri, 13 Dec 2002 12:56:29 -0800

Message Body:

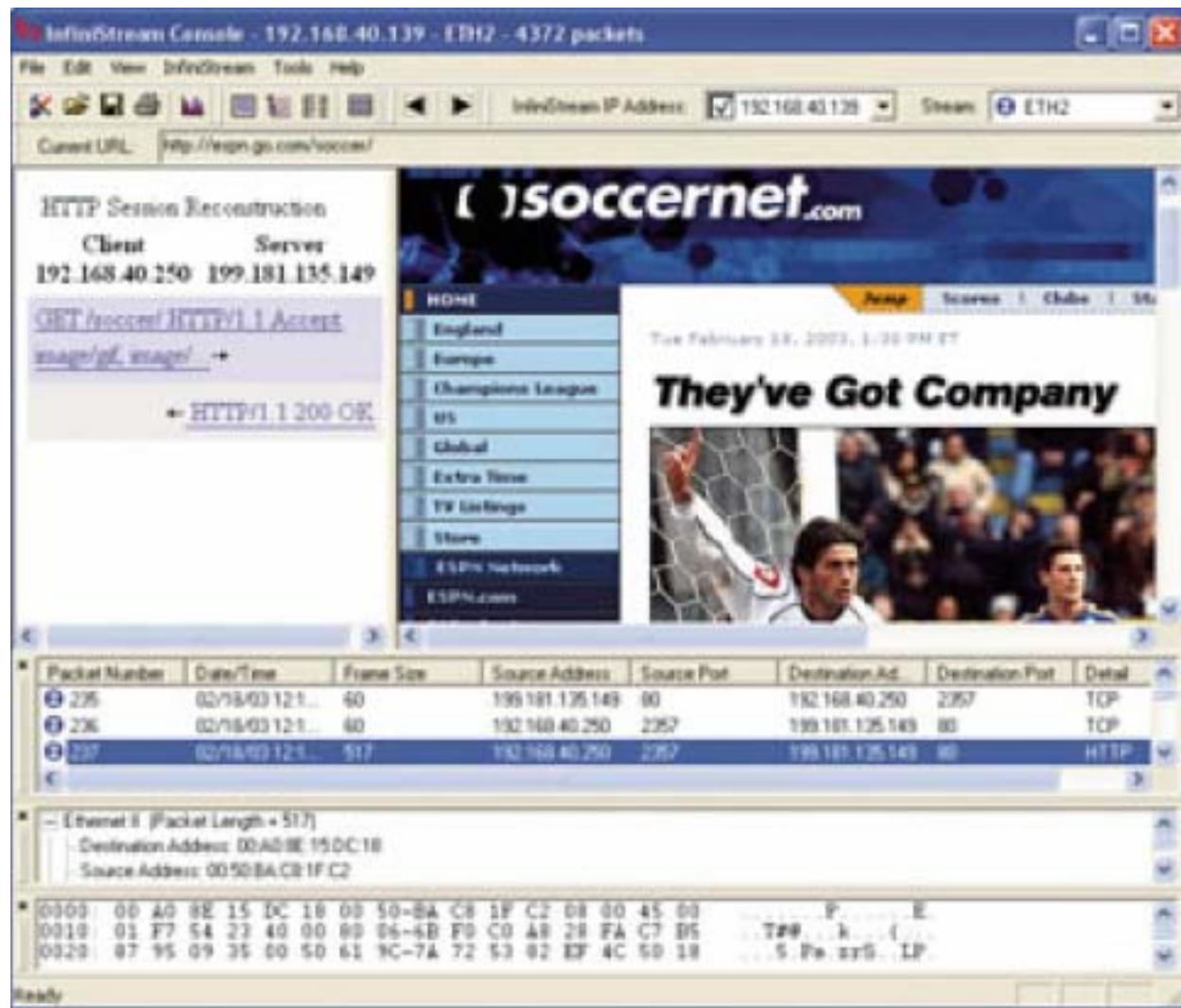
more >>
Have you considered SSL?
Then "all" you need is a CSP for your card.
--
Eric Perlin [MS]

McAfee Infinistream Security Forensics

- Archives all data necessary for maintaining packet level traffic history
- Vast storage capacity that provides superior visibility and network protection
- Ease in accessing the information addresses the issues such as when, who, how
- Ensures security and reliability



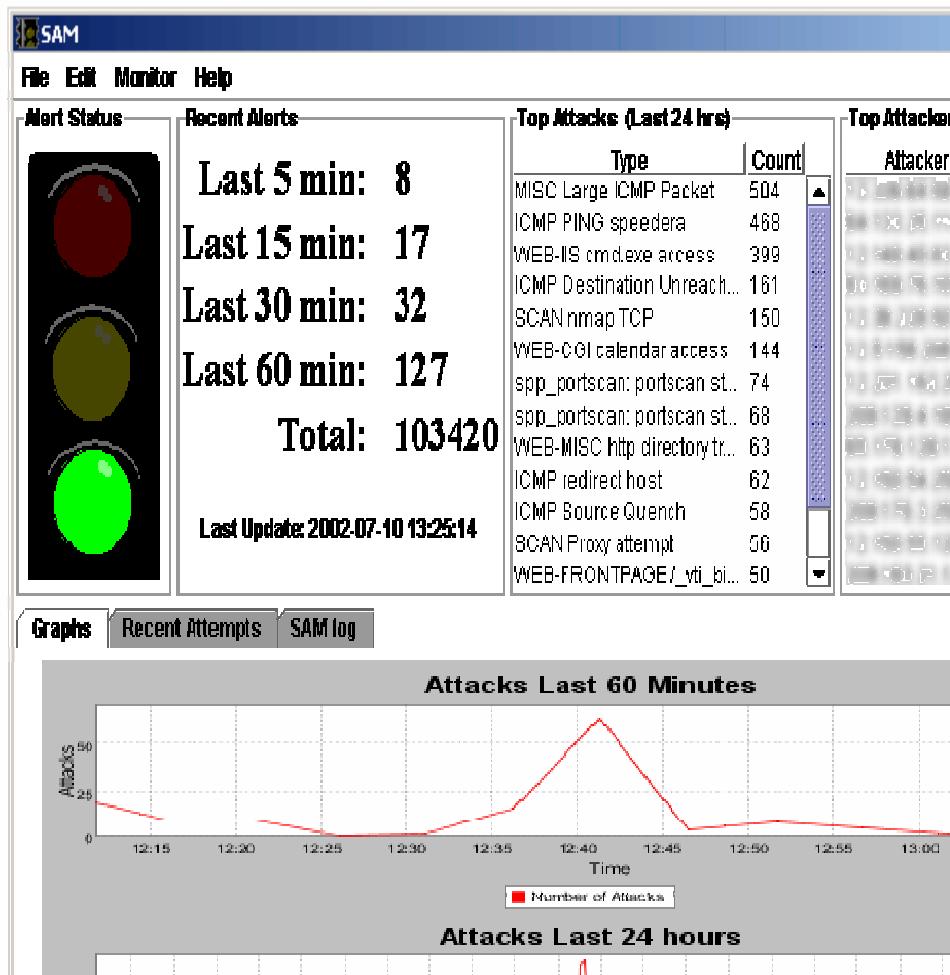
Screenshot: Infinistream Console



Snort 2.1.0

- Snort is an open source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks

- It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts



Documenting the Gathered Evidence on a Network

- If the network logs are small, a print out can be taken and attested
- The evidence gathering process should be documented by mentioning the name of the person who collected the evidence, from where it was collected, the procedure used to collect evidence and the reason for collecting evidence
- The process of documenting digital evidence on a network becomes more complex when the evidence is gathered from systems which are on remote locations

Evidence Reconstruction for Investigation

- Gathering evidence trails on a network is very cumbersome for the following reasons:
 - Evidence is not static and is not concentrated at a single point on the network
 - The variety of hardware and software found on the network makes the evidence gathering process more difficult
- Three fundamentals of reconstruction for investigating crime are:
 - *Temporal analysis*; helps to identify time and sequence of events
 - *Relational analysis*; helps to identify the link between suspect and the victim with respect to the crime
 - *Functional analysis*; helps to identify events that triggered the crime

Summary

- The physical layer does the function of transmitting raw bits over a communication channel
- The data link layer does the function of taking a raw transmission facility and converting them into a line that appears without transmission errors in the network layer
- Sniffers , which put NICs in promiscuous mode are used to collect digital evidence at the physical layer
- MAC address , a part of the data-link layer is associated with the hardware of a computer.
- The DHCP database also provides as a means for determining the MAC addresses associated with the computer in custody



Computer Hacking Forensic Investigator

Module XVIII Router Forensics

Scenario

Jonas David works as the network administrator of a renowned IT firm. Since he was not performing up to the expected standards, he was fired. An infuriated Jonas plans to attack the firm's "master router".

After attacking the router, his target is the web server which hosts the company's business website. He triggers a flood attack on the web server, using the router. He crashes the web server resulting in the firm ending up in huge amount of losses.

Forensic examiners were contacted by the company to identify the reason of the crash and also locate the culprit.

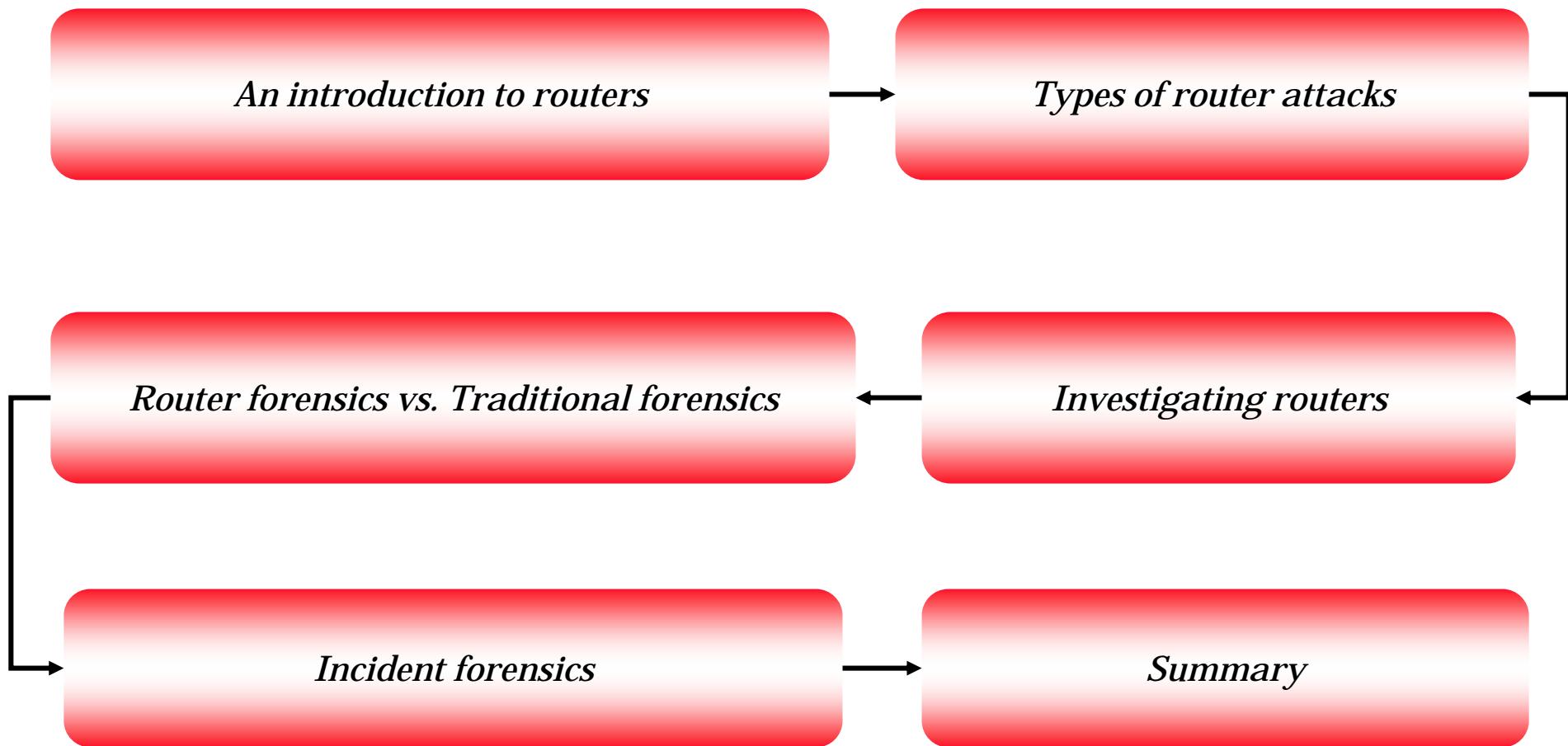
But how did they locate the vulnerability? How did they find the culprit?



Module Objective

- An introduction to routers
- Types of router attacks
- Router forensics vs. traditional forensics
- Investigating routers
- Incident forensics
- Summary

Module Flow



What Is a Router?

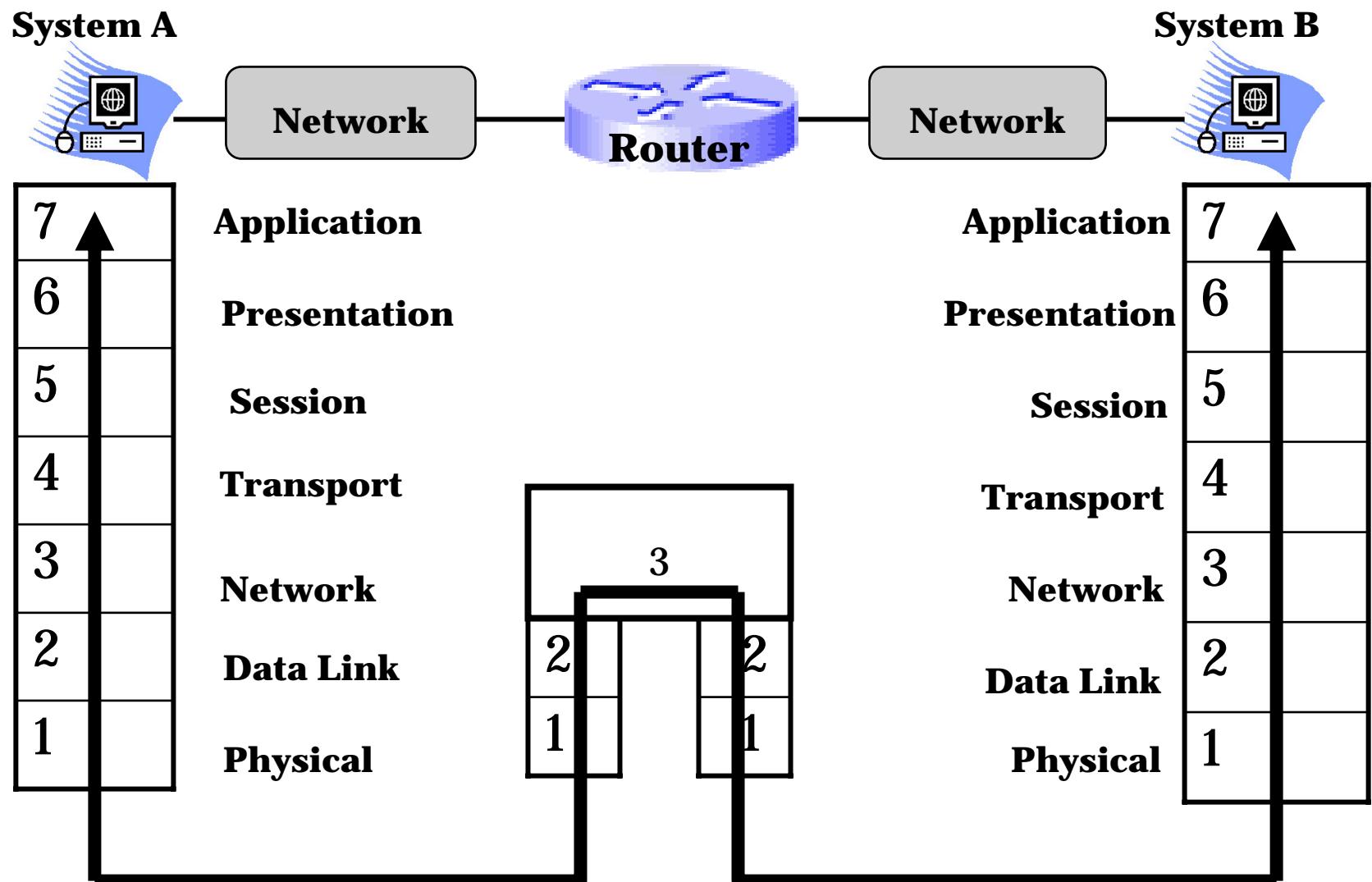
- Device to transmit data packets along networks
- Connected to at least two networks, commonly a LAN and its ISP's network or two LANs
- Has access to network layer addresses
- Contains software that determines which of the several possible paths between those addresses is suited for a particular transmission
- Uses headers and forwarding tables to determine the best path for forwarding the packets
- Uses protocols such as ICMP to communicate and configure the best route between any two hosts

Functions of a Router

- Decides the most effective path for a packet to reach its final destination
- Transfers link state data within and amid the routing groups
- Acts as a default gateway
- Limits the network broadcasts to the local LAN
- “Protocol translator” – provided if there are suitable hardware and software



A Router in an OSI Model



Routing Table and Its Components

- Determines the final destination of the data packet through the router
- It consists of the following:
 - An address prefix
 - Interface on which packets corresponding to the address prefix are forwarded
 - A next-hop address
 - A preference value for choosing between several routes with similar prefix
 - Route duration
 - Specification showing whether the route is advertised in a routing advertisement
 - Kind of route

Router Architecture

① Memory

- Non-Volatile Random Access Memory(NVRAM) :
 - Content: Startup Configuration
- Static RAM/Dynamic RAM
 - Content: Current Internetwork Operating System(IOS), Routing tables
- BootROM
 - Content: ROMMON Code

② Hardware

- Model/Series
 - Content: Motherboard, CPU, Input/Output Interfaces

③ Internetwork Operating System(IOS)

Implications of a Router Attack

- Router is considered to be a crucial component in the infrastructure of a network
- If an intruder can acquire control over a router, he/she can:
 - Interrupt communications by dropping or misrouting packets passing through the router
 - Completely disable the router and its network
 - Compromise other routers in the network and possibly the neighboring networks
 - Observe and log both incoming and outgoing traffic
 - May avoid firewalls and Intrusion Detection Systems
 - Forward any kind of traffic to the compromised network

Types of Router Attacks

- Denial of Service attack
- Packet mistreating attacks
- Routing table poisoning
- Flooding
- Hit-and-run attacks
- Persistent attacks



Denial of Service(DoS) Attacks

- Makes a router unusable for network traffic and completely inaccessible by overloading its resources
- A DoS attack may lead to:-
 - **Destruction** – Damage the capability of the router to operate
 - **Resource Utilization** – Achieved by overflowing the router with numerous open connections at the same time
 - **Bandwidth Consumption** – Attempted to utilize the bandwidth capacity of the router's network



Investigating Dos Attacks

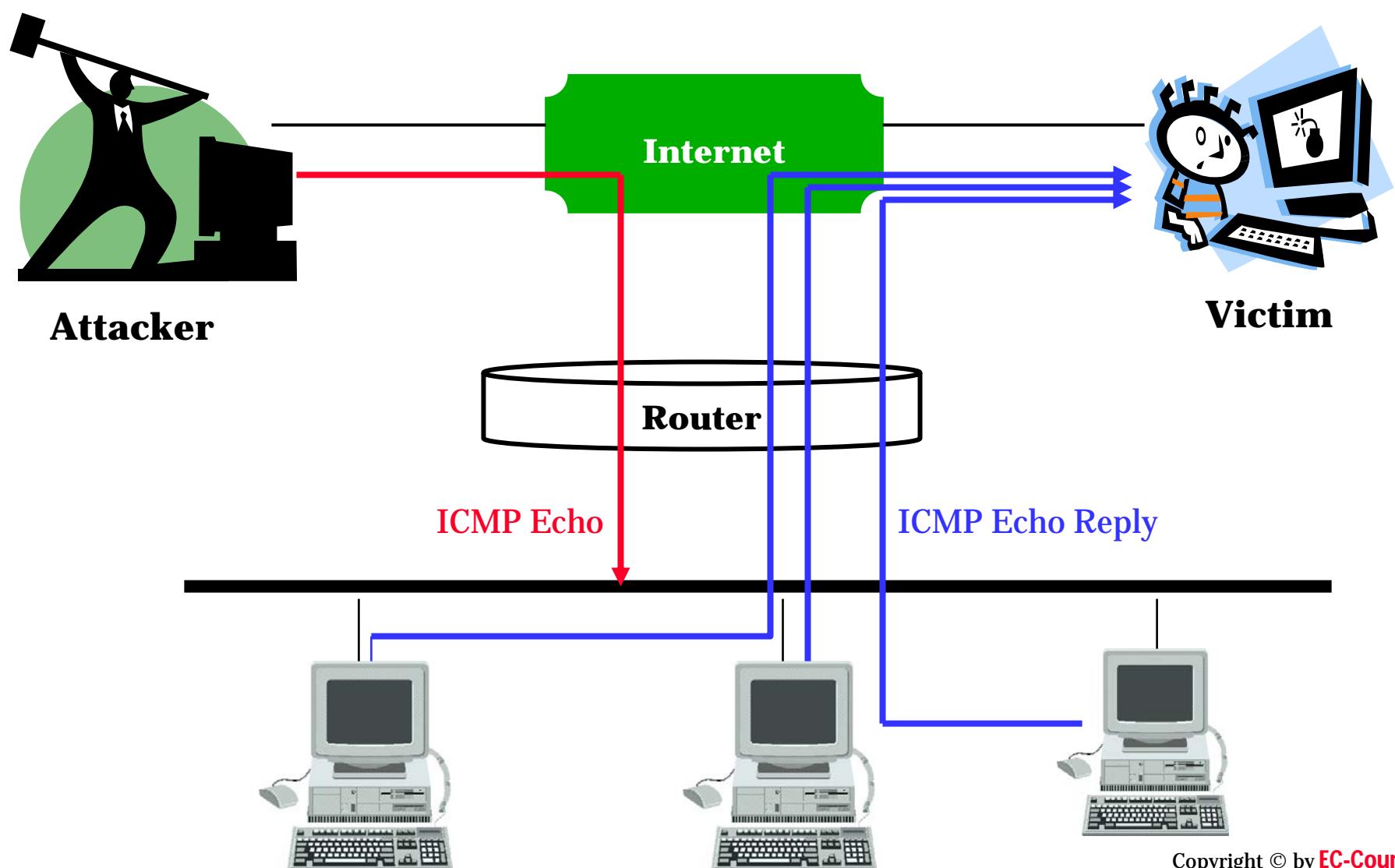
- Look at the log files for evidence such as IP address and the protocol
 - `Access-list 101 deny ip 10.0.0.0 0.0.0.255 any log`
- The following command configures the router to redirect the log to syslog server
 - `#config terminal`
 - `Logging 10.0.0.23`
 - Now all log messages will be sent to the syslog server

Smurfing – Latest in Dos Attacks

- Manipulating Internet Protocol broadcast addressing and several other features of Internet functioning
- Using “smurf” program:
 - Constructs a network packet that seems to originate from another address. Also known as spoofing
 - Packet consists of an ICMP ping message to be sent to an IP broadcast address
 - Echo responds to the ping message by sending it back to the “victim” address
 - Numerous pings and consequential echoes flood the network making it ineffective for real traffic



Smurfing – Diagrammatic Representation



Packet “Mistreating” Attacks

- ◉ Compromised router misleads packets leading to
 - Congestion
 - Denial of Service
 - Decrease in throughput
- ◉ Becomes difficult if the router particularly disrupts or misroutes packets leading to triangle routing
- ◉ Complicated to detect



Routing Table Poisoning

- Malicious alteration or poisoning of routing tables
- Accomplished by maliciously altering the routing data update packets needed by the routing protocols
- Results in wrong entries in the routing table
- Leads to a breakdown of one or more systems on the network



Hit-and-run Attacks Vs. Persistent Attacks

◎ Hit- and- run attacks

In these type of attacks,

- Attacker injects a single or a few bad packets into the router
- Causes a long-lasting damage
- Usually these type of attacks are very hard to detect

◎ Persistent attacks

In these type of attacks,

- Attacker constantly injects bad packets into the router
- Causes significant damages



Router Forensics Vs. Traditional Forensics

<u>Router forensics</u>	<u>Traditional forensics</u>
System needs to be online for investigation purpose.	System needs to be shutdown for investigation purpose.
Flash data most likely remains constant.	Create a copy for forensic investigations and analysis.
Live system data needs to be recovered and is critical for analysis.	Live system data is usually not recovered.

Investigating Routers

- Chain of custody
- Incident response & session recording
- Accessing the router
- Volatile evidence gathering
- Analyzing the intrusion



Chain of Custody

- Essential to maintain chain of custody
- Shows who collected and handled the evidence
- Avoids confusion during testimony



Sample Chain of Custody(coc) Form

Chain of Custody				
Item	Date/Time	Released By	Received By	Purpose & Location
		Name Organization Signature	Name Organization Signature	
Final Disposition of Evidence				
Final Actions Taken: <i>(returned to owner, destroyed, etc...)</i>	<i>Persons receiving items/witnessing destruction</i>			
	1)	Name	Signature	Date
	2)			
	3)			
	4)			

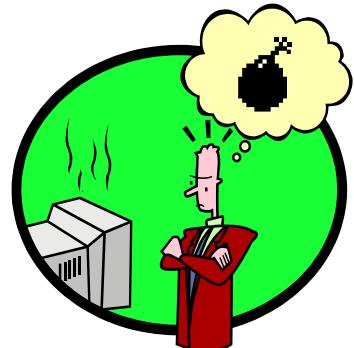
Incident Response & Session Recording

○ Incident response

- Never restart the router
- Nothing should be modified but recorded

○ Recording session

- Start recording session before logging on to the router
- Show the current time using the *show clock detail* command



Accessing the Router

- Access the router to gain attack related information
- Certain points need to be kept in mind while accessing the router
 - Access the router through the console and not through the network
 - Execute *show* commands and not *configuration* commands
 - Give more preference to recovering volatile data as compared to persistent data

Volatile Evidence Gathering

Divided into two types:

- Direct Access
 - Using show commands
- Indirect Access, if passwords are changed
 - Port scan
 - SNMP Scan



Router Investigation Steps - I

1. Link to the console port
2. Document system time

Router# show clock detail

3. Examine logs

Router# show users

4. Examine router's uptime and all other data on the router since the previous boot-up

Router# show version

5. Determine listening sockets

Enumerates current vulnerable services

Router Investigation Steps - II

6. Save router configuration – both running and startup

Router# show running-config

Router# show startup-config

7. Evaluate routing table

Router# show ip route

Detects vulnerable static routes altered by the router using Routing Information Protocol (RIP) spoofing

8. Verify interface configuration

Router# show ip interface

9. Inspect ARP cache

Router# show ip arp

Analyzing the Intrusion

- Check logging
- Inspect timestamps
- Verify running and startup configurations
- Examine IOS vulnerabilities



Logging

- *Syslog logging* - The syslog server receives and stores all the log messages
- *Buffer logging* - When show logging command is executed, contents of the router log buffer are revealed
- *Console logging* – Record console sessions
- *Terminal logging* – Record non console sessions and view log messages
- *SNMP logging* - Log server accepts and records all SNMP traps
- *ACL Violation Logging*
 - Access Control Lists configured for logging packets matching their rules by stopping the ACL using log or log-input keywords
 - Router's log buffer receives and stores these log messages
 - These log messages are also sent to the syslog server

Incident Forensics

Four common incidents are:

- Direct compromise incident
- Routing table manipulation
- Theft of information
- Denial of Service



Handling a Direct Compromise Incident

- Listening services offer possible attack points
- Restart to gain console access
- Access modem due to improper log off
- Passwords
 - Cracking passwords
 - Pilfering from configuration files
 - Sniffing using SNMP, telnet, HTTP, TFTP
- Trivial File Transfer protocol(TFTP)
 - Stores and reloads config files
 - Intruder first scans the network for a router and the TFTP server
 - Guesses configuration file name
 - Receives the configuration file through TFTP
 - This enumerates all the possible passwords to gain access to the router



Other Incidents

- Routing table manipulation
- Review routing table
 - Router# show ip route
- Theft of information
 - Examine Network topology and access control contained in routers
- Denial of Service
 - Reboot the router



Summary

- Router needs to be online for investigations
- Router forensics is different from traditional forensics
- Various steps under investigation of routers such as incident response, and volatile evidence gathering
- Investigator must be extremely careful while accessing the router
- Volatile evidence must be given priority
- Incident forensics help in finding the true reason of an event and also avoid future events



Certified Hacking Forensic Investigator

Module XX
Investigating Web Attacks

Scenario

The website of Broknint, an online brokerage firm was down for 2 days. Customers were redirected to a website that contained illicit contents. The company had lost many customers and business during the breakdown.

