

# CS6004 CYBER FORENSICS

---

## UNIT – III

---

# UNIT - III

---

## INTRODUCTION TO COMPUTER FORENSICS

Introduction to Traditional Computer Crime, Traditional problems associated with Computer Crime. Introduction to Identity Theft & Identity Fraud. Types of CF techniques – Incident and incident response methodology – Forensic duplication and investigation. Preparation for IR: Creating response tool kit and IR team. – Forensics Technology and Systems – Understanding Computer Investigation – Data Acquisition.

---

# Computer Forensics

---

- ❑ Goal: The goal of computer forensics is to do a structured investigation and find out exactly what happened on a digital system, and who was responsible for it.
- ❑ Computer crime is any criminal offense, activity or issue that involves computers
- ❑ Computer misuse tends to fall into two categories
  - ❑ Computer is used to commit a crime
  - ❑ Computer itself is a target of a crime. Computer is the victim. Computer Security Incident.
- ❑ Computer is used to commit a crime
  - ❑ Computer pornography, threatening letters, e-mail spam or harassment, extortion, fraud and theft of intellectual property, embezzlement – all these crimes leave digital tracks
  - ❑ Investigation into these types of crimes include searching computers that are suspected of being involved in illegal activities
  - ❑ Analysis of gigabytes of data looking for specific keywords, happened at certain times is used in illegal activities: child examining log

---

## Computer security Incident

- Unauthorized or unlawful intrusions into computing systems
- Scanning a system - the systematic probing of ports to see which ones are open
- Denial-of-Service designed to disrupt the ability of authorized users to access data
- Malicious Code – any program or procedure that makes unauthorized actions (virus, worm, Trojan horse)

## Computer forensics:

- Computer Forensic Analysis
- Electronic Discovery
- Electronic Evidence Discovery
- Digital Discovery
- Data Recovery
- Data Discovery
- Computer Analysis
- Computer Examination

# What is Computer Forensics?

---

- ❑ **Definition:** Involves obtaining and analyzing digital information, often as evidence in civil, criminal, or administrative cases
  - ❑ **Computer forensics**
    - ❑ Investigates data that can be retrieved from a computer's hard disk or other storage media
    - ❑ Task of recovering data that users have hidden or deleted and using it as evidence
    - ❑ Evidence can be *inculpatory* (“incriminating”) or **exculpatory**
  - ❑ **Examples**
    - ❑ Recovering thousands of deleted emails
    - ❑ Performing investigation post employment termination
    - ❑ Recovering evidence post formatting hard drive
    - ❑ Performing investigation after multiple users had taken over the system
-

# Computer Forensics Vs Other Disciplines

---

## ❑ Network forensics

- ❑ Yields information about how a perpetrator or an attacker gained access to a network

## ❑ Data recovery

- ❑ Recovering information that was deleted by mistake, or lost during a power surge or server crash
- ❑ Typically you know what you're looking for

## ❑ Disaster recovery

- ❑ Uses computer forensics techniques to retrieve information their clients have lost

- ❑ Investigators often work as a team to make computers and networks secure in an organization

# Digital Evidence

---

- ❑ Locard's principle: "every contact leaves a trace"
- ❑ any information, stored or transmitted in digital form, that a party to a court case may use at a trial
- ❑ To be accepted in court, digital evidence must meet certain criteria ...
  - ❑ Admissibility
  - ❑ Authenticity
- ❑ **Reason for Evidence**
  - ❑ **Non-Business Environment:** evidence collected by Federal, State and local authorities for crimes relating to: Theft of trade secrets, Intellectual property breaches, Fraud, Unauthorized use of personal information, Extortion, Forgery, Industrial espionage, Perjury, Position of pornography, SPAM investigations, Virus/Trojan distribution, Homicide investigations
  - ❑ **Business Environment:** Theft of or destruction of intellectual property, Unauthorized activity, Tracking internet browsing habits, Reconstructing Events, Inferring intentions, Selling company bandwidth, Wrongful dismissal claims, Sexual harassment, Software Piracy

# Case study

---

- ❑ In this case, American Express (Amex) claimed that Mr. Vinhnee had failed to pay his credit card debts, and took legal action to recover the money. But the trial judge determined that Amex failed to authenticate its electronic records, and therefore Amex could not admit its own business records into evidence. Among other problems, the court said that Amex failed to provide adequate information about its computer policy & system control procedures, control of access to relevant databases & programs, how changes to data were recorded or logged, what backup practices were in place, and how **Amex** could provide assurance of continuing integrity of their records.
- ❑ The judge pointed out that, “... the focus is not on the circumstances of the creation of the record, but rather on the **circumstances of the preservation of the record** so as to assure that the document being proffered is the same as the document that originally was created ...”
- ❑ Lesson:
  - ❑ **Document** your access control and backup procedures and policies and test effectiveness of your controls.
  - ❑ Have the changes to your databases and content/record management system **routinely recorded and logged**.
  - ❑ **Protect your electronic record** from post-archival tampering with modern data integrity and trusted time-stamping technologies.
  - ❑ Document the audit procedures you use to provide assurance of the continuing authenticity of the records.



# Who use Computer Forensics?

---

- ❑ Criminal Prosecutors - Rely on evidence obtained from a computer to prosecute suspects and use as evidence
- ❑ Civil Litigations - Personal and business data discovered on a computer can be used in fraud, divorce, harassment, or discrimination cases
- ❑ Insurance Companies - Evidence discovered on computer can be used to mollify costs (fraud, worker's compensation, arson, etc)
- ❑ Private Corporations - Obtained evidence from employee computers can be used as evidence in harassment, fraud, and embezzlement cases
- ❑ Law Enforcement Officials - Rely on computer forensics to backup search warrants and post-seizure handling
- ❑ Individual/Private Citizens - Obtain the services of professional computer forensic specialists to support claims of harassment, abuse, or wrongful termination from employment
- ❑ **Computer Forensics Services:** Content, Comparison against known data, Transaction sequencing, Extraction of data, Recovering deleted data files, Format conversion, Keyword searching, Decrypting passwords, Analyzing and comparing limited source code

# Cyber Crime

---

- ❑ Crime committed using a computer and the internet to steal a person's identity or illegal imports or malicious programs.
- ❑ Cybercrime is nothing but where the computer used as an object or subject of crime.
- ❑ Current Scenario: 556 million victims per year, 1.5+ Million victims per day, 18 victims per second...
- ❑ In this Tech-savvy world of 21st Century every one is engaged with internet, through whatsapp, twitter, facebook, net banking & lots of other platforms are there.
- ❑ Cyber criminal: Person or Group who commits Cyber Crime using computers Hackers, criminals groups, hacktivists, virus writers, terrorists

# History of cyber crime

---

- ❑ The first recorded cyber crime took place in the year 1820. The first spam email took place in 1978 when it was sent over the Arpanet. The first VIRUS was installed on an Apple computer in 1982.
- ❑ **Mid-1980s**
  - ❑ Xtree Gold appeared on the market: Recognized file types and retrieved lost or deleted files
  - ❑ Norton DiskEdit soon followed: Became the best tool for finding deleted file
- ❑ **1987 Apple Mac SE**
  - ❑ A Macintosh with an external Easy Drive hard disk with 60 MB of storage
- ❑ **1990**
  - ❑ **International Association of Computer Investigative Specialists (IACIS)**
  - ❑ IRS created search-warrant programs
  - ❑ Expert witness for the Macintosh
    - ❑ First commercial GUI software for computer forensics
    - ❑ Created by ASR Data
  - ❑ Expert Witness for the Macintosh
    - ❑ Recovers deleted files and fragments of deleted files
  - ❑ Other software – iLook & AccessData Forensic Toolkit (FTK)

# Cyber Crime & its Category

---

- ❑ The Computer as a Target : using a computer to attack other computers. virus/worm attacks, Dos attacks etc. E.g Hacking,
  - ❑ The computer as a weapon : using a computer to commit real world crimes. Eg. Cyber terrorism, card Cyber frauds, Child pornography etc..
  - ❑ **Category: Against Person, Property, Government**
  - ❑ **Against Person:** Harassment via email, cyber stalking, email spoofing, carding, assault by threat. The potential harm of such a crime to humanity can hardly be overstated.
  - ❑ **Against Property:** cybercrimes against all forms of property. Unauthorized computer trespassing through cyberspace, computer vandalism, transmission of harmful programs, and unauthorized possession of computerized information.
  - ❑ **Against Government:** Cyber terrorism, damaging critical information infrastructure. Damaging gov or mil websites.
-

# Types of Cybercrime

---

- Hacking: illegal intrusion or unauthorized access to or control over a computer system or network.
  - DOS attack: attempt to make a machine or network resource unavailable to its intended users
  - Virus Dissemination: Malicious s/w attack (Trojan horse, web jacking..)
  - Computer Vandalism: Damaging or destroying data rather than stealing.
  - Piracy: theft of s/w through the illegal copying of genuine programs
  - Credit card Fraud: Fraudsters might use the information to purchase goods in your name or obtain unauthorized funds from an account.
  - Net Extortion: Copying of someone's confidential data in order to extort for huge amount.
  - Ransomware: type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users files unless a ransom is paid.
  - Phishing: to request confidential information over the internet or by telephone under false pretenses in order to fraudulently obtain credit card numbers, passwords or other personal data.
  - Child Pornography: The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide.
  - Cyber Terrorism: Terrorist attacks on the Internet is by distributed DOS attacks, hate websites and hate emails, attacks on sensitive computer networks, etc.
-

# How to tackle these activities?

---

- Awareness is the first step in protecting yourself, family and business. Invest in anti virus, firewall and SPAM blocking software for your PC.
- Secure websites when conducting transactions online.
- Don't respond for unknown emails.
- Set very tuff passwords.
- Cyber Law: There is absolutely no comprehensive law on cybercrime any where in the world. This is reason that the investigating agencies like FBI are finding the cyberspace to be an extremely difficult terrain.
- Electronic Transaction act 2061 BS ( 2005 AD).
- Information Technology policy – 2000.

# Traditional Pbm asso. W. comp. crime

---

- ❑ Any offence against morality, social order or any unjust or shameful act.
- ❑ "Offence" -in the Code of Criminal Procedure to mean as an act or omission made punishable by any law for the time being in force.
- ❑ Cyber Crime is emerging as a serious threat. World wide governments, police departments and intelligence units have started to react.
- ❑ **Cyber crime variants:**
  - ❑ **Hacking** is a crime, which entails cracking systems and gaining unauthorized access to the data stored in them. Hacking had witnessed a 37 per cent increase this year.
  - ❑ **Cyber Stalking** is use of the Internet or other electronic means to stalk someone.
    - ❑ This term is used interchangeably with online harassment and online abuse.
    - ❑ Stalking generally involves harassing or threatening behaviour that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property.

# Cyber crime variants

---

- ❑ **Cyber Squatting** is the act of registering a famous Domain Name and then selling it for a fortune.
- ❑ **Phishing** is just one of the many frauds on the Internet, trying to fool people into parting with their money.
- ❑ Phishing refers to the receipt of unsolicited emails by customers of Financial Institutions, requesting them to enter their Username, Password or other personal information to access their Account for some reason.
- ❑ The fraudster then has access to the customer's online bank account and to the funds contained in that account.
- ❑ **Vishing** is the criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private personal and financial information from the public for the purpose of financial reward.
- ❑ Vishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals.



# Introduction to Identity Theft & Fraud

---

- What is Identity theft?
  - Someone steals your personal information
  - Uses it without permission
  - Can damage your finances, credit history and reputation
- How do you know if your identity was stolen?
  - mistakes on accounts or your Explanation of Medical benefits
  - regular bills go missing
  - calls from debt collectors for debts that aren't yours
  - notice from the IRS
  - calls or mail about accounts in your minor child's name
- How does identity theft happen?
  - steal information from trash or from a business
  - trick you into revealing information
  - take your wallet or purse
  - pretend to offer a job, loan, or apartment to get your information

# Reduce the Risk

---

- Identity protection means treating your personal information with care. Make it a habit.
  - like buckling your seatbelt, or
  - locking your doors at night
- Read your bank, credit and account statements, and
- Explanation of Medical benefits.
  - Look for charges you didn't make.
  - Be alert for bills that don't arrive when you expect them.
  - Follow up if you get account statements you don't expect.
- Protect Your Personal Information.
  - Keep your important papers secure.
  - Be careful with your mail.
  - Shred sensitive documents.
  - Don't over share on social networking sites.

# Reduce the Risk

---

- Respond quickly to notices from the Internal Revenue Service.
  - If someone has used your Social Security number on
  - a tax return, contact IRS's Specialized Identity Theft
  - Protection Unit 1-800-908-4490
- Be alert to online impersonators.
  - Do you know who is getting your personal information?
  - Don't click on links in emails.
  - Contact customer service.
- Protect your computer.
  - Use anti-virus software, anti-spyware software, and a firewall.
  - Create strong passwords. Lock up your laptop.
  - Keep your computer's operating system, browser, and security up to date.
  - Encrypt your data.
  - Be wise about wi-fi.
  - Read privacy policies.

# What to do if someone has stolen identity?

---

- Act fast to limit the damage.
- Take these steps immediately.
- STEP 1: Place an initial fraud alert on your credit report.
  - Contact any one of the three nationwide credit reporting companies.
  - Equifax 1-800-525-6285 Experian 1-888-397-3742 TransUnion 1-800-680-7289
- Step 2: Order your credit reports.
  - Contact each of the three credit reporting companies.
  - ID theft victims get a copy of their reports for free.
  - Read your reports carefully and correct any errors.
- Step 3: Create an Identity Theft Report.
  - Gives you rights that help you to recover more quickly.
  - File a complaint with the FTC.
  - This will become your FTC Affidavit.
  - File a police report.

