Date :
Page No.

Understanding the digital forensics profession & Invest

Digital forensics / Computer forensics

Definition : ① The application of computer science & investigative procedures for a legal purpose involving the analysis of digital evidence after ① proper search authority,
② Chain of custody
③ validation with mathematics (Hash functions)
④ use of validated tools
⑤ repeatability
⑥ reporting
⑦ and possible expert presentation.

DF is the process of collecting, preserving, analyzing & presenting digital evidence in a legally acceptable manner. (integrity, to maintain chain of custody.)

↳ applies to
① Criminal investigations
② Civil investigations
③ Administrative investigations

② Given by Ken Zatyko
↓ director of defense computer forensics laboratory.

③ Also encompasses research & incident response.

→ Digital Evidence: Information of probative value (tendency to prove or disprove) that is stored or transmitted in binary form.

→ International Organization for standardization (ISO) standard for DF was ratified (made valid) in October 2012.

Key standard: ISO 27037 → Information technology – Security techniques – Guidelines for identification, collection, acquisition & preservation of digital Evidence.

defines personnels & methods for acquiring & preserving digital evidence.

Date:
Page No.

Objectives of digital forensics:
① Identify digital evidence
② Preserve integrity of data
③ Recover hidden/deleted information
④ Maintain chain of custody
⑤ Present findings in court
⑥ follow court approved methods to preserve & recover evidence.

Characteristics of digital evidence:
① Fragile & easily altered : volatile
② Can be duplicated exactly (bit by bit) using bit stream Copy.
③ Requires validation via hash value (MD5, SHA-1 etc)
④ May reside in multiple devices (Cloud, mobile, servers)
⑤ Must maintain proper chain of custody.

History

1960s → first computer crime cases
↓
FBI CART formed ← computer analysis & response team, 1984 to handle cases w/ computer/digital evidence
↓
2000s: Rise of cybercrime, digital evidence laws.

* federal rules of evidence (FRE) → to ensure consistency in federal proceedings

Digital Evidence:
→ Information of probative value that is stored or transmitted in digital form & can be used in court of law
→ Can reside on → ① computer hard disk drive ③ cloud storage
② solid state drive (SSDs) ⑥ USB, CDs, DVDs
③ Mobile devices
④ Servers.
→ Includes both Active & latent data.

Date:
Page No.

Requirement
Investigating digital devices/evidence. Points to consider:
→ ① Collecting data securely
② Examining suspect data to determine details such as origin and content ③ presenting digital information to courts, and ④ applying laws to digital device practices.

# Digital forensics	Data recovery (Scenario: jug wants data back.)
① Used to investigate data that can be retrieved from a computer's hard drive or other storage media.	① Involves retrieving info that was deleted by mistake or lost during a power surge or server crash.
② DF is the task of recovering data that users have hidden or deleted, with the goal of ensuring that recovered data is valid.	② Here, you know what you're looking for. You are aware of a specific deleted file
③ Used as evidence: follows legal procedures to ensure admissibility	③ Not necessarily used as Evidence.
④ Need to investigate the point	④ You know a particular point to recover.
⑤ Requires detailed documentation	⑤ Documentation is not usually a priority

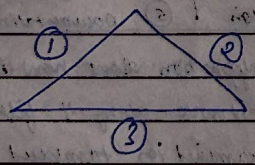
→ Network forensics: → Information about how attackers gain access to a network along w/ files they might have copied, examined or tampered with.
→ Examines use log files to determine when user logged on, URLs user accessed, how they logged onto network & from what location

When digital devices are retrieved, their contents are examined. It can be

Evidence
- Inculpatory Evidence → Incriminating
- Exculpatory Evidence → Clears the suspect of charges.

* Examiners often don't know if digital devices contain evidence.
  - → search storage media & piece together any data they find.
  - → Forensics software tools are used.
  - → In extreme cases, electron microscopes & other expensive equipments are used to recover info that has been purposefully destroyed or reformatted.

Forensics investigators
- → they work as a team known as the investigation triads.
- → Investigation Triads made up of funcions:
  1. vulnerability / threat assessment & risk management
  2. Network intrusion detection & incident response
  3. Digital Investigations.



→ Each side of triad represents a group or department responsible for performing the associated tasks.

→ Each function operates independently but all 3 groups draw from one another.

Bigger organization: 3 groups → all aspect of digital investigation covered
Smaller companies: one group might perform all 3 tasks or might contract w/ service providers.

1. vulnerability / threat assessment & risk management.
   - ① Test + verify the integrity of standalone workstation & network servers.
   - ② This covers ① physical security of systems
     ② Security of OS
     ③ Security of Applications.
   - ③ People working here are called penetration Testers
   - ④ Pentesters conduct authorized attacks on network → to assess vulnerabilities of OS & applications used in network.
   - ⑤ Pen testers poke holes in n/w to help organization be prepared for a real attack.

2. Network Intrusion detection & Incident response.
   - ① detects an intruder attack by using automated tools & monitoring network firewall logs.
   - ② When external attack detected, response team
     ① traces ② identifies the intrusion method
     ② locates ④ denies further access to n/w
   - ③ If intruder launches an attack → caused damage then this team collects necessary evidence for civil & criminal litigation.

④ If internal user is engaged in illegal acts or policy violations, the network intrusion detection team assists in locating the user

↓

Eg: if college student → sends virus via email

↳ team traces that email comes from an internal node.

③ Digital Investigations

↳ ① Manages investigations + conducts forensics analysis of systems suspected of containing evidence related to crime.

② May retrieve resources from other two teams for complex cases.

③ This group typically, resolves/terminates case investigations.

Challenges faced by digital forensics.

① Rapid technological advancement : new OS, cloud computing environments, Mobile devices, IoT etc.

∴ forensic investigators must upgrade tools & trainings to keep up.

② Modern systems generate large amount of data (100 log files, network traffic etc.)

∴ volume of digital evidence increases analysis time & complexity.

③ Cloud & remote storage → data may be stored in multiple diff. locations making it hard to accumulate.

History of digital forensics.

① In 1970s → electronic crimes increasing (especially in financial sector)

↳ mainframe era crimes

Eg: Equity Funding Corp. of America crime.

↓

② Federal Law Enforcement Training Center (FLETC) program to train law enforcement in handling digital data.

↓

③ By early 1990s, International Association of Computer Investigative Specialists (IACIS)

↓

Introduced training on s/w for DF examination

↓

④ IRS created search warrant programs.

↓

⑤ ASR Data created expert witness for Macintosh → 1st commercial SW s/w for DF

↳ could recover deleted files

↳ later developed EnCase.

↓

⑥ ILOOK → maintained by IRS criminal Investigation Division

↳ can analyze & read special files that are copies of a disk.