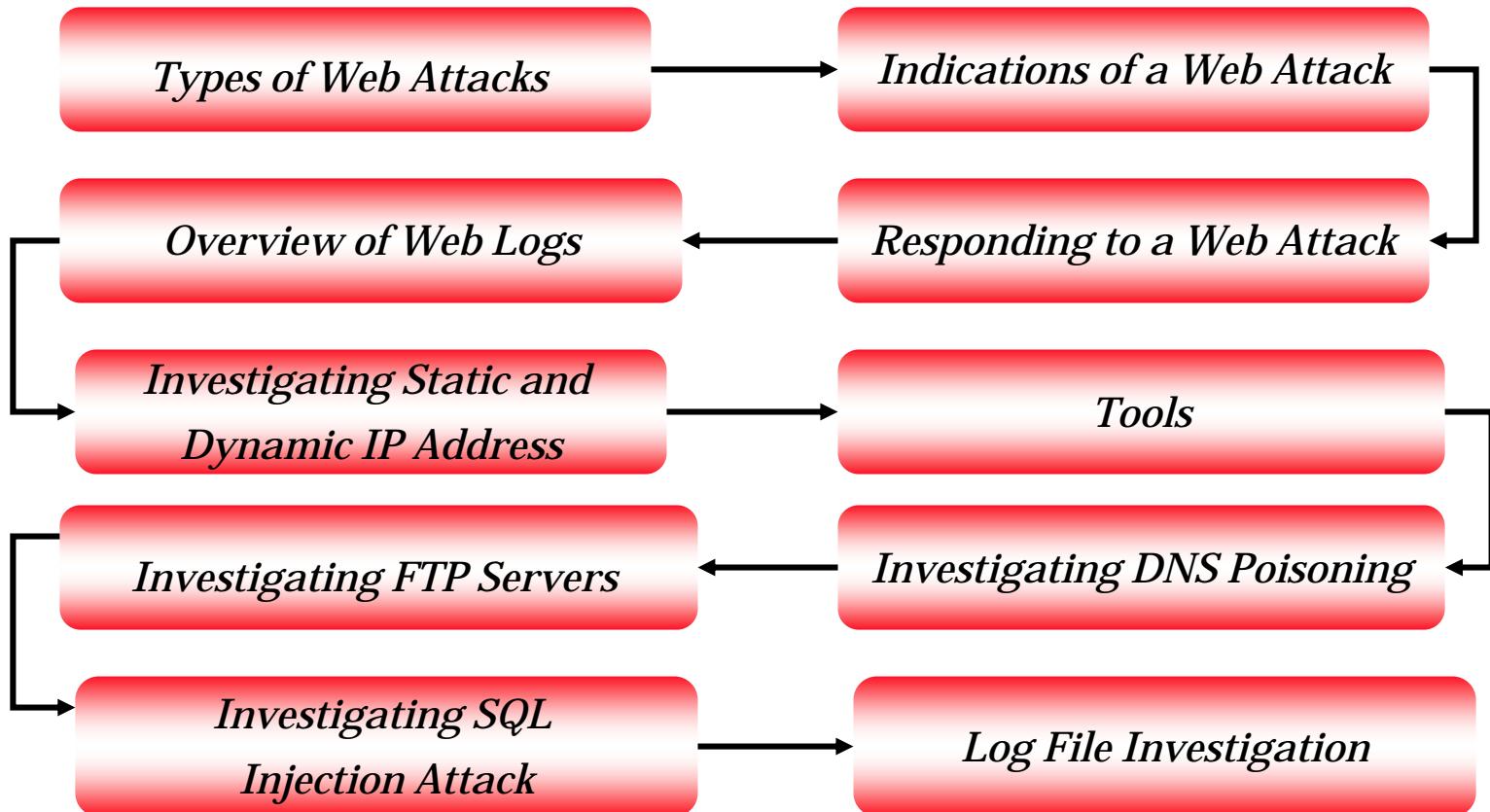
The network administrator at Broknint was not able to restore the webserver. The management at the brokerage firm called in investigators from Xsecurity , a prominent investigative agency.

Investigators suspected a case of DNS poisoning. After investigating the site and collecting evidence the investigators were able to track down the culprits behind the attack.

Module objective

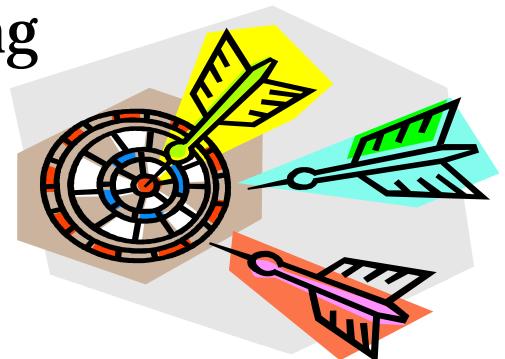
- Types of web attacks
- Indications of a web attack.
- Responding to a web attack.
- Overview of web logs
- Investigating static and dynamic IP address.
- Tools
- Investigating DNS Poisoning
- Investigating FTP Servers
- Investigating SQL Injection attack
- Log File Investigation

Module Flow



Types of web attacks

- Attacks that are targeted at HTTP/HTTPS protocols are classified as web attacks.
- Following are the common types of web attacks:
 - Cross-site scripting
 - SQL injection
 - Buffer overflow
 - Denial of Service
 - Directory traversal/forceful browsing
 - Command injection
 - Cookie/session poisoning
 - Web services attacks
 - Authentication hijacking



Indications of a web attack

- Customers reporting to an organization, that they are not able to access its online service.
- A legitimate web page being redirected to an unknown website.
- Frequent rebooting of the server.
- Anomalies found in the log files is also an indication of an attack.



Responding to a web attack

1. Identify the nature of the attack. Is it a DDoS attack, or an attack targeted just at you?
2. Is someone trying to shut down your network altogether, or attempting to infiltrate individual machines?
3. Localize the source.
4. Use your firewall and IDS logs to attempt to identify where the attack is coming from (or came from!)
5. This will help you identify whether the attack/penetration is coming from a compromised host on your network or from the outside world.
6. Block the attack.
7. Once you know where the attack is coming from, you can take action to stop it.
8. If you've identified specific machines that have been compromised, pull them from the network until you can disinfect them and return them to service.
9. If an attack or attempted attack is coming from outside, block access to your network from that IP address.
10. START YOUR INVESTIGATION – from the IP address!

Overview of web logs

- Log files come handy in detecting web attacks
- The source, nature and time of attack can be determined by analyzing log files of the compromised system
- Log files have HTTP status codes that are specific to the type of incidents
- Web servers that run on IIS or Apache are prone to log file deletion by any attacker who has access to the web server
- The reason being log files are stored on the web server itself

Mirrored Sites

- Web pages can be clichéd in a few minutes.
- Hosted on another server probably by a totally different person than the real content provider.
- Mirroring occurs when a web server has one IP address but two different domain names.



N-Stealth

- N-Stealth 5 is a Web vulnerability scanner that scans over 18000 HTTP security issues.
- Stealth HTTP Scanner writes scan results to an easy HTML report.
- N-Stealth is often used by security companies for penetration testing and system auditing, specifically for testing Web servers.



Investigating static and dynamic IP address

- Static IP address of a particular host can be found with the help of tools such as *Nslookup*, *Whois*, *Traceroute*, *ARIN*, *NeoTrace*.
- Nslookup is an inbuilt Windows NT program to query Internet domain name servers. Displays information that can be used to diagnose Domain Name System (DNS) infrastructure.
- The DHCP server allocates dynamic IP address to the hosts on a network.
- The DHCP log file stores information regarding the IP address allocated to a particular host at a particular time.

Tools for locating IP Address: Nslookup

- http://www.btinternet.com/~simon.m.parker/IP-utils/nslookup_download.htm
- Nslookup is a program to query Internet domain name servers. Displays information that can be used to diagnose Domain Name System (DNS) infrastructure.
- Helps find additional IP addresses if authoritative DNS is known from whois.
- MX record reveals the IP of the mail server.
- Both Unix and Windows come with a Nslookup client.
- Third party clients are also available – E.g. Sam Spade

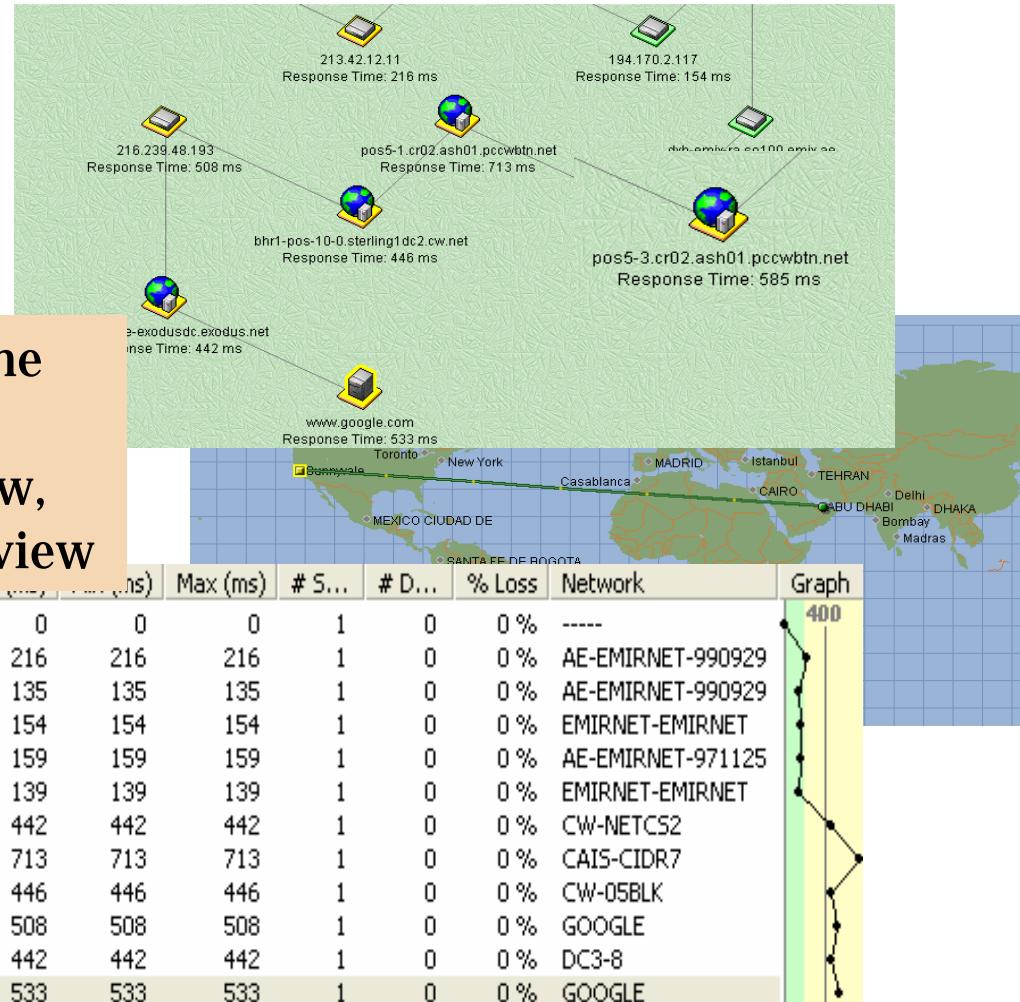
Tools for locating IP Address: Traceroute

- Traceroute works by exploiting a feature of the Internet Protocol called TTL, or Time To Live.
- Traceroute reveals the path IP packets travel between two systems by sending out consecutive UDP packets with *ever-increasing* TTLs .
- As each router processes a IP packet, it *decrements* the TTL. When the TTL reaches zero, it sends back a "TTL exceeded" message (using ICMP) to the originator.
- Routers with DNS entries reveal the *name* of routers, *network affiliation* and *geographic location*.

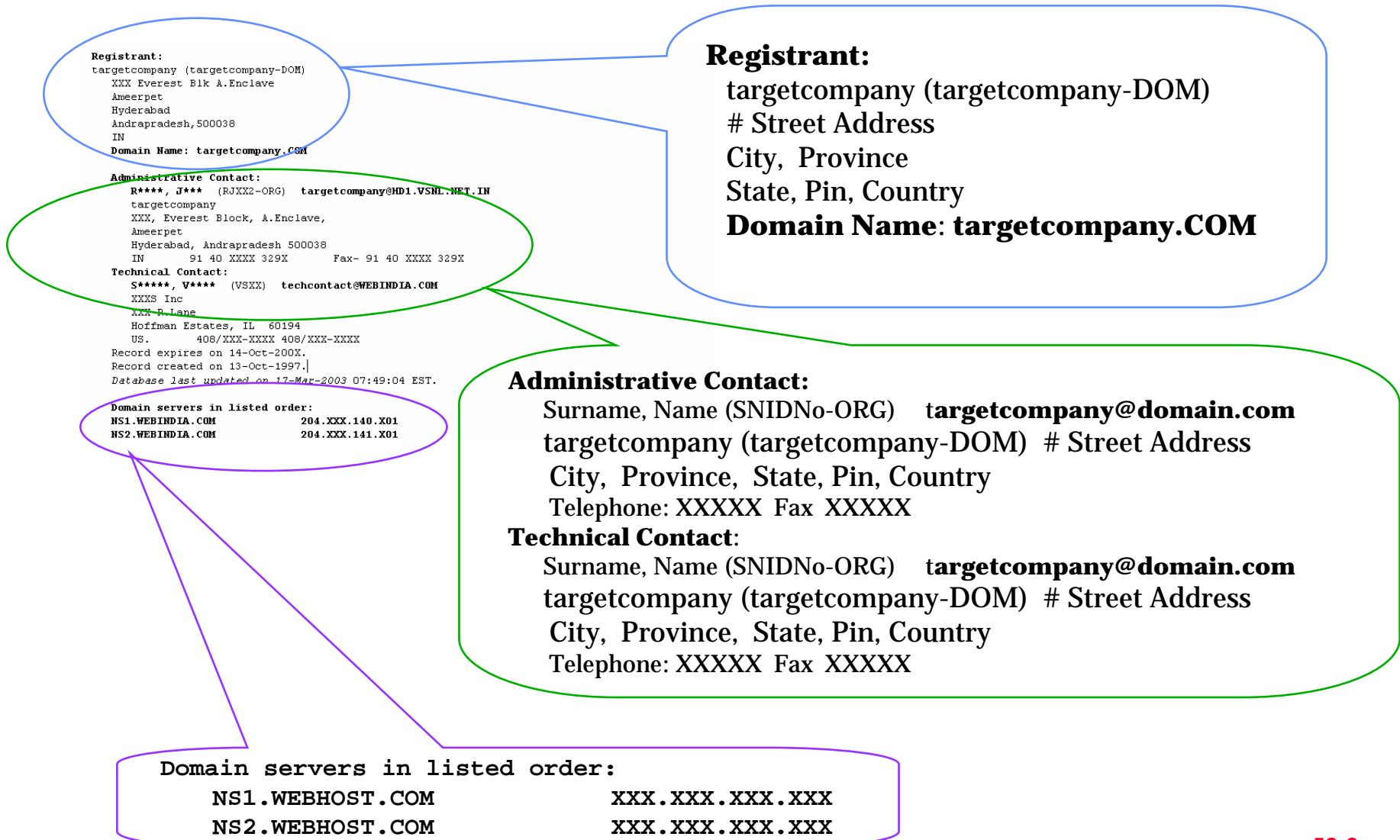
Tools for locating IP Address: NeoTrace (Now McAfee Visual Trace)



NeoTrace shows the traceroute output visually – map view, node view and IP view



Tools for locating IP Address: Whois



Web page defacement

- Web page defacement requires write access privileges in web server root directory.
- Write access means full blown web server compromise.
- The compromise could come from any security vulnerability such as Unicode, RPC etc.
- The web page defacements are the results of:
 - Weak administrator password
 - Application misconfiguration
 - Server misconfigurations
 - Accidental permission assignments

Defacement using DNS compromise

- The attacker could deface a website indirectly.
- The attacker can compromise the authoritative domain name server for the web server by redirecting DNS requests for a website to his defaced website.
 - Webserver DNS entry
 - www.example.com 192.2.3.4
 - Compromised DNS entry by the attacker
 - www.example.com 10.0.0.3
 - Now all requests for www.example.com will be redirected to 10.0.0.3

Investigating DNS Poisoning

- If you notice that DNS cache has been corrupted then dump the contents of the DNS server's cache to look for inappropriate entries.
- On Linux systems use the BIND command:
 - #ndc dumpdb
 - Database dump initiated.
- You can enable DNS logging in named.conf but it will slow the performance of the DNS server.

SQL Injection Attacks

- SQL Injection is simply a term describing the act of passing SQL code into an application that was not intended by the developer.
- SQL injection is usually caused by developers who use "string-building" techniques in order to execute SQL code.
- For example, in a search page, the developer may use the following code to execute a query (VBScript/ASP sample shown):
 - Set myRecordset = myConnection.execute("SELECT * FROM myTable WHERE someText ='" & request.form("inputdata") & "'")
- Attack on website like "blah or 1=1 --" will produce the following code in the ASP:
 - Set myRecordset = myConnection.execute("SELECT * FROM myTable WHERE someText ='" & blah or 1=1 -- & "'")
 - The above statement always evaluates to true and returns the recordset.

Investigating SQL Injection Attacks

- Look for SQL Injection attacks incidents in 3 locations
 - IDS log files
 - Database server log files
 - Web server log files
 - The attack signature may look like this in the logfile:
 - 12:34:35 192.2.3.4 HEAD GET
/login.asp?username=blah' or 1=1 –
 - 12:34:35 192.2.3.4 HEAD GET
/login.asp?username=blah' or)1=1 (--
 - 12:34:35 192.2.3.4 HEAD GET
/login.asp?username=blah' or exec
master..xp_cmdshell 'net user test testpass' --

Example of FTP Compromise

- Attacker runs port scanning:

```
#nmap -o 23.3.4.5 -p 21
```

```
Starting nmap Interesting ports
```

Port	State	Service
------	-------	---------

21/tcp	open	ftp
--------	------	-----

80/tcp	open	www
--------	------	-----

Remote OS is Windows 2000

- The attacker connects using ftp

```
ftp 23.3.4.5
```

```
Connected to 23.3.4.5
```

```
Username: administrator
```

```
Password:
```

Investigating FTP Servers

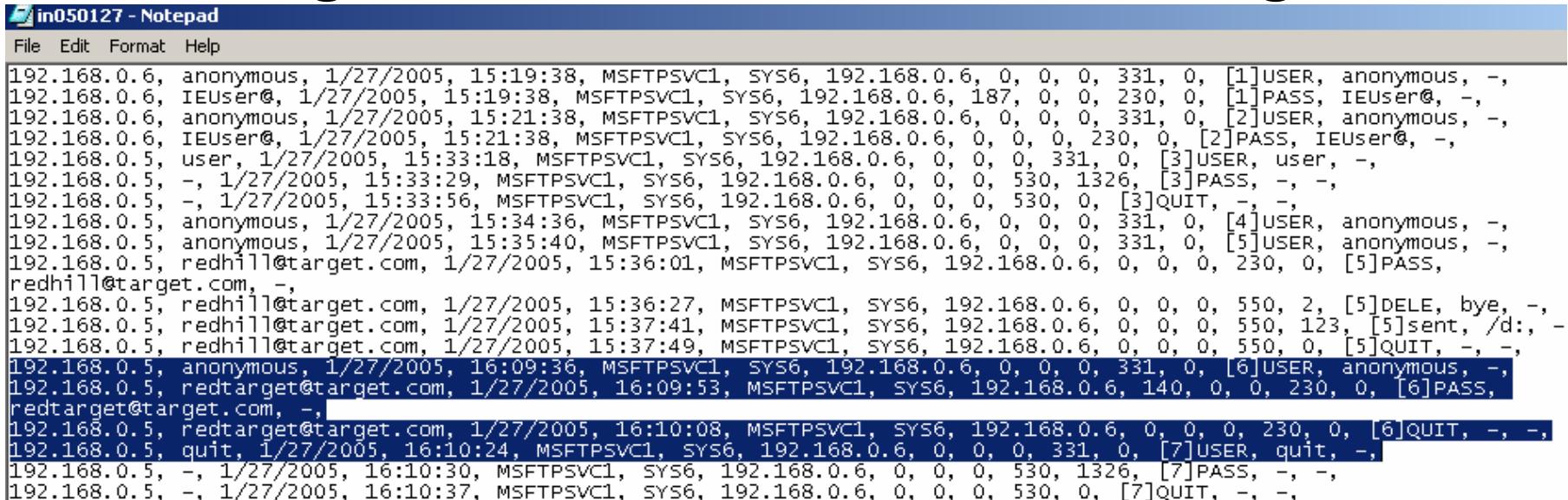
- ◉ FTP server vulnerabilities allow an attacker to directly compromise the system hosting the FTP server.
- ◉ Direct compromise of an FTP server can be simple as obtaining legitimate passwords by:
 - Social engineering
 - Brute-force guessing
 - Network sniffing
- ◉ Network and FTP logs provide valuable records that can provide valuable evidence.

Investigating FTP Logs

- The FTP logs in a Windows 2000 is stored in the directory:

C:\WINNT\system32\LogFiles\MSFTPSVC1

- Below given is a screenshot of an FTP log



The screenshot shows a Notepad window titled "in050127 - Notepad". The window contains a large amount of text representing an FTP log file. The log entries are timestamped and show various commands such as USER, PASS, QUIT, and DELE. The log is from an MSFTPSVC1 service on an IP address of 192.168.0.6, with users connecting from 192.168.0.6 and 192.168.0.5.

```
File Edit Format Help
192.168.0.6, anonymous, 1/27/2005, 15:19:38, MSFTPSVC1, SYS6, 192.168.0.6, 0, 0, 0, 331, 0, [1]USER, anonymous, -, 192.168.0.6, IEUser@, 1/27/2005, 15:19:38, MSFTPSVC1, SYS6, 192.168.0.6, 187, 0, 0, 230, 0, [1]PASS, IEUser@, -, 192.168.0.6, anonymous, 1/27/2005, 15:21:38, MSFTPSVC1, SYS6, 192.168.0.6, 0, 0, 0, 331, 0, [2]USER, anonymous, -, 192.168.0.6, IEUser@, 1/27/2005, 15:21:38, MSFTPSVC1, SYS6, 192.168.0.6, 0, 0, 0, 230, 0, [2]PASS, IEUser@, -, 192.168.0.5, user, 1/27/2005, 15:33:18, MSFTPSVC1, SYS6, 192.168.0.6, 0, 0, 0, 331, 0, [3]USER, user, -, 192.168.0.5, -, 1/27/2005, 15:33:29, MSFTPSVC1, SYS6, 192.168.0.6, 0, 0, 530, 1326, [3]PASS, -, -, 192.168.0.5, -, 1/27/2005, 15:33:56, MSFTPSVC1, SYS6, 192.168.0.6, 0, 0, 0, 530, 0, [3]QUIT, -, -, 192.168.0.5, anonymous, 1/27/2005, 15:34:36, MSFTPSVC1, SYS6, 192.168.0.6, 0, 0, 0, 331, 0, [4]USER, anonymous, -, 192.168.0.5, anonymous, 1/27/2005, 15:35:40, MSFTPSVC1, SYS6, 192.168.0.6, 0, 0, 0, 331, 0, [5]USER, anonymous, -, 192.168.0.5, redhill@target.com, 1/27/2005, 15:36:01, MSFTPSVC1, SYS6, 192.168.0.6, 0, 0, 0, 230, 0, [5]PASS, redhill@target.com, -, 192.168.0.5, redhill@target.com, 1/27/2005, 15:36:27, MSFTPSVC1, SYS6, 192.168.0.6, 0, 0, 0, 550, 2, [5]DELE, bye, -, 192.168.0.5, redhill@target.com, 1/27/2005, 15:37:41, MSFTPSVC1, SYS6, 192.168.0.6, 0, 0, 0, 550, 123, [5]sent, /d:, -, 192.168.0.5, redhill@target.com, 1/27/2005, 15:37:49, MSFTPSVC1, SYS6, 192.168.0.6, 0, 0, 0, 550, 0, [5]QUIT, -, -, 192.168.0.5, anonymous, 1/27/2005, 16:09:36, MSFTPSVC1, SYS6, 192.168.0.6, 0, 0, 0, 331, 0, [6]USER, anonymous, -, 192.168.0.5, redtarget@target.com, 1/27/2005, 16:09:53, MSFTPSVC1, SYS6, 192.168.0.6, 140, 0, 0, 230, 0, [6]PASS, redtarget@target.com, -, 192.168.0.5, redtarget@target.com, 1/27/2005, 16:10:08, MSFTPSVC1, SYS6, 192.168.0.6, 0, 0, 0, 230, 0, [6]QUIT, -, -, 192.168.0.5, quit, 1/27/2005, 16:10:24, MSFTPSVC1, SYS6, 192.168.0.6, 0, 0, 0, 331, 0, [7]USER, quit, -, 192.168.0.5, -, 1/27/2005, 16:10:30, MSFTPSVC1, SYS6, 192.168.0.6, 0, 0, 0, 530, 1326, [7]PASS, -, -, 192.168.0.5, -, 1/27/2005, 16:10:37, MSFTPSVC1, SYS6, 192.168.0.6, 0, 0, 0, 530, 0, [7]QUIT, -, -,
```

Investigating IIS Logs

- IIS logs all the visits in log files. The log file is located at <%systemroot%>\logfiles.
- If proxies are not used, then IP can be logged.
- This command lists the log files:

```
http://victim.com/scripts/..%c0%af../..%c0%af../..%c0%af../..%c0%af..  
/..%c0%af../..%c0%af../..%c0%af../..%c0%af./winnt/system32/cmd.exe  
?/c+dir+C:\Winnt\system32\Logfiles\W3SVC1.
```

Investigating Apache Logs

- ① The Apache server has two logs namely:

- Error log:
 - The Apache server saves diagnostic information and error messages that it encounters while processing requests.
 - The default path of this file is ***usr/local/apache/logs/error_log*** in Linux
 - It is an important piece of evidence from investigator's point of view.

[Sat Dec 11 7:12:36 2004] [error] [client 202.116.1.3] Client sent malformed Host header

- Access log:

- Requests processed by the Apache server are contained in this.
- By default access logs are stored in the common log format.
- The default path of this file is ***usr/local/apache/logs/access_log*** in Linux

202.116.1.3 - shilp [11/Dec/2004:6:23:13 -0500] "GET /apache_ft.gif HTTP/1.0"
200 1577

Investigating DHCP Server Logfile

- Windows 2000 Server

C:\WINNT\system32\dhcp\dhcpsrvlog

- Linux

/var/db/dhcpd.leases

```
Lease 10.1.1.1 {  
    starts 0 2003 03/12 3:00:00;  
    ends 0 2003 03/24 8:00:00;  
    hardware ethernet 00:10:3b:35:d7:fd;  
    uid 01:10:3b:35:d7:fd  
    client-hostname "vicky"  
}
```

Summary

- Attacks that are targeted at HTTP/HTTPS protocols are classified as web attacks.
- 32% of website defacements were due to configuration mistakes
- Log files have HTTP status codes that are specific to the type of incidents.
- FTP server vulnerabilities allow an attacker to directly compromise the system hosting the FTP server.
- The Apache server has two logs namely access logs and error logs.



Computer Hacking Forensic Investigator

Module XX

Tracking E-mails and Investigating E-mail crimes

Scenario

Daniel, a contract employee of computer services at the reputed organization intentionally downloaded a zipped file called ‘ZIP-78’ from the Internet

Aware of the consequences, he sent the ‘ZIP-78’ file to an e-mail account on the company’s e-mail server, on at least seven different occasions

His action not only shuts down the email server but incurred heavy losses in bringing the e-mail server back to production



Module Objective

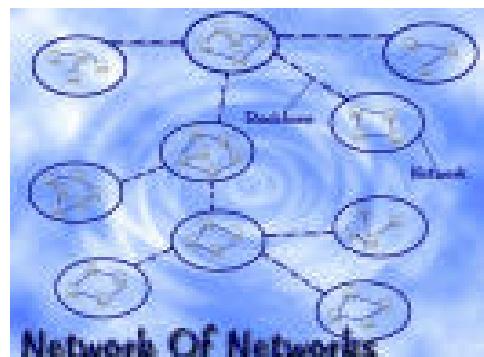
- Understanding Internet fundamentals
- Exploring the roles of client and sever in e-mail
- Investigating e-mail crimes and violations
- Sending fakemail
- Examining e-mail message
- Examining e-mail headers
- Tracing an e-mail message
- Using network logs related to e-mail
- Tracing back
- Searching e-mail addresses
- Handling Spam
- Protecting e-mail address from Spam

Module Flow



Understanding Internet Fundamentals

- ◎ **Internet** – It is a huge collection of networks connecting millions of computers
- ◎ **Internet Service Provider (ISP)** – According to Webopedia.com “It is a company that provides access to the Internet”
- ◎ **Dial-Up Connection** – According to Webopedia.com “It refers to connecting a device to network via a modem and a public telephone network”



Understanding Internet Protocols

- ***Internet Protocols*** –

- A set of standards determining the format and transmission of data

- TCP/IP is the protocol used for E-mail (including SMTP ,POP3, and IMAP)

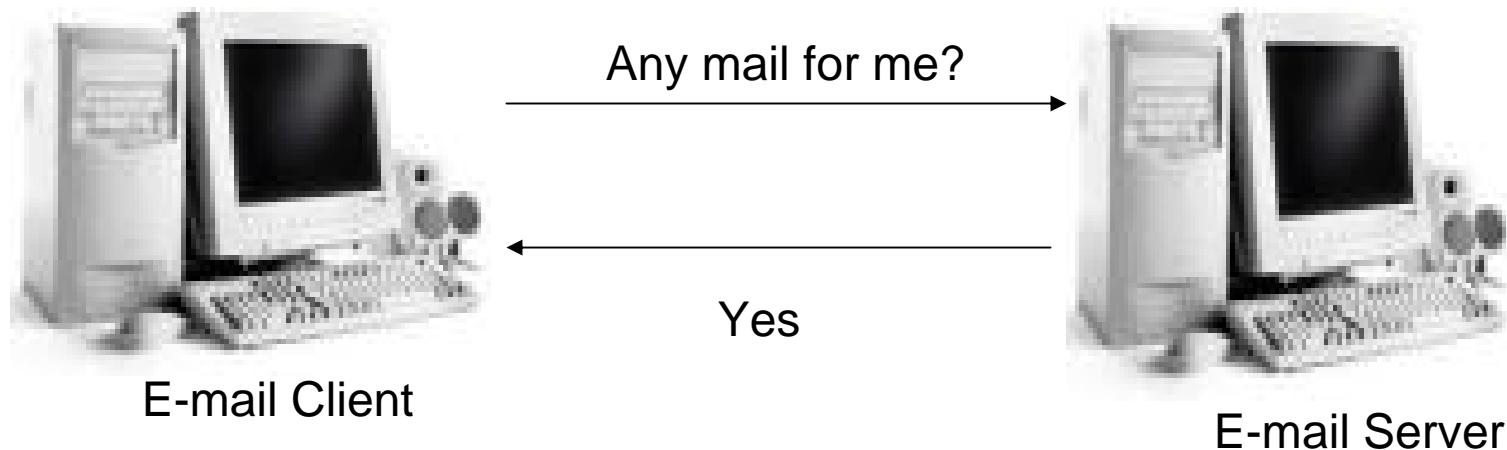
- ***Transmission Control Protocol(TCP)*** –

- A connection-oriented protocol that enables the devices to establish connection and then guarantees the delivery of data in the same order they were sent

- ***Internet Protocol(IP)***-

- It is a connectionless protocol that provides addressing scheme. It operates at the network layer

Exploring the Roles of the Client and Server in E-mail



E-mail Crime

- ◎ **E-mail Crime** is a “new-age crime” that is growing rapidly
- ◎ E-mail crime can be categorized in two ways :
 - **Crime committed by sending e-mails**
E.g. – Spamming, mail bombing
 - **Crime supported by e-mails.**
E.g. – Harassment, child pornography



Spamming, Mail Bombing, Mail Storm

- **Spamming** can be defined as sending unsolicited mails. The more common word for spam is “*junk mails*”
- **Mail bombing** can be defined as the act of sending unwanted mails in excessive amount, which makes recipient’s mailbox full
- According to DictionaryWords.net “**Mail Storm** is flood of incoming mail that brings the machine to its knees”



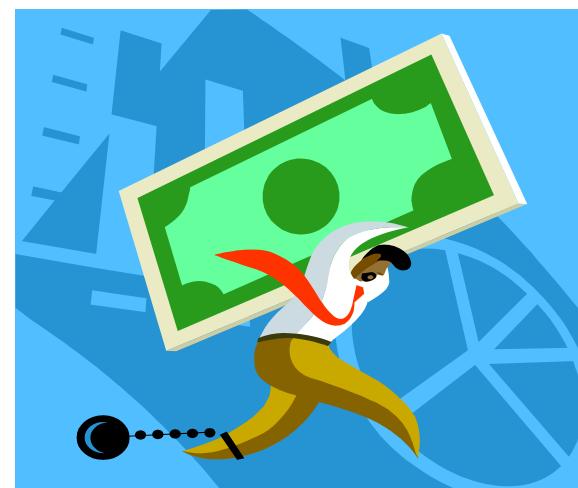
Chat Rooms

- Chat rooms are open target for the pedophiles to use them for the sexual abuse of children
- According to WordNetDictionary “**Child pornography** can be defined as illegal use of children in pornographic pictures and films”
- Internet has become easy-to-use tool for harassment and e-mail has become the most vulnerable feature of it



Identity Fraud , Chain Letter

- ① **Identity fraud** can be defined as using or stealing one's personal information like name, address, and credit card number for economic gain
- ② According to DictionaryWords.net “**Chain Letter** is a letter that is sent successively to several people.”