# TYPES OF CYBER FORENSICS

---

- Military Computer Forensic Technology
- Law Enforcement Computer Forensic
- Business Computer Forensic

# TYPES OF CYBER FORENSICS

---

- ❑ Military Computer Forensic Technology
- ❑ Key objectives of cyber forensics include rapid discovery of evidence, estimation of potential impact of the malicious activity on the victim, and
- ❑ assessment of the intent and identity of the perpetrator.
- ❑ National Law Enforcement and Corrections Technology Center (NLECTC) - demonstrate New Methodology
- ❑ National Institute of Justice (NIJ) sponsors research and development or identifies best practices to address those needs.
- ❑ Integrated forensic analysis framework
- ❑ Possible to accurately determine the motives, intent, targets, sophistication, identity, and location of cyber criminals and cyber terrorists Synthesizing Information from Forensic Investigations (SI-FI) integration environment supports the collection, examination, and analysis processes employed during a cyber-forensic investigation
- ❑ SI-FI prototype uses digital evidence bags (DEBs) – investigators can seal & Authorized user can reopen the DEBs

# TYPES OF CYBER FORENSICS

---

- Law Enforcement Computer Forensic
  - Computer Evidence Processing Procedures
  - Preservation of Evidence
  - Disk Structure : evidence can reside at various levels within the structure of the disk
  - Data Encryption : should become familiar with different forms
  - Matching a Diskette to a Computer: use special software tools to complete this
  - Data Compression
  - Erased Files
  - Internet Abuse Identification and Detection
  - The Boot Process and Memory Resident Programs
-

# TYPES OF CYBER FORENSICS

---

- ❑ Business Computer Forensic
- ❑ Remote Monitoring Of Target Computers - Data Interception by Remote Transmission (DIRT)
- ❑ Creating Trackable Electronic Documents - intrusion detection tool
- ❑ Theft Recovery Software For LaptopsAnd PCs



# Forensics Services Available

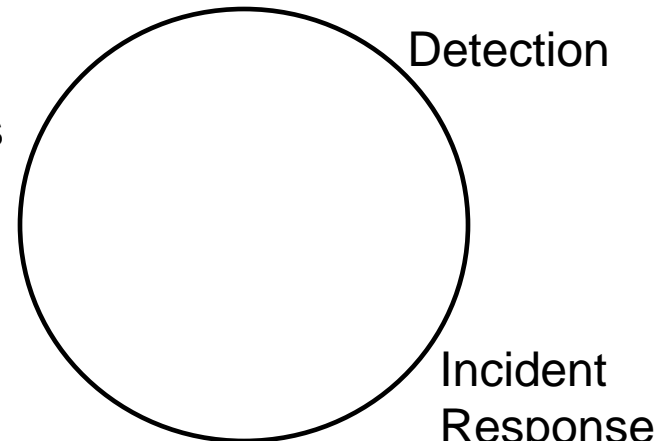
---

- Tracking and location of stolen electronic files
- Honey pot sting operations
- Location and identity of unauthorized software users
- Theft recovery software for laptops and PCs
- Investigative and security software creation
- Protection from hackers and viruses

# Incident Response

- Business Continuity Planning: deals with
  - Outage: Due to natural disasters, electrical failures, ...
- Incident Response: deals with
  - Adverse events that threaten security.
- CIA related incidents
  - Confidentiality
  - Integrity
  - Availability
- Other Types
  - Reconnaissance Attacks
  - Repudiation : - Someone takes action and denies it later on.
  - Harassment
  - Extortion
  - Pornography Traficking
  - Organized Crime Activity
  - Subversion : - Bogus financial server
  - Hoaxes

Countermeasures



Incident Response: Actions taken to deal with an incident.

# Rationale for Incident Response

---

- Abundance of Security-Related Vulnerabilities.
- Availability of Attack Systems and Networks.
- Actual and Potential Financial Loss
- Potential for Adverse Media Exposure
- Need for Efficiency
- Limitations in Intrusion Detection Capabilities.
- Legal Considerations
  - Due care.
  - Provisions of Law

# Incident Response Architecture

---

## Policy

- High-level description of essential elements of information security.
- Do's and Don'ts for users and sys admins.
- Sanctions for infractions.
- Describes security stance of the organization.
  - Sanctioning of incident response capability: IR is a required function of inform

# Incident Response Risk Analysis

---

- No generally accepted methodology for assessing risks.
- Criteria:
  - Monetary costs.
  - Operations impact.
  - Public relations fallout.
  - Impact on humans.
- Risk Categories:
  - Break-in.
    - Break-in in a single system at NASA delayed a launch.
    - System was mission critical.
    - Needed to be recertified before launch.
  - Unauthorized execution of programs or commands.
  - Privilege Escalation.
  - Exploitation of CGI
    - Web servers have frequently cgi scripts installed for demonstration purposes. These have known weaknesses.

# Incident Response Risk Analysis

---

- Denial of Service attacks
- Web Defacement
- Virus and worm attacks
- Malicious active content
- Back door attacks
- Spoofing, Session tampering, hijacking, replay
- Determining Risk Probabilities
  - Collect data within the organization.
  - Collect data by other organizations.
    - CERT Coordinating Center
    - National Infrastructure Protection Center NPIC
- Vulnerability Analysis
  - CERT, ALLDAS, ANTIONLINE

# Incident Response Methodology

---

- ❑ Structure and Organization
    - ❑ Incidents create pandemonium
    - ❑ Incidents occur in bursts
  - ❑ Efficiency
  - ❑ Facilitates the process of responding to incidents.
  - ❑ Facilitates dealing with the unexpected.
  - ❑ Legal Considerations.
  - ❑ Preparation
    - ❑ Setting up a reasonable set of defenses and controls based on threads.
    - ❑ Creating a set of procedures to deal with the incident efficiently.
    - ❑ Obtaining the resources and personnel to deal with the problem.
    - ❑ Establish an infrastructure to support incident response activity.
-

# Incident Response Methodology

---

- ❑ Detection
  - ❑ Intrusion Detection Systems
  - ❑ Detection Software & Reporting
- ❑ Containment: Strategies
  - ❑ Shutting down a system
  - ❑ Disconnect from the network
  - ❑ Change filtering rules of firewalls
  - ❑ Disabling or deleting compromised accounts
  - ❑ Increasing monitoring levels
  - ❑ Setting traps
  - ❑ Striking back at the attacker's system ☹️
- ❑ Adhering to containment procedures.
  - ❑ Record all actions
  - ❑ Define acceptable risks in advance
- ❑ Eradication: Eliminate the cause of the incident.
- ❑ Software available for most virus, worm attacks. Procedures are very important.



# Incident Response Methodology

## ❑ Eradication in UNIX System

- Check .forward for unauthorized entries
- Use ps to find stray processes
- Ensure that essential files are not modified
  - /etc/exports
  - .login
  - .logout
  - .profile
  - /etc/profile
  - .cshrc
  - /etc/rc directory
  - .rhosts
  - /etc/hosts.equiv
  - at
- Examine system commands for changes
  - netstat
  - ls
  - sum
  - find
  - diff
  - /etc/nsswitch.conf
  - /etc/resolv.conf
  - /var/spool/cron
  - kerb.conf

# Incident Response Methodology

---

## ❑ Eradication in UNIX System

- Discover real modification times for files
- Discover suid programs
- Ensure that all password files are the same
- Ensure that there are no unauthorized entries in the .rhost files
- Ensure that there are no unauthorized services running
- Search for all files created or modified during the time of the attack.
- Use the strings command to inspect binaries for clear text that might indicate mischief

# Incident Response Methodology

---

## ❑ Eradication in Window System

- Ensure that the following have not been modified
  - Security Accounts Manager (SAM) Database
  - Services
  - All .dll files
  - Dial-in settings
  - User manager for domain settings
  - All logon scripts
  - The integrity of all registry keys and values below Winlogon and LSA in the registry.
  - Run entries in registry.
  - Membership in all privileged groups.
  - System and user profiles.

# Incident Response Methodology

---

## ❑ Eradication in Windows 2000

- Ensure that the following have not been modified
  - Security Accounts Manager (SAM) Database
  - Services
  - All .dll files
  - Scheduler
  - Policy settings.
  - Membership in privileged groups
  - All logon scripts
  - All security options
  - All permissions for Active Directory.
  - All DNS settings.
  - Registry keys and values under Winlogon and Run in the registry.
  - Permissions and ownerships in `\%systemroot%\ntds ...`

# Incident Response Methodology

---

- Recovery: Return compromised systems back to its normal mission status.
  - Recovery procedures: Safest is:
    - Full rebuilt for system files.
    - Restore data from last backup.
  - Record every action.
  - Keep users aware of status.
  - Advise appropriate people of major developments that might affect them.
  - Adhere to policy regarding media contact.
  - Return logging to normal level.
  - Install patches for any exploited vulnerability.

# Incident Response Methodology

---

## Follow-Up

- Perform a post mortem analysis on each significant incident.
  - Exact description and timeline.
  - Adequacy of staff response.
  - What information was needed at what time.
  - What would the staff do differently.
  - How was interaction with management.
  - What was the damage?
- Use for legal reasons: forensically sound evidence.
  - Includes monetary damage.
- Reevaluation and modification of staff response.
  - Example: Break-in at Human Genome database.
  - Nobody knew who had called when more info was needed.
  - Gap in procedure was remedied during follow-up.

---

## Summary

1. Methodology is needed to deal with quickly evolving, chaotic situations. 2. Takes time to implement and to learn. Use mock events for training. 3. Stages flow into each other. 4. Methodology needs to be tailored to situation. 5. Follow-up needed to improve and adapt methodology.

# Incident Response

## Forming and Managing an IR-Team

---

- Incident response team vs. incident handlers
  - Reasons for outsourcing:
    - Specialists can maintain and add to a complex skill set.
    - Specialists can charge for service.
    - Company might lack resources.
    - Small organizations do not need a team.
  - Reasons for in-house incident response:
    - Sensitive data is better handled by employees.
    - In house team responds better to corporate culture.
-

# Incident Response

## Why an incident team?

---

- Expertise.
- Efficiency.
- Ability to work proactively.
- Ability to meet agency or corporate requirements.
- Teams serve as liaison.
- Ability to deal with institutional barriers.



# Incident Response Basic Requirements

---

- Control over incidents:
  - Full control over incident and data / resources involved **or**  
Control sharing **or** Advisory role.
- Interagency / corporation coordination / liaison
- Clearinghouse
- Contingency planning and business continuity services
- Information security development
- Incident response planning and analysis
- Training and awareness

# Incident Response:

## Determining / Dealing with Constituency

---

- Identify constituency
- Sys Ads are different than general user population
- Failure of dealing adequately with constituency leads to long-term failure
- Failures:
  - Not getting back to an incident reporter.
  - Spreading misinformation.
  - Becoming too intrusive.
  - Causing embarrassment or leaking information without authorization.
  - Betrayal.

# Incident Response: Success Metrics

---

- Good security → No incidents.
- Makes success metrics difficult:
  - Nr. of incidents
  - Estimated financial loss.
  - Self-evaluation / questionnaires
  - Written or verbal reports by constituency
  - Average time and manpower per incident
  - Documentation by team members
  - Awards / other forms of external recognition

# Incident Response: Organization of IR Team

---

## Training the team

- Mentoring
- Self-Study
- Courses
- Library
- Exercises

## Testing the team / procedure

## Dealing with resistance

- Budget: not a revenue source, hard to quantify impact
- Management reluctance
- Organizational resistance: rival organizations, turf warfare
- Internal politics
- User awareness

# Incident Response: Organization of IR Team

---

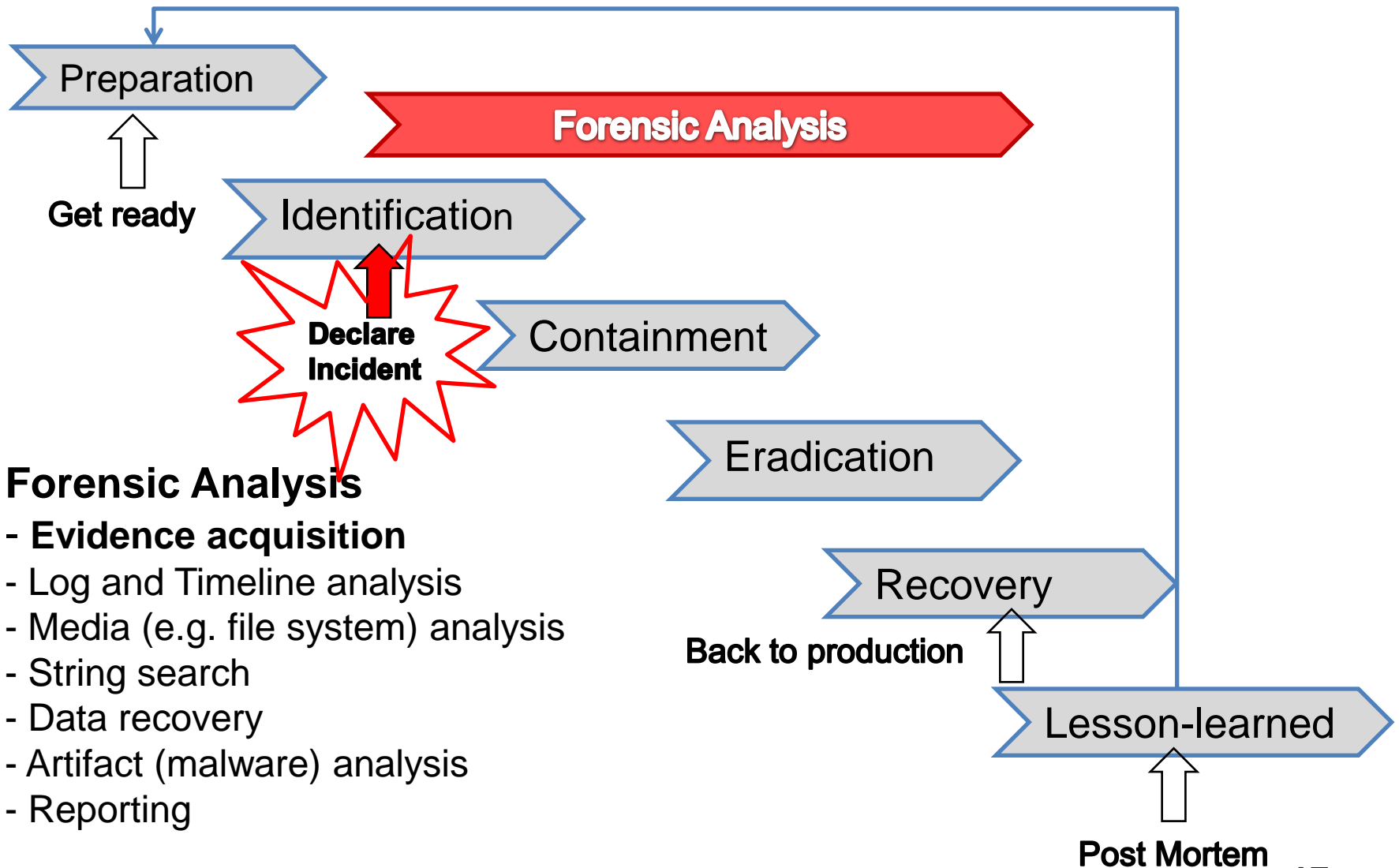
- External Coordination
  - Law Enforcement
  - Media
  - Other Incident Response Teams
    - Infraguard
- Managing Incidents
  - Bursty load: surviving the long haul
  - Assigning incident ownership
  - Tracking charts
  - Prioritization

# Incident Response: Role of Computer Forensics

---

- ❑ Determines policies:
  - ❑ Ethical boundaries of response
  - ❑ Legal boundaries of response
    - ❑ To protect right's of insiders and outsiders
    - ❑ To preserve evidence as legal evidence
      - ❑ Rules for thorough documentation
      - ❑ Protect evidence against accidental or intentional tampering / destruction
- ❑ Technical Response
  - ❑ How to document
  - ❑ How to establish chain of custody
  - ❑ How to gather all possibly important evidence

# Incident Handling Lifecycle



# Be warned!

---

- ❑ No two incidents are identical
- ❑ No one-for-all solution, tailor it for your OWN need!
- ❑ Many types of incidents
  - ❑ DoS, Virus/Worm, Inappropriate usage, unauthorized access etc.
- ❑ Focus on “hacking scenario”
- ❑ But the principle remains the same!