↓ Access

⑦ Data Forensic Toolkit (DFTK)

4th amendment: Protects against unreasonable search & seizure.
Critical in Public sector investigations

Date:
Page No.

Understanding Case Law.

↳ ① Existing laws & statutes can't keep up w/ rate of technological change. (law falls behind technology)

② ∴ when statutes don't exist
↳ Case law is used.

③ Case law allows legal counsel to apply previous similar cases to current ones in an effort to address ambiguity in laws.

④ Examiners must be familiar w/ recent court rulings on search & seizure in the electronic environment.
↳ to avoid mistakes like exceeding a search warrant's authority.

⑤ Law enforcement can confiscate anything on the arrested person but they don't have the right to search the device.

⑥ Digital Evidence must Comply w/ laws/rules of Evidence, Rules of criminal procedure & search & seizure laws.

Developing Digital forensics resources.

① To be a successful digital forensics investigator, be familiar w/ computing platforms.

② To supplement knowledge, develop contact w/ digital, network & investigative professionals.

③ Join computer user groups in both public & private sectors.
Eg: Computer Technology Investigators Network (CTIN)
↳ discuss problems that digital forensics examiners encounter.
Eg: Infragard.

Date:
Page No.

④ Consult outside experts + local groups.
⑤ Conduct professionally.

Preparing for Digital Investigations

Public Sector Investigations	Private Sector Investigations
① Involves government agencies responsible for criminal investigations & prosecution.	① Involves Private Organizations. Mainly focuses on company policy violations & litigation disputes.
② focus on the legal guidelines of the government agency's jurisdiction.	② focus more on policy violation. Eg: violation of HIPAA regulations
③ To conduct them, you must understand laws on computer related crimes, including: standard legal process, guidelines on search & seizure & how to build a criminal case.	③ May start as civil case, but later develop into criminal case. Eg: Corporate Espionage.

Computers + networks —Analogous to→ to explore as a burglar uses.
to commit crime.

Eg: Govt has expanded definition of laws Eg: theft to include taking data from a computer w/o owner's permission

Computer fraud & Abuse Act → 1986.

Following legal processes:

① Broadly a criminal case follows 3 stages:
   ① complaint
   ② the investigation
   ③ the prosecution.

② When conducting a computer investigation, legal processes must follow ① local customs
   ② legislative standards
   ③ rules of evidence

③ someone files a complaint → specialist investigates the complaint
→ with the help of prosecution, collects evidence & builds a case.
→ if evidence sufficient, case proceeds to trial.

Ⓘ Criminal investigation begins when someone finds evidence of or witnesses an illegal act.
↳ Witness or victim makes an allegation to the police
↳ an accusation of fact that a crime has been committed

Ⓘ Police officer interviews the complainant & writes a report about the crime.
↳ report is processed.
↳ Management decides to start an investigation or log the information in a police blotter
↳ Blotter is a historical database of previous crimes.

This done :: criminals often repeat actions in their illegal activities & police blotter helps find a pattern by analyzing the previously committed crimes.

→ not every police officer is a computer expert
∴ 2 categories defined by ISO standard 2-7037, differentiating the training & experience officers have.

① Digital evidence first responder (DEFR)
↳ has skill + training to assist on an incident scene.
↳ can assess the situation
↳ takes precaution to acquire & preserve evidence.

② Digital Evidence Specialist (DES).
↳ has the skills to analyze the data and determine when another specialist should be called in to assist w/ the analysis.

Examiner's responsibility

Ⓘ If you're an examiner:
① Recognize the level of expertise of police officers & others in the case.
② You should have DES training to conduct examination of systems & manage digital forensics aspect of case
③ Assess the scope of the case: ① includes device's OS, hardware & peripheral devices.
④ Determine resources available to process evidence
⑤ Determine if you have right tools to collect & analyze evidence & if you need to call other specialist to assist in collecting and processing evidence.

Date:
Page No.

⑥ After collecting resources, your role is to delegate, collect & process the info" related to the complaint.

III After examine builds the case, information is turned over to the prosecutor.

IV → As an investigator, you must then present the collected evidence with a report to government's attorney.

→ Affidavit: ① Also called declaration
② a sworn statement of support of facts about or evidence of a crime
↳ submitted to a judge with request for a search warrant before seizing evidence.

③ Responsibility to write → investigator

④ Must include exhibits that support allegations to justify the warrant.

⑤ Have the affidavit notarized under sworn oath to verify info" in affidavit is true.

⑥ After a Judge approves & signs the search warrant, a DEFR can collect evidence as defined by the warrant.

⑦ After collection of evidence, you process & analyze it to determine whether a crime actually occured.

⑧ Evidence can be presented on court in a hearing.

⑨ After this Judge renders a judgement or Jury gives a verdict after

Date:
Page No.

computer crimes

↳ Any criminal activity in which a computer or network is used as: ① target of the crime
② Tool used to commit the crime.
③ or incidental to the crime.

↳ These devices can contain information that helps law enforcement officers determine the chain of events leading to a crime.

classification of computer crimes

① Computer as the target
↳ computer is attacked or traumatized
Example: ① Intrusion ② DOS ③ Malware attack
④ Ransomware ⑤ Data breaches etc.

→ Hackers exploit the vulnerability in the computer & gain access to it via some kind of backdoor which could be created with the use of programs like malware, worm etc.

② Computer as the tool
↳ computer is used to commit crimes.
Example: ① Identity theft ② Credit card fraud
③ Phishing ④ Online scams etc.

→ Fraudsters make use of techniques called social engineering to trick people into revealing confidential information, granting access, or performing actions to compromise security

(3) Computer stores evidence related to other crimes
↳ Incidental to Crime.

Eg: ① Drug trafficking records ② financial transaction records
③ Terrorism planning document etc.

→ This could be found by analysing log files, email artifacts, browser history or unallocated of the computer.

Common Types of High Tech Crimes

① Intellectual property theft
② Industrial espionage
③ Insider threats
④ Corporate data theft
⑤ Cyberterrorism
⑥ Child exploitation
⑦ Financial fraud.

Public Sector Investigations

① Requires search warrant, probable cause & compliance with criminal procedure & federal rules of evidence.

② Involves criminal laws violations like fraud, cyberattacks, identity theft

③ Protection: Fourth amendment protection against unreasonable search & seizure.

④ Proof: Must prove guilty to avoid any reasonable doubt in criminal court

⑤ Evidence handling: strict maintenance of chain of custody, evidence integrity & admissibility standards

⑥ May lead to arrest, prosecution, imprisonment.

Private Sector Investigations.

① Based on company policies, Acceptable use policy (AUP), & employment agreements.

② Involves policy violations, email abuse, internet misuse, & insider threats.

③ Constitutional protections generally don't apply here if systems are company-owned & policies are defined.