Sending Fakemail

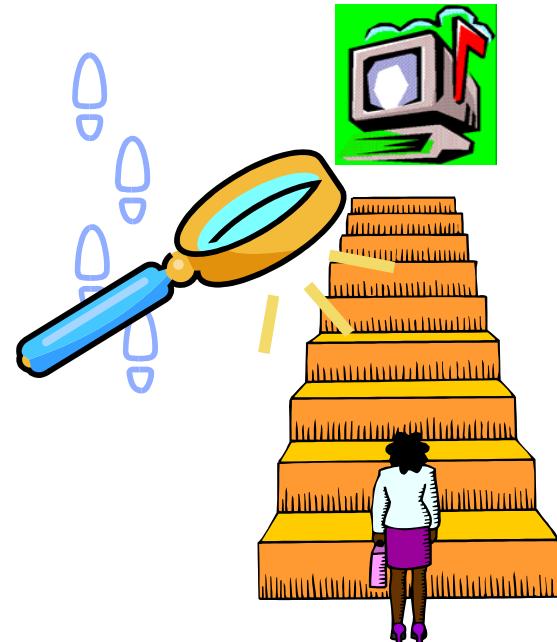
```
% telnet localhost smtp
Trying ::1...
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 server.geektimes.com ESMTP Sendmail ...
helo username
250 server.geektimes.com Hello localhost [127.0.0.1], pleased to meet you
mail from:sender@example.com
250 2.1.0 sender@example.com... Sender ok
rcpt to:recipient@GeekTimes.com
250 2.1.5 recipient@GeekTimes.com... Recipient ok (will queue)
data
354 Enter mail, end with "." on a line by itself
This is a test message from sender@example.com to
recipient@GeekTimes.com.
The next line contains a period followed by the Return key.

.
250 2.0.0 g8S87cpB000444 Message accepted for delivery
quit
221 2.0.0 server.geektimes.com closing connection
Connection closed by foreign host.
%
```

Investigating E-mail Crime and Violation

◎ Investigation process:

- Examining an e-mail message
- Copying an e-mail message
- Printing an e-mail message
- Viewing e-mail headers
- Examining an e-mail header
- Examining attachments
- Tracing an e-mail



Viewing E-mail Headers

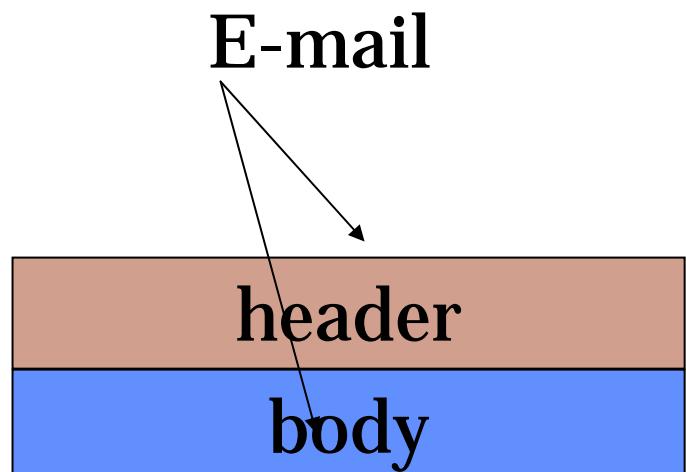
- An e-mail message is composed of two parts:

- **Header**

E-mail header contains information about the email origin like address from where it came, how it reached and who send it

- **Body**

Body contains the message



Examining an E-mail Header

- Navigate My Computer or Windows Explorer to locate the saved e-mail message
- Open the e-mail message

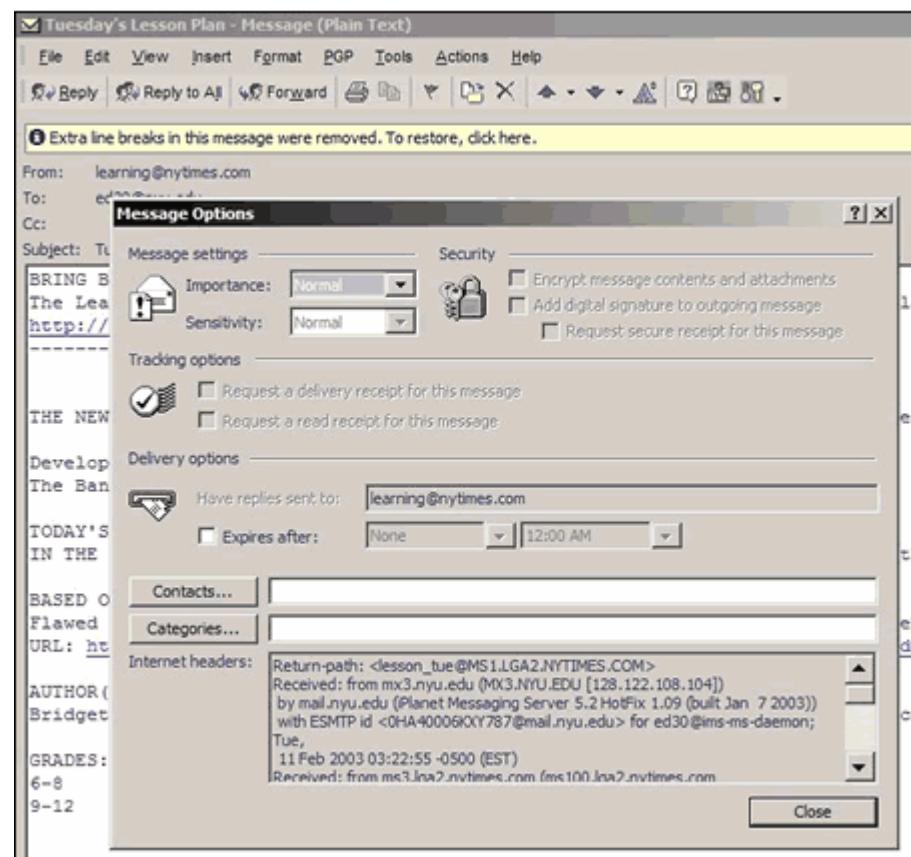


The screenshot shows a Microsoft Notepad window titled "message_header_yahoo.txt - Notepad". The menu bar includes File, Edit, Format, and Help. The main content area displays the following e-mail header information:

```
1. Return-Path: <forensic@yahoo.com>
2. Delieverd To: badguy@jailhouse.com
3. Recieived:(qmail 12780 invoked by uid 0); 12 Dec 2005 08:23:37-0000
4. Recieived: from Unknown(HELO smtp.jailhouse.com)(192.152.64.20) by mail.jailhouse.com with SMTP;12 Dec 2005
08:23:37-0000
5. Recieved: from Web4009.mail.yahoo.com(Web40009.mail.yahoo.com[192.218.78.27])
    by smtp.jailhouse.com(16.12.6/16.12.6) with SMTP id gBC8ILAJ005229
    for<badguy@jailhouse.com>;Thu 12 Dec 2005 00:18:21 -0800
6. Message-ID:<20051212082330.40429.qmail@web40009mail.yahoo.com>
7. Recieved: from[10.187.241.199] by Web4009.mail.yahoo.com via HTTP;Thu 12 Dec 2005 00:23:30 PST
    Date: Thu,12Dec 2005 00:23:30 -0800(PST)
    MIME Version: 1.0
```

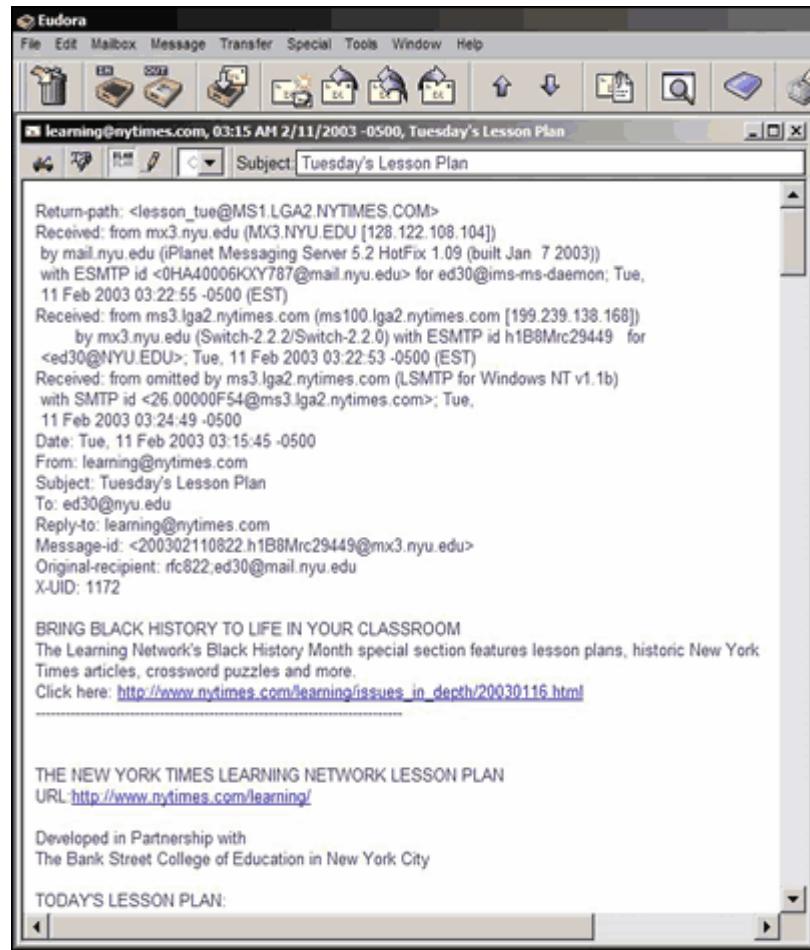
Viewing Header in Microsoft Outlook

- ① Initiate the Outlook program and open the copied email message
- ② Right-click the message received and click Options to open the dialog box
- ③ Select the header text and make a copy of it
- ④ Paste the header text in any text editor and save the file with the name Filename.txt
- ⑤ Close the program



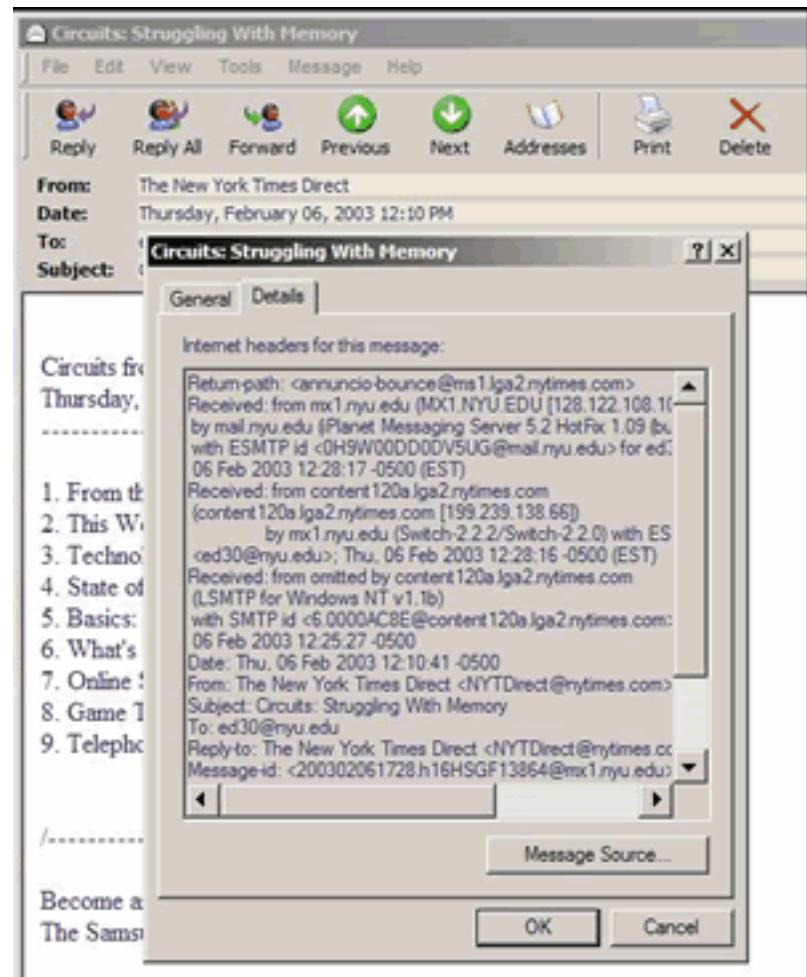
Viewing Header in Eudora

- Initiate Eudora
- Go to the Inbox folder
- Double-click the message received
- Click the BLAH BLAH BLAH button
- Select message header text and copy it
- Paste the text in any text editor and save the file as Filename.txt
- Close the program



Viewing Header in Outlook Express

- ① Initiate the program
- ② Right-click the message received and click Properties
- ③ To view header, click Details
- ④ Press Message Source button to get the details
- ⑤ Select message header text and copy it
- ⑥ Paste the text in any text editor and save the file as Filename.txt
- ⑦ Close the program

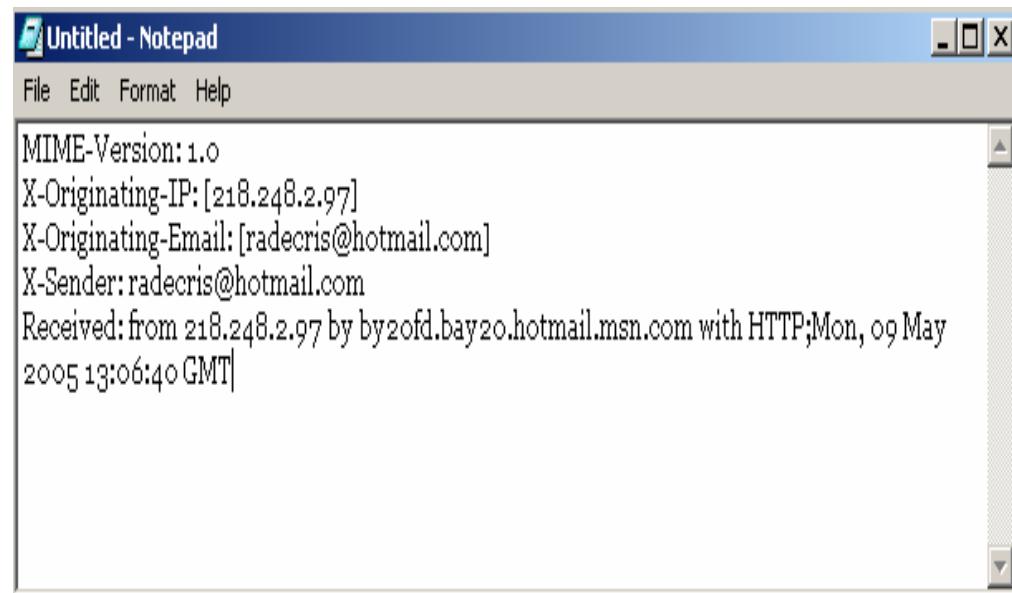


Viewing Header in AOL

- Initiate the program
- Open the received message
- Click the DETAILS link
- Select message header text and copy it
- Paste the text in any text editor and save the file as Filename.txt
- Close the program

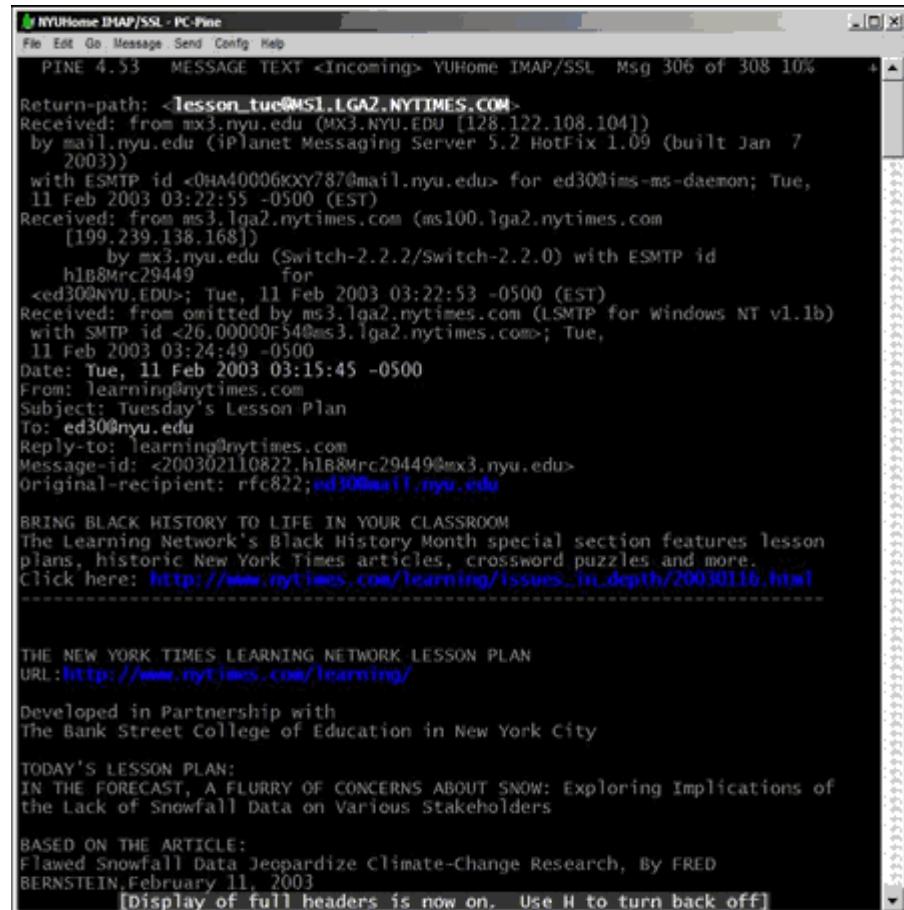
Viewing Header in Hot Mail

- Initiate the program
- Open the received message
- Go to Options and click Preferences. For version8 click Mail Display Settings
- Select message header text and copy it
- Paste the text in any text editor and save the file as Filename.txt
- Close the program



Viewing Header using Pine for Unix

- Initiate the program by typing Pine at command prompt
- For setup options press S
- For the e-mail configuration press C
- Exit the mode of configuration by pressing E
- Save the changes by typing Y
- After selecting the message using arrow keys, select O from the bottom screen
- View header by typing H
- Close the program by typing Q

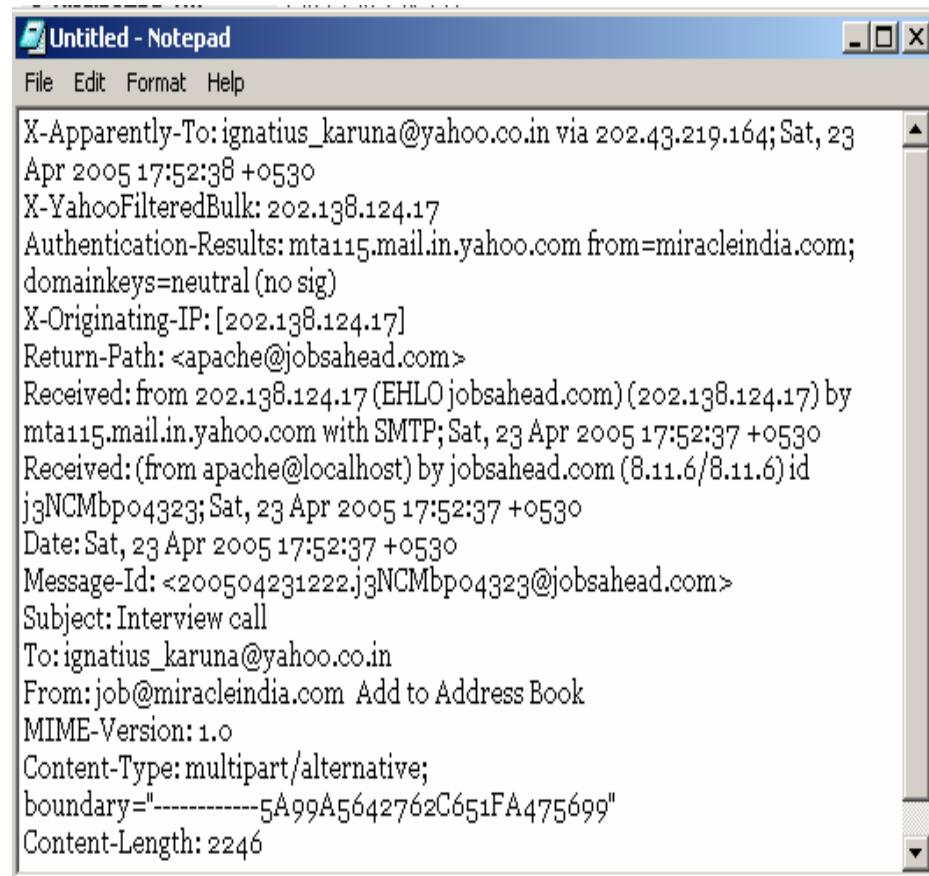


Viewing Header in Juno

- Initiate the program
- Go to E-mail Options
- Select Show Headers under Preferences and save it
- Go to Inbox and open the message to view header

Viewing Header in Yahoo

- Initiate the program
- Go to Mail Options on the right
- Go to the General Preferences link, click Show All headers on incoming messages and save it
- Select message header text and copy it
- Paste the text in any text editor and save the file as Filename.txt
- Close the program



The screenshot shows a Windows Notepad window with the title bar 'Untitled - Notepad'. The menu bar includes 'File', 'Edit', 'Format', and 'Help'. The main content area displays the following email header text:

```
X-Apparently-To: ignatius_karuna@yahoo.co.in via 202.43.219.164; Sat, 23
Apr 2005 17:52:38 +0530
X-YahooFilteredBulk: 202.138.124.17
Authentication-Results: mta115.mail.in.yahoo.com from=miracleindia.com;
domainkeys=neutral (no sig)
X-Originating-IP: [202.138.124.17]
Return-Path: <apache@jobsahead.com>
Received: from 202.138.124.17 (EHLO jobsahead.com) (202.138.124.17) by
mta115.mail.in.yahoo.com with SMTP; Sat, 23 Apr 2005 17:52:37 +0530
Received: (from apache@localhost) by jobsahead.com (8.11.6/8.11.6) id
j3NCMbp04323; Sat, 23 Apr 2005 17:52:37 +0530
Date: Sat, 23 Apr 2005 17:52:37 +0530
Message-Id: <200504231222.j3NCMbp04323@jobsahead.com>
Subject: Interview call
To: ignatius_karuna@yahoo.co.in
From: job@miracleindia.com Add to Address Book
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="-----5A99A5642762C651FA475699"
Content-Length: 2246
```

Examining Additional Files

- E-mail messages are saved as files either on client computer or server
- Microsoft Outlook maintains e-mail in .pst or .ost files
- Online e-mail program like AOL, Hotmail, Yahoo store e-mail messages in folder like history, cookies, and temp
- Unix stores e-mail messages as per user

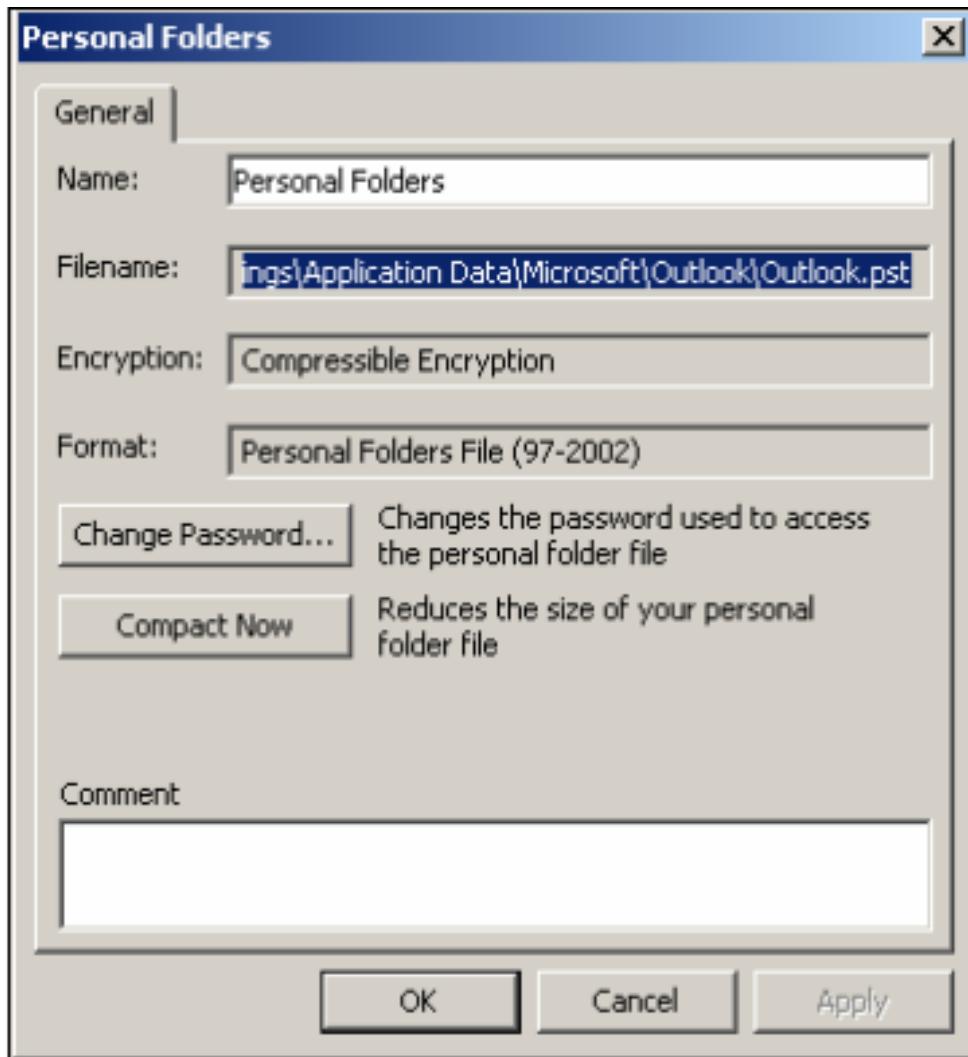


Microsoft Outlook Mail

- ① Microsoft Outlook Mail acts like a personal information manager
- ① The e-mail database is normally located at \user account\Local Settings\Application Data\Microsoft\Outlook directory
- ① The files stored in Outlook Mail are known to be *.pst files
- ① The pst files have archive of all folders like Outlook, Calendar, Drafts, Sent Items, Inbox, notes etc



Pst File Location



Tracing an E-mail Message

- Information regarding the Internet domain registration can be found from:

- www.arin.net
- www.internic.com
- www.freealinity.com
- www.google.com



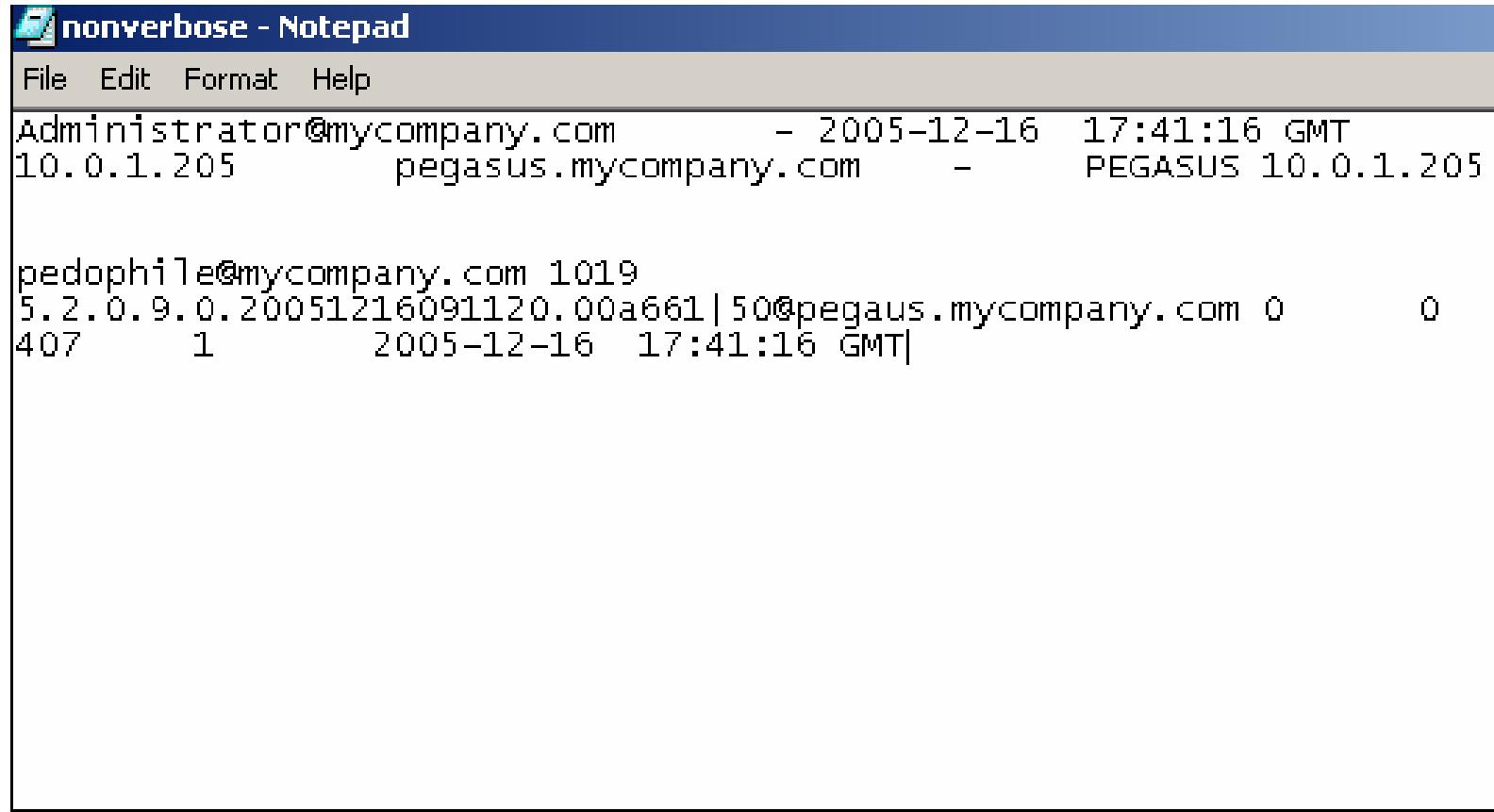
Using Network Logs Related to E-mail

Application Name	PID	Protocol	Local Address:Port	Remote Address:Port
aim.exe	424	TCP	0.0.0.0:3029	Listening for connections
aim.exe	424	TCP	0.0.0.0:3032	Listening for connections
aim.exe	424	TCP	24.46.220.84:3029	64.12.24.104:5190
aim.exe	424	TCP	24.46.220.84:3032	64.12.27.79:5190
alg.exe	488	TCP	127.0.0.1:3007	Listening for connections
LEXPPS.EXE	3D0	TCP	0.0.0.0:1026	Listening for connections
lsass.exe	1B8	UDP	0.0.0.0:500 (isakmp)	Listening for packets
navapw32.exe	338	TCP	127.0.0.1:3013	Listening for connections
svchost.exe	284	UDP	127.0.0.1:2234	Listening for packets
svchost.exe	26C	UDP	0.0.0.0:135 (epmap)	Listening for packets
svchost.exe	284	UDP	192.168.0.1:123 (ntp)	Listening for packets
svchost.exe	284	UDP	192.168.0.1:53 (domain)	Listening for packets
svchost.exe	284	UDP	0.0.0.0:3011	Listening for packets
svchost.exe	284	UDP	192.168.0.1:68 (bootpc)	Listening for packets
svchost.exe	284	UDP	127.0.0.1:3012	Listening for packets
svchost.exe	284	UDP	0.0.0.0:1041	Listening for packets
svchost.exe	284	UDP	24.46.220.84:2234	Listening for packets

www.privacyware.com/

Firewall Log

Understanding E-mail Server



The screenshot shows a Windows Notepad window with the title "nonverbose - Notepad". The menu bar includes "File", "Edit", "Format", and "Help". The main content area displays an e-mail log entry:

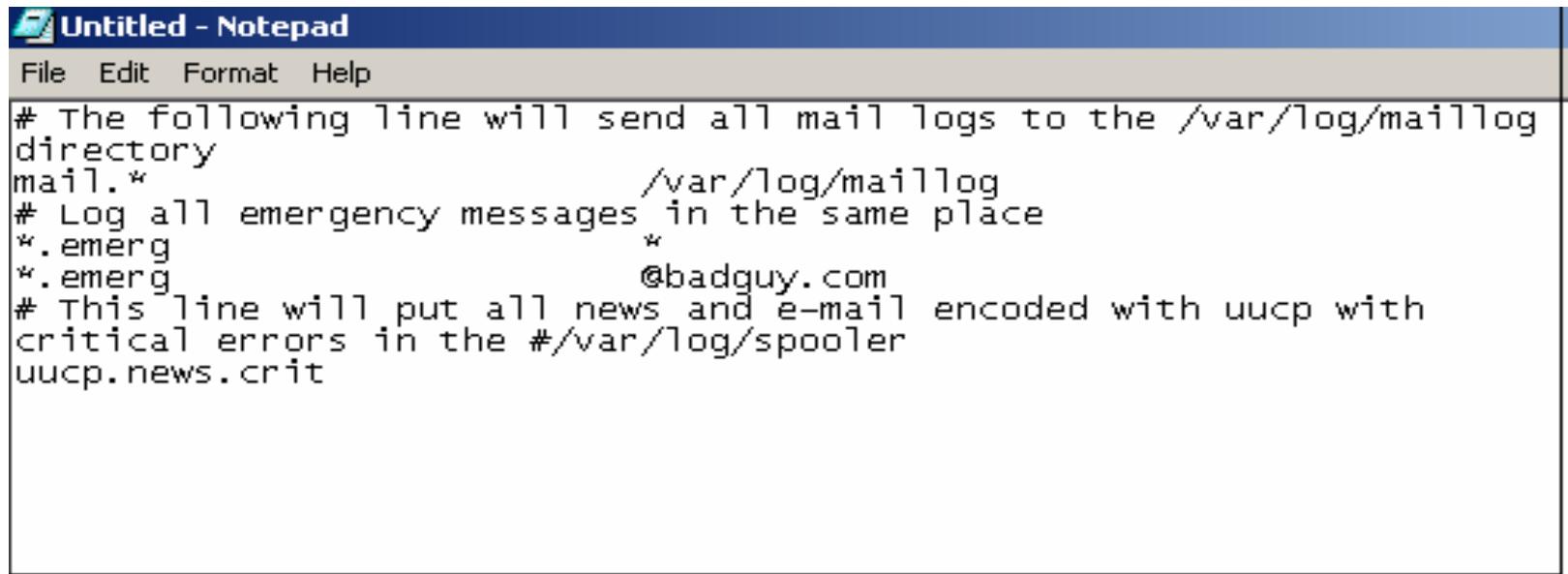
```
Administrator@mycompany.com      - 2005-12-16 17:41:16 GMT
10.0.1.205          pegasus.mycompany.com - PEGASUS 10.0.1.205

pedophile@mycompany.com 1019
5.2.0.9.0.20051216091120.00a661|50@pegaus.mycompany.com 0      0
407      1          2005-12-16 17:41:16 GMT|
```

E-mail server log file

Examining UNIX E-mail Server Logs

- Log files and configuration files provide information related to e-mail investigation
- The **syslog.conf** file gives specification for saving various types of e-mail log files

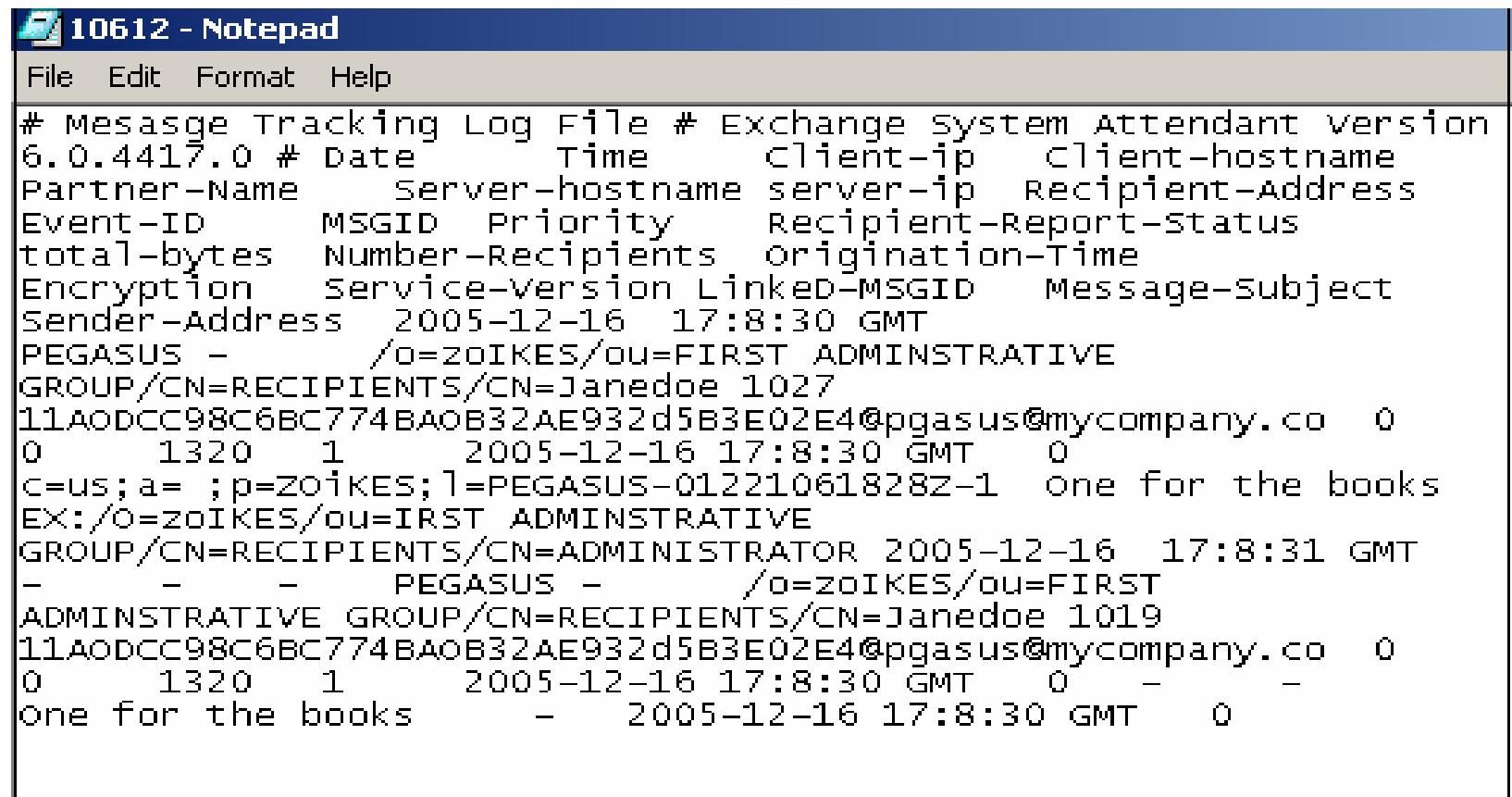


The screenshot shows a Windows Notepad window titled "Untitled - Notepad". The menu bar includes File, Edit, Format, and Help. The main content area contains the following text:

```
# The following line will send all mail logs to the /var/log/maillog directory
mail.*          /var/log/maillog
# Log all emergency messages in the same place
*.emerg         *
*.emerg         @badguy.com
# This line will put all news and e-mail encoded with uucp with
critical errors in the #/var/log/spooler
uucp.news.crit
```

Typical syslog.conf file

Examining Microsoft E-mail Server Logs



The screenshot shows a Microsoft Notepad window titled "10612 - Notepad". The content is a message tracking log from an Exchange System Attendant version 6.0.4417.0. The log entries are as follows:

```
# Message Tracking Log File # Exchange System Attendant version
# 6.0.4417.0 # Date      Time     Client-ip   Client-hostname
# Partner-Name    Server-hostname server-ip   Recipient-Address
# Event-ID        MSGID    Priority    Recipient-Report-status
# total-bytes     Number-Recipients Origination-Time
# Encryption       Service-Version Linked-MSGID   Message-Subject
# Sender-Address  2005-12-16  17:8:30 GMT
PEGASUS -          /o=zoIKES/ou=FIRST ADMINISTRATIVE
GROUP/CN=RECIPIENTS/CN=Janedoe 1027
11AODCC98C6BC774BAOB32AE932d5B3E02E4@pgasus@mycompany.co 0
0      1320  1      2005-12-16 17:8:30 GMT  0
c=us; a= ; p=zoIKES; l=PEGASUS-01221061828Z-1  One for the books
EX:/o=zoIKES/ou=IRST ADMINISTRATIVE
GROUP/CN=RECIPIENTS/CN=ADMINISTRATOR 2005-12-16 17:8:31 GMT
-      -      PEGASUS -          /o=zoIKES/ou=FIRST
ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=Janedoe 1019
11AODCC98C6BC774BAOB32AE932d5B3E02E4@pgasus@mycompany.co 0
0      1320  1      2005-12-16 17:8:30 GMT  0      -
One for the books      -      2005-12-16 17:8:30 GMT  0
```

Message tracking log in verbose mode

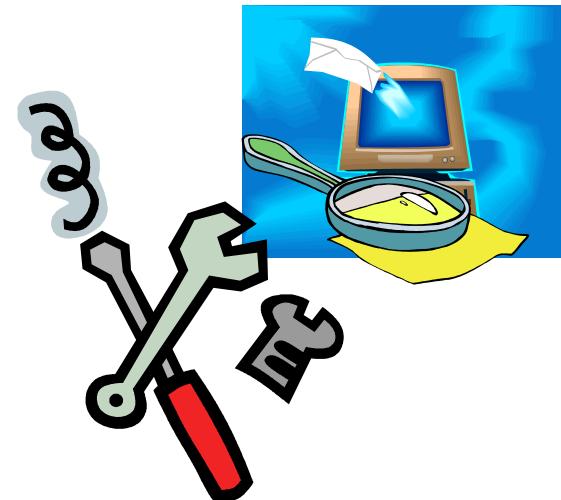
Examining Novell GroupWise E-mail Logs

- **GroupWise** – The Novell e-mail server software is a database server like Microsoft Exchange and UNIX Send mail
- Group Wise organize mailbox in two ways:
 - Permanent index files with IDX extension
 - Group Wise QuickFinder action
- Group Wise manage the e-mail server in a centralized manner using NGWGUARD.Db

Using Specialized E-mail Forensic Tools

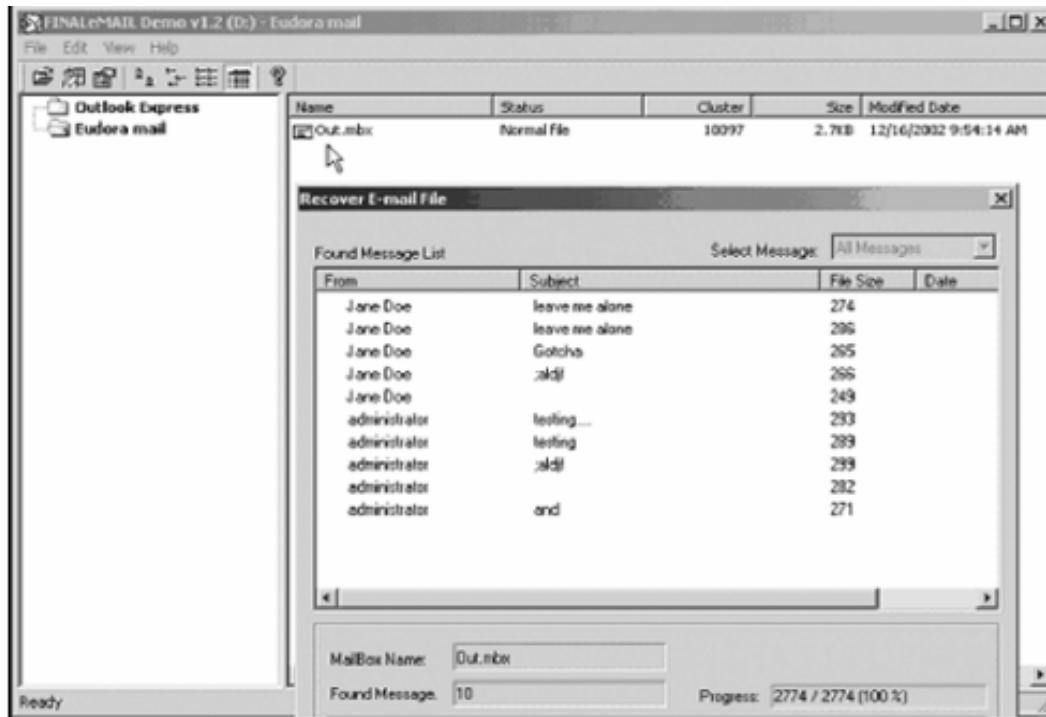
- Tools that can investigate e-mail messages:

- EnCase
- FTK
- FINALeMAIL
- Sawmill-GroupWise
- Audimation for Logging



Tool:FINALeMAIL

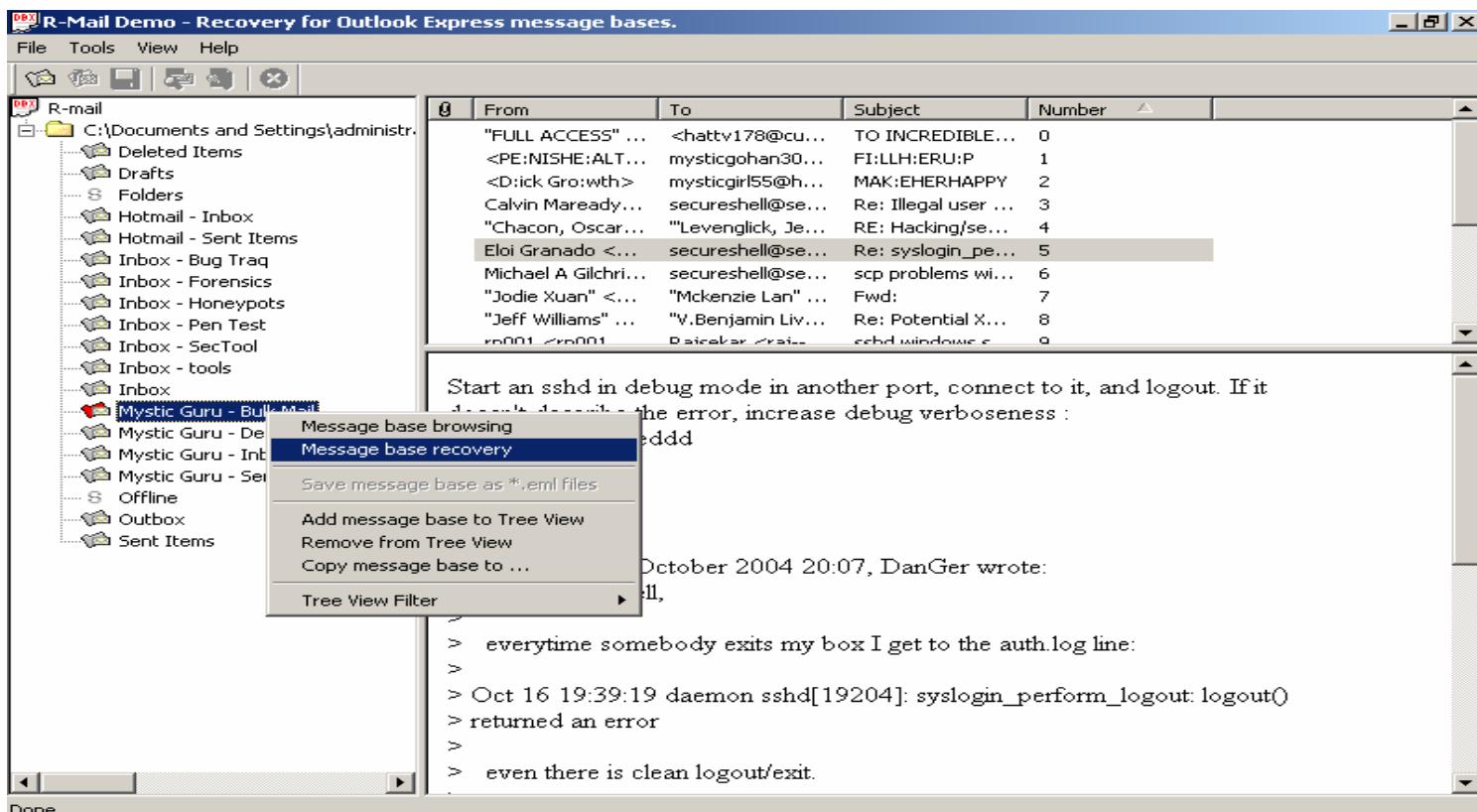
- Can restore lost emails to their original state.
- Can recover the entire e-mail database files



FINALeMAIL e-mail search results

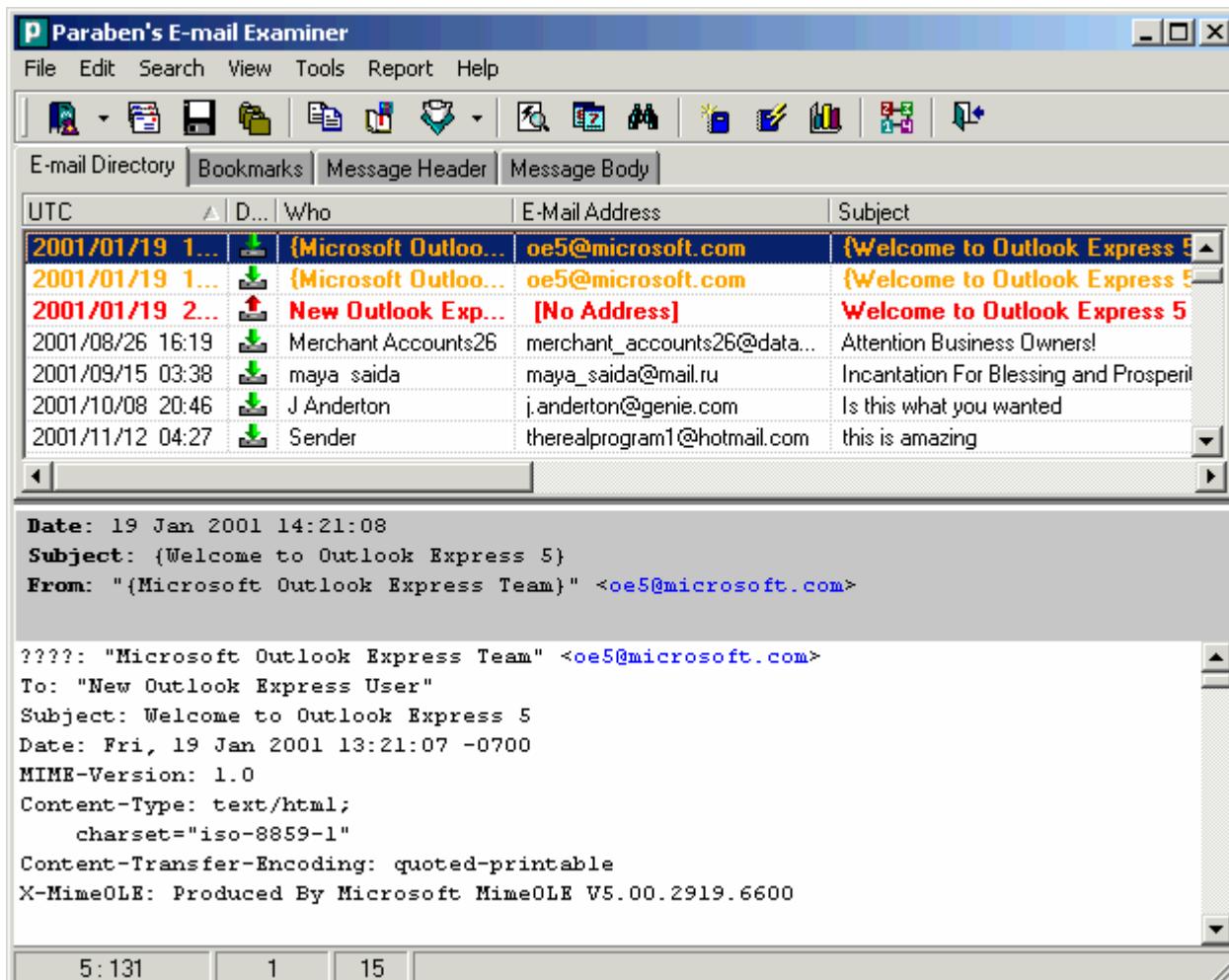
Tool: R-Mail

- ① R-Mail is basically an e-mail recovery tool, which recovers the e-mail messages deleted accidentally



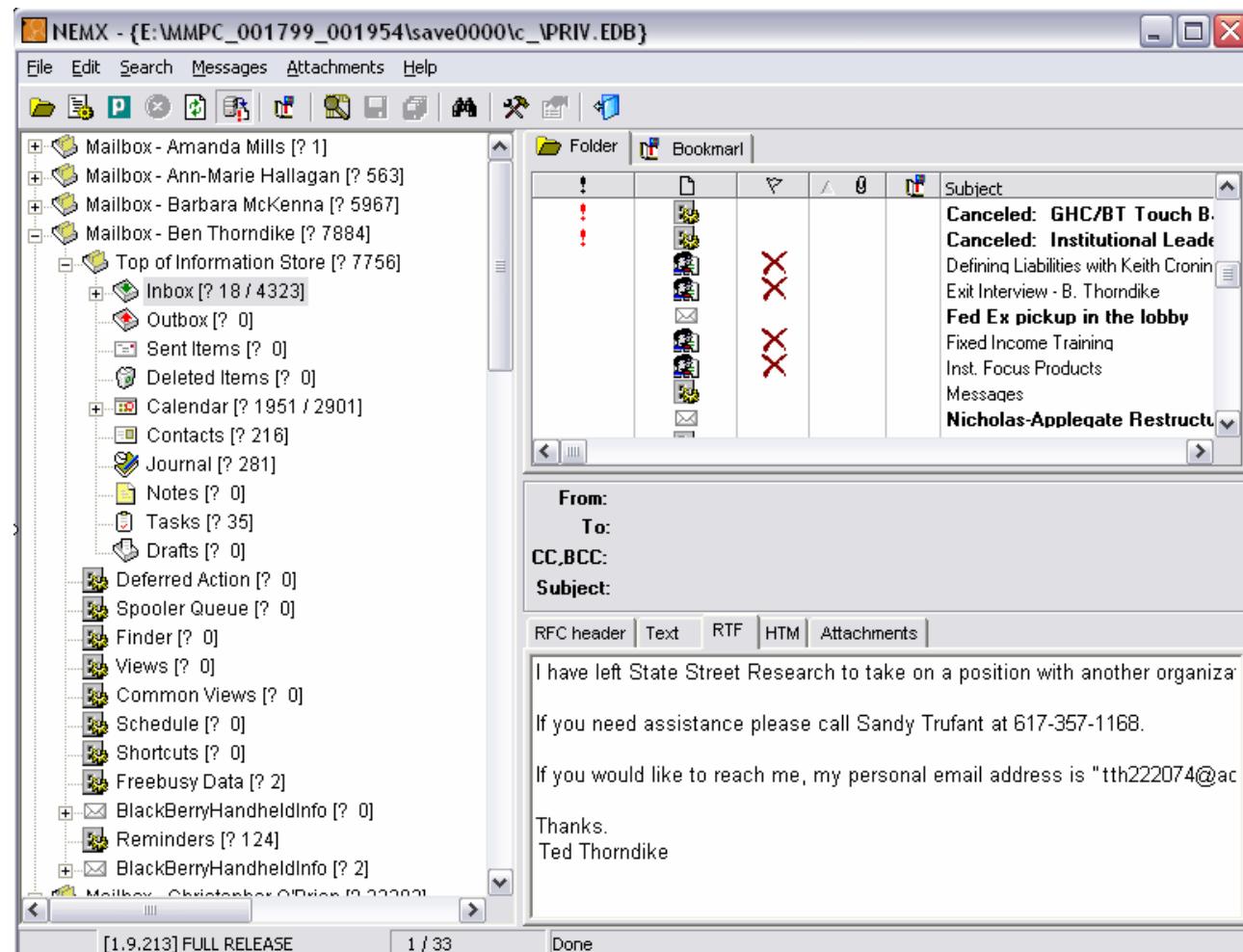
E-Mail Examiner by Paraben

- Deleted mails can be recovered
- Examines more than 14 mail types
- Recovers email deleted from deleted items
- Supports Windows 95/98/2000/2003/NT 4/ME/XP



Network E-Mail Examiner by Paraben

- Examine variety of network e-mail archives like Exchange Server, Lotus Domino Server etc
- Views all the individual email accounts
- Supports Microsoft Exchange and Lotus Notes



Tracing Back

- The first step in tracing back fakemail is to view the header information
- The header will show the originating mail server ex: mail.example.com
- With a court order served by law enforcement or a civil complaint filed by attorneys, obtain the log files from mail.example.com to determine who sent the message



Tracing Back Web Based E-mail

- Web based e-mail accounts (Webmail) can make establishing the identity of the sender more difficult
- It is possible to create a new online Webmail account easily

- www.hotmail.com
- www.yahoo.com
- www.lycosmail.com
- www.hushmail.com

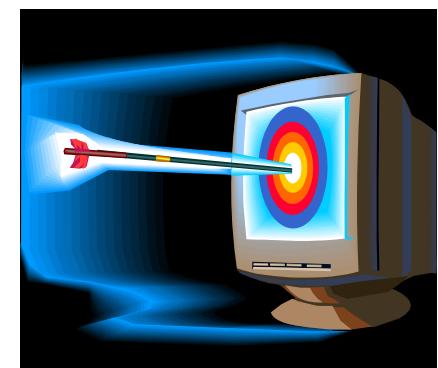


- The above sites maintain the source IP address of each connection that accesses the online webmail
- Contact the mail provider (ex: Microsoft) to reveal subscriber information

Searching E-mail Addresses

- Internet search engines make the search of specific e-mail addresses easy
- The following sites provide e-mail searching services:

- <http://www.emailaddresses.com>
- <http://www.dogpile.com>
- <http://www.google.com>
- <http://www.altavista.com>
- <http://www.infospace.com>
- <http://www.mamma.com>
- <http://www.searchscout.com>



E-mail Search Site

- **EmailChange.com** is the one providing the Internet's first email change registry and search engine since Oct 1996

The screenshot shows the homepage of EmailChange.com. At the top left is a logo featuring a globe with three computer monitors on a blue background. Below the logo is the URL <http://www.emailchange.com>. The main title "EmailChange.com" is in large blue letters with a trademark symbol. A dark blue banner below the title contains the text "The Internet's FREE **Change of E-mail Address** Registry & Search Engine". Below the banner, two bullet points are listed:

- **FREE Registration of your OLD & NEW Email Address**
- **FIND Someone's NEW Email Address by Searching for their OLD one**

The page is divided into four main sections:

- E-mail Address Search**: A box containing text about finding a friend's changed email address and a "Search Now!" button.
- FREE E-mail Address Registration**: A box containing text about registering a new email address and a "Register Now!" button.
- Search Area**: A box containing a text input field for "Enter Old Email Address OR Person's Name", a "SEARCH NOW!" button, and a link to "(Advanced Search)".
- Registration Area**: A box containing a text input field for "OLD Email Address", a text input field for "NEW Email Address", a "REGISTER NOW!" button, and a link to "(Advanced Registration)".