# Step 1 - Preparation

---

- Know existing policies, regulations and laws
  - Authority** of investigation
    - Job description
    - Incident handling procedure
  - What information can be collected?
  - Privacy and wiretapping issue
- Do not violate any existing security policies
- And do not break laws!
- Security policy and incident handling procedure
  - Policies & procedures, write them down on PAPER
  - A simple and easy-to-follow procedure is very helpful

# Preparation

---

- Building a team
  - Information about the team - "Organizational Models for Computer Security Incident Response Teams (CSIRTs) (<http://www.cert.org/archive/pdf/03hb001.pdf>)
- Contacts information and communication channels
  - Name, telephone, email, PGP keys etc.
- Incidents Prevention
  - Risk assessment
  - Patching, hardening, best practice, education etc.
  - Be aware of your organization's security policy
- Known your systems before an incident**
  - Profile systems and network
  - Know normal behaviours

# Toolkit – Live CDs

---

- ❑ Incident response toolkit
  - ❑ Linux forensic live CDs
    - ❑ Helix (no longer free ☹) - <http://e-fense.com/>
      - ❑ Live response, live/dead acquisition and analysis
    - ❑ FCCU GNU/Linux Forensic Boot CD
      - ❑ Belgian Federal Computer Crime Unit
      - ❑ <http://www.lnx4n6.be/>
    - ❑ BackTrack 4 has an option to boot into forensic mode
      - ❑ <http://remote-exploit.org/backtrack.html>
    - ❑ Many others
  - ❑ Will not modify the target system harddisk
    - ❑ Will not auto-mount devices on target system
    - ❑ Will not use target system swap partition
    - ❑ Build-in some well-known open source forensic tools

# Toolkit - Forensic

---

- ❑ Any Linux system plus proper open source forensic tools
  - ❑ US CERT forensic appliance (fedora)
    - ❑ A fully functional Linux VM forensics appliance
    - ❑ Linux Forensics Tools Repository (RPMs for fedora)
    - ❑ <http://www.cert.org/forensics/tools/>
  - ❑ SANS SIFT workstation (Ubuntu)
    - ❑ VM forensic appliance
    - ❑ <https://computer-forensics2.sans.org/community/siftkit/>
    - ❑ Free, but registered first
  - ❑ BackTrack
  - ❑ Load of tools readily available
-

# Toolkit - Forensic

---

- ❑ TSK + Autopsy (GUI-frontend)

  - ❑ The Sleuth Kit and Autopsy browser

  - ❑ <http://www.sleuthkit.org/>

  - ❑ Alternative – PSK (GUI-frontend)

    - ❑ <http://ptk.dflabs.com/>

- ❑ The Coroner's Toolkit (TCT)

  - ❑ <http://www.porcupine.org/forensics/tct.html>

# Toolkit – Network forensic

---

- ❑ Wireshark/tshark
- ❑ Tcpdump
- ❑ Nmap
- ❑ Snort
- ❑ P0f (OS passive fingerprinting)
- ❑ Antivirus software
  - ❑ <http://www.clamav.net/>
  - ❑ AVG and avast! for Linux, free!

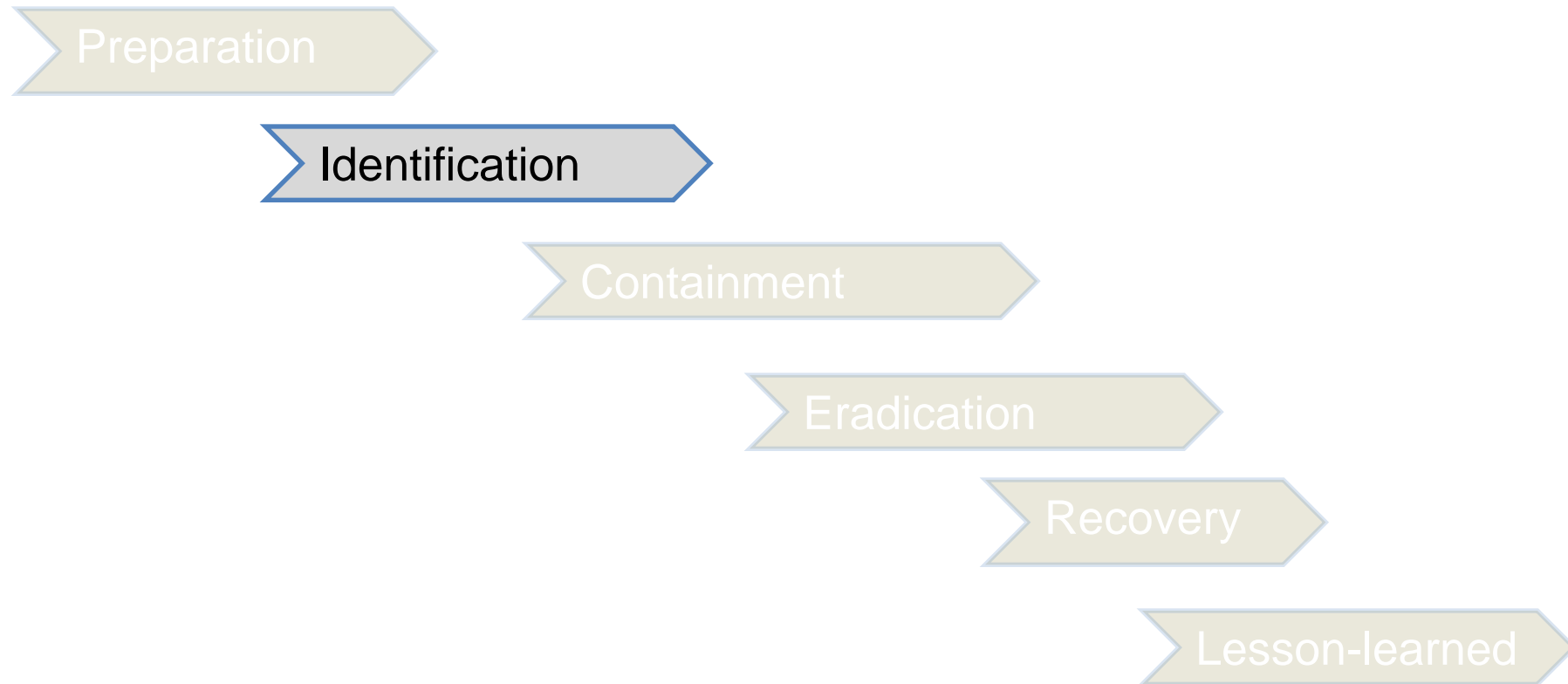
# Toolkit – Build in

---

- ❑ Trusted binaries - **statically compiled** binaries run from CD or USB
  - ❑ ls, lsof, ps, netstat, w, grep, uname, date, find, file, ifconfig, arp ... ..
- ❑ Test before use
  - ❑ different Linux distributions and kernels
  - ❑ both 32 bit and 64 bit platform
- ❑ Will not modify A-time of system binaries;
- ❑ Be aware of limitation – can be cheated as well
  - ❑ Kernel mode rootkit

# Incident Handling Lifecycle

---





# Step 2 - Identification

---

- Detect deviation from normal status
  - Alerted by someone else;**
  - Host & network IDS alerts;
  - antivirus/antispyware alerts;
  - Rootkit detection tools;
  - file integrity check;
  - System logs;
  - firewall logs;
  - A trusted central logging facility is essential;
  - Correlate all information available to minimise **false alarm**

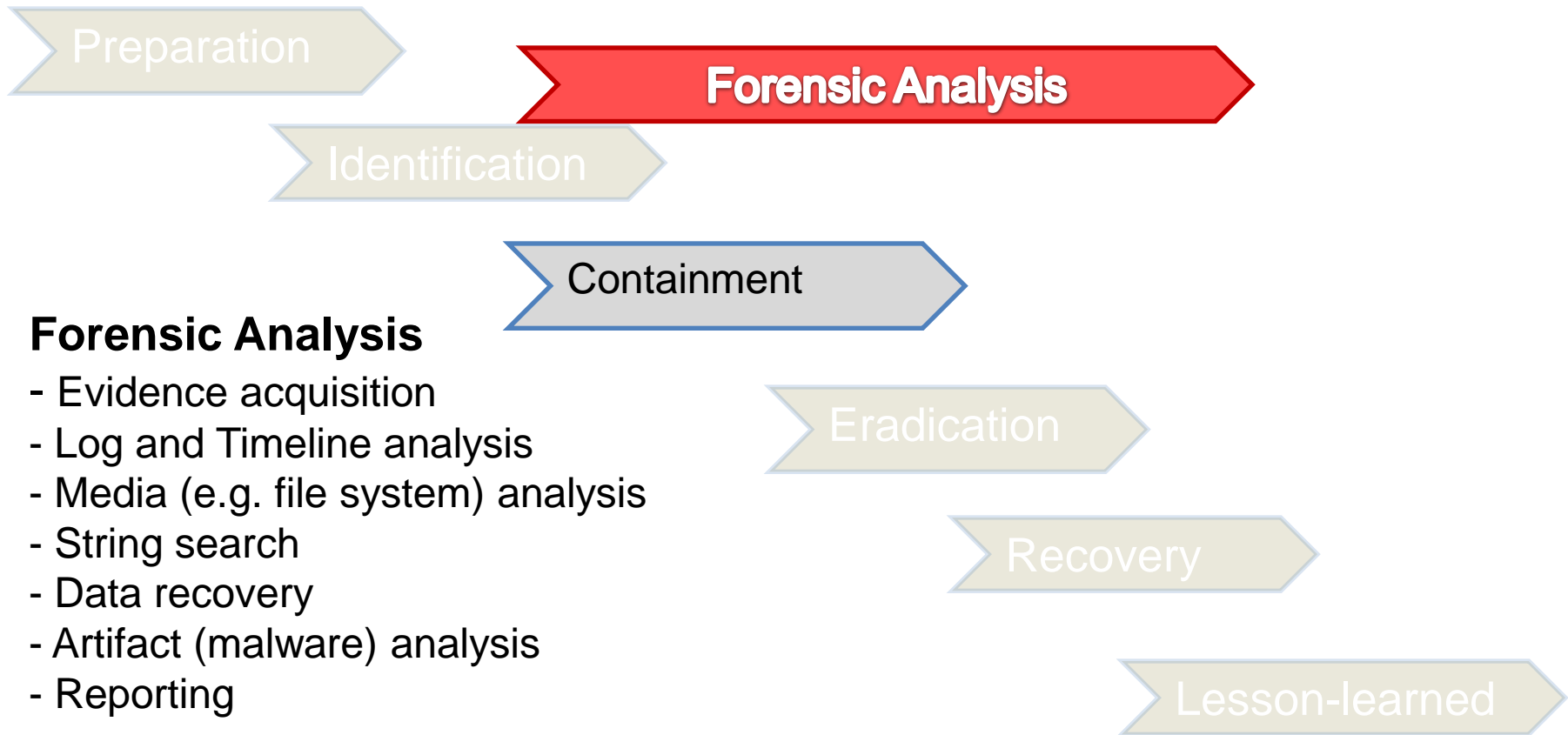
# Identification

---

- Declare** an incident once confirmed
  - Make sure that senior management is informed
  - Notification – who should be notified?
  - EGEE CSIRTs: [PROJECT-EGEE-SECURITY-CSIRTS@in2p3.fr](mailto:PROJECT-EGEE-SECURITY-CSIRTS@in2p3.fr)
- Following incident handling **procedures**
  - EGEE incident response procedure
  - <https://edms.cern.ch/document/867454>

# Incident Handling Lifecycle

---



# Step 3 – Containment & Forensic Analysis

---

- Prevent attackers from further damaging systems
- Questions to be answered!
  - Online or Offline?
    - Pull the network cable?
  - Live or Dead system?
    - Pull the plug?

# Forensic Analysis

---

- Start up forensic analysis process once incident has been identified
  - Aim to obtain forensic sound evidences
  - Live system information
    - Will lose once powered off
  - Bit by bit disk image
  - Logs analysis
  - Timeline analysis
  - Data/file recovery
- Collect volatile data FIRST, if possible!


# How to collect evidences

---

- ❑ Volatile data collection
- ❑ Hard disk image
- ❑ Where to store evidences?
  - ❑ Attach a USB device
  - ❑ Transfer data over network with *netcat*
  - ❑ Evidence workstation (192.168.0.100):
    - ❑ # *./nc -l -p 2222 > evidence.txt*
    - ❑ Compromised host:
      - ❑ # *./lsof -n | nc 192.168.0.100 2222*

# Volatile Data Collection

---

- Aim:
  - Collect as much volatile data as possible
  - But **minimise** footprint on the target system
- In the order of most volatile to least
  -  Memory
  - Network status and connections
  - Running processes
  - Other system information
- Be warned: system status will be **modified**
- Document everything you have done
- Be aware of the concept of “chain of custody”
  - Maintain a good record (a paper trail) of what you have done with evidence

# Volatile Data Collection?

---

- System RAM
  - Raw memory image with *memdump*
  - Available at <http://www.porcupine.org/forensics/tct.html>
  - Hardware-based memory acquisition?
  - Virtual Machine
    - Take a snapshot
- Network Information
  - open ports and connections
    - lsof* and *netstats*
    - Nmap*
- Process information
  - Running processes with *ps*
  - Process dumping with *pcat*
    - Available at <http://www.porcupine.org/forensics/tct.html>



# Other volatile data

---

## System Information

- System uptime: *uptime*
- OS type and build: *uname -a*
- Current date/time: *date*
- Partition map: *fdisk -l*
- Mount points: *mount*
- ... ..?