④ Decision based on amount of evidence or internal disciplinary standards.

⑤ Documentation & integrity maintained by governed by organizational procedures.

⑥ May lead to employment termination, disciplinary action, civil litigation.

Private Sector Investigations.

→ Involves Private companies & lawyers

→ Crime: Company policy violation & litigation disputes

① Wrongful Termination
② White collar crimes
③ email harassment
④ gender & age discrimination
⑤ Embezzlement
⑥ Sabotage
⑦ falsification of data
⑧ Industrial Espionage.
→ selling sensitive info & corporate secrets to competitors

→ Business must continue w/o disruption ∴
→ focus on stopping the violations & minimizing the damage or loss to a company
→ then confront the suspect.

Ways to avoid litigation (tips for an organization)

① Establishing Company Policies
① → Publish & maintain policies that employees find easy to read & follow.
② → Acceptable use policy: most imp policies which define rules for using the company's computers or network.
→ Signed by all employees.

③ Line of Authority: states who has the legal right to initiate an investigation, who can take possession of evidence & who has access to evidence.

④ well defined policies ⇒ ① Authority to conduct an investigation
② Org. intends to be fair minded & will follow due process

⑤ No well defined policy ⇒ ① litigation/ cons from current/ former employees.

② Display warning Banners on the Screens.
→ ① Warning Banner → ① appears when a computer starts & connects with company network or VPN

You are about to access NSU computer system that is for intended use only. You have no expectation of privacy in use of this s/w. use of this network constitutes consent to monitoring. Retrieval use OK for any purpose including criminal prosecution

② informs end users that org. reserves the right to inspect computer & network traffic at this will.

③ Log on.

② If right isn't stated explicitly, people might assume right to privacy while using company network.

③ strong worded & well worded banner → no need for company to request a search warrant or court order for its equipment.

④ Sample text for warning Banner:
① → Access to this system & network is restricted.
② → use of this system & network is for official Business only.
③ → System & network are subject to monitoring at any time by the owner.

Date :
Page No.

④ Using this system implies consent to monitoring by the owners
⑤ Users of this system agree that they have no expectation of privacy relating to all activities performed on this system.

→ Text displayed when user attempts to log on can include:

① This system is property of company X
② This system is authorized for use only!! Any unauthorized access is a violation of law & will lead to prosecution.
③ All activity, software, N/W traffic, comms can subject to monitoring.

* W/o a banner, your DF authority to inspect conflicts with user's expectation of privacy.

③ Designating an Authorized Requester

① Business are advised to specify an authorized authority (Authorized requester) who has the power to initiate investigations.

② Must also define & limit who's authorized to request a computer investigation & forensics analyst. (i.e. of internet comfort)

③* Examples of groups w/ authority to request computer forensics investigation

① Corporate security investigations
② Corporate ethics office
③ Internal auditing
④ Corporate equal employment opportunity office
⑤ The general counsel or legal department.

Date :
Page No.

→ All groups to request via Corporate security investigations group.

→ This policy separates investigative process from process of employee discipline.

Conducting security investigations

① → almost same as public sector
② → During private investigations, you search for evidence to support allegations of violation of company's rules or an attack on its assets.
→ During ~~Private~~ Public investigations, you search for evidence to support criminal allegations.

③ Three types of common situations in private sector environments:
① Abuse or misuse of digital assets
② E-mail abuse
③ Internet abuse.

Misuse of digital assets → Company rules violation

④ Types: ① Digital abuse → using company software for Personal profit.
② E-mail abuse → ① Excessive use of company's email system for personal use & making threats or harassing others via email.
② This can lead to hostile work environment.

③ Internet abuse: ① Spending all day web surfing, watching pornography on internet at work.
Eg: viewing illegal (contraband) pornographic images, such as child pornography

Role of Digital forensics examiner in Authority / Investigations
↳ give management proper complete & accurate information so that they can verify & correct/solve problem in an organization.
↳ minimize risk to company

When you give case to law enforcement, you begin working as an agent of law enforcement too.

→ As your further progress, civil case might turn to criminal case so maintain security & accountability.

Distinguishing Personal & Company Property

↳ Difficult ∵ cellphone, smartphone, tablets are here.
↳ Eg: an employee brings his personal tablet to work & connects it company's wireless network.
↳ as employee synchronizes the information on the tablet with info on company n/w, some data gets copied to the tablet.
↳ Does the info on tablet, belong to company or employee?

Big Challenge in digital investigations / Complaints w/ Regulations etc.

→ In today's BYOD (Bring your own device) environment, some companies simply state
• if you connect a personal device to the business network, it falls under same rule as company property.

Maintaining Professional Conduct
↳ includes ethics, morals, & standards of behaviour

An investigator must:

① Maintain objectivity
↳ ① form opinion based on your training experience & evidence in the case
② Avoid reaching to conclusions about your finding till you've exhausted all reasonable leads.

② Find relevant digital evidence
↳ avoid prejudice or bias to maintain integrity of your fact-finding in investigation

③ Maintain confidentiality
↳ ① Discuss case only with people who need to know about it. Eg: other investigators involved in this case.
② In case you need advice, discuss only general terms & facts about the case w/o mentioning specifics.
③ Only release reports if requested by the attorney or the court.
④ V. imp in Private sector environment.
Eg: termination contract of an employee.

Attorney- Attorney - work - product rule applies to all communication
↳ you can only discuss the case with attorney or other members of the team working with the attorney

(4) Continue your training (expand resources)
↳ ① stay current with latest technical changes in computer hardware & s/w, networking & forensic tools.

② gain certification + membership in professional organization

(5) Conduct yourself w/ integrity

→ Any indiscreet action can embarass you & give opposing attorneys opportunities to discredit you during your testimony in court.

Preparing a digital forensics investigation.

↳ Role as digital forensics professional : → gather data from suspect's computer

→ determine evidence whether that a crime was committed or company policies were violated.

① If evidence says → crime/policy violation committed
then prepare a case

Case : collection of evidence you can offer in court or at a private sector inquiry.

① gather evidence → prepare a case → preserve evidence

② Investigate suspect's computer
then preserve the evidence on a different computer.

③ Follow an accepted method to prepare case

④ Evaluate Evidence thoroughly

⑤ Document the chain of custody,
↳ the route evidence takes from the time you find it until the case is closed or goes to court.

CASE STUDIES

(I) Computer crime

→ Police raided a suspected drug dealer's home

→ found desktop computer, USB/flash drive, tablet computer & a cellphone

follow proper procedures ↓ necessary to avoid any damage investigation

→ computer was bagged & tagged along w/ storage media & labeled as part of search & seizure

→ find evidence: files containing names, contacts of drug dealer, text messages, photos etc.