Handling Spam

- Before taking legal action send a short notice on the illegality of spam to the system administrator of the domain

Ladies and Gentlemen:

The enclosed spam mail is being forwarded to you because your system name or that of a system for which you are a listed system admin appears in the headers or as a reference in the text. As you are doubtless aware, this sort of electronic junk mail is completely contrary to established guidelines for use of the Internet email service. Please take whatever steps are necessary to see that this person sends out no more of these, and that this practice is curtailed on your system.

By US Code Title 47, Sec.227(a) (2) (B), a computer/modem/printer meets the definition of a telephone fax machine. By Sec.227(b) (1) (C), it is unlawful to send any unsolicited advertisement to such equipment. By Sec.227 (b) (3) (C), a violation of the aforementioned Section is punishable by action to recover actual monetary loss, or \$500, whichever is greater, for each violation.



Network Abuse Clearing House

NETWORK **ABUSE** CLEARINGHOUSE

Look up an address in the abuse.net contact database

Enter the name of the domain that you would like to check, such as example.com.



Look up another domain



Return to the [abuse.net home page](#).

This page updated: 09/05/2003

© 1999-2001 I.E.C.C.

Abuse.Net

- Abuse.net provides a platform to report abusive activity on the Internet to people who can do something about it
- It provides only complaining services and has nothing to do with blacklist or spam analysis services
- Once registered, messages can be sent to domain-name@abuse.net where source of abusive practices is the domain-name and from there message is re-mailed to the best reporting address(es)

Protecting Your E-mail Address From Spam

- One way to protect is to "encode" the e-mail address, making it more difficult to discover

Worldwide Contact at EC-Council

General Enquiries
E-Mail: info@eccouncil.org

Membership
E-Mail: ethan@eccouncil.org

Certification and Exams
E-Mail: jesse@eccouncil.org

- Be cautious before giving e-mail address online as posting email address on web-site will make spam the inbox

Tool: Enkoder Form

- Enkoder Form is a powerful tool designed to prevent e-mail harvesting

The Basic Form

Email Address:

The email address to be displayed

Link Text:

The text users will see and click

Link Title:

The "pop-up" text seen when your mouse is over the link

Subject (Optional):

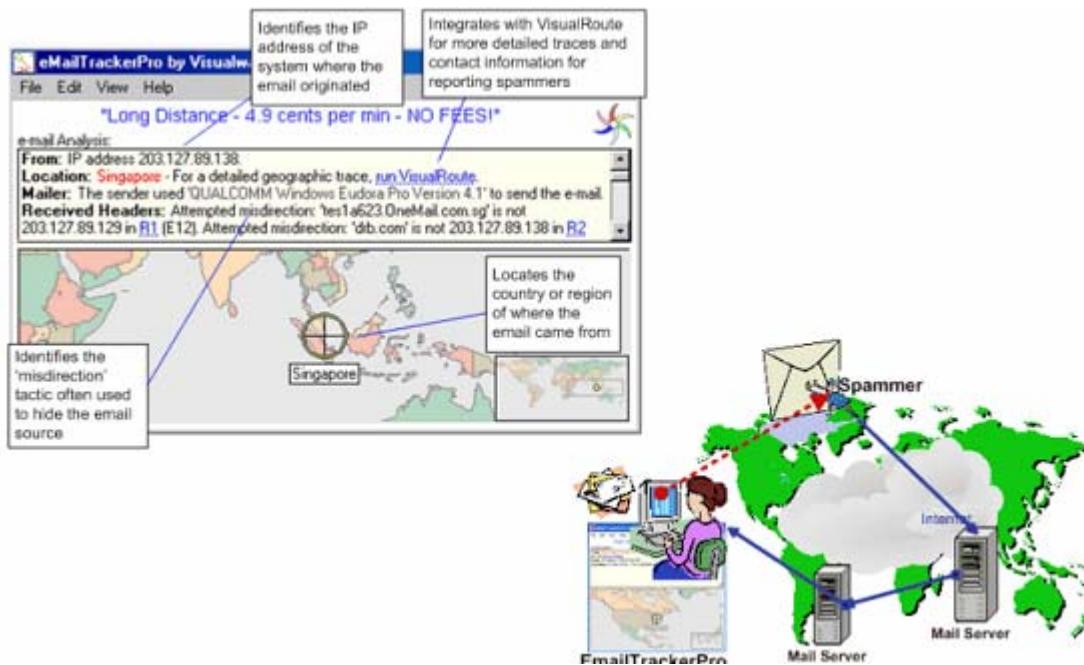
An optional subject line for the email

Enkode It >

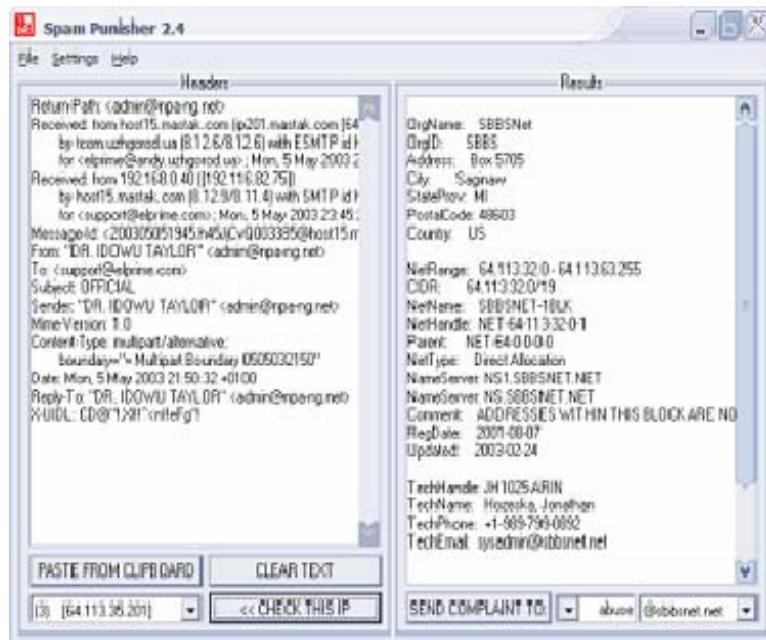
<http://automaticlabs.com/cgi-bin/index.cgi>

Tool:eMailTrackerPro

- eMailTrackerPro analyzes the e-mail header and provides the IP address of the machine that sent the e-mail



Tool:SPAM Punisher



- ④ This anti-spam tool makes the search for spammer ISP address easy
- ④ A complain can be send to the ISP of the sender using *Send Complaint to*

Summary

- To investigate an e-mail, know how an e-mail server records and handles e-mail messages
- E-mail servers are databases of user information and e-mail messages
- All e-mail servers contain a log file which can tell valuable information when investigating a crime
- For many e-mail investigations, rely on the message files, e-mail headers, and e-mail server log files to investigate e-mail crimes



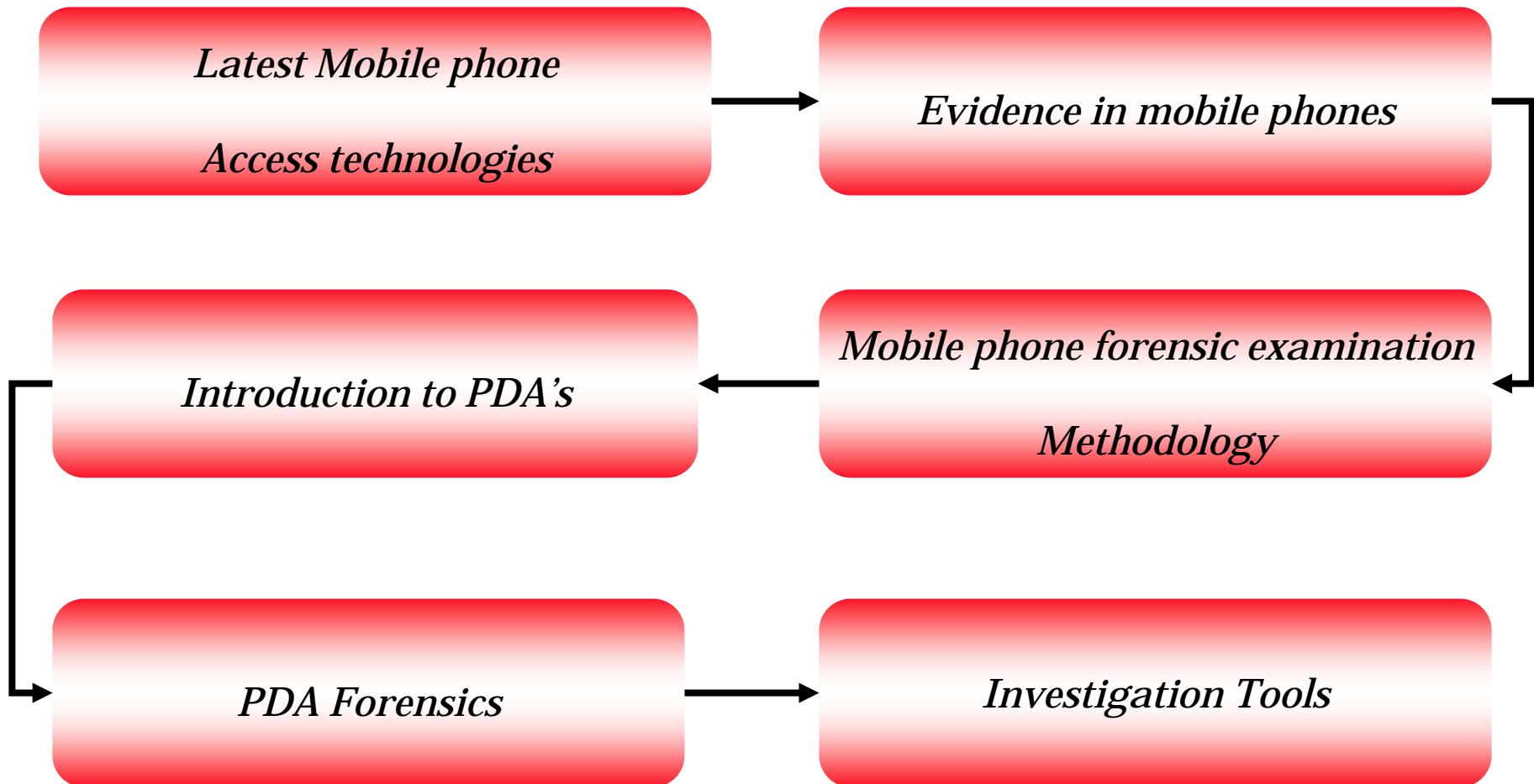
Computer Hacking Forensic Investigator

Module XXI
Mobile and PDA Forensics

Module Objective

- Latest Mobile phone Access technologies
- Evidence in Mobile phones
- Mobile phone Forensic Examination Methodology
- Introduction to Personal Digital Assistants (PDAs)
- PDA Forensics
- Investigation Tools

Module Flow



Latest Mobile Phone Access Technologies

- GSM - Global System for Mobile communications
- UMTS - Universal Mobile Telephone Standard
- CDMA - Code Division Multiple Access
- GPRS - General Packet Radio Services
- Flash OFDM - Orthogonal Frequency Division Multiplexing
- Bluetooth

Evidence in Mobile Phones

- Subscriber Identity Module (SIM) in GSM/UMTS
 - Contains user related information
- Phone Internal Memory
 - Majority of the phone information is stored in the Internal memory
- Flash memory cards
 - Usually accessed as a file system where the user may move the items from the Phone or SIM memory
- Information from the Network providers
 - Call data records



Mobile Phone Forensic Examination Methodology

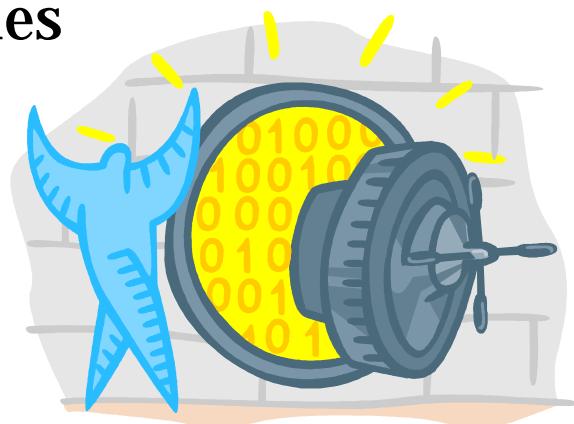
1. Switch off the phone to avoid contamination
2. Examining evidence media separately to avoid contamination
3. Acquiring access codes from the user or service provider for examining SIM
4. Examining flash memory cards
5. Examining internal phone numbers by taking a bit stream backup of the phone memory



Examining Phone Internal Memory

Creating a bit stream backup of the memory content

- ◉ Desolder the memory chip and read off its contents
 - Phone might get destroyed beyond repair
- ◉ Hooking on to the phone system board and read off the memory chip
 - Can bypass any security access mechanism that is used by the phone like phone specific PIN-codes

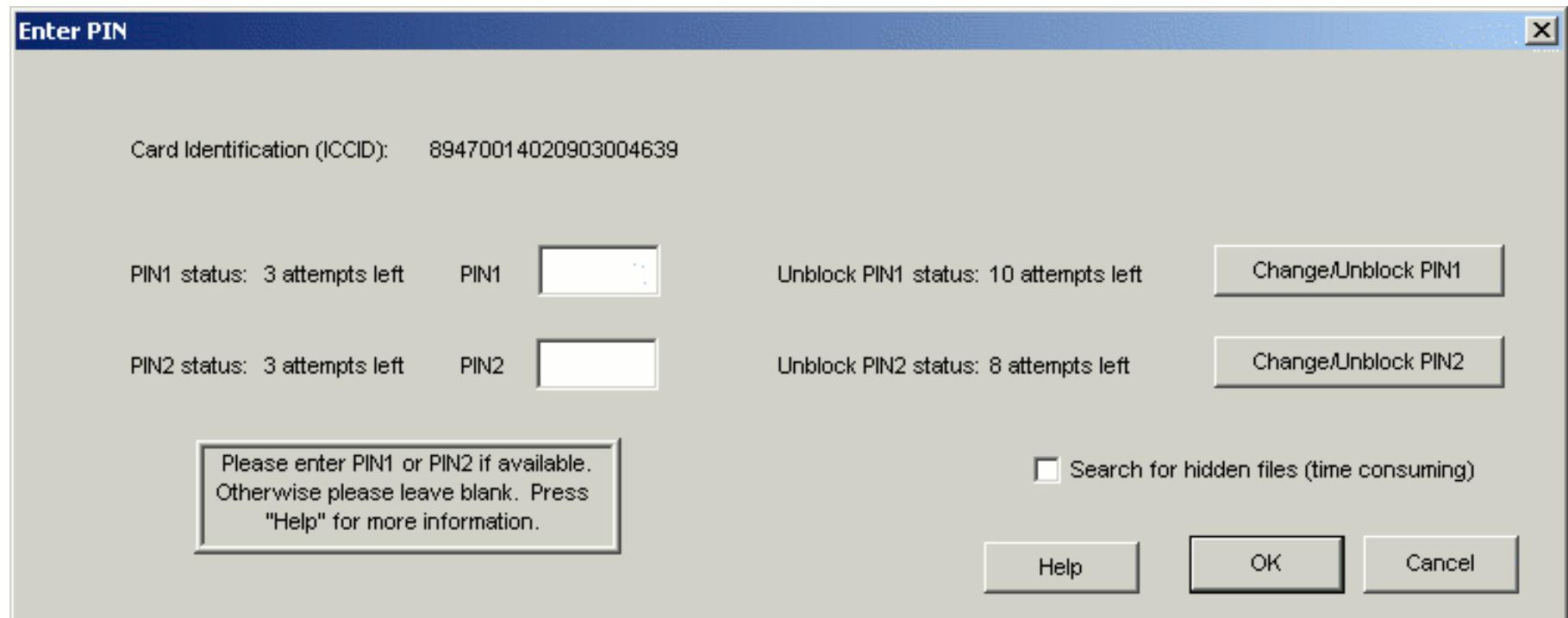


Examining SIM

- Examine using any standard smart card reader
- Tool: **SIMCon – SIM Content Controller**
 - Allow the user to securely image all files on a GSM SIM card to a computer file with a standard smart card reader
 - User can later examine the contents of the card including stored numbers and text messages
 - Enables the user to read all available files on a SIM card and store in an archive file
 - Examine and interpret content of file including text messages and stored numbers
 - Recover deleted text messages stored on the card
 - Manage PIN and PUK codes

SIMCon – Screenshot

Reading SIM



SIMCon - Screenshot

The screenshot shows the SIMCon software interface. On the left is a tree view of SIM card data, including MF, EF_ICCID, DF_GSM, DF_TELECOM (with sub-items like EF_ADN, EF_FDN, EF_SMS, EF_CCP, EF_MSISDN, EF_SMSS, EF_LND), and Short Message 1 through 12. The right side displays a table of messages with columns for Item, Value, and File. Below this is a detailed content view for 'Short Message 8'.

Item	Value	File
Short Message 1	(in) Any chance to see you Today?	EF_SMS
Short Message 2	(out) w8 10 sec	EF_SMS
Short Message 3	(out) hello darling, i will be late today. loads of work...	EF_SMS
Short Message 4	(in) Ok	EF_SMS
Short Message 5	(in) Not AGAIN! See you tonight	EF_SMS
Short Message 6		EF_SMS
Short Message 7	(del) Hi again sweetie. That bitch still believes me. Your pl...	EF_SMS
Short Message 8	(del) Hi again sweetie. That bitch still believes me. Your pl...	EF_SMS
Short Message 9	(in) Ok see you later sexy,	EF_SMS
Short Message 10		EF_SMS
Short Message 11		EF_SMS
Short Message 12		EF_SMS

Content:

Short Message 8:

```
Status : deleted
Service Center Type of Number : international
Service Center Numbering plan : E.164 ISDN
Service Center Number : 4790002100
Message Type (TP-MTI) : SMS-SUBMIT
Reply Path (TP-RP) : no RP
Status Report Request (TP-SRR) : status report not requested
Message Reference (TP-MR) : 213
Destination Type of Number : international
Destination Numbering plan : E.164 ISDN
Destination Address (TP-DA) : 4741428707
Protocol Identifier (TP-PID) : mobile-mobile
Data Coding Scheme-Coding : GSM
Data Coding Scheme-Class : Immediate display
Data Coding Scheme-Class : 
Validity Period : 63 weeks
Text : Hi again sweetie. That bitch still believes me. Your place at 5?
```

**SIM Files
and Content**

SIMCon - Screenshot

File permissions and Hash

The screenshot shows a software interface titled "SIMCon - Screenshot". On the left is a tree view of file paths under "DF_GSM" and "DF_TELECOM". The main area is a table with columns: Update, Increase, Invalidate, Rehabilitate, and Hash. The table lists various file names and their corresponding permissions and hash values.

	Update	Increase	Invalidate	Rehabilitate	Hash
ways	O1 - PIN1	OF - Never	OE - Administr...	OE - Administr...	85 E5 32 71 E1 40 06 F0 26 5
ways	O1 - PIN1	OF - Never	OE - Administr...	OE - Administr...	85 E5 32 71 E1 40 06 F0 26 5
ways	O1 - PIN1	OF - Never	OE - Administr...	OE - Administr...	85 E5 32 71 E1 40 06 F0 26 5
ways	OE - Administr...	OF - Never	OE - Administr...	OE - Administr...	5B A9 3C 9D B0 CF F9 3F 52 I
N1	O1 - PIN1	OF - Never	OE - Administr...	O1 - PIN1	69 51 10 9C 8C A0 21 27 73 C
N1	O1 - PIN1	OF - Never	OE - Administr...	O1 - PIN1	83 6A 31 45 44 D4 CF EC D4
N1	O1 - PIN1	OF - Never	OE - Administr...	O1 - PIN1	5B A9 3C 9D B0 CF F9 3F 52 I
ways	OE - Administr...	OF - Never	OE - Administr...	OE - Administr...	5B A9 3C 9D B0 CF F9 3F 52 I
N1	O1 - PIN1	OF - Never	OE - Administr...	OE - Administr...	8E 44 FF A1 3E 8C C4 D0 44
N1	O1 - PIN1	OF - Never	OE - Administr...	OE - Administr...	68 94 91 2D 76 DC A5 D1 2B
N1	O1 - PIN1	OF - Never	OE - Administr...	OE - Administr...	BD 9F CB 33 E1 34 E0 13 99 4
N1	O1 - PIN1	OF - Never	OE - Administr...	OE - Administr...	1E D3 8E 0F D9 C2 33 A6 31
N1	O1 - PIN1	OF - Never	OE - Administr...	OE - Administr...	C1 C4 45 B3 FC 75 1E 3A 80
N1	O1 - PIN1	OF - Never	OE - Administr...	OE - Administr...	31 49 14 4D 78 38 5F 6C 28 E
N1	O1 - PIN1	OF - Never	OE - Administr...	OE - Administr...	DE 90 67 FF 40 F0 B4 62 43 C
N1	O1 - PIN1	OF - Never	OE - Administr...	OE - Administr...	69 1C 70 00 93 54 BC B8 EE 2
N1	O1 - PIN1	OF - Never	OE - Administr...	OE - Administr...	FC D4 34 7A E2 7D E6 79 44 I
N1	O1 - PIN1	OF - Never	OE - Administr...	OE - Administr...	EC 88 AA E2 2E BB E6 3B 3F E

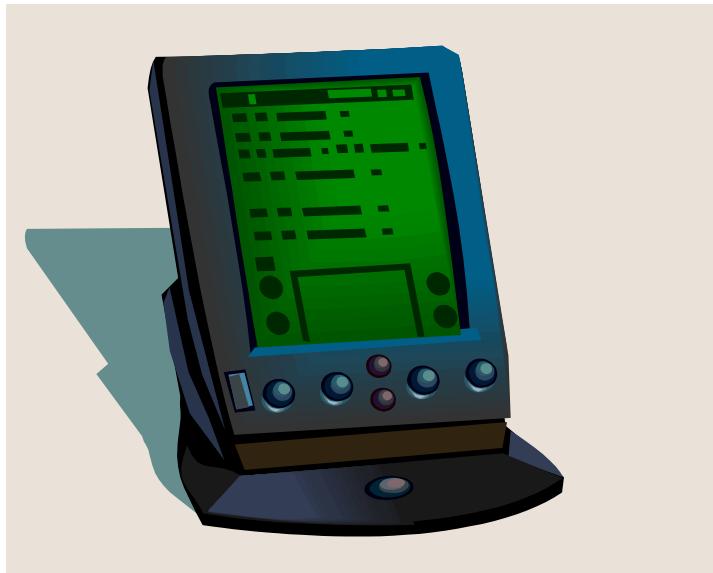
Examining Flash Memory and Call data records

- Flash memory cards normally utilize FAT file system
- Can be read by attaching the device to a computer
- Forensic tools must be used to prevent modifications in original evidence
- Tools include EnCase, Accessdata Forensic Toolkit, SMART and WinHex
- Call data records includes
 - Originating number
 - Terminating number
 - Originating and terminating equipment number
 - Call duration
 - Type of service
 - Initial serving base station

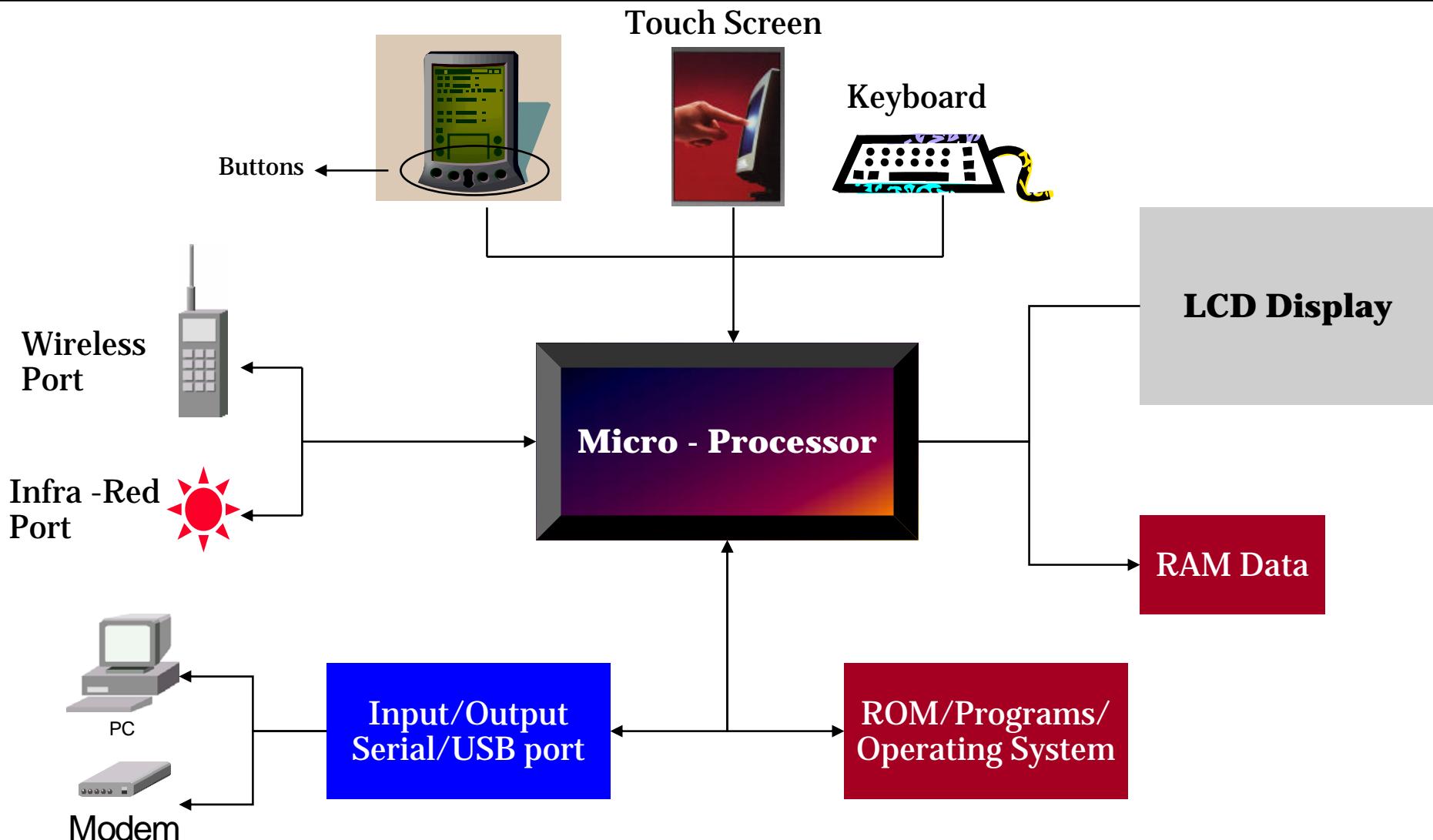
Personal Digital Assistant (PDA)

According to Webopedia.com, PDA is

- *A handheld device that combines computing, telephone/fax, Internet and networking features*
- *A Device that can function as a cellular phone, fax sender, Web browser and a personal organizer*



PDA Components



PDA Forensics

- Examination
- Identification
- Collection
- Documentation



PDA Forensics - Examination

◉ Sources of Evidence

- Device
- Device Cradle
- Power Supply
- Other Peripherals and Media

◉ Removable media are identified by

- The number of pins or pin receptacles located on the media
- The placement of pins or pin receptacles located on the media

◉ Memory cards and PC's synchronized with PDA should also be examined

PDA Forensics - Identification

- Identify type of device
- Identify type of operating system
 - Some PDA's may run two operating systems
- Interfaces that allow identification of a device
 - Cradle Interface
 - Manufacturer Serial number
 - The Cradle type
 - Power Supply

PDA Forensics - Collection

- Collect other memory devices such as
 - SD
 - MMC or CF semiconductor cards
 - microdrives and
 - USB tokens must also be collected
- Seize power leads, cables, the manual and cradles of the PDA
- Do not abandon but gather any damaged equipments

PDA Forensics - Collection

- ◉ Collect both dynamic and volatile information
 - Volatile information must be given priority
- ◉ PDA must be switched off while seizure
 - If switched on during collection
 - Document the time and date of the current device state
- ◉ PDA must be put in an envelope and then kept in the evidence bag
- ◉ The power adaptor should be connected to the PDA through the evidence bag for charging

PDA Forensics - Documentation

- Record all visible data
- Document the following during labeling
 - Case number
 - A precise description of the case
 - Date and time evidence was collected
- All devices connected to the PDA must be photographed and documented
- Create a report documenting the state of the device during collection
- Maintain chain of custody
- All the documentations must be preserved in a secure location

Points to Be Remembered While Conducting Investigation

◎ If the device is switched on

- Preserve device in active state with sufficient power
- Take a photograph of the device
- If charge is low, then replace the battery or charge with a proper power adaptor
- Maintain sufficient charge in the replacement batteries

◎ If device is switched off

- Leave device in off state
- Switch on the device and record current battery charge.
- Take a photograph of the device

Points to Be Remembered While Conducting Investigation

◎ If device is in its cradle

- Avoid any further communication activities.
- Remove USB/Serial connection from PC
- Seize cradle and chords

◎ If device is not in its cradle

- Seize cradle and chords

◎ If wireless is on/off

- Avoid further communication activities.
- Eliminate wireless activity by packing the device in an envelope, anti-static bag and an isolation envelope
- Take away wireless enabled cards

Points to Be Remembered While Conducting Investigation

- If card present in expansion card slot
 - Do not initiate any further activity inside the device
 - Do not remove any peripheral/media card
- If card not present in expansion card slot
 - Seize related peripheral/media cards.
- If expansion sleeve is removed
 - Seize expansion sleeve
 - Seize other related peripherals/media cards.