# What to do with memory image?

---

- ❑ Linux memory dump
  - ❑ Very limited option (at least with open source tools)
  - ❑ Strings search for IP, email or strange strings etc
  - ❑ Can be used to cross check with evidence found in file system/logs
  - ❑ Some ongoing researches in open source community

# Collect Evidence – Disk Image

---

- Bit by bit disk image
  - Capture both allocated and unallocated space
- Do not use gzip/tar or normal backup tools
  - Lose unallocated space
  - Can't recover deleted files
- How to do it?
  - Live system vs dead system image?
  - Full disk vs Partition?

# Disk Image

---

- Live system image vs Dead system image?
  - Helix Live CD or FCCU Live CD
  - Or USB
  - Writeblocker?
- Full disk vs. Partition?
- Full disk if possible
  - Get everything in one go
  - Can copy host protection area - HPA (after reset)
  - Might not be feasible
    - RAID system: too big, RAID reconstruction?
- Image only partition
  - OS partitions

# Disk image

---

## Linux *dd* command

### Full disk

`dd if=/dev/sda of=/mnt/usb/sda.img bs=512`

### Partition

`dd if=/dev/sda1 of=/mnt/usb/sda1.img bs=512`

## Enhanced *dd* – e.g. *dc3dd* or *dcfldd*

<http://dc3dd.sourceforge.net/>

<http://dcfldd.sourceforge.net/>

`dcfldd if=/dev/sourcedirve hash=md5 hashwindow=10M  
md5log=md5.txt bs=512 of=driveimage.dd`

## *dd\_rescue*

<http://www.gnu.org/software/ddrescue/ddrescue.html>

# What to do with disk images?

---

- ❑ Mount disk image/partition to the loop device on a forensic workstation in READ ONLY mode
  - ❑ *mount -o loop, ro, offset=XXXX disk\_image.dd /mnt/mount\_point*
- ❑ Partition information can be obtained
  - ❑ *sfdisk -l disk\_image.dd*
  - ❑ *fdisk -lu disk\_image.dd*
  - ❑ *mmls -t type disk\_image.dd*
    - ❑ In the TSK toolset
- ❑ Either work on the whole image
  - ❑ Use the “offset” parameter
- ❑ Or, split the image to individual partitions and then mount them separately
  - ❑ *dd if=disk\_image.dd bs= 512 skip=xxx count=xxx of=partition.dd*

# Evidence Collection

---

- Memory dump;
- Network status;
- Process dump;
- Other system information;
- Disk images;
- Forensic analysis done on the images NOT on the original disk;

# After Evidence Collection

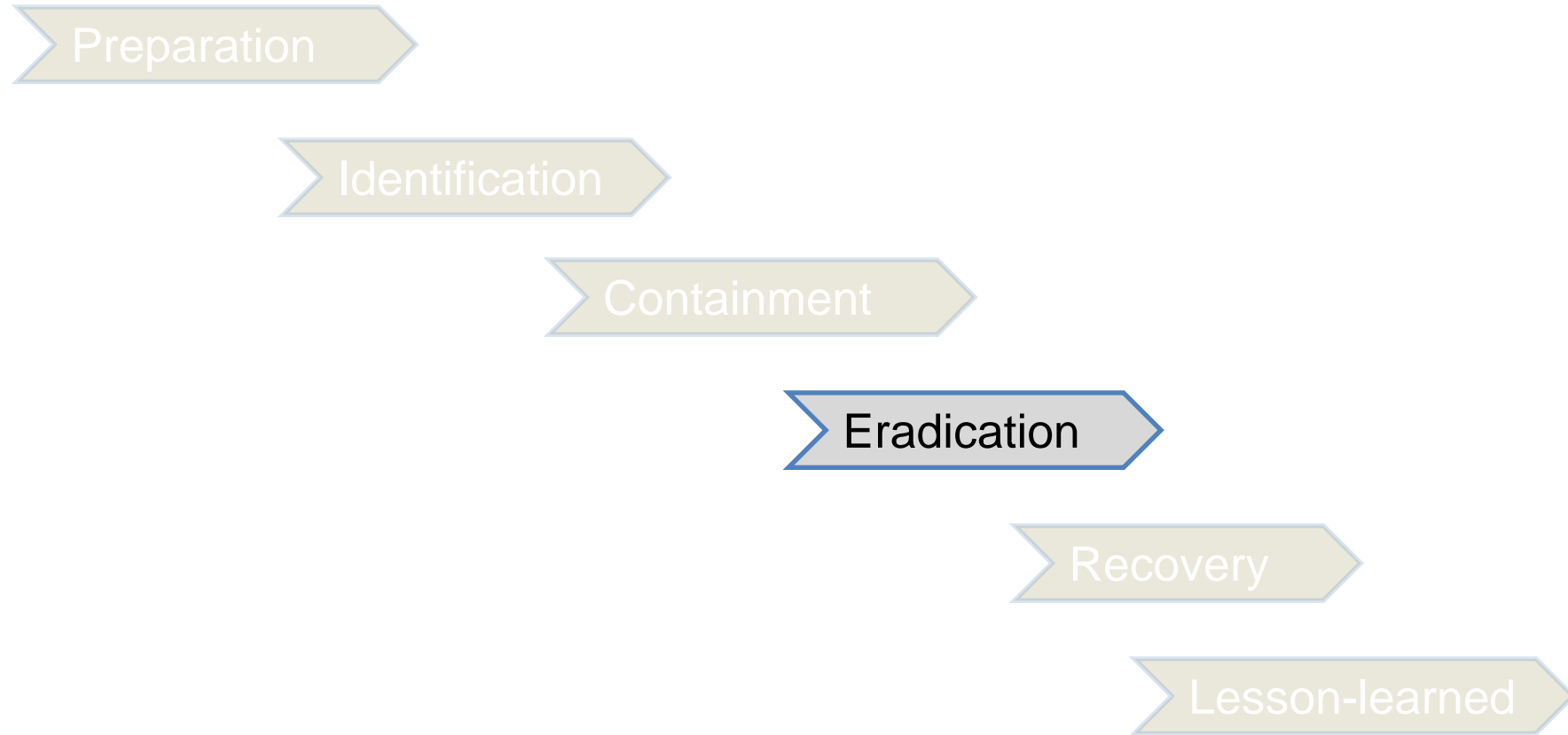
---

- Mount disk/partition images on a trusted system
- Timeline analysis with *TSK*
  - What had happened?
- Media (e.g. file system) analysis with *TSK*
  - What was modified/changed and or left?
- String search on both allocated and unallocated areas with *strings*
- Data recovery with *TSK*
  - What was deleted?
- Artifact (malware) analysis
  - To understand the function of the malware
- Sharing findings with relevant parties



# Incident Handling Lifecycle

---



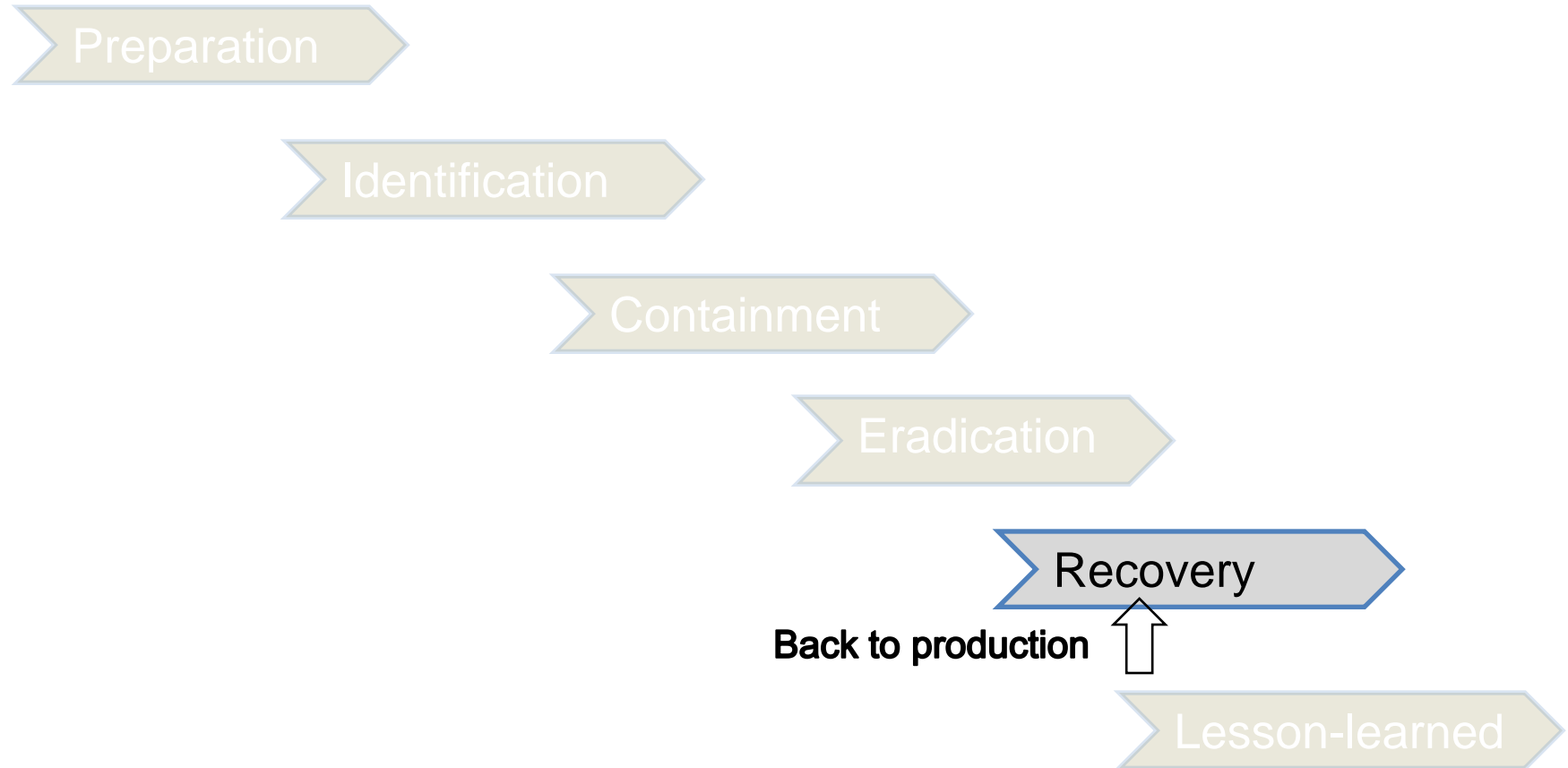
# Step 4 Eradiation

---

- Remove compromised accounts
- Revoke compromised credentials
- Remove malware/ artifact left over by the attackers
- Restore from most recent clean backup
- If root-compromised, **rebuild** system from scratch
- Harden, **patch** system to prevent it from re-occurrence

# Incident Handling Lifecycle

---



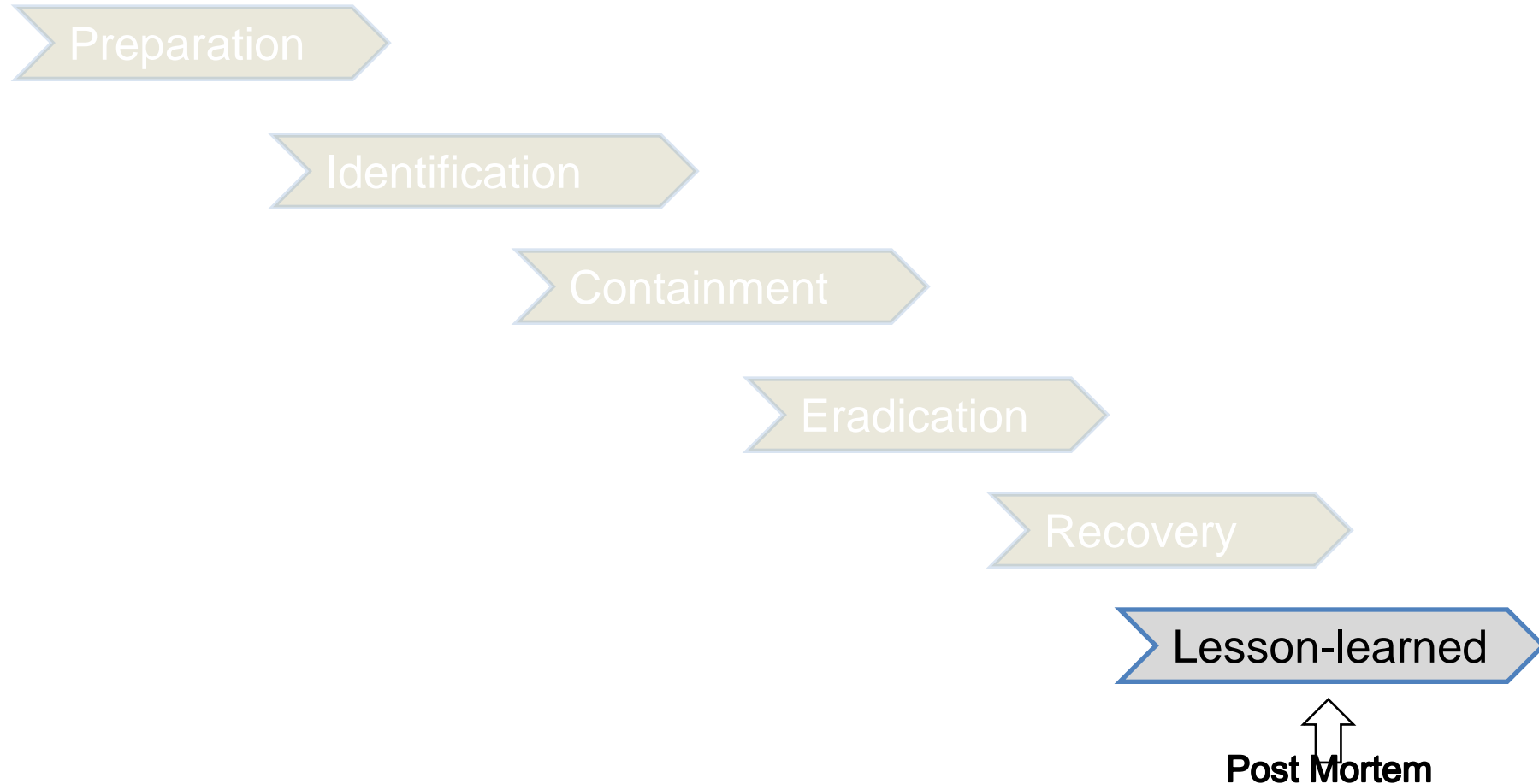
# Recovery

---

- Put system back to production in a control manner
- Decision should be made by management
- Closely monitoring the system