* Computer helped:
① determine chain of events leading to crime
② evidence that can lead to conviction

(II) Company Policy Violation

→ Misuse of Company resources:
① surfing web ② sending personal e-mail
③ using computers for personal tasks.

→ This lead to company policy violation.

→ George is not fired on now
↳ didn't inform anyone
↳ confiscate his hard drive to find its whereabouts & job performance concerns.

(I)

Systematic & Standard approach to preparing a case.

① Make an initial assessment about the type of case you're investigating.
   → ① Talk to others involved in case & ask questions about the incident
   ② • Have law enforcement or security officers already seized the computer?
   • Do you need to visit any particular location?
   • Was computer used to commit a crime?
   • Does it contain evidence about another crime?

② Determine a preliminary design or approach to the case
   → ① outline general steps you need to follow to investigate the case.
   ② If suspect → ① employee → when you can seize their system? work hours or evening?
   ② criminal case → determine what info law enforcement officers have already gathered.

③ Create a detailed checklist.
   → refine the general outline by creating a detailed list of steps & estimated time for each of them.
   → helps you stay on track

④ Determine the resources you need
   → Based on OS, which software to use for investigation

⑤ obtain & copy an evidence drive
   → Make forensic copy of the disk

⑥ Identify the risks.
   → Standard risk assessment: list of problems you normally expect in the type of case you're handling.
   Risks may include: if the suspect knew about computers, he/she might have set up a logon screen that shuts down the computer or overwrites data on hard disk when someone tries to change the password.

⑦ Mitigate & minimize the risks.
   → identify how to minimize the risks
   → Eg: if working on password protected hard drive, make multiple copies of it. If you destroy a copy during retrieval process, you still have a copy left.

⑧ Test the Design
   → Review decisions & steps you've completed.
   → Eg: compare hash value of copy & original media to ensure you've copied correctly

⑨ Analyze & recover the digital evidence
   → Using software tools, examine the disk to find digital evidence

⑩ Investigate the data you recover
   → View the information recovered from the disk, including existing files, deleted files, e-mail & web history & organize the files to find patterns/info.

⑪ Complete the case report
   → Write a complete report detailing what you did & what you found.

⑫ Critique the case.
   → self evaluation & peer review
   → To identify successful actions & actions & determine how you could have improved.

* Always have contigency (alternate) plan for investigation
   Eg: alternate s/w, h/w tools.

→ A systematic approach helps you discover the information you need for your case & you should gather as much information as possible.

Date:
Page No.

(III) Requirements of the case.

Assessing the Case.

Systematically outline the case details.

① Situation (Eg: employee, boss of company)
② Nature of Case (Eg: side business on company computers)
③ Specifics of the case (Eg: side business - no time for company tasks - company policy - all digital assets owned by company can be inspected)
④ Type of Evidence (Eg: small capacity USB)
⑤ Known disk format (Eg: NTFS)
⑥ Location of Evidence (Eg: one USB drive recovered from assigned computer)

→ Based on these, you can determine case requirements

Eg: Task: To gather data from storage media to confirm or deny the allegations of side business on company time & computers.

Planning your investigation

→ Includes identifying the specific steps to gather the evidence, ② establish chain of custody & ③ perform forensic analysis.

→ Includes what you should do & when.

Steps:

① Acquire the evidence
② Complete an evidence form & establish a chain of custody
③ Transport the evidence to a computer forensic lab
④ Place the evidence in an approved secure container
⑤ Prepare your forensic workstation
⑥ Retrieve your evidence from the secure container
⑦ Make a forensic copy of the evidence

Date:
Page No.

⑧ Return the evidence to the secure container
⑨ Process the copies evidence with computer forensics tools.

This approved secure container → should be locked, fireproof locker or cabinet that has limited access.

↳ it is used to preserve the evidence from tampering & contamination.

Documenting the Evidence (step 2)

↳ ① To record details about the media, includes who recovered the evidence & when, who possessed it → when.

② An Evidence custody form: helps you document what has been done with the original evidence and its forensic copies

Chain of evidence form

→ It should be easy to read & use.
→ can contain information for one or more evidence.
→ Types: ① Single Evidence form: lists each piece of evidence on a separate page.
② Multi evidence form: same page, multiple evidence.
→ Include clear instructions on how to use your evidence custody form
↳ so that everyone uses same definitions for collected items

Date:
Page No.

Evidence Custody form contains:

① Case number: no. your org. assigns when an investigation is initiated.

② Investigating organization: The name of your organization

③ Investigator: name of lead investigator assigned to the case.

④ Nature of case: A short description of the case
Eg: "data recovery for corporate litigation" or "employee policy violation case"

⑤ Location evidence was obtained
↳ exact location of collection of evidence
↳ In case of multiple evidence forms, a new form for each location.

⑥ Description of evidence: • A list of evidence items.
• on multi evidence form, write a description for each item of evidence you acquire & include photos.

⑦ Vendor name: → Name of manufacturer of the computer component.
→ diff manufacturers, diff data recovery mechanisms

⑧ Model number / serial number → List of model number of computer components. Eg Hard drives, memory chips → model no but no serial number

⑨ Evidence recovered by → Name of investigator who recovered the evidence
↳ Chain of custody for evidence starts with this information.
→ This person is responsible for preserving, transporting & securing the evidence

Date:
Page No.

* To account for what was done to the evidence & what was found.
→ notes

⑩ Date & Time: When evidence was taken into custody. (ASC)
↳ when chain of custody starts

⑪ Evidence placed in location: Specific where approved secure container is used to store evidence & when the evidence was placed in the container

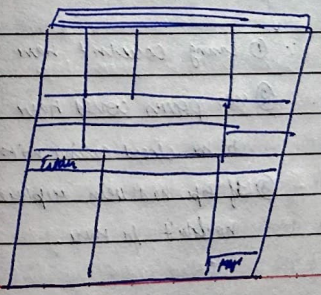
⑫ Item # / Evidence Processed by / Disposition of evidence / Date / Time
↳ When another authorized investigator retrieves evidence from the evidence locker for processing & analysis.
↳ describe what was done to the evidence.

⑬ Page: forms used to catalog all evidence for each location should have page numbers.
↳ To indicate the total number of pages for this group of evidence.

Eg: if you collected 15 pieces of evidence at one location & your form has only 10 lines, you need to fill out two multi evidence forms. page 1 of 2 & page 2 of 2.

→ This evidence forms as a reference for all actions taken during your investigative analysis.

→ Track separate pieces of evidence for your chain of custody log.



Date:
Page No.

Securing your evidence.

↳ ① To secure & catalog the evidence contained in large computer components, you can use large evidence bags, tape, tags, labels etc.

② To avoid damaging the components of the computer with scoring into contact with static electricity, which can destroy digital data
↳ use antistatic bags when collecting evidence. + antistatic pads.