PDA Seizure by Paraben

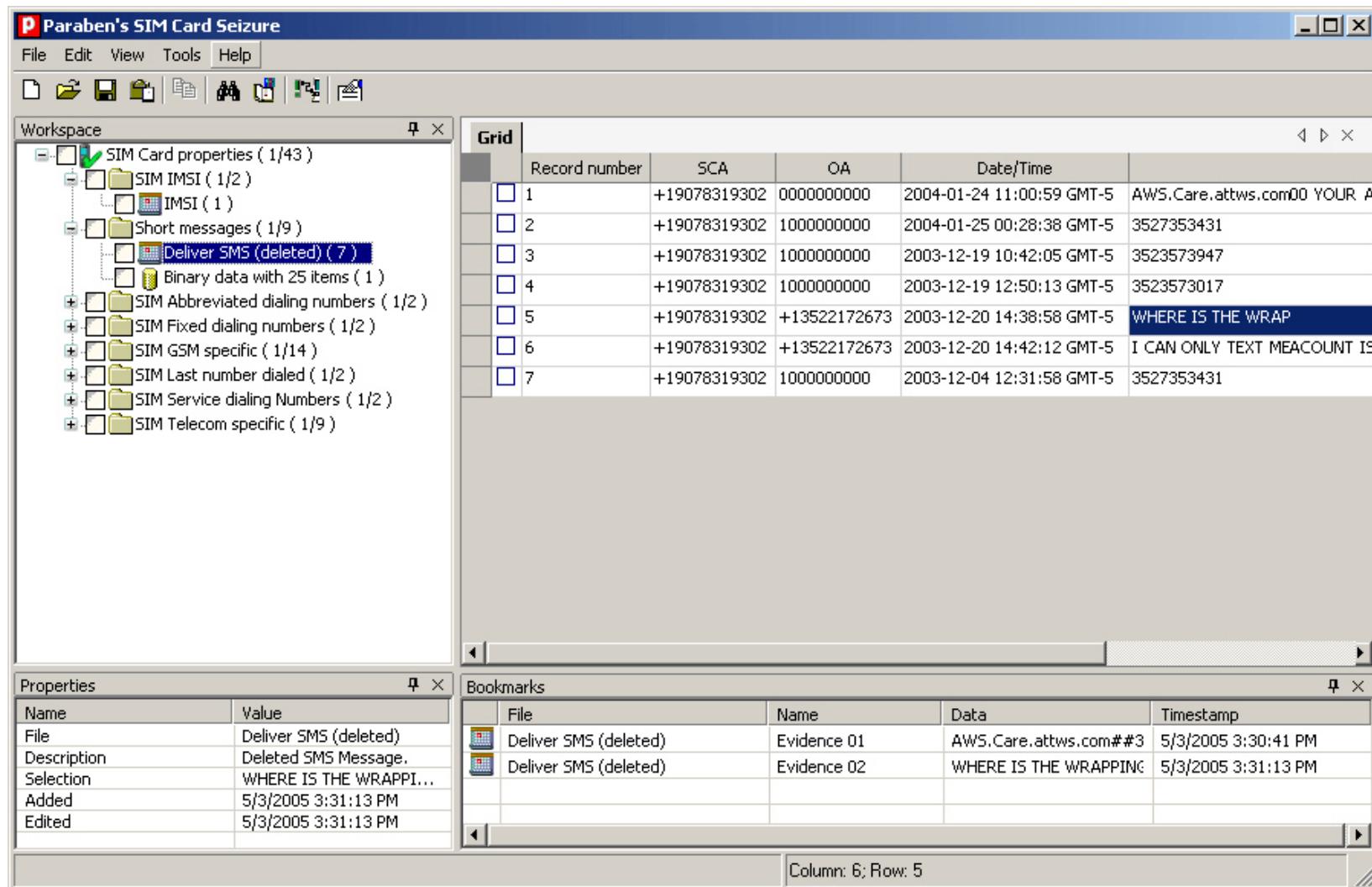
- Paraben's PDA Seizure is a comprehensive tool that allows PDA data to be acquired, viewed, and reported on, all within a Windows environment
- You can also analyze Palm data that is stored on a PC

The screenshot shows the Paraben PDA Seizure application window. The title bar reads "PDA Seizure - C:\Program Files\Paraben Corporation\PDA Seizure\Jornada.PDA". The menu bar includes File, Edit, Tools, View, and Help. Below the menu is a toolbar with various icons. The main area has tabs for Files, Search, Graphics, and Bookmarks, with Files selected. A table lists 634 files with columns for File Path, File Name, Type, Create Date, Modify Date, Attributes, Size, Status, L..., and MD5 Hash. The table shows various file types like Registry, MemoryImage, .ink, .wma, .pxt, .psw, and .pwi, along with their acquisition status (Acquired or RAM) and file sizes.

File Path	File Name	Type	Create Date	Modify Date	Attributes	Size	Status	L...	MD5 Hash
	Registry					3,966	Registry		3050A80D7
	MemImage					3,680	MemoryImage		F2C444104
\Program Files\Win default.lnk	.lnk		2000/01/01 20	2000/01/01 20:A		23	Acquired	RAM	6BD33A62:
\My Documents\Welcome To W.wma	.wma		2000/01/01 20	2000/01/01 20:A		24	Acquired	RAM	818AA698:
\My Documents\Te Vehicle Mileage.pxt	.pxt		2000/01/01 20	2000/01/01 20:HRA		7,498	Acquired	RAM	9C91BBEFE
\My Documents\Te To Do.psw	.psw		2000/01/01 20	2000/01/01 20:HRA		2,616	Acquired	RAM	0F7982DEE
\My Documents\Te Phone Memo.p.psw	.psw		2000/01/01 20	2000/01/01 20:HRA		2,008	Acquired	RAM	9443F21C4
\My Documents\Te Memo.psw	.psw		2000/01/01 20	2000/01/01 20:HRA		2,112	Acquired	RAM	523694AF6
\My Documents\Te Meeting Notes.psw	.psw		2000/01/01 20	2000/01/01 20:HRA		1,908	Acquired	RAM	40FB8E424
\My Documents\Te Blank Documen.psw	.psw		2000/01/01 20	2000/01/01 20:HRA		0	Acquired	RAM	
\My Documents\Te To Do.pwi	.pwi		2000/01/01 20	2000/01/01 20:HRA		3,096	Acquired	RAM	B25EAC50:
\My Documents\Te Phone Memo.p.pwi	.pwi		2000/01/01 20	2000/01/01 20:HRA		2,008	Acquired	RAM	7F2CCAB0I
\My Documents\Te Memo.pwi	.pwi		2000/01/01 20	2000/01/01 20:HRA		2,112	Acquired	RAM	CAC4C826
\My Documents\Te Meeting Notes.pwi	.pwi		2000/01/01 20	2000/01/01 20:HRA		1,592	Acquired	RAM	B876D7DE
\My Documents\Te Blank Note.pw.pwi	.pwi		2000/01/01 20	2000/01/01 20:HRA		0	Acquired	RAM	
\Windows\Home M HP game buttc.lnk	.lnk		2000/01/01 20	2000/01/01 20:A		18	Acquired	RAM	72E4BACB:
\Windows\Home M HP backup.lnk	.lnk		2000/01/01 20	2000/01/01 20:A		20	Acquired	RAM	8DA836DA
\Windows\Home M Regional Settir.lnk	.lnk		2000/01/01 20	2000/01/01 20:A		28	Acquired	RAM	E0723177E
\Windows\Home M Network.lnk	.lnk		2000/01/01 20	2000/01/01 20:A		28	Acquired	RAM	AD4F5D1A
\Windows\Home M Clock.lnk	.lnk		2000/01/01 20	2000/01/01 20:A		28	Acquired	RAM	2FA61C9B:
\Windows\Home M Modem.lnk	.lnk		2000/01/01 20	2000/01/01 20:A		28	Acquired	RAM	AC946E0E:
\Windows\Home M PC.lnk	.lnk		2000/01/01 20	2000/01/01 20:A		28	Acquired	RAM	C02FC610:
\Windows\Home M Today.lnk	.lnk		2000/01/01 20	2000/01/01 20:A		28	Acquired	RAM	6A65E55E3
\Windows\Home M Buttons.lnk	.lnk		2000/01/01 20	2000/01/01 20:A		28	Acquired	RAM	7CCAC999

634 Files

SIM Card Seizure by Paraben (SIM Card acquisition tool)



Forensic Tool – Palm dd (pdd)

- Command line driver program used to perform a physical acquisition of data from Palm OS devices
- Integrated by paraben in PDA Seizure and used for extracting data from a Palm OS device
- Programmed to run on the Motorola DragonBall Processor
- Allows the user to acquire an image of every bit of the PDA's memory can be collected
- The output is in binary form and some in ASCII characters
- <http://www.atstake.com>

Forensic Tool - POSE

- A Program that can be executed on various operating systems
- It functions exactly as a Palm OS hardware device, only if a suitable ROM image is attached to it
- Allows the examiner to view and operate the imaged device
- It is programmed to run, test and debug Palm OS applications without loading them on to the device. It is useful for presentations and taking screenshots of evidence
- It can be configured to map the Palm OS serial port to any of the serial ports of a computer
- <http://www.palmos.com>

Summary

- The SIM of a mobile phone is considered to be a crucial evidence
- SIMCon allows the user to securely image all files on a GSM SIM card to a computer file with a standard smart card reader
- PDAs can function as a cellular phone, fax sender, Web browser and a personal organizer.
- PDA forensics include Examination, Identification, Collection and Documentation
- Seize the cradle and chords attached to the PDA even if the device is in or not in the cradle



Computer Hacking Forensics Investigator

Module XXII

Investigating Trademark and
Copyright Infringement

Scenario

The News Community was shocked by the infamous “ Jayson Blair scandal” in the spring of 2003.

Jayson Blair, a reporter with New York Times, was accused of plagiarizing works from other news papers. The New York Times accused him of goofing up reports from other parts of the state while he was in town.

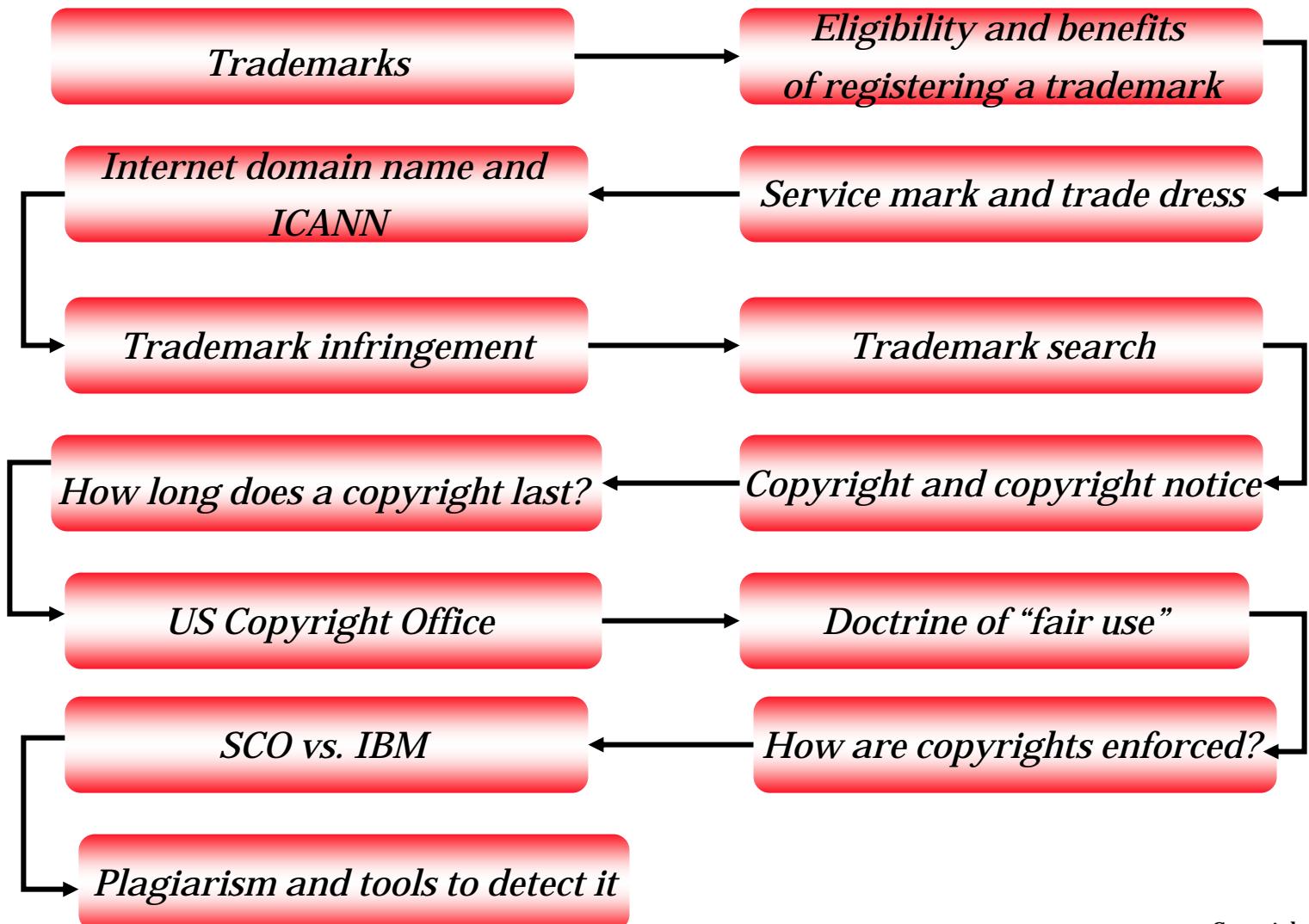
On May 1, 2003 Jayson Blair resigned from the post.

The act of Jayson Blair put the credibility of New York Times at stake.

Module Objective

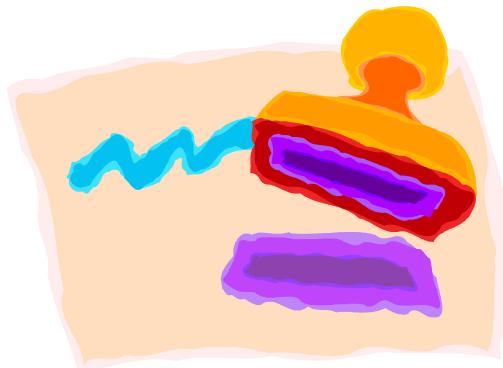
- Trademarks
- Trademark eligibility and benefits of registering it.
- Service mark and trade dress
- Internet domain name
- Trademark infringement
- Trademark search
- Copyright and copyright notice
- Copyright “fair use” doctrine
- U.S. Copyright office
- How are copyrights enforced?
- SCO vs. IBM
- What is plagiarism?
- Turnitin
- Plagiarism detection tools

Module Flow



Trademarks

- ◉ According to **www.uspto.gov** “*A trademark is a word, phrase, symbol or design, or a combination of words, phrases, symbols or designs, that identifies and distinguishes the source of the goods of one party from those of others*”
- ◉ Trademarks, are of following types namely:
 - Service marks
 - Collective marks
 - Certification marks



Trademark Eligibility and Benefits of Registering It

- ◉ Individual/Business unit intending to use a trademark to categorize its goods or services
- ◉ Trademark should be unique and not misleading
- ◉ Benefits of registering a trademark are as follows:

- Protects an organization's name/logo, which is an important asset
- Owner attains exclusive rights of the mark
- Protection against Trademark infringement



Service Mark and Trade Dress

- According to **www.uspto.gov** “*A service mark is any word, name, symbol, device, or any combination, used, or intended to be used, in commerce, to identify and distinguish the services of one provider from services provided by others, and to indicate the source of the services*”
- **www.nolo.com** defines trade dress as “*In addition to a label, logo or other identifying symbol, a product may come to be known by its distinctive packaging*”

Trademark Infringement

- ◉ According to **www.legal-definitions.com**
“An infringement is the authorized use of another’s right or privilege, usually an intellectual property right, such as a patent, copyright, or trademark”
- ◉ A party that owns the rights to a particular trademark can sue other parties for trademark infringement based on the standard “*likelihood of confusion*”



Trademark Search

- Trademark search is primarily done to verify the existing ones so that if a particular trademark is selected, there would not be a case of trademark infringement
- Websites such as www.uspto.gov, www.google.com, www.thomasregister.com and www.whois.net can be used as a tool for searching trademarks
- The website of Sunnyvale Center for Invention, Innovation, and Ideas; www.sci3.com and Thomson & Thomson; www.thomson-thomson.com should also be looked for



 United States Patent and Trademark Office

[Home](#) | [Site Index](#) | [Search](#) | [FAQ](#) | [Glossary](#) | [Guides](#) | [Contacts](#) | [eBusiness](#) | [eBiz alerts](#) | [News](#) | [Help](#)

[Trademarks](#) > [Trademark Electronic Search System \(TESS\)](#)

Trademark Electronic Search System(Tess)

TESS was last updated on Fri Apr 29 04:00:52 EDT 2005

[PTO HOME](#) | [TRADEMARK](#) | [TESS HOME](#) | [NEW USER](#) | [STRUCTURED](#) | [FREE FORM](#) | [BROWSE DICT](#) | [BOTTOM](#) | [HELP](#)

[Logout](#) Please logout when you are done to release system resources allocated for you.

Record 1 out of 1

[Check Status](#) (*TARR contains current status, correspondence address and attorney of record for this mark. Use the "Back" button of the Internet Browser to return to TESS*)



Word Mark C EH CERTIFIED ETHICAL HACKER
Goods and Services IC 016. US 002 005 022 023 029 037 038 050. G & S: Educational publications, namely, educational technology training manuals for e-business, e-commerce and security technologies; printed instructional, educational, and teaching materials and vouchers for e-business, e-commerce and security technologies. FIRST USE: 20011023. FIRST USE IN COMMERCE: 20011023
Mark Drawing (3) DESIGN PI US WORDS I FTTFRS AND/OR NUMRFRS

Copyright and Copyright Notice

- According to USPTO “*Copyright is a form of protection provided to the authors of “original works of authorship” including literary, dramatic, musical, artistic, and certain other intellectual works, both published and unpublished*”
- Though not compulsory to include copyright notice for works that are published after March 1, 1989, it is advisable to include one
- A copyright notice for visually perceptible copies should have the word “Copyright” followed by the symbol “©”, published date and name of author/owner of the entire copyright rights in the published work



Investigating Copyright Status of a Particular Work

- ◉ Given below are three basic ways to investigate the copyright status of a particular work
 - By examining the copy of work for finding elements included in the copyright notice
 - Doing a search at the copyright office
 - Have Copyright Office search for one's purpose
- ◉ While investigating the status changes made under Copyright Act of 1976; the Berne Convention Implementation Act of 1988, the Copyright Renewal Act of 1992, and the Sonny Bono Copyright Term Extension Act of 1998 must be considered

How Long Does a Copyright Last?

- ⦿ Duration of copyright is different for joint works, anonymous works ,works that have pseudo names or for “ work for hire” kind of works
- ⦿ In general, copyrights for works that are published after 1977 are valid for a life span of the author plus another 70 years after his/her death
- ⦿ Works published before 1923 in the USA are in the public domain
- ⦿ Copyrights for works published between 1923 and 1977 have a validity of 95 years from the date of first publication



U.S Copyright Office

- ◎ In 1897 the U.S Copyright Office came into existence as a separate department of the Library of Congress, with Thorvald Solberg appointed as the first Registrar of Copyrights
- ◎ Following are the missions of the U.S Copyright Office
 - To administer the copyright law
 - To create and maintain the public record
 - Providing technical support to Congress
 - Providing information service to the public
 - To serve as a resource to international and domestic communities
 - Providing support to the Library of Congress

Doctrine of “Fair Use”

- Section 107 of the Copyright Law mentions the doctrine of “fair use”
- The doctrine is a result of a number of court decisions over the years
- Reproduction of a particular work for criticism, news reporting, comment, teaching, scholarship, and research is considered as fair according to Section 107 of the Copyright Law



How Are Copyrights Enforced?

- ◉ Lawsuit can be filed against anyone who has violated the rights of the copyright owner
- ◉ In this regard the copyright owner can
 - Issue orders to prevent escalation of copyrights
 - Ask for compensation from the infringer for the damage done
 - Ask the infringer to pay the attorney's paycheck



SCO Vs. IBM

- On 7th March 2003 SCO filed a civil lawsuit of \$1 billion against IBM. The damages were later incremented to \$3 billion and then \$5 billion
 - source www.wikipedia.com
- SCO claims that IBM breached contract with its predecessors regarding the non disclosure of the UNIX code
- SCO Lawsuit claims Linux contains plagiarized UNIX source code.
- Updates regarding this lawsuit can be obtained from www.groklaw.net

SCO Vs Linux

SCO UNIX System V Copyright Infringements in Linux®

Literal Copying Line-for-line code copied from System V into Linux kernels 2.4+	Derivative Works Modifications of System V created by vendors contributed to Linux kernels 2.4+ in violation of contracts
Obfuscation Copying, pasting, removing legal notices, reorganizing the order of the programming structures	Non-literal transfers Methods, structures and sequence from System V contributed to Linux kernels 2.4+

Source: SCO Forum 2003

Line by Line Copying

System V Code

```
/* Copyright (c) 1990, 1991 UNIX System  
Laboratories, Inc. */  
/* Copyright (c) 1984, 1986, 1987, 1988, 1989,  
1990 AT&T */  
/* All Rights Reserved */  
  
/* THIS IS UNPUBLISHED  
PROPRIETARY SOURCE CODE OF */  
/* UNIX System Laboratories, Inc. */  
/* The copyright notice above does not  
evidence any actual or intended publication of  
such source code. */  
  
#ιδεντ    ΑΞ(">#)υτσ-χομμ:υτιλ/ξξξξ.χ  
1.3Α  
#ινχλυδε <υτιλ/παραμ.η>  
#ινχλυδε <υτιλ/τψπεσ.η>  
#ινχλυδε <σωχ/σψστμ.η>  
...  
...
```

Linux Kernel Code

```
/* This file is subject to the terms and
conditions of the GNU General Public
* License. See the file "COPYING" in the
main directory of this archive for more
details.

* Copyright (C) 1992 - 1997, 2000-2002
xxxxxxxxx, Inc. All rights reserved.

*/
#include <linux/types.h>
#include <linux/slab.h>
#include <asm/sn/xxx.h>
#include <asm/sn/addrs.h>
...
```

Plagiarism

- ⦿ According to www.hyperdictionary.com plagiarism “*is an act of taking someone's words or ideas as if they were your own*”
- ⦿ The plagiarism act can prove costly especially to students as they would be given a failing grade for a particular paper or a class if their work is found to be plagiarized
- ⦿ Paraphrasing original ideas without quoting the source is an act of plagiarism



Turnitin

- Turnitin is an online plagiarism detection tool mainly targeted at educators and students
- Turnitin detects plagiarism by a comparative study of the work submitted to pages available on the Internet and its database
- Key features include plagiarism prevention, peer review, Grademark, Gradebook, digital portfolio
- <http://www.turnitin.com>

Turnitin Screenshot

The screenshot shows the Turnitin homepage as it would appear in Microsoft Internet Explorer. The browser window has a blue title bar with the text "Turnitin® - Microsoft Internet Explorer". Below the title bar is a toolbar with standard buttons for Back, Forward, Stop, Home, Search, Favorites, Media, and others. The address bar shows the URL "http://www.turnitin.com/static/home.html?session-id=0efdc796acf1edbd1c27bd49121cd29b". The main content area displays the Turnitin logo at the top left, followed by a banner image showing students in a classroom setting. The banner text reads: "What if the Internet could help students take more responsibility for learning and let teachers focus on teaching? NOW IT CAN." To the right of the banner is a login form with fields for "email address" and "password", a "Log In" button, and a "security" link. Below the login form are links for "password help" and "create a user profile". A red navigation bar at the top of the page includes links for HOME, PRODUCTS & SERVICES, TRAINING, FAQS, PRESS, LEGAL, and ABOUT US. On the left side, there's a sidebar with sections for "WHAT'S NEW" (links to success stories and training movies), "TURNITIN'S PRODUCT HIGHLIGHTS" (links to Plagiarism Prevention, GradeMark™, Peer Review, and GradeBook), and a "TESTIMONIALS" section featuring a quote from Prof. Gillian Mothersill, Ryerson University. The right side of the page contains a sidebar with links for "New to Turnitin?", "Training Materials", "Turnitin Tour", and "Pricing & Licensing". At the bottom right, there's a "Read more testimonials" link.

Turnitin Screenshot

The screenshot shows a Turnitin Originality Report interface. On the left, the 'Report text' window displays a paragraph about wireless networks. On the right, the 'Source' window shows the same text from a source article by BOB BREWIN. A yellow box highlights the similarity index of 75% matching text. Another yellow box points to the 'View different versions of each report, based on custom analysis' link. A third yellow box points to the 'Print version shows list of links with paper text' link. A fourth yellow box points to the 'Use the tabs to navigate through all matching sources' link at the top right. A fifth yellow box points to the 'Exclude and re-analyze selected sources to customize your report' link. A sixth yellow box points to the 'Link opens a new window directly to the source; info distinguishes between current and expired Web pages, student database matches, and commercial database content' link.

Turnitin Originality Report (Side-by-Side View)

version: # 1 (04-04-03)

author: Ed...
title: Is S...
submitted: 04-04-03
paper ID: 1123054
similarity index: 75% (75% matching text)

Report text:

hop onto their net... offices, and other completely unprotected.

Similarity index indicates percentage of a paper for which we found matching sources

print version help

links (% match): 13% 11% 8% 7% 7% 6% 4% 2% 2% 2% next 10

url: http://www.computerworld.com/mobiletopics/mobile/story/0.108_01.74321.00.html

info: This is an Internet source. For all Internet sources, we first try to display the "live" web page linked to above. If the page has changed or moved, we display a text version stored in our database.

Source:

Home > Bro... > wireless > Story

Link opens a new window directly to the source; info distinguishes between current and expired Web pages, student database matches, and commercial database content

Sniffing, war-chalking and more: A wireless vocabulary evolves

By BOB BREWIN
SEPTEMBER 17, 2002

War-driving

Wireless LAN war drivers routinely cruise their immediate areas in cars equipped with laptops loaded with a wireless LAN card, an external high-gain antenna and a GPS receiver. The wireless LAN card and GPS receiver feed signals into freeware, such as NetStumbler, which detects APs and their identifiers along with their GPS-derived locations. NetStumbler also automatically detects whether or not built-in Wi-Fi Wired Equivalent Protocol (WEP) is turned on.