# Incident Handling Lifecycle

---



# Step 6 – Lesson learned

---

- Know what went right and what went wrong
  - Learning & improving
  - A post-mortem meeting/discussion

# DEMO

---

- ❑ How to detect rootkit in a live Linux system?
  - ❑ Captured in last year incident
  - ❑ Kernel mode rootkit with sniffing backdoor
  - ❑ Hide itself and relevant files from normal detection
  - ❑ Can survive from system reboot
  - ❑ Protected with password

# EX2/EX3 file system premier

---

## Superblock

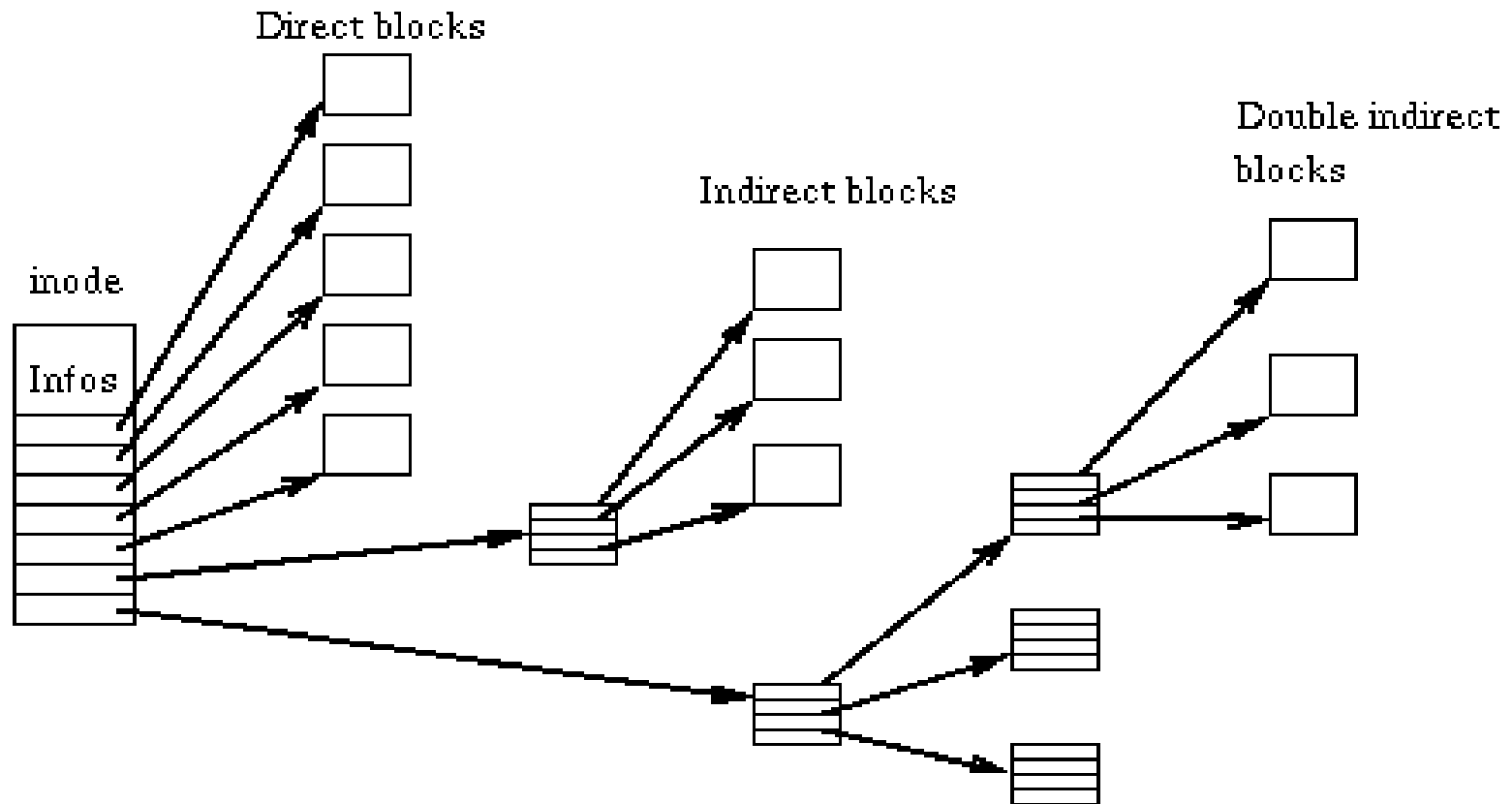
- Block size, number of blocks, number of Inodes, number of reserved blocks, number of blocks per group, number of Inodes per Group

## Block Groups

- All blocks belong to a Block Group
- Begins from block 0, after reserved blocks
- Each Block Group
  - Superblock backup
  - Group Descriptor Table
  - Block Bitmap, Inode Bitmap
  - Inode Table, Data Blocks



# EX2/3 Meta Data structure



# Directories

---

- ❑ Directory itself is a file
- ❑ A sequence of entries
  - ❑ Inode number
  - ❑ File name
  - ❑ Size of file name

Byte Offset	Inode Number	File Names
0	80	.
16	8	..
32	1674	init
48	69	fstab
64	1978	passwd
80	115	group
...	...	...

# Computer Forensic Requirements

---

## **Hardware**

- Familiarity with all internal and external devices/components of a computer
- Thorough understanding of hard drives and settings
- Understanding motherboards and the various chipsets used
- Power connections
- Memory

**Software:** Familiarity with most popular software packages such as Office

**Forensic Tools:** Familiarity with computer forensic techniques and the software packages that could be used

# 4 Steps of Computer Forensics

---

- ❑ **Acquisition** : Physically or remotely obtaining possession of the computer, all network mappings from the system, and external physical storage devices
- ❑ **Identification** : This step involves identifying what data could be recovered and electronically retrieving it by running various Computer Forensic tools and software suites
- ❑ **Evaluation** : Evaluating the information/data recovered to determine if and how it could be used against the suspect for employment termination or prosecution in court
- ❑ **Presentation** : This step involves the presentation of evidence discovered in a manner which is understood by lawyers, non-technically staff/management, and suitable as evidence as determined by United States and internal laws

---

# Understanding Computer Investigation

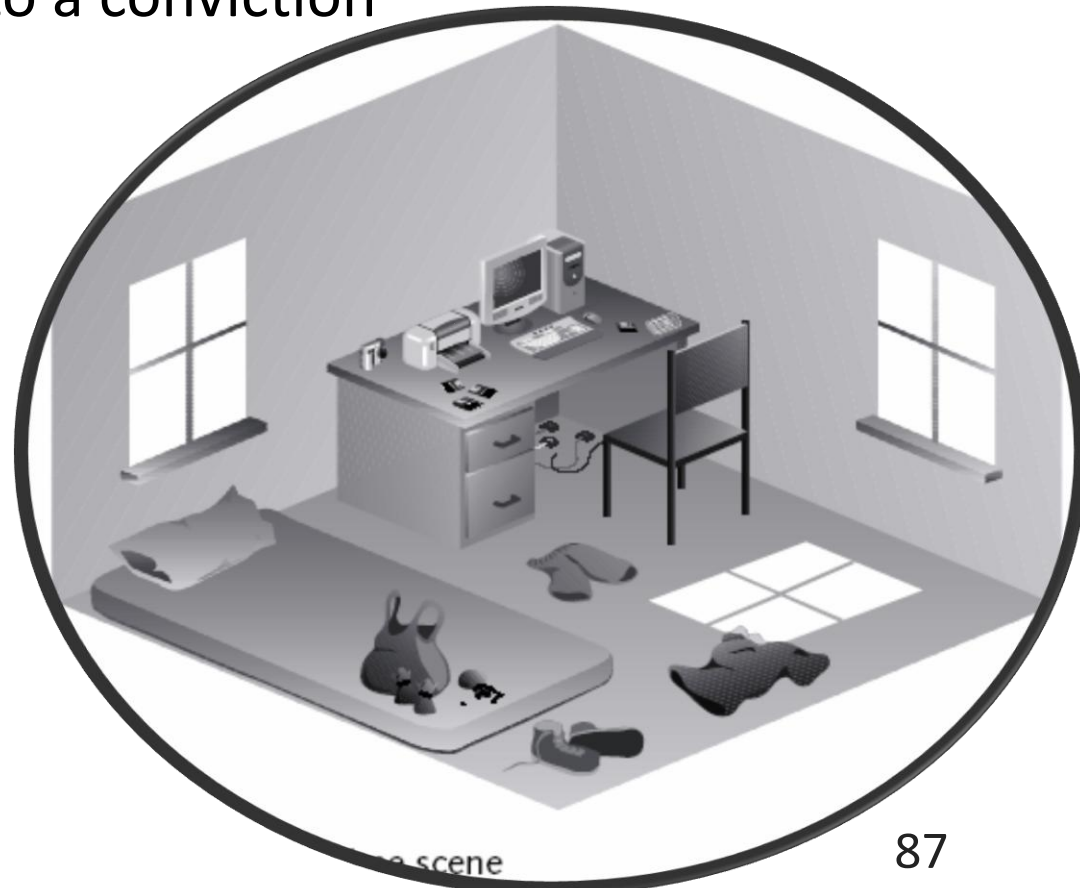
# Preparing a Computer Investigation

---

- ❑ Role of computer forensics professional is to gather evidence to prove that a suspect committed a crime or violated a company policy
- ❑ Collect evidence that can be offered in court or at a corporate inquiry
  - ❑ Investigate the suspect's computer
- ❑ Preserve the evidence on a different computer Follow an accepted procedure to prepare a case
- ❑ **Chain of custody**
  - ❑ Route the evidence takes from the time you find it until the case is closed or goes to court

# An Overview of a Computer Crime

- ❑ Computers can contain information that helps law enforcement determine:
  - ❑ Chain of events leading to a crime
  - ❑ Evidence that can lead to a conviction
- ❑ Law enforcement officers should follow proper procedure when acquiring the evidence
  - ❑ Digital evidence can be easily altered by an overeager investigator
- ❑ Information on hard disks might be **password protected**



# An Overview of a Company Policy Violation

---

- Employees misusing resources can cost companies millions of dollars
- Misuse includes:
  - Surfing the Internet
  - Sending personal e-mails
  - Using company computers for personal tasks



# Taking a Systematic Approach

---

- Steps for problem solving
  - Make an initial assessment about the type of case you are investigating
  - Determine a preliminary design or approach to the case
  - Create a detailed checklist
  - Determine the resources you need
  - Obtain and copy an evidence disk drive
  - Identify the risks
  - Mitigate or minimize the risks
  - Test the design
  - Analyze and recover the digital evidence
  - Investigate the data you recover
  - Complete the case report and Critique the case

# Assessing the Case

---

- Systematically outline the case details
  - Situation
  - Nature of the case
  - Specifics of the case
  - Type of evidence
  - Operating system
  - Known disk format
  - Location of evidence
- Based on case details, u can determine the case requirements
  - Type of evidence
  - Computer forensics tools
  - Special operating systems

# Planning Your Investigation

---

- A basic investigation plan should include the following activities:
  - Acquire the evidence
  - Complete an evidence form and establish a chain of custody
  - Transport the evidence to a computer forensics lab
  - Secure evidence in an **approved secure container**
  - Prepare a forensics workstation
  - Obtain the evidence from the secure container
  - Make a forensic copy of the evidence
  - Return the evidence to the secure container
  - Process the copied evidence with computer forensics tools
- An **evidence custody form** helps you document what has been done with the original evidence and its forensics copies
- Two types
  - Single-evidence form**: Lists each piece of evidence on a separate page
  - Multi-evidence form**

# Planning Your Investigation

Corporation X Security Investigations This form is to be used for one to ten pieces of evidence			
Case No.:		Investigating Organization:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			
	Description of evidence:	Vendor Name	Model No./Serial No.
Item #1			
Item #2			
Item #3			
Item #4			
Item #5			
Item #6			
Item #7			
Item #8			
Item #9			
Item #10			
Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	
Item #	Evidence Processed by	Disposition of Evidence	Date/Time
			Page __ of __

Figure 2-2 A sample multi-evidence form used in a corporate environment

Metropolis Police Bureau High-tech Investigations Unit This form is to be used for only one piece of evidence. Fill out a separate form for each piece of evidence.			
Case No.:		Unit Number:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			
Item # ID	Description of evidence:	Vendor Name	Model No./Serial No.
Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	
Evidence Processed by	Disposition of Evidence	Date/Time	
			Page __ of __

Figure 2-3 A single-evidence form

# Securing Your Evidence

---

- Use **evidence bags** to secure and catalog the evidence
- Use computer safe products
  - Antistatic bags
  - Antistatic pads
- Use well padded containers
- Use evidence tape to seal all openings
  - Floppy disk or CD drives
  - Power supply electrical cord
- Write your initials on tape to prove that evidence has not been tampered with
- Consider computer specific temperature and humidity ranges

# Procedures for Corporate High-Tech Investigations

---

- Develop formal procedures and informal checklists
  - To cover all issues important to high-tech investigations
- Employee Termination Cases
- Majority of investigative work for termination cases involves employee abuse of corporate assets
- Internet abuse investigations
  - To conduct an investigation you need:
    - Organization's Internet proxy server logs
    - Suspect computer's IP address
    - Suspect computer's disk drive
    - Your preferred computer forensics analysis tool
  - Recommended steps
    - Use standard forensic analysis techniques and procedures
    - Use appropriate tools to extract all Web page URL information
    - Contact the network firewall administrator and request a proxy server log
    - Compare the data recovered from forensic analysis to the proxy server log
    - Continue analyzing the computer's disk drive data