③ Use well padded containers
↳ to prevent damage to the evidence as you transport it to your secure Evidence locker.

④ Save discarded hard drive boxes, antistatic bags & packing materials for computer hardware.

⑤ Securing evidence often requires building secure containers
↳ use evidence tape to seal all openings.
↳ Placing evidence tape over insertion slots & CD drive bays to ensure security of evidence.
↳ write your initials on tape to prove it hasn't been tampered with.
↓
∴ ① casing couldn't have been opened
② non power could have been supplied to the closed casing with this tape
③ if tape had been replaced your initials wouldn't be there.

⑥ Computer components require specific temperature & humidity ranges.
↳ Heated car seats → can damage digital media
↳ Placing a computer on top of a two way car radio in the trunk → can damage magnetic media

∴ While collecting computer evidence, ensure you have a safe environment for transporting & storing it until a secure evidence container is available.

Procedures for Private Sector High Tech Investigations
↳ ① As an investigator, you need to develop formal procedures & informal checklists.
↳ ① To cover all issues important to high tech investigations
② Ensures that correct techniques are used in an investigation.
② Use informal checklists → to be certain that all evidence is collected & processed correctly.

Common Procedures that digital investigators use in private sector high tech investigations.

① Employee Termination Cases
↳ ① Majority of investigative work for termination cases involves employee abuse of company assets.
② Incidents that create a hostile work environment are the predominant types of cases investigated
- viewing pornography in the workplace
- Sending inappropriate e-mails.
③ Consult general counsel or HR of the company on specific directions

on how to handle these investigations.

④ Proper policies should be in place.

(I) Internet abuse Investigations

① Applies to organization's internal private network, not public ISP.

Prerequs

② To conduct an investigation, you need:

1- Organization's Internet proxy server logs

2- Suspect computer's IP address
↳ obtained from company's network administrator

3- Suspect computer's hard drive

4- Your preferred computer forensics analysis tools

Investigation

③ Recommended steps to process an Internet abuse case:

① Use standard forensics analysis techniques

② Search for & extract all web page URLs & other relevant information

③ Contact firewall administrator & request a proxy server log of suspect computer's IP address or device name

- Confirm how long DHCP IP address assignments are retained (TTL settings)

④ Compare data recovered from forensics with network server logs to confirm that they match.

⑤ If URL data matches network logs & disk findings:

- Continue analyzing the suspect's disk
- Collect supporting evidence (photos, webpages)

if no match found:

→ report allegations as unsubstantiated (wrong)

* Keep privacy laws in mind

* for companies w/ international operations, jurisdiction is a problem.
↳ what is legal in US might not be legal in Germany.

NOTE → Continue examining suspect computer's disk drive
↳ in case when network server logs don't match forensics analysis

→ Determine if inappropriate data was downloaded to the computer and whether it was through an organization's intranet connection.

(II) Email Abuse Investigations.

① ↳ includes spam, inappropriate & offensive messages, harassment or threats.

② Email abuse must have a defined policy in an organization (Tip for private investigations)

Prerequs

③ What you need for email abuse investigation:

(a) electronic copy of offending email
+ full message header data

(b) email server log records

(c) Access to centralized email server (mail server administrator or manager)

(d) Access to local computer if messages are stored in files like Outlook .pst or .ost

(e) Suitable digital forensics tool

Date :
Page No.

Investigations

④ Recommended Procedure for E-mail Investigations

① Computer based E-mail files like outlook .pst or .ost → apply standard forensic drive examination.

② obtain electronic copies of suspect's & victim's email folders/data. (contact email server administrator)

③ Search for relevant keywords and extract all related email address information.

④ Analyze header data of all relevant messages to trace origin & routing information.

3 key focus:

① Work w/ email server administrator
② follow proper forensic procedures
③ Ensure legal & organizational policy compliance.

(A C P)

III Attorney Client Privilege Investigation.

① → under ACP rules for an attorney, everything & all findings are confidential

② → Attorney controls & directs the investigation

③ → common challenges:

(a) many attorneys like to have printouts of data you recovered but its a problem when you have log files with several thousand pages of data or CAD drawing programs.

Date :
Page No.

(b) some files like CAD programs require specialized programs/w

(c) discovery demands may require preparing evidence for expert witness.

steps for conducting an ACP case.

① obtain a memorandum from the attorney authorising the investigation

② Confirm the investigation is privileged & list all assigned personnel

③ Review keywords relevant to the investigation

④ Begin investigation only after you receive the memorandum

⑤ Create 2 bit-stream (forensic) images of drives.
→ use diff tools (∵ each has its strengths & weaknesses)
→ Keep images uncompressed so even if it gets corrupted, we can analyze uncompressed

⑥ ~~Verify file~~ compare hash signatures on all files on the original & re-created disks

⑦ Examine every portion of disk drive & extract all data.

⑧ Run keyword search on allocated & unallocated disk spaces.

⑨ For Windows OS, use special tools to analyze the registry
↓
access Data registry viewer

⑩ For Binary data files like CAD, locate correct software & if possible make printouts of Binary file content.

⑪ Consolidate recovered data in an organized format for attorneys

Other guidelines

① Minimize written communication with the attorney

② Label all documentation written to attorney as 'Privileged Legal Communication - Confidential Work Product'

③ Assist paralegals & attorney in analyzing data.

Date :
Page No.

(IV) Industrial Espionage Investigations.

(1) All suspected Industrial espionage cases should be treated as criminal investigations.

(2) Staff needed for planning an Industrial espionage investigation

(I) Digital Investigator responsible for disk forensic examinations.

(II) Technology Specialist → Knowledgeable about suspected compromised technical data

(III) Network specialist → to perform log analysis and setup network sniffers

(IV) Threat assessment → Attorney familiar w/ specialist laws related to ITAR or EAR

(3) Guidelines when initiating an investigation (International)

(1) Determine whether this investigation involves industrial espionage.

if yes → does it fall under ITAR or EAR?

(2) Consult corporate attorneys & upper management

(3) Determine info needed to substantiate the allegation of industrial espionage

(4) Generate a list of keywords for disk forensics & network monitoring.

(5) List & collect resources for investigation

(6) Determine goal & scope of investigation

(7) Initiate investigation after approval from management.

(4) Planning considerations for Industrial espionage investigation.

(1) Examine all e-mails of suspected employee

(2) Search Internet forums/ blogs for any posting related to the incident.

(3) Initiate physical surveillance with cameras on people or things of interest to the investigation.

(4) Examine facility physical access logs for sensitive areas

(5) Determine suspect's location in relation to vulnerable assets compromised

(6) Study suspect's movement habit

(7) Collect all incoming & outgoing phone logs.

(5) Steps to Conducting an industrial espionage case.