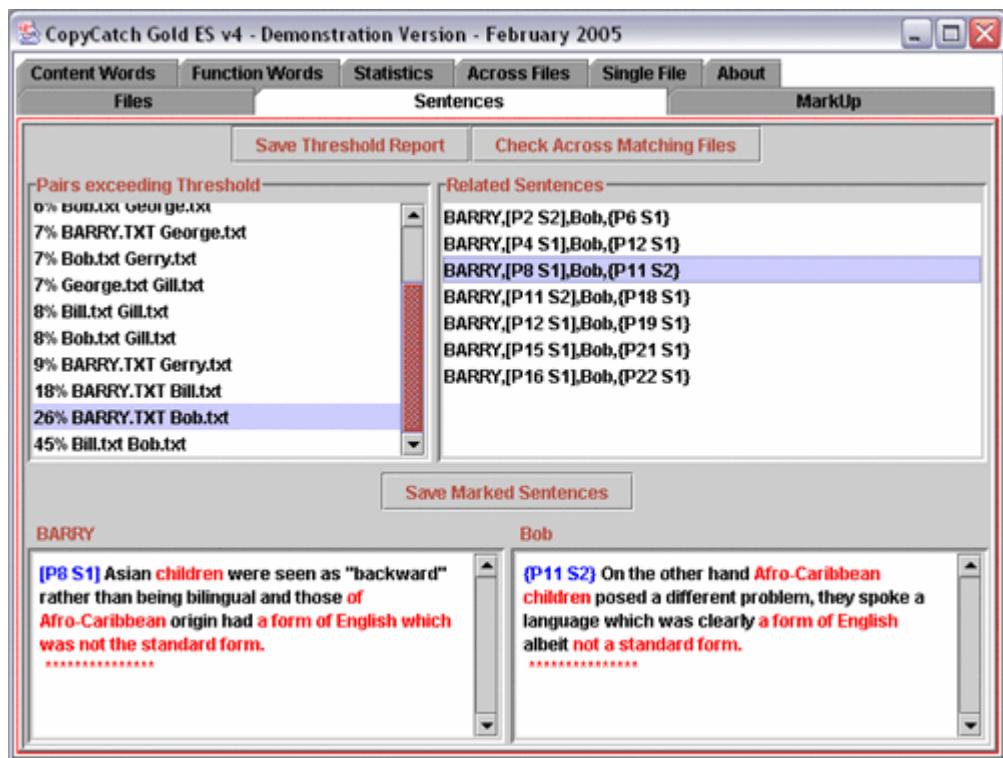
Color-coded text indicates matches to a given source. The left window contains the text of the submitted paper; the right window contains the source content

Plagiarism detection tools

- There are three categories of plagiarism detection tools:
 - Tools to detect plagiarism in text
 - Submit.ac.uk & CopyCatch are available free for higher educational institutions in U.K
 - Eve helps in checking plagiarism in works submitted in MS Word, Corel Word perfect/ documents in text format
 - Tools to detect plagiarism in source code
 - JPlag helps in finding similar source code from multiple sets
 - CodeMatch claims to have algorithm which is superior to other tools
 - Tools which assist in process such as data collection
 - BOSS is a online submission system for assessing work of students from Warwick University's computer science department

CopyCatch

- CopyCatch is a dedicated tool designed to ensure accuracy in checking documents for plagiarism
- It takes few seconds to check plagiarism in documents written in various formats such as rtf, doc, and txt
- Employed for various purposes such as detection, deterrence, and investigation



Patent

- According to USPTO “A patent for an invention is the grant of a property right to the inventor, issued by the Patent and Trademark Office.”
- Types of patents:
 - **Utility patent** - granted to an individual who discovers or invents new machine, process, useful composition of matter or manufacture
 - **Design Patent:** granted to an individual who invents a new, original design for an article of manufacture. It protects the appearance of an article
 - **Plant Patents:** granted to an individual who invents, discovers or asexually reproduced a distinct variety of plant



Patent Infringement

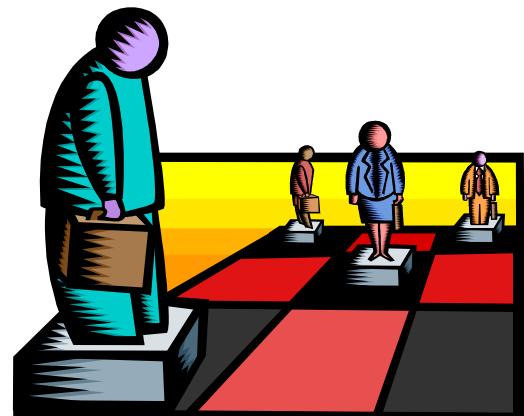
- According to USPTO, “Patent infringement is unauthorized making, using, offering to sell, selling or importing into the United States any patented invention.”
- Direct, indirect, and contributory are the ways in which infringement can be done.
- Resolving patent infringement is a two-step process:

- Analysis of claim by going through all relevant patented documents
- Verifying the claim for validation



Patent Search

- USPTO recommended seven-step strategy for patent search:
 1. *Index to the U.S. Patent Classification*
 2. *Manual of Classification*
 3. *Classification Definitions*
 4. *Browse Patent Titles and Abstracts*
 5. *Retrieve Subclass Listing*
 6. *Official Gazette - Patent Section*
 7. *Complete Patent Document*



Case Study: Microsoft Vs Forgent

Microsoft Sued Over JPEG Patent

By [Nate Mook](#), BetaNews

April 22, 2005, 1:27 PM

Scheduling software maker [Forgent](#) has filed suit against Microsoft for allegedly infringing on its patent that covers the [technology](#) behind JPEG image compression. But Microsoft has already made the first strike, filing its own lawsuit last week that asks the courts to nullify Forgent's patent.

Forgent says it was in talks with Microsoft over licensing the patent when Redmond made the first legal move. Forgent's lawsuit was filed in the U.S. District Court in the Eastern District of Texas by the company's Compression Labs subsidiary.

[Ads by Goooooogle](#)

[Is Your Patent Infringed?](#)

General Patent Corporation Intl We enforce patents on contingency
www.patentclaim.com

[Accutane lawsuit](#)

Information and Links about Accutane

"It's unfortunate that, despite Microsoft's recent inquiries about licensing the patent, they chose to file a lawsuit, leaving us no alternative but to assert infringement claims against it," Forgent CEO Richard Snyder said in a statement.

Internet Domain Name and ICANN

- According to **www.webopedia.com** a domain name is “*A name that identifies one or more IP addresses*”
- A domain name has a suffix that points out the corresponding top level domain (TLD) it belongs to
- The Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit organization that is responsible for the allocation of Internet Protocol (IP) address, protocol identifier assignment, generic (gTLD) and country code (ccTLD), Top-Level Domain name system management, and root server system management functions

Domain Name Infringement

- Domain names creating confusion regarding affiliation of trademark holder with them can fall prey to infringement
- According to the USPTO "A mark composed of a domain name is registerable as a trademark or service mark only if it functions as a source identifier. The mark as depicted on the specimens must be presented in a manner that will be perceived by potential purchasers as indicating source and not as merely an informational indication of the domain name address used to access a web site."



Case Study: Microsoft.com Vs MikeRoweSoft.com

Microsoft Demands Entire Family To Drop Their Last Name

Technology News

Tuesday, January 20, 2004

TheDailyFarce.com - Marcelo Lewin

Rate This Story

Current Rating: Not Rated Yet

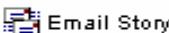
Choose...

Rate Story!

Story Features



Print Story



Email Story



Vote For Story

Mike Rowe, a 17 year old 12th grader needed a "hip" name for his website design company he was starting. Having a sense of humor, Mike decided to add "soft" to the end of his first and last name, which read MikeRoweSoft.com. This, of course, sounds like Microsoft.com.

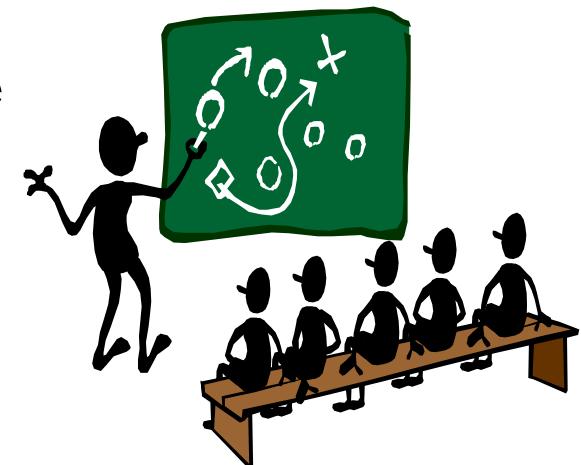
Microsoft, a multibillion dollar company with

thousands of employees and offices all over the world and absolutely no sense of humor, decided that this 17 year old one man shop could end up hurting its business and demanded that Mike Rowe drop the domain name MikeRoweSoft.com and turn it in.

 MIKEROWESOFT DESIGN	 Microsoft
2003 Revenues: Microsoft: \$30 Billion	MikeRoweSoft: \$59 plus a cool MP3 player from his friend Mike.
Employees: Microsoft: 55,000+	MikeRoweSoft: Mike 3/4 Time + Mom helps out once in a while
Customer Base: Microsoft: Millions	MikeRoweSoft: Around 10, possibly 11 if his cousin lets him design her wedding web site.

How To Check For Domain Name Infringement?

- Use popular search engines such as *Google* to find out whether domain name is already in use or not
- Search *Whois.net* to find if any other business contains text identical to your domain name
- Examine *Trademark Electronic Search System* (TESS). This database contains all federally registered trademarks and service marks.
- Engage an efficient search firm to do a national trademark, service mark and domain name search
- Appoint a trademark attorney to perform all activities described in above steps



Summary

- Trademarks are of three types namely service mark, collective mark and certification mark
- Based on the standard “likelihood of confusion” the trademark owner can sue other parties for trademark infringement
- Works published before 1923 in the USA are in the public domain
- Paraphrasing is an act of plagiarism
- Plagiarism tools are of three types namely, tools for text, tools for code and tools for data collection/submission



Computer Hacking Forensic Investigator

Module: XXIII
Investigative Reports

Scenario

Simon a computer forensic investigator with Xsecurity was put on the job to investigate a child molestation case. After series of investigation Simon was able to track down the criminal responsible for the crime.

Evidence related to the case were collected to present as a proof before the Judiciary.

On the judgment day the court acquitted the accused. Simon could not believe it and wondered what went wrong.

The reason for loosing the case was lack of proper documented evidence. The report that Simon had presented before the court lacked the basics of Investigative report writing.



Module Objective

- Need of an investigative report
- Report specifications
- Report classification
- Report and opinion
- Layout of an investigative report
- Writing report
- Use of supporting material
- Importance of consistency
- Salient features of good report
- Investigative report format
- Before writing the report
- Writing report using FTK

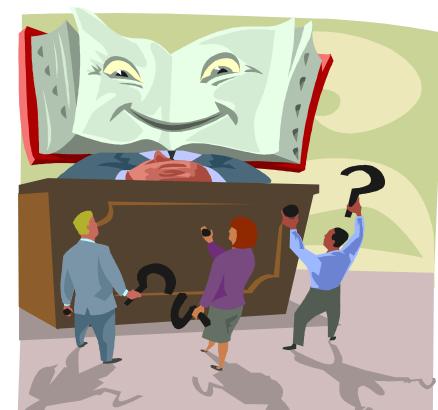
Module Flow



Need of an investigative report

○ Purpose of an investigative report:

- Communicate results of computer-forensic examination
- Organize the information so that anyone can read and understand the report without reference to enclosures or other material
- Present evidence as testimony
- Express expert opinion
- Specify fees paid for expert's service



Report specification

- ◉ PDF is the format for digital reports
- ◉ Do not file a report directly with the court
- ◉ Definition of goal or mission is must
- ◉ Order of writing should match the development of the case
- ◉ Use of outline or arrangement is suggested



Report Classification

- Reports can be categorized as:
 - Verbal and
 - Written
- Reports can be further categorized as:
 - Formal and
 - Informal
- Verbal formal report-
 - A structured report delivered to a board of directors/managers/jury



Contd.

◎ Verbal informal report-

- A report that is less structured than a formal report and is delivered in person, usually in an attorney's office

◎ Written formal report-

- A written report sworn under oath, such as an affidavit or declaration

◎ Written informal report-

- An informal or preliminary report in written form



Report and Opinion

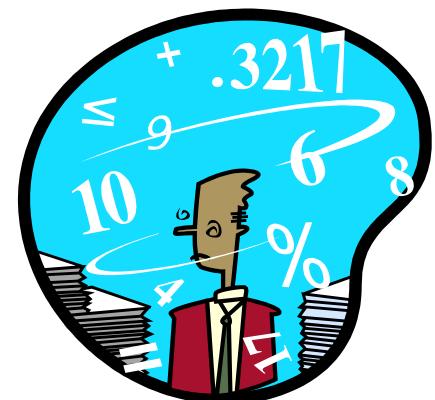
- To express an opinion following are the few guidelines:

- Report should be communicable
- No assumption while writing the report
- Refrain from specifying the leads
- Check for grammar and spellings
- Writing should be concise



Layout of an Investigative Report

- ◉ Presentation of accurate text is must
- ◉ Numbering structure can be chosen from two layout systems:
 - Decimal numbering
 - Legal- sequential numbering system
- ◉ Include signposts to communicate information clearly
- ◉ Use of proper style is must



Writing Report

- Logical order of ideas
- Flow in the report from beginning to end
- Avoid jargon, slang, or colloquial terms
- Define acronyms and abbreviations
- Employ active voice in writing



Use of Supporting Material

- Use figures, tables, data, and equation as supporting material
- Number figures and tables in the same order as they are introduced in the report
- Provide captions with complete information
- Insert figures and tables after the paragraph



Importance of Consistency

- The sections in the report format can be adjusted accordingly
- Consistency is more important than exact format in report
- Establish a template for writing report



Salient Features of a Good Report

- Explaining methods
- Data collection
- Including calculations
- Providing for uncertainty and error analysis
- Explaining results
- Discussing results and conclusions
- Providing references
- Including appendices
- Providing acknowledgements
- Litigation support reports versus technical reports



Investigative Report Format

- Get samples of previously established report format
- Project objectivity
- Document the findings in an impartial and accurate manner
- Try to find flaws in one's thinking or examination



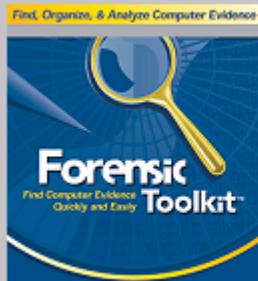
Before Writing the Report

- Create an image of the suspect disk using Image:

- Run command prompt.
- In work folder change to the **Tools** folder and execute **Toolpath.bat**.
- Create a folder and copy **Filename.img** from data files to this folder.
- Put a label on a blank, formatted floppy disk and insert it in the floppy disk drive.
- Type **Image Filename.img a:** at the command prompt and press **Enter**.

Writing Report Using FTK

AccessData FTK Startup



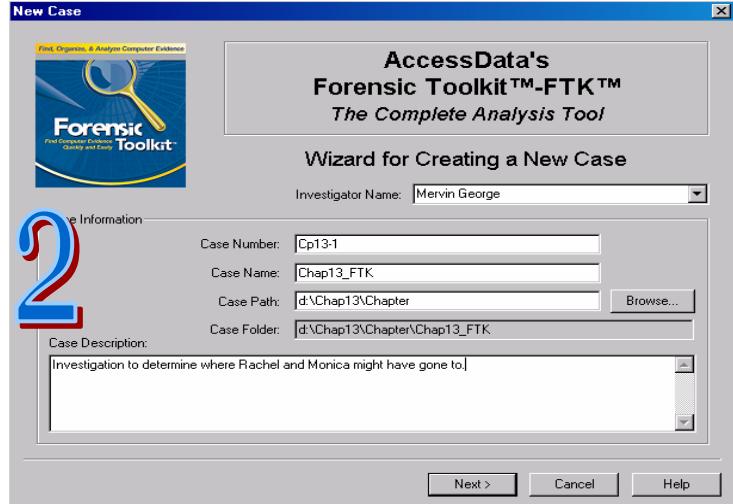
- Start a new case
- Open an existing case
- Preview evidence
- Go directly to working in program

OK
Cancel

Do not show this dialog on startup

1

New Case



AccessData's
Forensic Toolkit™-FTK™
The Complete Analysis Tool

Wizard for Creating a New Case

Investigator Name: Mervin George

Case Number: Cp13-1

Case Name: Chap13_FTK

Case Path: d:\Chap13\Chapter

Browse...

Case Folder: d:\Chap13\Chapter\Chap13_FTK

Case Description:
Investigation to determine where Rachel and Monica might have gone to.

Next > Cancel Help

Evidence Processing Options

Processes to Perform

Evidence is added to a case in several steps. Some of the processes are always performed, while others are optional, depending on your needs and time/resource constraints.

File Extraction	The file extraction process is always performed. It automatically extracts files, mail messages, data streams, etc. from zip archives, most email archives, and OLE storages.
<input checked="" type="checkbox"/> MD5 Hash	An MD5 hash is a 16 byte value generated based upon a file's content. It is used to uniquely identify files. Hashes can be used to verify a file's integrity, or to identify duplicate files. MD5 hashes are used by the KFF to identify known files.
<input type="checkbox"/> SHA Hash	A SHA hash is a 20 byte value. The SHA hashing algorithm is newer than MD5, but is not yet as widely used. The KFF library can contain SHA hashes, but generally doesn't.
<input checked="" type="checkbox"/> KFF Lookup	KFF (Known File Filter) is a utility that compares file hashes against a database of hashes from known files. The purpose of KFF is to eliminate files known to be unimportant, or to alert the investigator to known illicit or dangerous files. It also checks for duplicate files.
<input checked="" type="checkbox"/> Entropy Test	For unknown file types, an entropy test is used to determine whether the file's data is compressed or encrypted. Such files contain no plain text and will not be indexed. Unnecessary indexing of such files can waste an enormous amount of time and resources.
<input checked="" type="checkbox"/> Full Text Index	The Forensic Toolkit includes a very powerful search engine, dtSearch, which enables the investigator to do instantaneous searching of textual data. In order to take advantage of this search feature, the data must first be indexed.
<input checked="" type="checkbox"/> Store Thumbnails	Create and store thumbnails for all graphics in the case. This option speeds up browsing through the Graphics view at the expense of consuming more space in the case folder.

4

Case Log Options

Case Log Options

The case log is a text file named FTK.log in the case folder. It gets created automatically by FTK and contains a record of events that occur during the course of the case. You can choose which type of events you would like to be logged.

You can also add your own comments to the log file at any time by selecting "Add Case Log Entry..." under the "Files" menu item, and you can view the log file by selecting "View Case Log" under the "Files" menu item.

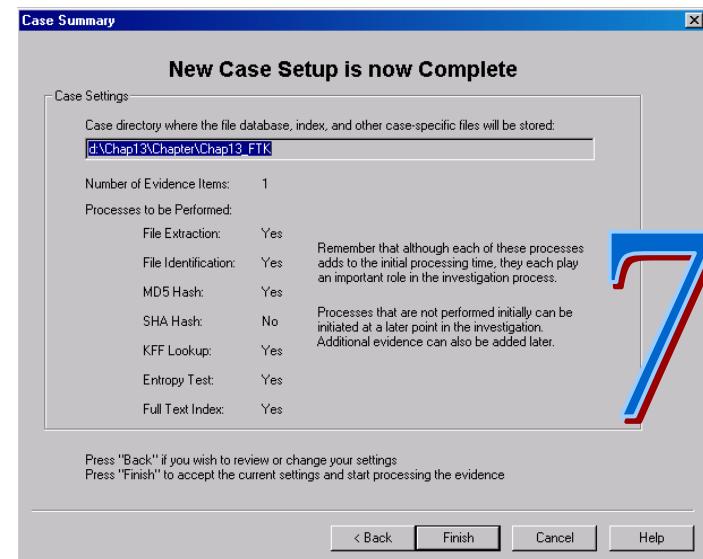
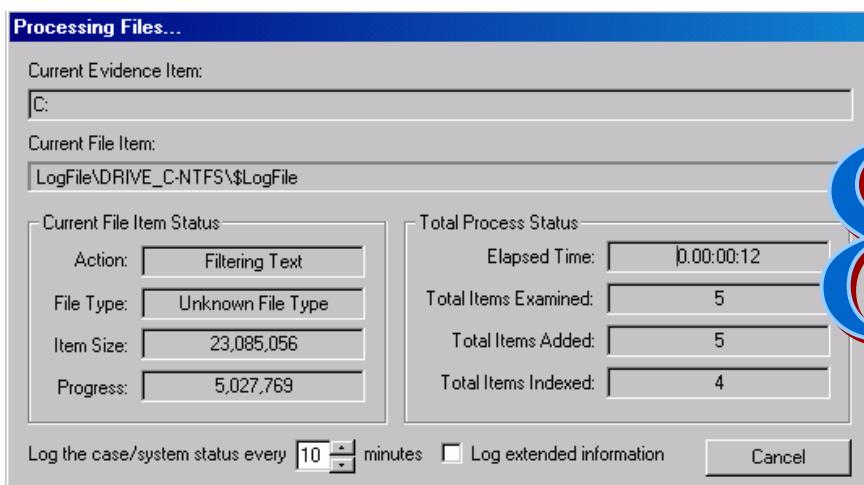
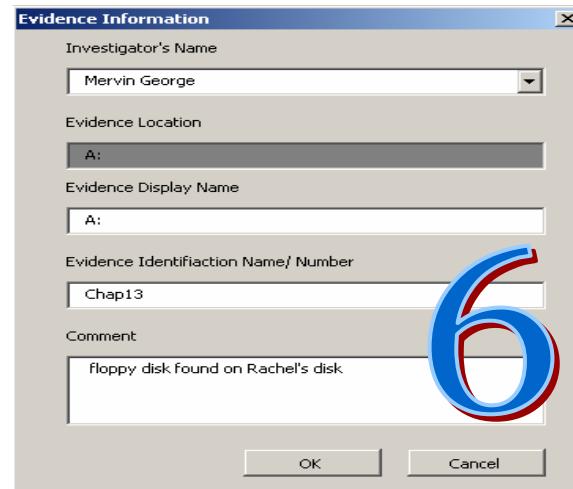
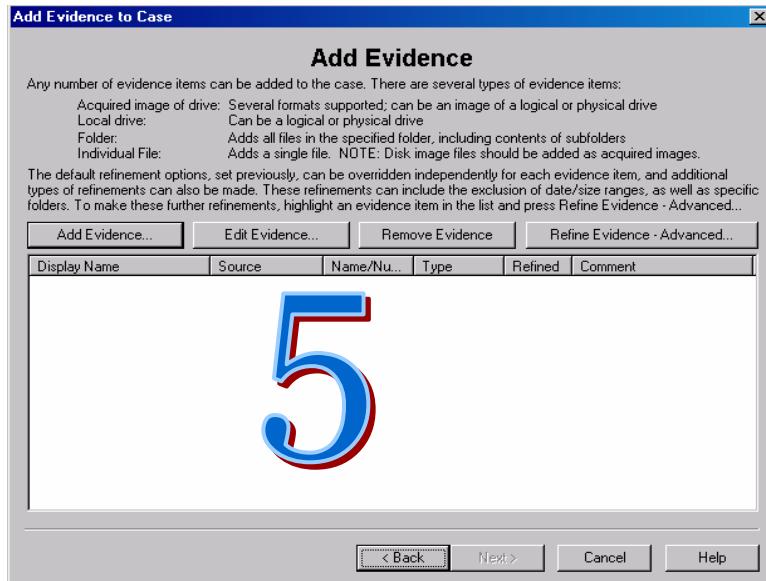
Events to go in the Case Log

- Case and evidence events
 - Error messages
 - Bookmarking events
 - Searching events
 - JPEG/Internet searches
 - Other events
- Events related to the addition and processing of file items when evidence is added or when using Analysis Tools later in the case.
Events related to any error conditions encountered during the case.
Events related to the addition and modification of bookmarks.
Events related to searching. All search queries and resulting hit counts will be recorded.
Events related to special JPEG or internet keyword searches that are performed during the case.
Other events not related to the above, such as copying, viewing, and ignoring files.

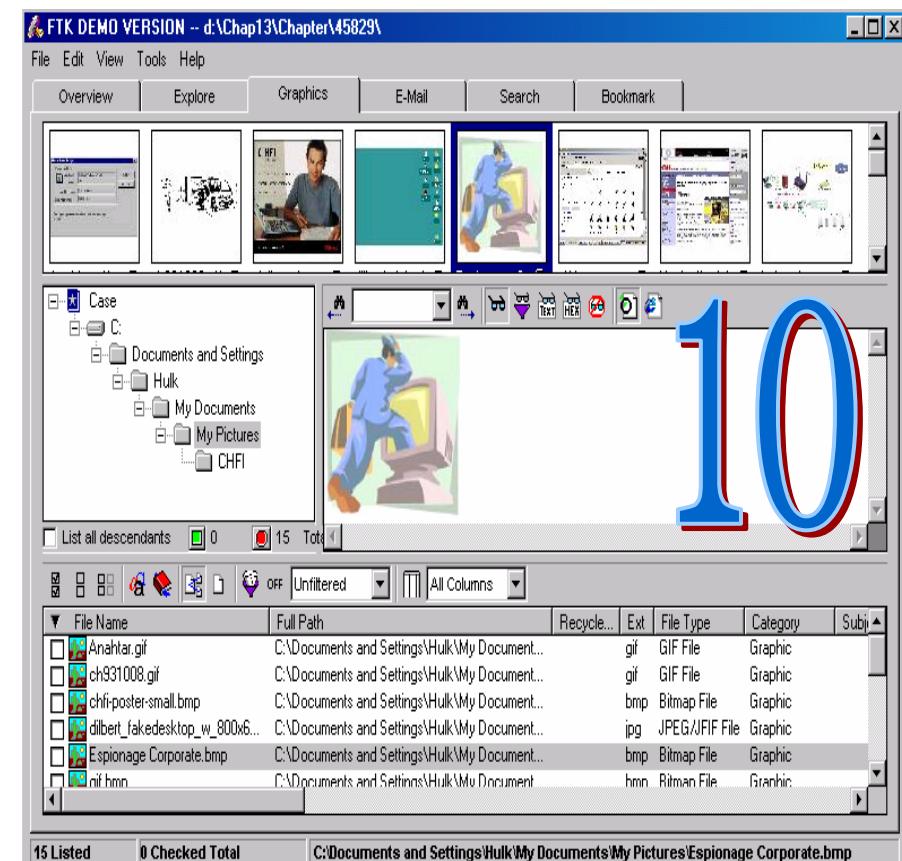
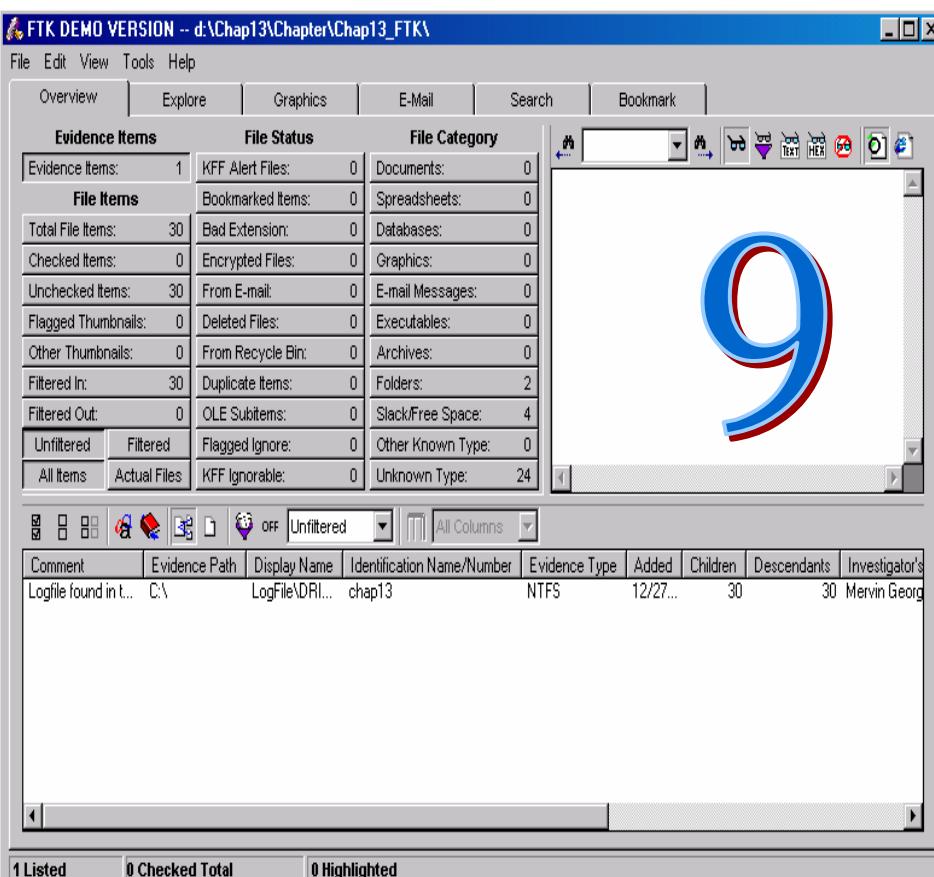
3

< Back Next > Cancel Help

Writing Report Using FTK



Writing Report Using FTK



Writing Report Using FTK

The screenshot shows the FTK DEMO VERSION interface. On the left, there's a summary of evidence items:

Evidence Items	File Status	File Category
1	KFF Alert Files: 0	Documents: 0
21	Bookmarked Items: 0	Spreadsheets: 0
21	Bad Extension: 0	Databases: 0
0	Encrypted Files: 0	Graphics: 20
21	From E-mail: 0	E-mail Messages: 0
0	Deleted Files: 0	Executables: 0
20	From Recycle Bin: 0	Archives: 0
21	Duplicate Items: 0	Folders: 0
0	OLE Subitems: 0	Slack/Free Space: 0
0	Flagged Ignore: 0	Other Known Type: 0
0	KFF Ignorable: 0	Unknown Type: 1

The main pane displays a large blue graphic of the number '11'. Below it is a file list table:

File Name	Full Path	Recycle...	Ext	File Type	Category	Subject
Encryption.jpg	C:\Documents and Settings\Hulk\My Document...		jpg	JPEG/Exif file	Graphic	
Hacker.jpg	C:\Documents and Settings\Hulk\My Document...		jpg	JPEG/Exif file	Graphic	
Investigator.jpg	C:\Documents and Settings\Hulk\My Document...		jpg	JPEG/Exif file	Graphic	
Investigator2.jpg	C:\Documents and Settings\Hulk\My Document...		jpg	JPEG/Exif file	Graphic	

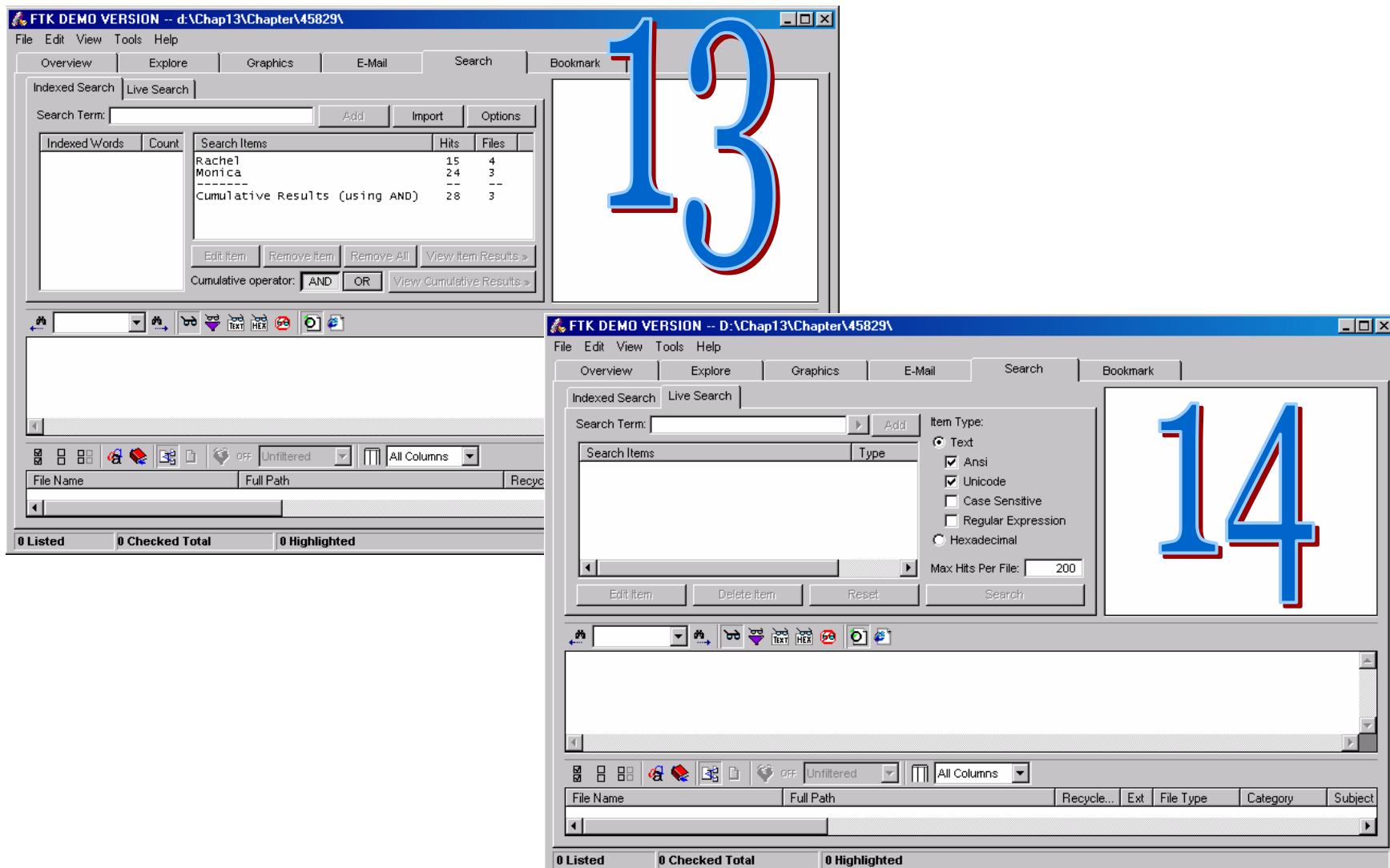
At the bottom, status indicators show 0 Listed, 0 Checked Total, and 0 Highlighted.