# Employee Termination Cases

---

- ❑ E-mail abuse investigations
    - ❑ To conduct an investigation you need:
      - ❑ An electronic copy of the offending e-mail that contains message header data
      - ❑ If available, e-mail server log records
      - ❑ For e-mail systems that store users' messages on a central server, access to the server
      - ❑ Access to the computer so that you can perform a forensic analysis on it
      - ❑ Your preferred computer forensics analysis tool
    - ❑ Recommended steps
      - ❑ Use the standard forensic analysis techniques
      - ❑ Obtain an electronic copy of the suspect's and victim's e-mail folder or data
      - ❑ For Web-based e-mail investigations, use tools such as FTK's Internet Keyword Search option to extract all related e-mail address information
      - ❑ Examine header data of all messages of interest to the investigation
-

# Attorney-Client Privilege Investigations

---

- Under **attorney-client privilege (ACP)** rules for an attorney
  - You must keep all findings confidential
- Many attorneys like to have printouts of the data you have recovered
  - You need to persuade and educate many attorneys on how digital evidence can be viewed electronically
- You can also encounter problems if you find data in the form of binary files
- Steps for conducting an ACP case
  - Request a memorandum from the attorney directing you to start the investigation
  - Request a list of keywords of interest to the investigation
  - Initiate the investigation and analysis
  - For disk drive examinations, make two bit-stream images using different tools
  - Compare hash signatures on all files on the original and re-created disks
  - Methodically examine every portion of the disk drive and extract all data
  - Run keyword searches on allocated and unallocated disk space
  - For Windows OSs, use specialty tools to analyze and extract data from the Registry: AccessData Registry Viewer



# Attorney-Client Privilege Investigations

---

- ❑ Steps for conducting an ACP case (continued)
  - ❑ For binary data files such as CAD drawings, locate the correct software product
  - ❑ For unallocated data recovery, use a tool that removes or replaces nonprintable data
  - ❑ Consolidate all recovered data from the evidence bit-stream image into folders and subfolders
- ❑ Other guidelines
  - ❑ Minimize written communications with the attorney
  - ❑ Any documentation written to the attorney must contain a header stating that it's "Privileged Legal Communication—Confidential Work Product"
  - ❑ Assist attorney and paralegal in analyzing the data
- ❑ If you have difficulty complying with the directions
  - ❑ Contact the attorney and explain the problem
- ❑ Always keep an open line of verbal communication
- ❑ If you're communicating via e-mail, use encryption

# Media Leak Investigations

- In the corporate environment, controlling sensitive data can be difficult
- Consider the following for media leak investigations
  - Examine e-mail
  - Examine Internet message boards
  - Examine proxy server logs
  - Examine known suspects' workstations
  - Examine all company telephone records, looking for calls to the media
- Steps to take for media leaks
  - Interview management privately
    - To get a list of employees who have direct knowledge of the sensitive data
  - Identify media source that published the information
  - Review company phone records
  - Obtain a list of keywords related to the media leak
  - Perform keyword searches on proxy and e-mail servers
  - Discreetly conduct forensic disk acquisitions and analysis
  - From the forensic disk examinations, analyze all e-mail correspondence
    - And trace any sensitive messages to other people
  - Expand the discreet forensic disk acquisition and analysis
  - Consolidate and review your findings periodically
  - Routinely report findings to management

# Industrial Espionage Investigations

---

- All suspected industrial espionage cases should be treated as criminal investigations
- Staff needed
  - Computing investigator who is responsible for disk forensic examinations
  - Technology specialist who is knowledgeable of the suspected compromised technical data
  - Network specialist who can perform log analysis and set up network sniffers
  - Threat assessment specialist (typically an attorney)
- Guidelines
  - Determine whether this investigation involves a possible industrial espionage incident
  - Consult with corporate attorneys and upper management
  - Determine what information is needed to substantiate the allegation
  - Generate a list of keywords for disk forensics and sniffer monitoring
  - List and collect resources for the investigation
  - Determine goal and scope of the investigation
  - Initiate investigation after approval from management
- Planning considerations
  - Examine all e-mail of suspected employees
  - Search Internet newsgroups or message boards
  - Initiate physical surveillance
  - Examine facility physical access logs for sensitive areas

# Industrial Espionage Investigations

---

- Planning considerations (continued)**
  - Determine suspect location in relation to the vulnerable asset**
  - Study the suspect's work habits**
  - Collect all incoming and outgoing phone logs**
- Steps**
  - Gather all personnel assigned to the investigation and brief them on the plan**
  - Gather resources to conduct the investigation**
  - Place surveillance systems**
  - Discreetly gather any additional evidence**
  - Collect all log data from networks and e-mail servers**
  - Report regularly to management and corporate attorneys**
  - Review the investigation's scope with management and corporate attorneys**

# Interviews and Interrogations in High-Tech Investigations

---

- Becoming a skilled interviewer and interrogator can take many years of experience**
  - Interview**
    - Usually conducted to collect information from a witness or suspect**
      - About specific facts related to an investigation**
  - Interrogation**
  - Trying to get a suspect to confess**
    - Role as a computing investigator**
      - To instruct the investigator conducting the interview on what questions to ask**
        - And what the answers should be**
  - Ingredients for a successful interview or interrogation**
    - Being patient throughout the session**
    - Repeating or rephrasing questions to zero in on specific facts from a reluctant witness or suspect**
    - Being tenacious**
-

# Understanding Data Recovery

## Workstations and Software

---

- Investigations are conducted on a computer forensics lab (or data-recovery lab)
- Computer forensics and data-recovery are related but different
- Computer forensics workstation**
  - Specially configured personal computer
  - Loaded with additional bays and forensics software
- To avoid altering the evidence use:
  - Forensics boot floppy disk OR cd
  - Write-blocker devices

# Write Blocker

---

- ❑ Connects a hard drive in trusted read-only mode
- ❑ There are also Linux boot CDs that mount all drives read-only, such as Helix and some Knoppix distributions



# Setting Up your Computer for Computer Forensics

---

- Basic requirements
    - A workstation running Windows XP or Vista
    - A write-blocker device
    - Computer forensics acquisition tool
      - Like FTK Imager
    - Computer forensics analysis tool
      - Like FTK
    - Target drive to receive the source or suspect disk data
    - Spare PATA or SATA ports
    - USB ports
  - Additional useful items
    - Network interface card (NIC), Extra USB ports, FireWire 400/800 ports, SCSI card, Disk editor tool, Text editor tool , Graphics viewer program , Other specialized viewing tools
-



# Conducting an Investigation

---

- Gather resources identified in investigation plan
- Items needed
  - Original storage media
  - Evidence custody form
  - Evidence container for the storage media
  - Bit-stream imaging tool
  - Forensic workstation to copy and examine your evidence
  - Securable evidence locker, cabinet, or safe

# Gathering the Evidence

---

- Avoid damaging the evidence

- Steps

  - Meet the IT manager to interview him

  - Fill out the evidence form, have the IT manager sign

  - Place the evidence in a secure container

  - Complete the evidence custody form

  - Carry the evidence to the computer forensics lab

  - Create forensics copies (if possible)

  - Secure evidence by locking the container

# Understanding Bit-Stream Copies

## ❑ Bit-stream copy

- ❑ Bit-by-bit copy of the original storage medium
- ❑ Exact copy of the original disk
- ❑ Different from a simple backup copy
  - ❑ Backup software only copies known files (active data)
  - ❑ Backup software cannot copy deleted files, e-mail messages or recover file fragments

## ❑ Bit-stream image

- ❑ File containing the bit-stream copy of all data on a disk or partition
- ❑ Also known as **forensic copy**
- ❑ Copy image file to a target disk that matches the original disk's manufacturer, size and model

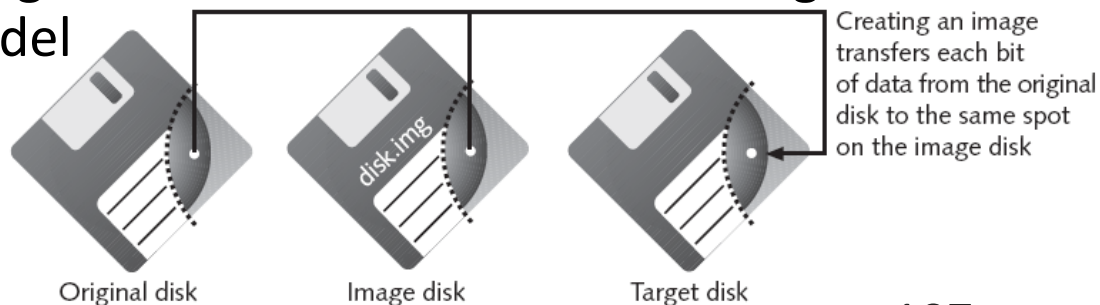


Figure 2-4 Transfer of data from original to image to target

# Acquiring an Image of Evidence Media

---

- ❑ First rule of computer forensics
  - ❑ Preserve the original evidence
- ❑ Conduct your analysis only on a copy of the data

# Completing the Case

---

- You need to produce a final report
  - State what you did and what you found
- Include report generated by your forensic tool to document your work
- Repeatable findings**
  - Repeat the steps and produce the same result, using different tools
- If required, use a report template
- Report should show conclusive evidence
  - Suspect did or did not commit a crime or violate a company policy

# Critiquing the Case

---

## Ask yourself the following questions:

How could you improve your performance in the case?

Did you expect the results you found? Did the case develop in ways you did not expect?

Was the documentation as thorough as it could have been?

What feedback has been received from the requesting source?

## Ask yourself the following questions (continued):

Did you discover any new problems? If so, what are they?

Did you use new techniques during the case or during research?

---

# *Data Acquisition*

# Understanding Storage Formats for Digital Evidence

---

- ❑ Two types of data acquisition
  - ❑ Static acquisition
    - ❑ Copying a hard drive from a powered-off system
    - ❑ Used to be the standard
    - ❑ Does not alter the data, so it's repeatable
  - ❑ Live acquisition
    - ❑ Copying data from a running computer
    - ❑ Now the preferred type, because of hard disk encryption
    - ❑ Cannot be repeated exactly—alters the data
    - ❑ Also, collecting RAM data is becoming more important
      - ❑ But RAM data has no timestamp, which makes it much harder to use
- ❑ Terms used for a file containing evidence data
  - ❑ Bit-stream copy, Bit-stream image, Image, Mirror and Sector copy
- ❑ They all mean the same thing
- ❑ Three formats
  - ❑ Raw format, Proprietary formats and Advanced Forensics Format (AFF)



# Raw Format

---

- This is what the Linux dd command makes
- Bit-by-bit copy of the drive to a file
- Advantages
  - Fast data transfers
  - Can ignore minor data read errors on source drive
  - Most computer forensics tools can read raw format
- Disadvantages
  - Requires as much storage as original disk or data
  - Tools might not collect marginal (bad) sectors
    - Low threshold of retry reads on weak media spots
    - Commercial tools use more retries than free tools
  - Validation check must be stored in a separate file
    - Message Digest 5 ( MD5)
    - Secure Hash Algorithm ( SHA-1 or newer)
    - Cyclic Redundancy Check ( CRC-32)

# Proprietary Formats

---

- Features offered
  - Option to compress or not compress image files
  - Can split an image into smaller segmented files
    - Such as to CDs or DVDs
    - With data integrity checks in each segment
  - Can integrate metadata into the image file
    - Hash data
    - Date & time of acquisition
    - Investigator name, case name, comments, etc.
- Disadvantages
  - Inability to share an image between different tools
  - File size limitation for each segmented volume
    - Typical segmented file size is 650 MB or 2 GB
- Expert Witness format is the unofficial standard
  - Used by EnCase, FTK, X-Ways Forensics, and SMART
  - Can produce compressed or uncompressed files
  - File extensions **.E01**, **.E02**, **.E03**, ...

# Advanced Forensics Format

---

- ❑ Developed by Dr. Simson L. Garfinkel of Basis Technology Corporation
  - ❑ Design goals
    - ❑ Provide compressed or uncompressed image files
    - ❑ No size restriction for disk-to-image files
    - ❑ Provide space in the image file or segmented files for metadata
    - ❑ Simple design with extensibility
    - ❑ Open source for multiple platforms and OSs
    - ❑ Internal consistency checks for self-authentication
  - ❑ File extensions include **.afd** for segmented image files and **.afm** for AFF metadata
  - ❑ AFF is open source
-

# Determining the Best Acquisition Method

---

- ❑ Types of acquisitions
  - ❑ **Static acquisitions and live acquisitions**
- ❑ Four methods
  - ❑ Bit-stream disk-to-image file
  - ❑ Bit-stream disk-to-disk
  - ❑ Logical
  - ❑ Sparse

# Bit-stream disk-to-image file

---

- ❑ Most common method
- ❑ Can make more than one copy
- ❑ Copies are bit-for-bit replications of the original drive
- ❑ Tools: ProDiscover, EnCase, FTK, SMART, Sleuth Kit, X-Ways, iLook

# Bit-stream disk-to-disk

---

- ❑ Used when disk-to-image copy is not possible
  - ❑ Because of hardware or software errors or incompatibilities
  - ❑ This problem is more common when acquiring older drives
- ❑ Adjusts target disk's geometry (cylinder, head, and track configuration) to match the suspect's drive
- ❑ Tools: EnCase, SafeBack (MS-DOS), Snap Copy

# Logical and Sparse Acquisition

---

- ❑ When your time is limited, and evidence disk is large
- ❑ Logical acquisition captures only specific files of interest to the case
  - ❑ Such as Outlook **.pst** or **.ost** files
- ❑ Sparse acquisition collects only some of the data
  - ❑ I am finding contradictory claims about this—wait until we have a real example for clarity

# Compressing Disk Images

---

- Lossless compression might compress a disk image by 50% or more
- But files that are already compressed, like ZIP files, won't compress much more
  - Error in textbook: JPEGs use lossy compression and degrade image quality (p. 104)
- Use MD5 or SHA-1 hash to verify the image
- Tape Backup
  - When working with large drives, an alternative is using tape backup systems
  - No limit to size of data acquisition
    - Just use many tapes
  - But it's slow



# Returning Evidence Drives

---

- ❑ In civil litigation, a discovery order may require you to return the original disk after imaging it
- ❑ If you cannot retain the disk, make sure you make the correct type of copy (logical or bitstream)
  - ❑ Ask your client attorney or your supervisor what is required—you usually only have one chance