(1) Gather all personnel assigned to investigation & brief them on the plan

(2) Gather resources to conduct the investigation

(3) Start w/ placing surveillance like cameras & network sniffers at key locations

(4) discreetly gather any additional evidence, like suspect's drive & make a bit stream image for it.

(5) Collect all log data from network & email servers & examine them for things relating to investigation.

(6) Report regularly to upper management & corporate attorneys

(7) Review investigation's scope w/ ( ) & determine when it needs to be expanded.

Date:
Page No.

Interviews & Interrogations in High tech Investigations.

① Private sector digital Investigator: Technical person acquiring the evidence for an investigation

② You might be asked to assist in interviewing or interrogating a suspect when you have performed forensic disk analysis on suspect's machine.

Imp

③ Interview: conducted to collect information from a witness or suspect about specific facts related to an investigation.

Interrogation: Process of trying to get a suspect to confess to a specific incident or crime.

* Investigator might change from an interview to an interrogation when talking to a witness or a suspect.

④ More experience & training in art of interviewing or interrogating more easily they can determine whether a witness is credible or possibly a suspect.

⑤ As a digital Investigator → Instruct the investigator conducting the interview on what questions to ask and what answers should be.

⑥ Preparatory questions: ① What questions to ask suspect to get vital info about the case
② DO I know what I'm talking about or will I have to study about that topic or technology?
③ DO I need additional questioning to cover other indirect issues related to case?

Date:
Page No.

⑦ Common errors: ① being unprepared for the interview
② Not having right questions
③ Not having enough questions

⑧ Make sure you don't run out of convo topics.
Keep convo friendly to gain suspect's confidence
Avoid doubting your skills → might snow lack of confidence

⑨ Ingredients for successful interview or interrogation
① Being patient throughout the session
② Repeating/ rephrasing questions to get on a specific fact from a reluctant witness or suspect
③ Being tenacious.

Understanding data recovery workstations & software.

① Investigations are conducted on a computer forensics lab (or data recovery lab)

② To conduct your investigation & analysis → you need a specially configured PC known as forensic workstation.

③ Forensic workstation: A specially configured PC loaded with additional features & forensics software.

④ operating systems it can run: ① Mac OSX and macOS
② Linux
③ Windows 95, 98 or ME
④ Windows 2000, XP.

Most digital forensic tools work in MS-DOS

(5) Booting an OS while examining a hard disk can alter evidence.
↳ OS may:
① Write data to swap file
② Perform automatic updates
③ Record hardware serial number (which can be difficult to record)
This can damage the integrity of digital evidence.

(6) Least intrusive Microsoft OS is MS-DOS 6.22
It does minimal disk data changes.

(7) Newer file systems (like NTFS) are readable from:
① Window NT & later
② Linux OS
→ Use proper tools to avoid altering data.

(8) - Write blockers prevent writing data to evidence drive.
- Allows booting into windows without modifying evidence.
Types:
① Hardware Write Blockers
↳ Connect via USB
↳ Eg: Firefly, Tableau etc.

② Software Write Blockers
↳ Linux bootable DVD/USB
or
↳ Run independent OS in RAM.
↳ Helps prevent modification of suspect disk.

setting up your workstation for Digital forensics.

① Workstation running windows 7 or later
② Write - Blocker device
③ Digital forensics acquisition tool
④ Digital forensics analysis tool
⑤ Target drive to recieve suspect disk data
⑥ USB ports
⑦ Spare PATA & SATA ports

Additional useful items: ① NIC ② extra USB ports
③ FireWire 400/800 ports ④ SCSI card
⑤ Disk & text editor tools
⑥ Graphics viewer program
⑦ other specialized viewing tools.

Chain of custody: documented record of who collected, handled, transferred & stored evidence from the time it was seized till it is presented in court.

Chain of Evidence: logical link b/w the evidence, the suspect & the crime. How evidence proves its case.

V. Imp

Conducting an Investigation

Examples of Forensics tools ① OS Forensics
② Forensic Explorer
③ EnCase
④ FTK

Office suite : ① Libre office
graphics viewer : ① IrfanView

① To begin an investigation,
copy the evidence using various methods & tools
∴ no one tool retrieves all data from a disk.

② Gather resources identified in investigation plan.
① Original storage media
② Evidence custody form
③ Evidence containers for the storage media (Evidence bag)
④ Bit stream imaging tool (FTK Imager Lite)
⑤ Forensic workstation to copy & examine the evidence
⑥ Secure evidence locker, cabinet or safe.

③ To gather ~~evidence~~ evidence (storage media)
→ use anti-static bags, pads with wrist straps to prevent static electricity from damaging the evidence
Now Perform these steps :
① Meet IT manager → interview him + pick up storage media
② Fill out evidence form, have him sign it, sign yourself.
③ Store storage media in an evidence bag & then transport it to your forensic facility.
④ Carry evidence to a secure container
⑤ Complete Evidence custody form.
↳ multi evidence form → store form in file folder for the case
single evidence form → store form in secure container w/ the evidence

limit access to form → reduce risk of tampering
⑤ Secure evidence by locking the container.

Understanding Bit-stream Copies.

① Bit stream copy → ① Bit by Bit copy (also called forensic copy) of the original drive or storage media.
② It is an exact copy of original disk.
③ More exact the copy, better chances you have of retrieving the evidence you need.
④ This process is called "acquiring an image" or "making an image" of a suspect drive.

② **Bit stream copy** vs **Simple backup copy of a disk**

Bit stream copy	Simple backup copy of a disk
① Creates an exact bit by bit sector by sector copy of entire disk	① Can copy or compress only files that are stored in a folder or are of known file type (copies files & folders copied)
② It includes allocated, unallocated & slack space as well as deleted data	② It can't copy deleted files & emails or recover file fragments.
③ Used in digital forensics	③ Used for data recovery or system restoration
④ Preserves original file system structure & metadata	④ May not preserve full metadata or disk structure.
⑤ Ensures evidence integrity & allows hash verification	⑤ Doesn't capture hidden/deleted evidence. Mainly for regular backups

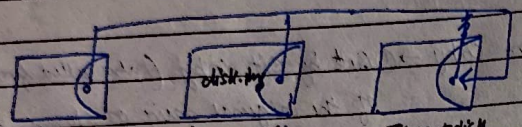
Every bitstream copy → bitstream image
but not every bitstream image is a bitstream copy.

Date:
Page No.

③ Bit stream Image:

① file containing the bit stream copy of all data on a disk or disk partition.

② Also known as 'image', "image save", "image file"



Creating an image transfers each bit of data from original disk to the same spot on the image disk.

③ To create an exact image of an evidence disk, copying the image to a target disk that matches original disk's: manufacturer, size & model.

④ If target disk is identical to the original, size in bytes & sectors on both disks should be same.