To the right, an 'Export Files' dialog box is open, showing the following settings:

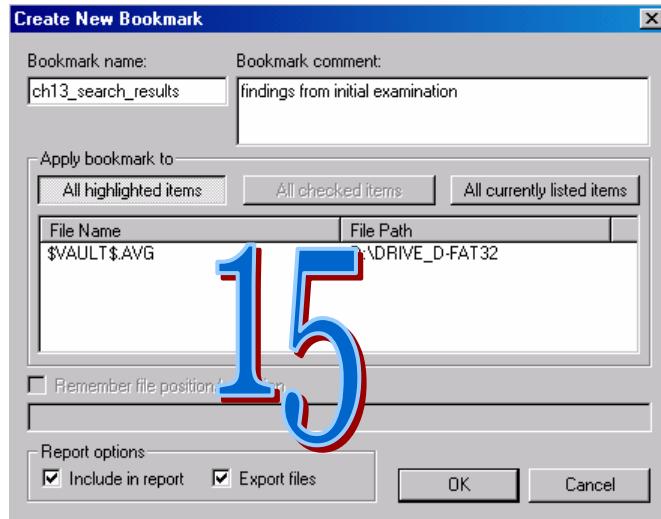
- File(s) to Export:
 - All highlighted files (radio button selected)
 - All checked files
 - All currently listed files
 - All files
- Include email attachments with email messages (checkbox)
- File Name: Encryption[13].jpg
- Original Path: C:\Documents and Settings\Hulk...
- Destination Path: d:\Chap13\Chapter45829\Export\
- Prepend archive name to file name (checkbox)
- Append item number to file name to guarantee uniqueness (checkbox)
- Append appropriate extension to file name if bad/absent (checkbox)
- Export raw email messages instead of converting to HTML (checkbox)

A large blue graphic of the number '12' is overlaid on the bottom right of the dialog box.

Writing Report Using FTK



Writing Report Using FTK



FTK DEMO VERSION -- D:\Chap13\Chapter\45829\

Evidence Items

Evidence Items	File Status	File Category
1	KFF Alert Files: 0	Documents: 0
	Bookmarked Items: 0	Spreadsheets: 0
Total File Items: 21	Bad Extension: 0	Databases: 0
Checked Items: 1	Encrypted Files: 0	Graphics: 20
Unchecked Items: 21	From E-mail: 0	E-mail Messages: 0
Flagged Thumbnails: 0	Deleted Files: 0	Executables: 0
Other Thumbnails: 20	From Recycle Bin: 0	Archives: 0
Filtered In: 21	Duplicate Items: 0	Folders: 0
Filtered Out: 0	OLE Subitems: 0	Slack/Free Space: 0
Unfiltered	Flagged: 0	Other Known Type: 0
All Items	Actual Files	Knowable: 0
		Unknown Type: 1

File Items

Total File Items:	Bad Extension:	Documents:
21	0	0

Rachel

I have encrypted the information regarding our salary accounts into this file. The account numbers of all the employees are given below:

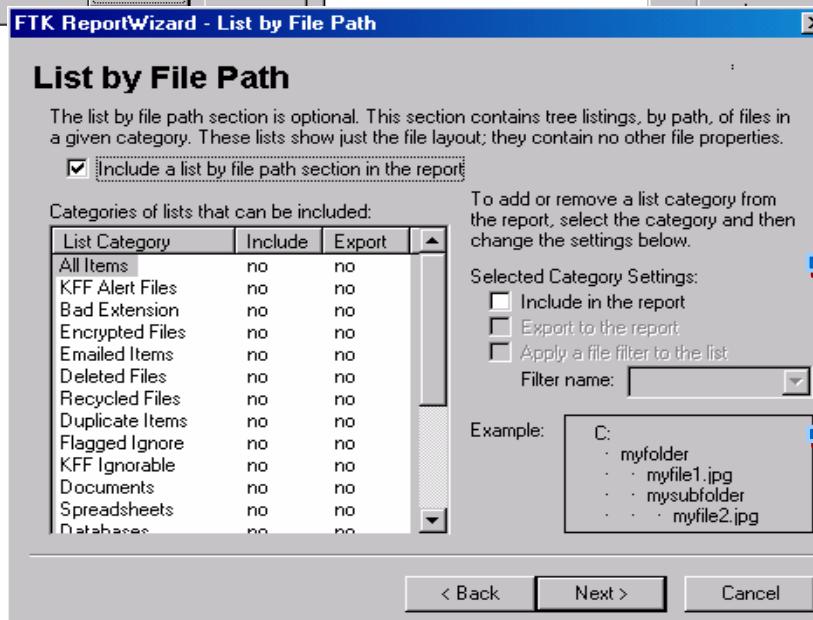
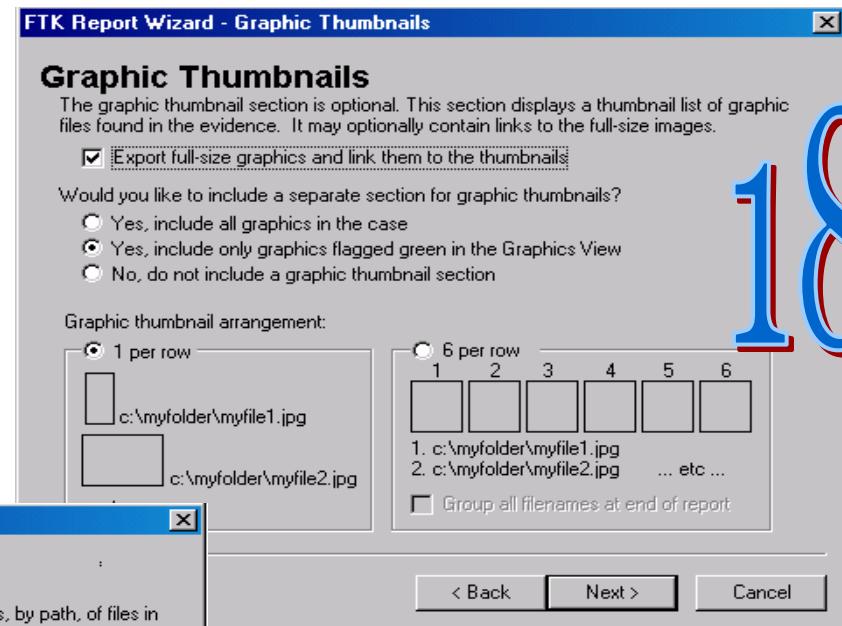
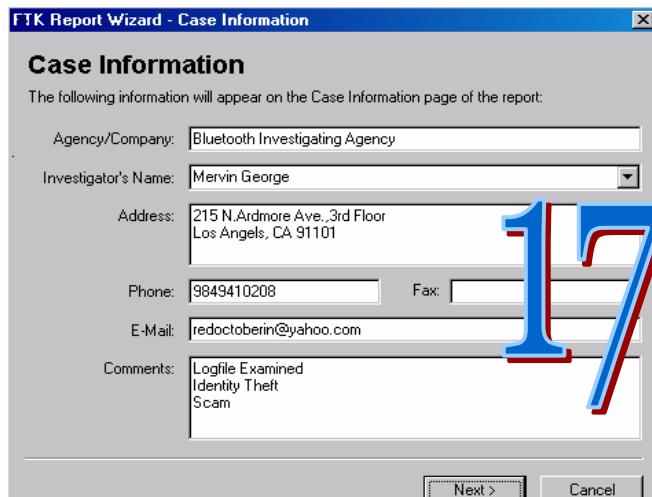
9845876
9549855
8484124

File Name Path Recycle... Ext File Type Category Subject

File Name	Path	Recycle...	Ext	File Type	Category	Subject
Computer Configuration	Documents and Settings\Hulk\My Document...		jpg	JPEG/Exif file	Graphic	
Encryption.i	\Documents and Settings\Hulk\My Document...		jpg	JPEG/Exif file	Graphic	
Hacker.jpg	C:\Documents and Settings\Hulk\My Document...		jpg	JPEG/Exif file	Graphic	
Investigator.jpg	C:\Documents and Settings\Hulk\My Document...		jpg	JPEG/Exif file	Graphic	
Investigator2.jpg	C:\Documents and Settings\Hulk\My Document...		jpg	JPEG/Exif file	Graphic	

0 Listed 0 Checked Total 0 Highlighted

Writing Report Using FTK



Writing Report Using FTK

FTKReport - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address D:\Chap13\Chapter\45829\report\index.htm

Google

FTK CASE REPORT

Case Information

Dec 27, 2004

FTK Version	Version 1.33, build 03.07.16
KFF Version	Unknown
Case Number	9847582
Case Location	D:\Chap13\Chapter\45829\
Case Description	
Report Created	Dec 27, 2004 3:55pm
Investigator	Mervin George
Agency	Bluetooth Investigating Agency
Address	215 N.Ardmore Ave., 3rd Floor Los Angels, CA 91101
Phone	9849410208
Fax	
Email	redoctoberin@yahoo.com
Comments	LogFile Examined Identity Theft Scam

20

AccessData Forensic Toolkit

Final Report

Summary

- ◉ Investigative Reports are critical to investigations because they communicate computer forensics findings and other information to the necessary authorities
- ◉ Reports can be formal or informal, verbal or written
- ◉ Reports need to be grammatically sound
- ◉ Use correct spelling, and avoid any writing errors
- ◉ Avoid jargon, slang, or colloquial terms



Computer Hacking Forensic Investigator

Module XIV

Becoming an Expert Witness

Case Study

On March 6, 1993

Phil McCalister, a disgruntled associate of a law firm "Steele & Hoffman", after watching the movie "The Firm", copies school board billing records from the firm's laptops onto some diskettes and resigns.

He then hands over those diskettes to postal inspectors as evidence of over billing of school systems by Charlie Steele, managing partner of Steele & Hoffman.

Despite a brilliant testimony by the computer expert witness, Charlie Steele is convicted of mail fraud and sentenced to 3 years in federal pen and \$80,000 fine.

"Justice consists not in being neutral between right and wrong, but in finding out the right and upholding it, wherever found, against the wrong"

- Theodore Roosevelt

Real Case

In the beginning of 1998, the following notice appeared at the official Kevin Mitnick website



Source: <http://www.shk-dplc.com/cfo/articles/hack.htm>

Wanted ASAP: Expert witness for Mitnick trial Computer Expert Witness Needed "Immediately"

A computer expert is needed immediately to testify as an expert witness in an ongoing criminal matter in Federal District Court in Los Angeles. Kevin Mitnick is seeking a highly credentialed expert in computer security, telecommunications, system and network administration to testify in this highly publicized computer "hacking" case.

This will be a groundbreaking case and is expected to attract significant media coverage. Testimony will be required as early as March 30, 1998 in Los Angeles, California. Further testimony will be needed at trial, later this year. Expert witness fees will be paid by the federal court.

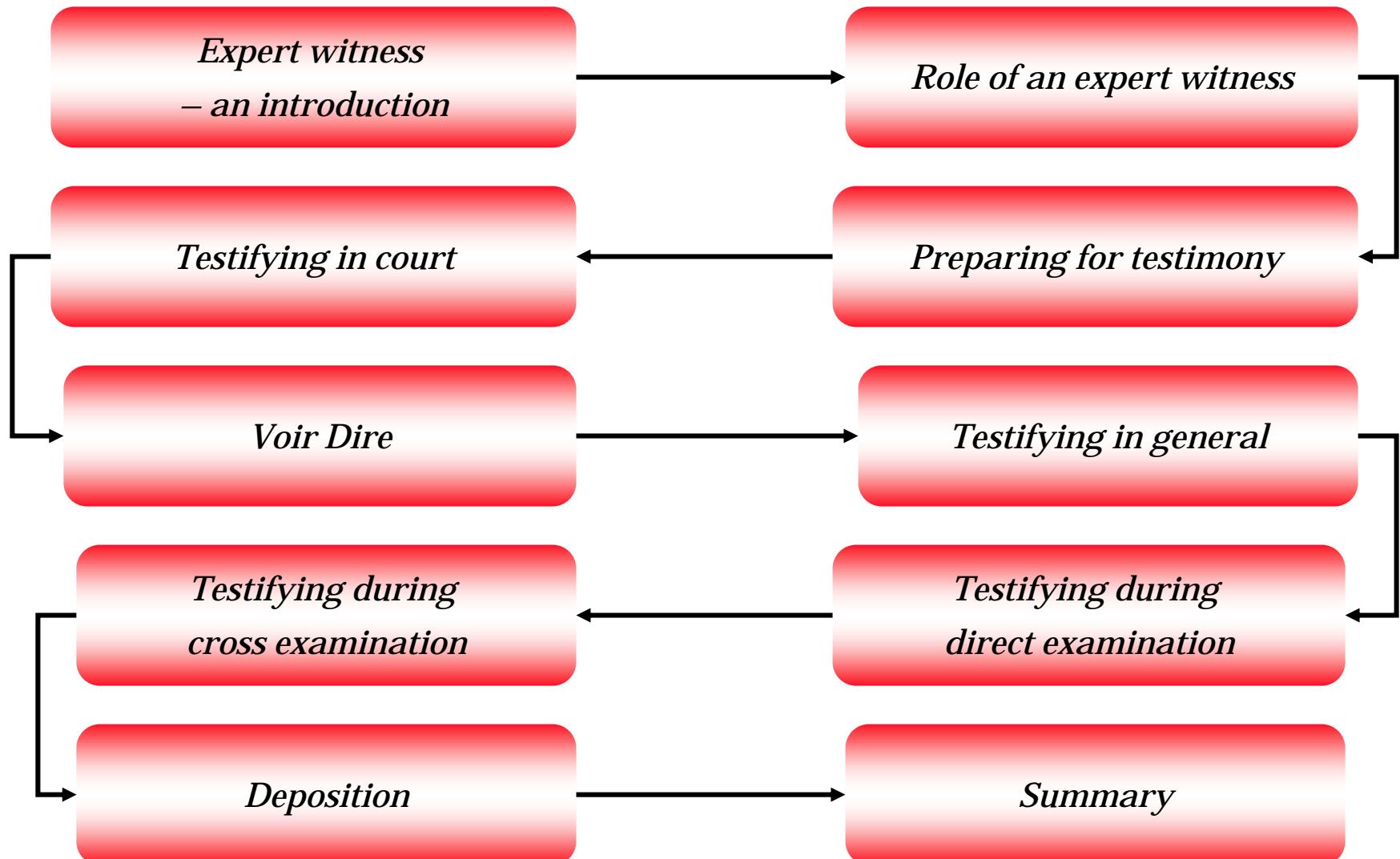
Qualified candidates must have an advanced degree and be knowledgeable in DOS, Windows, SunOS, VAX/VMS, and Internet operations. Experience with cellular telephone networks is a plus. Previous expert testimony and/or publication are preferred.

Qualified candidates please contact Mr. Mitnick through his appointed defense counsel, Donald C. Randolph, Esq. at [REDACTED]

Module Objective

- Expert witness – an introduction
- Role of an expert witness
- Preparing for testimony
- Testifying in court
- *Voir Dire*
- Testifying in general
- Testifying during direct examination
- Testifying during cross-examination
- Deposition

Module flow



Who Is an Expert?

According to Dan Poynter (An expert witness since 1974),

“*If something can break, bend, crack, fold, spindle, mutilate, smolder, disintegrate, radiate, malfunction, embarrass, leach, be abused or used incorrectly, infect or explode, there is someone who can explain how and why it happened. This person is an EXPERT*”



Who Is an Expert Witness?

○ An expert witness is a person who

- Investigates
- Evaluates
- Educates, and
- Testifies in court

○ An expert witness can be a

- Consulting expert or strategy advisor
- Court's expert
- Testifying expert



Role of an Expert Witness

- Assist the court in understanding intricate evidence
- Express an opinion in court
- Attend the entire trial in court
- Aid lawyers to get to the truth and not obscure it
- Qualified to exhibit their expertise



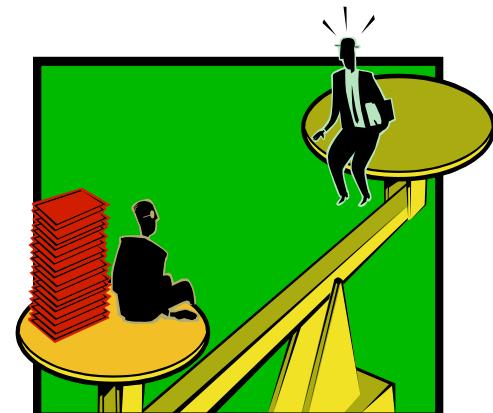
Technical Testimony Vs. Expert Testimony

◎ A Technical testimony is an individual who

- Does the actual fieldwork
- Submits only the results of his findings
- Does not offer a view in court

◎ An Expert testimony is an individual who

- Has absolute field knowledge
- Offers a view in court



Preparing for Testimony

⦿ Basic points to be kept in mind while preparing for testimony

- Deeply go through the documentation
- Establish early communication with the attorney
- Ascertain the basic concepts of the case before beginning with the examining and processing of evidence
- Substantiate the findings
 - with the documentation, and
 - by collaborating with other computer forensic professionals



Evidence Preparation and Documentation

- ⦿ Every important aspect in the case must be documented during investigations
- ⦿ Safeguard the integrity of all gathered evidence
- ⦿ Catalog and index for easier understanding
- ⦿ Use your professional experience and request peer reviews to support your findings



Evidence Processing Steps

- Examine, preserve and authenticate the documentation prepared
- Different checklists must be created for different evidence analysis
- Avoid personal comments or ideas in these notations
- Make simple and precise notes of the investigation



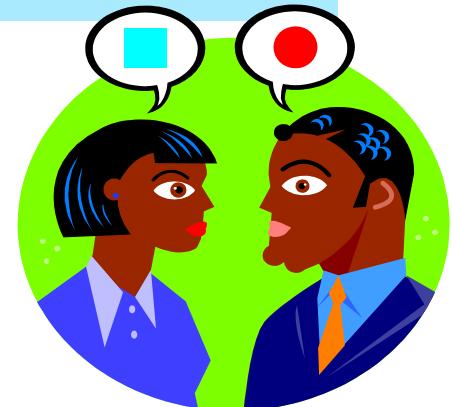
Evidence Processing Steps

- Use SHA-1 for evidence validation
 - MD5 or CRC32 can be used if SHA-1 is absent
 - An MD5 or SHA-1 hash check before and after evidence examination would ensure the integrity of the evidence
- Use well-defined search parameters while searching for key results
 - Helps in narrowing the search
 - Avoids false hits
- While writing the report, list only the evidence findings that are relevant to the case

Rules Pertaining to an Expert Witness' Qualification

- According to federal rules, to be present as an expert witness in a court, following information must be furnished

- Four years of previous testimony (*indicates experience*)
- Ten years of any published literature
- Previous payment received when giving testimony



Importance of Curriculum Vitae

- Curriculum Vitae shows the capability of an expert witness
- It is essential to regularly update your curriculum vitae
- The following things must be kept in mind while preparing a CV:

- Certifications/credentials/accomplishments
- Recent work as an expert witness or testimony log
- Expertise
- List of books written, if any
- Any training undergone
- Referrals and contacts



Technical Definitions

- ◉ Use lucid language and easily understandable words
- ◉ Some examples of technical definitions:

- Computer Forensics
- SHA-1, MD5, and CRC32 hash functions
- Image and bit-stream backup
- File slack and free space
- File time and date stamps
- Computer log files.



Testifying in Court

- ◉ Familiarize with the usual procedures followed during a trial
- ◉ The attorney introduces the expert witness with high regards
- ◉ The opposing counsel may try to discredit the expert witness
- ◉ The attorney would lead the expert witness through the evidence
- ◉ Later it is followed by the cross examination with the opposing counsel

The Order of Trial Proceedings

① *Motion in Limine*

(motion in beginning)

- Written list of objections to particular testimonies
- Allows judge to examine whether certain evidence should be admitted in the absence of the jury

② Opening Statement

- Offers an outline of the case

③ Plaintiff and defendant

- The attorney and the opposing counsel presents the case



The order of trial proceedings

- Rebuttal session
 - Cross examination by both plaintiff and defendant
- Jury orders
 - Proposed by the counsel
 - Approved and read by the judge to the jury
- Closing arguments
 - Statements that organize the evidence and the law

Voir dire

- French words meaning “*to speak the truth*”
 - Process of qualifying a witness as an expert in their particular field.
- The opposing counsel may attempt to degrade or disqualify the expert witness.
- The opposing counsel may accept the expert witness without any formal qualification.
 - The expert witness is well qualified or has been an expert witness on several occasions.
- The attorney will try to avoid this situation and impress the jury through the qualification process.

General Ethics While Testifying-i

- ◉ Ethics to be followed while presenting as an expert witness to any court or an attorney:
 - Be professional, polite and sincere in testimony
 - Always pay tribute to the jury
 - Be enthusiastic during testimony
 - Keep the jury interested in speech
 - Be aware and prepare for the possible rebuttal questions especially from the opposing counsel



General Ethics While Testifying-ii

- Avoid overextending opinions
- Develop repetitions into details and descriptions for the jury
- Augment your image with the jury by following a formal dress code

Evidence Presentation

- Identify evidence to defend opinion
- Associate the method used to arrive at the opinion
- Reaffirm your opinion
- Never exaggerate opinions
- Be prepared to defend your opinion
- Recall definitions
- Gather information about the opposing attorney and expert



Importance of Graphics in a Testimony

- Make graphical demonstrations such as charts
 - To illustrate and elucidate your findings.
- Make sure the graphics are seen by the jury
- Face the jury while exhibiting these graphics
- Make it a habit of using charts and tables for courtroom testimony
- Use clear and easily understandable graphical demonstrations



Helping Your Attorney

○ Prepare a list of questions that are vital.

- Enables the attorney to get the expert's testimony into the trial
- Provides a practice in the testimony for the direct examination
- Also helps the attorney review and improve on how he or she wants to try the case

○ Develop a script and work with the attorney to get the perfect language.

- Communicates the message to the jury.

Avoiding Testimony Problems

- Offer clear opinions
- Outline your boundaries of knowledge and ethics
- Create a case outline and summary for your attorney
 - Enables reviewing of your case plan
 - Offers a clear overview of your level of knowledge used in the case
- Make the best effort to coordinate testimony with other experts, who are retained by your attorney for the same case
- Meet with the paralegal to communicate necessary information to your attorney
 - Paralegal is a person with special training in either a specific or general area of law

Testifying During Direct Examination

- Direct examination is an important part of a testimony during a trial
- It offers a clear overview of all the findings
- Create an easy to follow and systematic plan for describing evidence collection methods
- Be lucid while describing complicated concepts
- Determine the speech to the education level of the jury



Testifying During Cross Examination

- The opposing counsel has the opportunity to ask questions about the expert witness' testimony and evidence. This phase of the trial is cross-examination
- Do not offer guesses when asked something irrelevant to the case
- Use own words and phrases when answering the opposing counsel
- Speak slowly as the best offense to problematic questions is to be patient with answers
- Turn towards the jury slowly while giving your response
 - Allows you to maintain control over the opposing counsel.

Deposition

- Deposition differs from a trial as
 - Both attorneys are present
 - No jury or judge
 - Opposing counsel asks questions
- Purpose of a Deposition
 - Enables opposing counsel to preview your testimony at trial
- Your attorney fixes a location for the deposition.



Guidelines to Testify at a Deposition

- Convey a calm, relaxed, confident and professional appearance during a deposition
- Do not get influenced by the opposing counsel's tone or expression or tactics
- Use the opposing counsel's name while responding him/her and reply confidently
- Have continuous eye contact with the opposing counsel
- Keep your hands on the table and hold out your elbows which makes you appear more open and friendly

Dealing With Reporters

- Avoid contact with media during a case
- Do not give opinions about the trial to media but simply refer the attorney
- Avoid conversing with the media because
 - It is unpredictable what the journalist might publish.
 - The comments might harm the case
 - Creates a record for future testimony, which can be used against you
- Record your interviews, if any, with the media



Summary

- An expert witness can express his opinion and attend the entire trial in court
- Convey a calm, relaxed, confident and professional appearance during a testimony
- Follow certain ethics while giving your testimony
- Project your voice and make your speech interesting for the jury and audience to listen
- Use graphics to make your testimony more appealing
- Avoid expressing an opinion to the media



Computer Hacking Forensic Investigator

Module XXV
Forensics in action

E-mail Hoax

On the eve of new year 2005, many relatives and friends of Tsunami affected victims were shocked to receive an email from the Foreign Office Bureau, Thailand.

The email notified them that their relatives had been killed by the tsunami waves. Incidentally people who received the email had posted their enquires regarding their relatives on the message board of Sky News website. Three recipients of the email enquired with Sky News and found out that the email was actually a hoax. An enquiry was conducted regarding the email hoax.

A 40 year old man, Christopher Pierson from Ruskington, Lincolnshire, UK was convicted of the crime and sentenced to 6 months of imprisonment.

Trade Secret Theft

In February 2004, some portion of Microsoft's source code for Windows NT and windows 2000 was illegally leaked to the Internet.

Microsoft sought help of online investigators and the FBI. In November 2004, a 27 year old Connecticut man , William P. Genovese, Jr. was arrested while selling the leaked source code from a website www.illmob.org.

A person with an identity "*illwill*" claimed to have obtained a copy of the leaked source code and was asking money for downloading the source code from the website's FTP server. During the course of investigation the identity of the person named "*illwill*" was mapped to William P. Genovese, Jr.

Special Agent Frank C. Manzi of the FBI and other online security firms hired by Microsoft conducted the investigation.

Operation Cyberslam

The website of Weaknees, an e-business firm ,which sells and upgrades personal digital video recorders faced a “Syn-flood” DDoS attack on October 6, 2003.

The website was struck by another DDoS attack on October 10, 2003. The website of Weaknees was hosted by Lexiconn. The second attack on Weaknees affected Lexiconn's other customers. As a result of this Lexiconn removed Weaknees as its customer.

Weaknees hired another web hosting company Rackspace at a higher price but in vain. As a result of the attacks the website of Weaknees was put off for two weeks.

FBI special agents Cameron Malin and Panico investigated the case. From several records collected during investigation Jay R. Echouafni, CEO of Massachusetts-based Orbit Communications was indicted of the crime.