

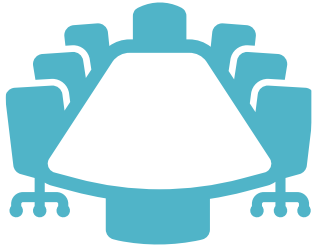
A person wearing a grey hoodie is seen from behind, sitting at a desk. In front of them is a computer monitor displaying lines of code. The background is filled with a digital aesthetic, featuring a grid of binary code (0s and 1s) in green and blue tones. The overall scene suggests a focus on digital technology and cybersecurity.

INCS-712: Digital Forensics

Chapter 3 - Investigation Readiness

Baljeet Malhotra, PhD

Digital Forensic Readiness Plan



Strategy

Identify the various scenarios in which digital evidence may be required.

Identify the technical and human resources needed to ensure financial support for the program.



Policy and Procedures

Define acceptable behaviors for members of the organization in the use of information systems resources. Specify what data will be monitored and when and how it will be retained.



Technology

Implement effective logging mechanisms to ensure that critical data can be captured.

Use proven tools to capture and analyze data to ensure its legal validity.

Establish secure storage solutions to protect the integrity and security of data.



Response

Define the response process and responsible parties within the organization in the event of a digital forensic incident.

Deciding whether to handle or outsource digital forensics tasks in-house, based on resources and capabilities.



Compliance

Conduct regular audits of digital forensics readiness programs to ensure compliance with policies and regulations.

Conduct regular training and awareness-raising activities to ensure that all employees are aware of relevant policies and procedures.



Initial Investigation

Part 1: Investigation Readiness Plans

Book Chapter: 3

Initial Investigation



Identify

Identify the subjects and data sources relevant to the investigation. This includes various devices (such as computers, laptops, smart devices) or services, systems, and so on.



Protect

Protect the scene and prevent evidence from being tampered with. Including the use of write-protected devices, and also the protection of systems and services. The protection phase ensures that all data is saved in a court-approved manner to prevent data from being tampered with or damaged during the evidence-collection process.



Collect

Use various forensic tools to create digital copies of data (e.g., images) to ensure that the original data has not been modified. The collected evidence may include active files, deleted files, operating system data, network configurations, and so on.

Protecting Data - Write Blockers

USB WriteBlocker (WiebeTech)



Purpose: USB WriteBlocker (WiebeTech) is an appliance that prevents any write operation of the original data during the acquisition. It safeguards the inflexion of the enclosed documents through a hardware component so that the source data is not written upon.



Function: The USB WriteBlocker (WiebeTech) can connect to USB flash disks and external hard disks. It provides reading capabilities while preventing data writing/modification. It also works with hash values by generating hashes off stored data as well as in verifying the same in case of inconsistent data.



Application: USB WriteBlocker (WiebeTech) connects to storage device while preventing it from being modified. During data acquisition, it affirms that the data has not been altered. Furthermore, it facilitates a logging function that enables recording all attempts to access the storage device and its status.

Initial Investigation

- An **evidence custody form** helps you document what has been done with the original evidence and its forensics copies
 - Also called a chain-of-evidence form
- Two types
 - **Single-evidence form**
 - Lists each piece of evidence on a separate page
 - **Multi-evidence form**



Chain of Custody

Part 2: Importance of Chain of Custody

Book Chapter: 3

Chain of Custody (CoC)



CoC refers to the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of physical or digital evidence.

CoC is also called a chain-of-evidence form. It is a cornerstone of digital forensics, ensuring that digital evidence is handled with the utmost care and precision from the moment it is identified to its presentation in court.

CoC Importance



Legal Admissibility

It must be proven that the evidence has been handled properly from the time it was collected until it is presented in the courtroom. Any breaks or inconsistencies in the CoC can lead to questions about the authenticity and integrity of the evidence, potentially rendering it inadmissible.



Evidence Integrity

CoC is crucial for preserving the integrity of digital evidence. Digital data is inherently fragile and can be easily altered or corrupted, either intentionally or accidentally. A documented CoC helps ensure that the evidence remains in its original state.



Accountability

The CoC provides a clear record of who has handled the evidence at each stage of the investigation. This accountability is essential for tracing any actions taken on the evidence and for identifying any potential mishandling or misconduct.

CoC Process



Identification of Evidence

Identification of potential digital evidence, such as computers, mobile devices, external drives, or network logs. The investigator must document the exact location and condition of the evidence at the time of identification.



Evidence Collection

Evidence is collected using appropriate tools and methods that ensure its integrity. Often involves creating a forensic image of the data, which is an exact bit-by-bit copy of the original.



Documentation

Every action taken with the evidence must be meticulously documented. This includes logging the time and date of collection, the method used to acquire the evidence, and the identity of the individual who collected it.



Secure Storage

The evidence must be stored securely to prevent unauthorized access or tampering. This might involve physical security measures, such as locked storage cabinets, or digital security measures, such as encryption and access controls.



Analysis and Examination

Examiner must document each step of the process, including the tools and techniques used, the data analyzed, and the findings. Any modifications to the evidence during analysis must be recorded.



Transfer and Handling

If the evidence needs to be transferred to another investigator, analyst, or location, this transfer must be documented. The CoC log should include the names of the individuals involved, the date and time of the transfer.



Presentation in Court

When the evidence is presented in court, the CoC must be demonstrated to show that the evidence has been handled correctly and remains in its original state. The documented chain provides assurance to the court.