Bit stream copy	Bit stream Image
① Process of copying data bit by bit	① The resulting file created from the bit stream copy
② refers to the act of duplicating the entire disk	② refers to the image file (e.g. .img, .dd, .E01)
③ Can copy directly to another physical disk	③ Stored as a single file on another storage device
④ Produces an exact duplicate	④ Contains the complete data inside one file

④ Acquiring an image of evidence.

↳ ① Preserve the original evidence

② Conduct your analysis only on copy of the data (image of original disk)

③ Windows tools require write blocking device when acquiring data from FAT or NTFS file system.

⑤ Analyzing your digital Evidence

↳ ① Your job is to recover data from: ① deleted files
② file fragments
③ existing files.

deleted files.

② As files are deleted → space they occupied gets freed up. Now it can be used for new files or existing files that are expanding.

→ The files that were deleted are still on the disk until a new file is saved to the same physical location, overwriting the original file.

→ Autopsy can retrieve deleted files to use as evidence.
- → Can display non printable/ binary data (audio, video, etc) in content viewer
- → Can do keyword search

⑥ Completing the case.

- → You need to produce a final report
- → state what you did & what you found.
- → include autopsy report to document more.

Repeatable findings: In any digital investigation, you should be able to repeat the steps you took & produce the same results.

→ report should show conclusive evidence → suspect did or didn't commit crime

→ Basic report format → answering 6 W's

Who, what, when, where, why & how

→ Keep a written journal of everything you do
↳ can be used in court.

→ explain computer & software process

→ Autopsy report generator → can generate notes in plain text, HTML & excel.

Critiquing the case.

↳ To improve your work:

① How could you improve your performance in the case?
② Did you expect the results you found?
Did the case develop in ways you didn't expect?
③ Was documentation thorough enough?
④ Feedback from requesting source?
⑤ Did you discover any new problem? if so, what are they?
⑥ Did you use new techniques?

Investigator's office & laboratory

⇒ Understanding digital forensics lab certification requirements

(I)* Digital forensics lab
→ Where you conduct your investigation
→ Store evidence
→ House your equipment, hardware + software.

(II) ANAB → ANSI-ASQ National Accreditation Board
→ Provides certification of crime & forensics lab worldwide
→ These Certification includes forensics labs that analyze digital evidence
→ Audits lab functions & procedures

(III) Lab manager duties:
① Set up procedures for managing cases
② Promote group consensus in decision making
③ maintain responsibility for lab needs
④ Enforces ethical standards among lab staff members.
⑤ Plan updates for the lab
⑥ Establish & promote quality assurance process
⑦ set reasonable production schedules
⑧ Estimate how many cases an investigator can handle
⑨ Estimate when to expect preliminary & final results
⑩ Create & Monitor lab policies for staff
⑪ provide a safe & secure workplace for staff & evidence.

(IV) staff member duties
① knowledge & training
→ Hardware & software
→ OS & file types
→ deductive reasoning.
② work is regularly reviewed by lab manager

(V) lab budget Planning

→ Break down cost into monthly, quarterly & yearly expenses

→ use past investigations expenses to extrapolate expected future cost

→ Expenses include: ① Hardware
② Software
③ facility space
④ Training personnel

→ ① Estimate no. of cases your lab expects to examine

→ ② Identify types of computers you're likely to examine.

③ Take into account changes in technology & gather insight on what kind of computer crimes are most likely to occur → use to this to plan lab requirement & costs.

④ When setting up a lab for a private company:
Check ① Hardware + Software inventory
② Problems reported last year
③ Future developments in computing technology.

Time manage a major issue than choosing these.

(VI) Acquiring certifications & Training

① Update your skills through appropriate training

② (IACIS) International Association of Computer Investigative Specialists
→ created by police officers who wanted to formalize credentials in digital investigation.
→ on passing IACIS test, candidates are designated as Certified Forensic Computer examiner (CFCE)

(II) ISC² certified cyber forensics professional (CCFP)
↳ requires knowledge of: ① Digital forensics
② Malware analysis
③ Incident reporting
④ E-discovery
⑤ other disciplines related to cyber investigations.

(III) High Tech Crime Network (HTCN)
CCCI → Certified computer crime investigator, Basic + Advanced level
CCFT → Certified computer forensics technician, Basic + Advanced level

(IV) Encase Certified Examiner (EnCE) Certification
→ open to public + private sectors
→ specific to mastery of EnCase forensics analysis
→ candidates are required to have licensed copy of EnCase

(V) AccessData Certified Examiner (ACE) certification
→ open to public + private sectors
→ specific to mastery of AccessData Ultimate Toolkit
→ Exam = knowledge base component + practical skill component

Other certifications & training
① Computer Technology Investigators Network (CTIN)
② Digital forensics certification Board (DFCB)
③ Cloud Security Alliance (CSA)
④ EC-Council
⑤ Defense Cyber Investigations Training Academy (DCITA)

Physical requirements for a Computer forensics lab

(1) Most of your investigations is conducted in lab
(2) Lab should be secure so evidence isn't lost, corrupted or destroyed.
(3) Provides a safe & secure physical environment
(4) Keep inventory control of your assets → (when to order more supplies)

Identifying lab security needs.

(1) Secure facility
   ↳ should preserve integrity of evidence data

(2) Minimum Requirements:
   (1) Small room with true floor to ceiling walls
   (2) Door access with locking mechanism
   (3) Secure containers
   (4) Visitor's log

(3) People working together should have same access level
(4) Brief your staff about security policy.

High Risk Investigation requirements:

(1) demands more security than minimum lab requirements
(2) Tempest facilities → Electromagnetic radiation (EMR) proofs.
(3) Tempest facilities → very expensive
   ∴ you can use low emanation workstations instead.

Using Evidence containers

(1) known as evidence lockers
   ↳ Must be secure so that no unauthorized person can easily access your evidence.

(2) Recommendation for storing storage containers:
   → locate them in a restricted area
   → Limit the no. of authorized people who can access the containers
   → Maintain records on who is authorized to access each container
   → Containers should be locked when not in use.

(3) If a combination locking system is used:
   → Provide same level of security for the combination as you did for container's content.
   → destroy any previous combinations after setting up a new combination
   → Allow only authorized people to change lock combination
   → change combination every 6 months or when required

(4) If you're using keyed padlock:
   → (1) Appoint a key custodian
   (2) Stamp sequential numbers on each duplicate key.
   (3) Conduct a monthly audit
   (4) Take an inventory of all keys
   (5) Mark keys in a locked container
   (6) Security level same for keys as for evidence containers
   (7) Change locks & keys annually
   (8) Maintain a registry which key is assigned to which authorized person

(5) Don't use master key for several locks.