# Contingency Planning for Image Acquisitions

---

- Create a duplicate copy of your evidence image file
- Make at least two images of digital evidence
  - Use different tools or techniques
- Copy host protected area of a disk drive as well
  - Consider using a hardware acquisition tool that can access the drive at the BIOS level (link Ch 4c)
- Be prepared to deal with encrypted drives
  - Whole disk encryption** feature in Windows Vista Ultimate and Enterprise editions

# Encrypted Hard Drives

---

- Windows BitLocker
- TrueCrypt
- If the machine is on, a live acquisition will capture the decrypted hard drive
- Otherwise, you will need the key or passphrase
  - The suspect may provide it
  - There are some exotic attacks
    - Cold Boot (link Ch 4e)
    - Passware (Ch 4f)
    - Electron microscope (Ch 4g)

# Using Acquisition Tools

---

- ❑ Acquisition tools for Windows
  - ❑ Advantages
    - ❑ Make acquiring evidence from a suspect drive more convenient
      - ❑ Especially when used with hot-swappable devices
  - ❑ Disadvantages
    - ❑ Must protect acquired data with a well-tested write-blocking hardware device
    - ❑ Tools can't acquire data from a disk's host protected area
- ❑ Windows Write-Protection with USB Devices
  - ❑ USB write-protection feature
    - ❑ Blocks any writing to USB devices
  - ❑ Target drive needs to be connected to an internal PATA (IDE), SATA, or SCSI controller
  - ❑ Works in Windows XP SP2, Vista, and Win 7

# Acquiring Data with a Linux Boot CD

---

- ❑ Linux can read hard drives that are mounted as read-only
  - ❑ Windows OSs and newer Linux automatically mount and access a drive
  - ❑ Windows will write to the Recycle Bin, and sometimes to the NTFS Journal, just from booting up with a hard drive connected
  - ❑ Linux kernel 2.6 and later write metadata to the drive, such as mount point configurations for an ext2 or ext3 drive
  - ❑ All these changes corrupt the evidence
  - ❑ Forensic Linux Live CDs mount all drives read-only
    - ❑ Which eliminates the need for a write-blocker
  - ❑ Using Linux Live CD Distributions
    - ❑ Forensic Linux Live CDs
      - ❑ Contain additional utilities
-

# Acquiring Data with a Linux Boot CD

---

- ❑ Configured not to mount, or to mount as read-only, any connected storage media
- ❑ Well-designed Linux Live CDs for computer forensics
  - ❑ Helix
  - ❑ Penguin Sleuth
  - ❑ FCCU (French interface)
- ❑ Preparing a target drive for acquisition in Linux
  - ❑ Modern linux distributions can use Microsoft FAT and NTFS partitions
- ❑ Preparing a target drive for acquisition in Linux (continued)
  - ❑ **fdisk** command lists, creates, deletes, and verifies partitions in Linux
  - ❑ **mkfs.msdos** command formats a FAT file system from Linux
- ❑ Acquiring data with dd in Linux
  - ❑ dd (“data dump”) command
    - ❑ Can read and write from media device and data file
    - ❑ Creates raw format file that most computer forensics analysis tools can read

# Acquiring Data with a Linux Boot CD

---

- ❑ Shortcomings of dd command
  - ❑ Requires more advanced skills than average user
  - ❑ Does not compress data
- ❑ dd command combined with the split command
  - ❑ Segments output into separate volumes
- ❑ dd command is intended as a data management tool
  - ❑ Not designed for forensics acquisitions
- ❑ dcfldd additional functions
  - ❑ Specify hex patterns or text for clearing disk space
  - ❑ Log errors to an output file for analysis and review
  - ❑ Use several hashing options
  - ❑ Refer to a status display indicating the progress of the acquisition in bytes
  - ❑ Split data acquisitions into segmented volumes with numeric extensions
  - ❑ Verify acquired data with original disk or media data

# Capturing an Image with ProDiscover Basic

---

- Connecting the suspect's drive to your workstation
  - Document the chain of evidence for the drive
  - Remove the drive from the suspect's computer
  - Configure the suspect drive's jumpers as needed
  - Connect the suspect drive to a **write-blocker device**
  - Create a storage folder on the target drive
- Using ProDiscover's Proprietary Acquisition Format
  - Image file will be split into segments of 650MB
  - Creates image files with an .eve extension, a log file (.log extension), and a special inventory file (.pds extension)



# Capturing an Image with ProDiscover Basic

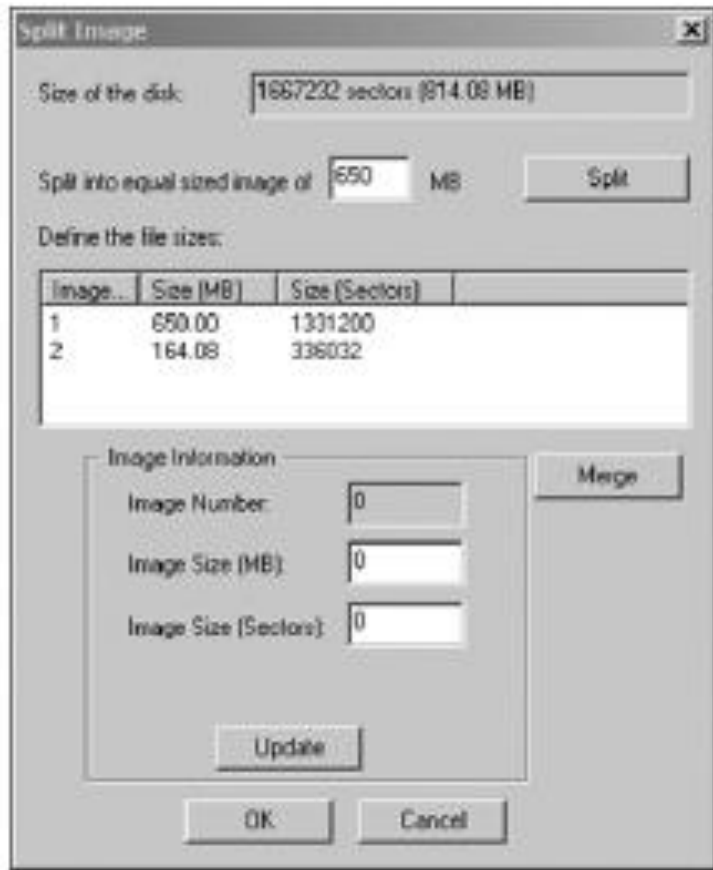


Figure 4-4 The Split Image dialog box

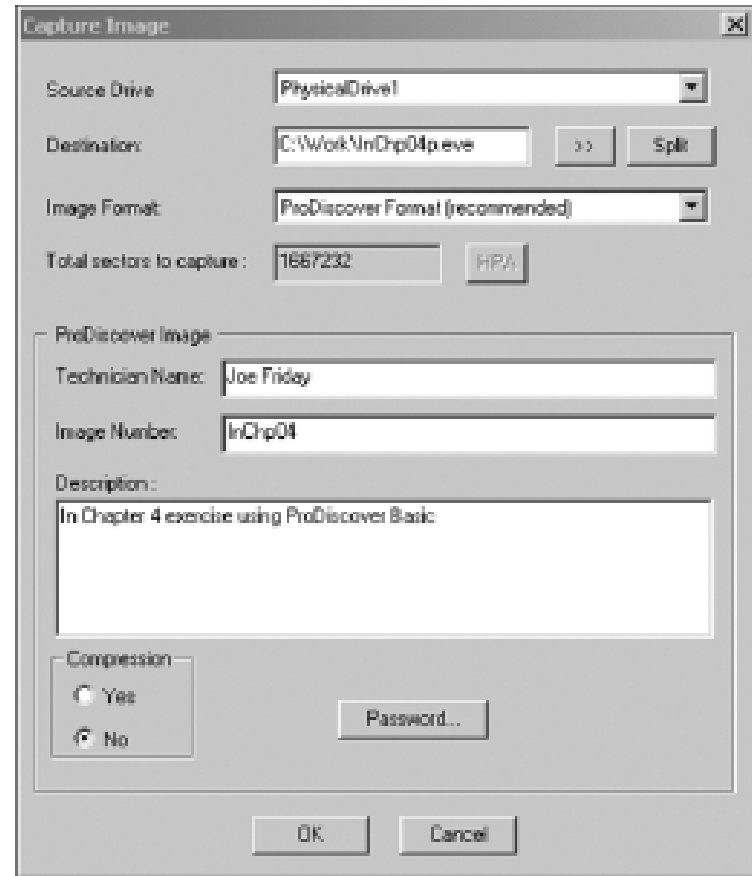


Figure 4-5 The Capture Image dialog box

## ❑ Using ProDiscover's Raw Acquisition Format

- ❑ Select the UNIX style dd format in the Image Format list box
- ❑ Raw acquisition saves only the image data and hash value

# Capturing an Image with AccessData FTK Imager

- Included on AccessData Forensic Toolkit
- View evidence disks and disk-to-image files
- Makes disk-to-image copies of evidence drives
  - At logical partition and physical drive level
  - Can segment the image file
- Evidence drive must have a **hardware write-blocking device**
  - Or the USB write-protection Registry feature enabled
- FTK Imager can't acquire drive's host protected area (but ProDiscover can)
- Steps
  - Boot to Windows
  - Connect evidence disk to a write-blocker
  - Connect target disk
  - Start FTK Imager
  - Create Disk Image
    - Use Physical Drive option