(5) Further requirements:
① Containers should be made of steel with an internal cabinet or external padlock.
② Acquire a media safe (if possible)
③ Try to build an evidence storage vroom in your lab
④ Keep an evidence log → update it everytime an evidence container is opened or closed

overseeing facility maintenance
① Immediately repair any physical damages
② Escort cleaning crews as they work
③ Minimize risk of static electricity
- antistatic pads
- Clean floor & Carpets
④ Maintain 2 separate trash Containers
- Material unrelated to an investigation
- sensitive material
⑤ Hire specialized Companies to dispose of sensitive materials.

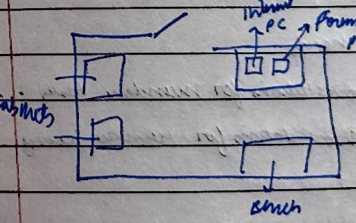
Physical Security needs.
① Enhance security by setting security policies
② Enforce your policy:
→ ① Maintain a sign-in log for visitors
→ Anyone not assigned to lab = visitor
→ Escort all visitors at all times.
② Use visible or audible indicator that a visitor is inside your premises
→ Visitor badge.
③ Install intrusion alarm system
④ Hire a guard force for your lab.

Auditing a digital forensics lab
→ ensures proper enforcing of policies
→ Audits include inspecting the following facility components & practices:
① Ceiling, floor, roof & exterior walls of the lab
② Doors & door locks
③ Visitor logs
④ Evidence containers logs
⑤ At end of every workday, secure any evidence that is not being processed in a forensic workstation.

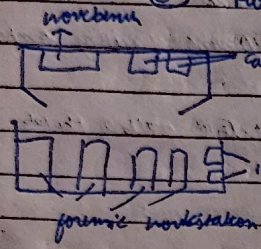
Determining floor plans for digital forensics lab.
① configuring work area depends on:
- Budget
- Available floor space
- No. of computers assigned to each computing investig

② Ideal configuration
→ 2 forensic workstations
→ 1 non-forensic workstation with internet access.

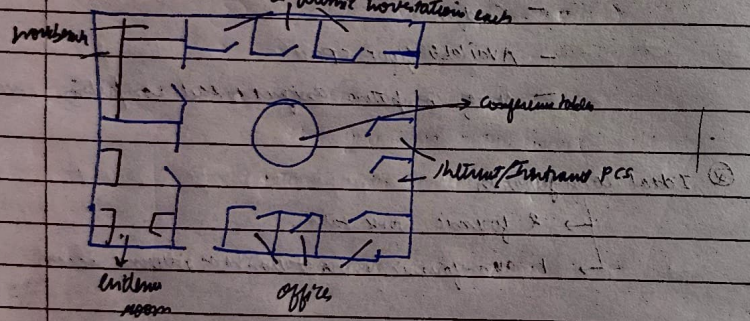
③ small labs consist of: ① 1-2 forensic workstations
② A Research Computer w/ internet
③ A workbench (if you have space)
④ storage cabinets



④ Mid size labs : ① Public business
② Have more workstations
③ Should have atleast 2 exits, for safety reasons
④ Cubicles → to reinforce need-to-know policy.
⑤ More library space for s/w & h/w storage



⑤ large size labs: ① State law enforcement or FBI
② Have a separate evidence room
③ 1+ custodians to manage & control the traffic in & out of the evidence room.
④ Should have atleast 2 controlled exits & no windows



Selecting workstations for a lab.
- Depends on budget & needs
- Use less powerful workstations for mundane tasks
- Use multipurpose workstations for resource heavy analysis.

① Public / investigation labs
↳ ① have most diverse needs for computing investigation tools.
↳ labs might need legacy systems & software to match what is used in the community.

② Small or local police department → ① 1 multipurpose forensic workstation
② 1-2 basic workstations
③ or high end laptops

③ Use a laptop PC w/ USB 3.0 or SATA hard disks to create lightweight mobile forensics workstation.

② Private sector labs
① Requirements are easy to define
↳ Business can conduct internal investigations

② Identify the environment you deal with
↳ Hardware platform
↳ operating systems

③ With some digital forensics programs
↳ you can move b/w Windows PC or examine both Windows & Macintosh disk drives.

Date :
Page No.

Stocking Hardware Peripherals

Any lab should have in stock :

1. Digital Camera
2. Assorted Antistatic bags
3. Graphics Cards, both PCI & AGP types
4. Hard disk drives & USB drives
5. IDE Cables
6. External CD/DVD drive - - so on.
7. Extra USB 3.0 or newer cables & SATA cards

Maintaining Operating systems & Software Inventories

→ Maintain licensed copies of s/w such as :

1. Microsoft office (older + newer)
2. Hexadecimal editor
3. Programming language (Perl, VS Code, Python)
4. Third party or open source office suite.
5. Specialized viewers (source code)

Disaster Recovery Plan

- ensures that you can restore your workstation & investigation files in their original condition
  - virus contamination, catastrophic situation, misconfiguration
- includes backup tools such as Norton Ghost
- Configuration management : Keep trace of software updates on your workstation
- for labs using high end RAID servers :
  - Consider methods for restoring large data sets
  - Large end servers must have data backup in place in case of major failure or more than one drive.

Date :
Page No.

Risk management : (1) Involves determining how much risk is acceptable for any process.

(2) Identify equipments your lab depends on, so that it can periodically be replaced.

(3) Identify equipments you can replace when it fails.

(4) Computing components last → 18-36 months normally ∴ schedule upgrade every 18 or 12 months.

Building Business case for developing a forensics lab.

(1) Business case → plan you can use to sell your services to management or clients

(2) Demonstrate how the lab will help your organization save money & increase profits
   - Compare cost of investigation vs cost of lawsuit
   - protect intellectual property, trade secrets & future business plans

(3) Use the support of managers & other team members.

(4) Investigators must plan ahead to ensure that money is available for facilities, tools, supplies & training for your forensics lab

(5) Justification : (1) Justify to person controlling the budget the reason a lab is needed.

(2) Requires constant effort to market lab's services to previous, current & future customers & clients

Date :
Page No.

⑥ Budget development → needs to include

① facility cost

② Hardware requirements

③ Software "

④ Miscellaneous budget needs.

⑦ Approval & Acquisition: Present a Business case with a budget to upper management for approval

⑧ Implementation: ① Describe how implementation of all approved items will be processed

② A timeline showing expected delivery, installation dates & expected completion dates must be included in your Business case.

③ Schedule inspection dates.

⑨ Acceptance testing: ① Inspect the facilities to make sure it meets security criteria

② Test all communication

③ Test all hardware to ~~check~~ verify if it is operational

④ Install & start all ~~hardware~~ S/W tools

⑩ Your Business case must anticipate problems that can cause delay in lab production.

⑪ Production: → After all essential corrections, lab can go into production

→ Implement lab operations procedures.