# Capturing an Image with AccessData FTK Imager

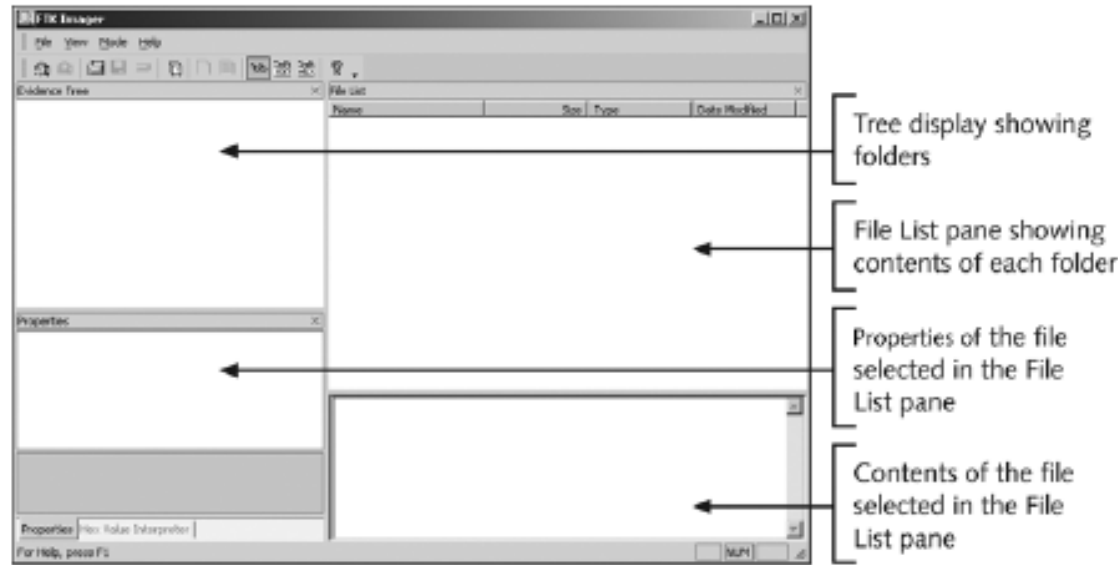


Figure 4-6 The FTK Imager main window

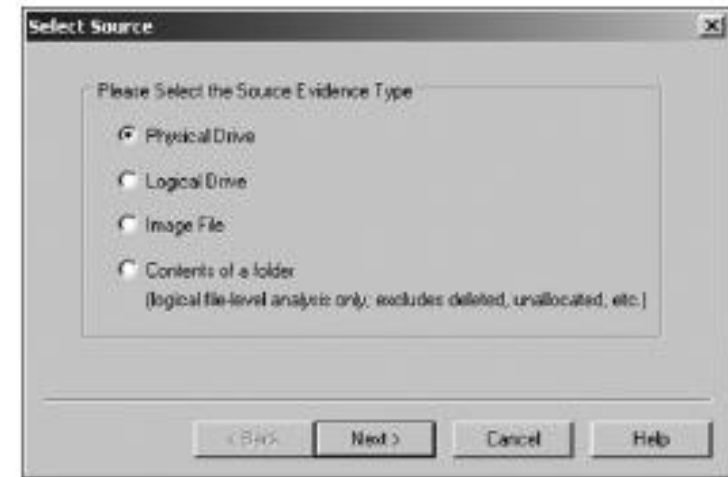


Figure 4-7 The Select Source dialog box

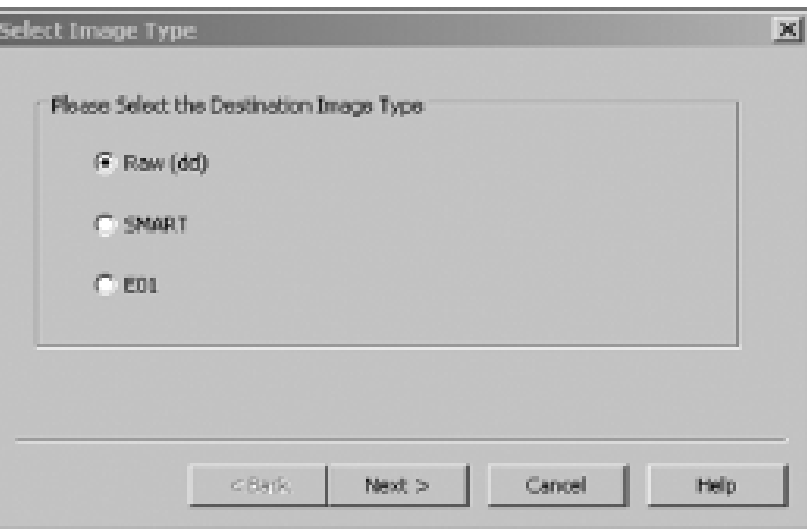


Figure 4-8 The Select Image Type dialog box

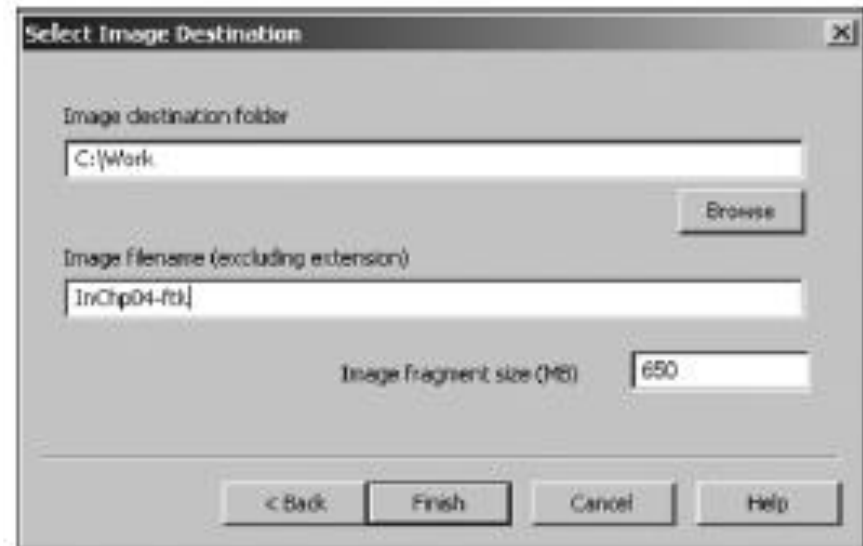


Figure 4-9 Selecting where to save the image file

# Capturing an Image with Access Data FTK Imager

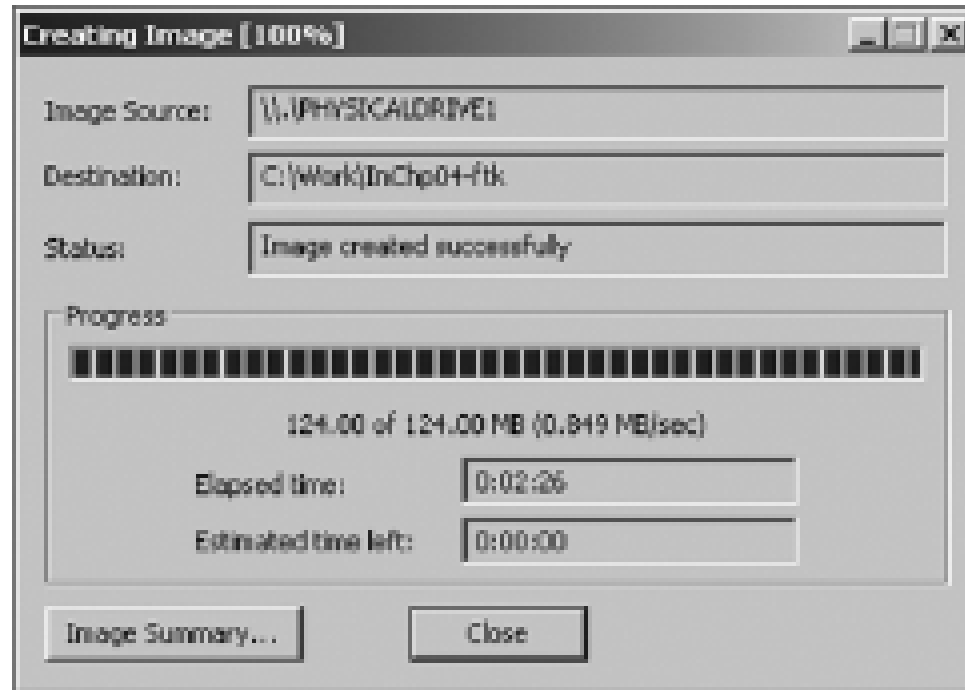


Figure 4-10 A completed image save

# Validating Data Acquisitions

---

- ❑ Most critical aspect of computer forensics
- ❑ Requires using a hashing algorithm utility
- ❑ Validation techniques
  - ❑ CRC-32, MD5, and SHA-1 to SHA-512
- ❑ MD5 has collisions, so it is not perfect, but it's still widely used
- ❑ SHA-1 has some collisions but it's better than MD5
- ❑ A new hashing function will soon be chosen by NIST
- ❑ Windows Validation Methods
  - ❑ Windows has no built-in hashing algorithm tools for computer forensics
    - ❑ Third-party utilities can be used
  - ❑ Commercial computer forensics programs also have built-in validation features
    - ❑ Each program has its own validation technique
- ❑ Raw format image files don't contain metadata
  - ❑ Separate manual validation is recommended for all raw acquisitions

# Linux Validation Methods

---

## ❑ Validating dd acquired data

- ❑ You can use md5sum or sha1sum utilities

- ❑ md5sum or sha1sum utilities should be run on all suspect disks and volumes or segmented volumes

## ❑ Validating dcfldd acquired data

- ❑ Use the hash option to designate a hashing algorithm of md5, sha1, sha256, sha384, or sha512

- ❑ hashlog option outputs hash results to a text file that can be stored with the image files

- ❑ vf (verify file) option compares the image file to the original medium

---

# Performing RAID Data Acquisitions

- ❑ Size is the biggest concern: Many RAID systems now have terabytes of data
- ❑ **Redundant array of independent** (formerly “inexpensive”) **disks**
  - ❑ Computer configuration involving two or more disks
  - ❑ Originally developed as a data-redundancy measure
- ❑ RAID 0 (Striped)
  - ❑ Provides rapid access and increased storage
  - ❑ Lack of redundancy
- ❑ RAID 1 (Mirrored)
  - ❑ Designed for data recovery
  - ❑ More expensive than RAID 0
- ❑ RAID 2
  - ❑ Similar to RAID 1 and Slower than RAID 0
  - ❑ Data is written to a disk on a bit level
  - ❑ Has better data integrity checking than RAID 0
- ❑ RAID 3: Uses data striping and dedicated parity
- ❑ RAID 4: Data is written in blocks

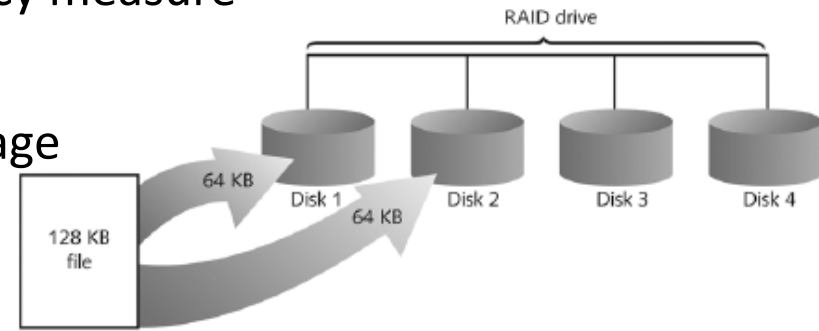


Figure 4-11 RAID 0: Striping

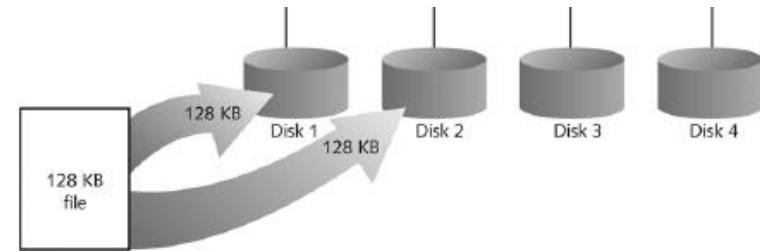


Figure 4-12 RAID 1: Mirroring

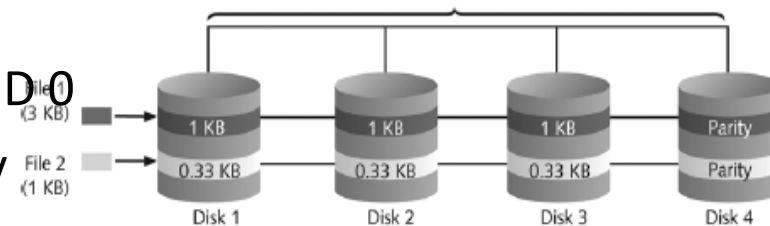


Figure 4-13 RAID 2: Striping (bit level)

# Understanding RAID

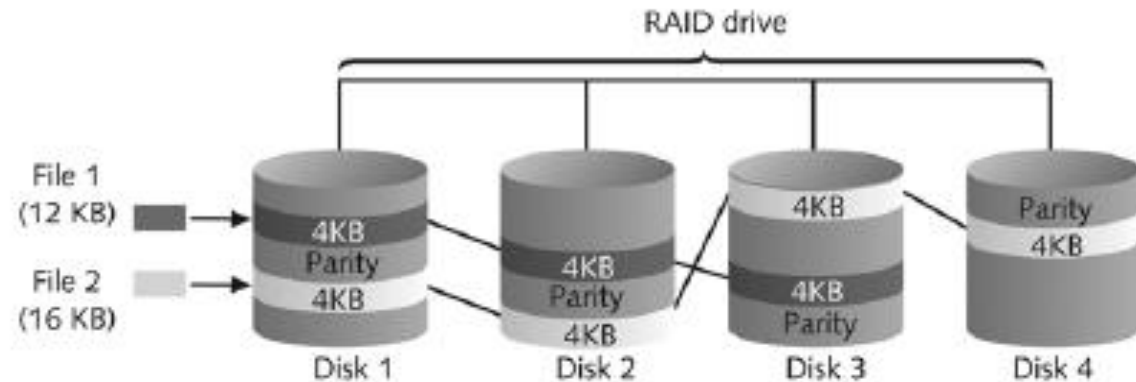


Figure 4-14 RAID 5: Block-level striping with distributed parity

## RAID 5

- Similar to RAID 0 and 3

- Places parity recovery data on each disk

## RAID 6

- Redundant parity on each disk

## RAID 10, or mirrored striping

- Also known as RAID 1+0

- Combination of RAID 1 and RAID 0



# Acquiring RAID Disks

---

- Concerns
  - How much data storage is needed?
  - What type of RAID is used?
  - Do you have the right acquisition tool?
  - Can the tool read a forensically copied RAID image?
  - Can the tool read split data saves of each RAID disk?
- Older hardware-firmware RAID systems can be a challenge when you're making an image
- Vendors offering RAID acquisition functions
  - Technologies Pathways ProDiscover
  - Guidance Software EnCase
  - X-Ways Forensics
  - Runtime Software
  - R-Tools Technologies
- Occasionally, a RAID system is too large for a static acquisition
  - Retrieve only the data relevant to the investigation with the sparse or logical acquisition method

# Using Remote Network Acquisition Tools

---

- ❑ You can remotely connect to a suspect computer via a network connection and copy data from it
  - ❑ Remote acquisition tools vary in configurations and capabilities
  - ❑ Drawbacks
    - ❑ LAN's data transfer speeds and routing table conflicts could cause problems
    - ❑ Gaining the permissions needed to access more secure subnets
    - ❑ Heavy traffic could cause delays and errors
    - ❑ Remote access tool could be blocked by antivirus
-

# Remote Acquisition with ProDiscover Investigator

---

- Preview a suspect's drive remotely while it's in use
- Perform a live acquisition
  - Also called a "smear" because data is being altered
- Encrypt the connection
- Copy the suspect computer's RAM
- Use the optional stealth mode to hide the connection

# Remote Acquisition with ProDiscover Incident Response

---

- ❑ All the functions of ProDiscover Investigator plus
  - ❑ Capture volatile system state information
  - ❑ Analyze current running processes
  - ❑ Locate unseen files and processes
  - ❑ Remotely view and listen to IP ports
  - ❑ Run hash comparisons to find Trojans and rootkits
  - ❑ Create a hash inventory of all files remotely

# PDServer Remote Agent

---

- ❑ ProDiscover utility for remote access
- ❑ Needs to be loaded on the suspect computer
- ❑ PDServer installation modes
  - ❑ Trusted CD
  - ❑ Preinstallation
  - ❑ Pushing out and running remotely
- ❑ PDServer can run in a stealth mode
  - ❑ Can change process name to appear as OS function

# Remote Connection Security Features

---

- Password Protection
- Encrypted communications
- Secure Communication Protocol
- Write Protected Trusted Binaries
- Digital Signatures

# Remote Acquisition with EnCase Enterprise

---

- Remotely acquires media and RAM data
- Integration with intrusion detection system (IDS) tools
- Options to create an image of data from one or more systems
- Preview of systems
- A wide range of file system formats
- RAID support for both hardware and software
- Other Remote Acquisition Tools**
  - R-Tools R-Studio
  - WetStone LiveWire
  - F-Response

# Remote Acquisition with Runtime Software

---

- Compact Shareware Utilities
  - DiskExplorer for FAT
  - DiskExplorer for NTFS
  - HDHOST (Remote access program)
- Features for acquisition
  - Create a raw format image file
  - Segment the raw format or compressed image
  - Access network computers' drives



# Using Other Forensics-Acquisition Tools

---

## Tools

- SnapBack DatArrest

- SafeBack

- DIBS USA RAID

- ILook Investigator IXimager

- Vogon International SDi32

- ASRData SMART

- Australian Department of Defence PyFlag

---

## ❑ SnapBack DatArrest

- ❑ Columbia Data Products
- ❑ Old MS-DOS tool
- ❑ Can make an image on three ways: Disk to SCSI drive, Disk to network drive & Disk to disk
- ❑ Fits on a forensic boot floppy
- ❑ Snap Copy adjusts disk geometry

## ❑ NTI SafeBack

- ❑ Reliable MS-DOS tool
- ❑ Small enough to fit on a forensic boot floppy
- ❑ Performs an SHA-256 calculation per sector copied
- ❑ Creates a log file
- ❑ Functions
  - ❑ Disk-to-image copy (image can be on tape)
  - ❑ Disk-to-disk copy (adjusts target geometry)
    - ❑ Parallel port laplink can be used
  - ❑ Copies a partition to an image file
  - ❑ Compresses image files

## DIBS USA RAID(Rapid Action Imaging Device)

- Makes forensically sound disk copies
- Portable computer system designed to make disk-to-disk images
- Copied disk can then be attached to a write-blocker device

## ILook Investigator IXimager (Iximager)

- Runs from a bootable floppy or CD
- Designed to work only with ILook Investigator
- Can acquire single drives and RAID drives

## ASRData SMART

- Linux forensics analysis tool that can make image files of a suspect drive
- Capabilities
  - Robust data reading of bad sectors on drives
  - Mounting suspect drives in write-protected mode
  - Mounting target drives in read/write mode
  - Optional compression schemes

## PyFlag tool

- Intended as a network forensics analysis tool
- Can create proprietary format Expert Witness image files
- Uses sgzip and gzip in Linux