CoC Challenges



Complexity of Digital Evidence

Unlike physical evidence, digital evidence can be easily duplicated, altered, or corrupted without leaving visible traces. Ensuring that the original data is preserved while working with copies requires careful handling and advanced forensic tools.



Volume of Data

The vast amounts of data involved in digital forensics can make maintaining a detailed CoC challenging. Multiple copies, devices, and storage locations increase the risk of errors or lapses in documentation.



Remote and Cloud Environments

The increasing use of cloud storage and remote systems adds complexity to the CoC, as data may be stored in multiple locations, including different jurisdictions. Ensuring secure access and proper documentation in these environments can be challenging.



Legal and Regulatory Differences

Different countries and regions may have varying legal standards and requirements for the CoC. Forensic investigators must be aware of these differences to ensure that evidence is handled in compliance with laws.





Evidence Custody Form

Part 3: Chain of Custody Forms

Book Chapter: 3

Single Evidence Form

Single Evidence Form		
Case No. <input type="text"/>	Evidence No. <input type="text"/>	Digital Forensics Lab
PLEASE COMPLETE FORM IN UPPERCASE		
Section B: Evidence Collection		
Date/Time Collected <input type="text"/>	Collected by <input type="text"/>	
Site Address <input type="text"/>		
Section C: Evidence Details		
Date/Time Stored <input type="text"/>	<input type="text"/>	
Storage Location <input type="text"/>		
Device Type <input type="text"/>	Capacity <input type="text"/>	
Manufacturer <input type="text"/>	Model <input type="text"/>	
Serial No. <input type="text"/>		
MD5 Sum <input type="text"/>		
SHA-1 Sum <input type="text"/>		
Additional Information... <input type="text"/>		
Note any damage, marks and scratches <input type="text"/>		
Digital Image Taken <input type="checkbox"/> Yes <input type="checkbox"/> No		
Section D: Image Details		
Date/Time Imaged <input type="text"/>	Imaged by <input type="text"/>	
Storage Location <input type="text"/>		
Image Filename <input type="text"/>	Image Size <input type="text"/> (inc. unit)	
Additional Information... <input type="text"/>		
This form is to be used when collecting a hardware device containing data that may be of interest in a case. Guidelines:		
<ul style="list-style-type: none">Ensure that this form only refers to one item of evidence and that one is completed for each item of evidenceThis form must be accompanied by Chain of Custody forms which detail the individuals that have handled the evidenceFurther remarks can be noted overleaf in Section E: RemarksIt is important that these forms are kept with the evidence at all timesUpon handover or disposal please complete Section F: Evidence Handover		

Chain of Custody Form for use with a Single Evidence form		
Case No. <input type="text"/>	Evidence No. <input type="text"/>	Page No. <input type="text"/>
This form must accompany a Single Evidence form and it's respective evidence		
Chain of Custody		
SUBMITTER	RECEIVER	
Name: <input type="text"/>	Name: <input type="text"/>	
Signature: <input type="text"/>	Signature: <input type="text"/>	
Date & Time: <input type="text"/>	Evidence Modified: Yes / No <input type="checkbox"/>	Date & Time: <input type="text"/>
SUBMITTER	RECEIVER	
Name: <input type="text"/>	Name: <input type="text"/>	
Signature: <input type="text"/>	Signature: <input type="text"/>	
Date & Time: <input type="text"/>	Evidence Modified: Yes / No <input type="checkbox"/>	Date & Time: <input type="text"/>
SUBMITTER	RECEIVER	
Name: <input type="text"/>	Name: <input type="text"/>	
Signature: <input type="text"/>	Signature: <input type="text"/>	
Date & Time: <input type="text"/>	Evidence Modified: Yes / No <input type="checkbox"/>	Date & Time: <input type="text"/>
SUBMITTER	RECEIVER	
Name: <input type="text"/>	Name: <input type="text"/>	
Signature: <input type="text"/>	Signature: <input type="text"/>	
Date & Time: <input type="text"/>	Evidence Modified: Yes / No <input type="checkbox"/>	Date & Time: <input type="text"/>
SUBMITTER	RECEIVER	
Name: <input type="text"/>	Name: <input type="text"/>	
Signature: <input type="text"/>	Signature: <input type="text"/>	
Date & Time: <input type="text"/>	Evidence Modified: Yes / No <input type="checkbox"/>	Date & Time: <input type="text"/>
SUBMITTER	RECEIVER	
Name: <input type="text"/>	Name: <input type="text"/>	
Signature: <input type="text"/>	Signature: <input type="text"/>	
Date & Time: <input type="text"/>	Evidence Modified: Yes / No <input type="checkbox"/>	Date & Time: <input type="text"/>
If this form is full please continue on another page		

Multi Evidence Form

Description of Evidence		
Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)

Chain of Custody				
Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location

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 ___	

Multi Evidence Form

Organization 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 ____

Securing Evidence

- Use **evidence bags** to secure and catalog the evidence
- Use computer safe products when collecting computer evidence
 - Antistatic bags
 - Antistatic pads
- Use well padded containers
- Use evidence tape to seal all openings
 - CD drive bays
 - Insertion slots for power supply electrical cords and USB cables



Securing Evidence

- Write your initials on tape to prove that evidence has not been tampered with
- Consider computer specific temperature and humidity ranges
 - Make sure you have a safe environment for transporting and storing it until a secure evidence container is available





Incident Response

Part 4: Importance of Response

Book Chapter: 3

Agenda

❑ Digital Incident Response

- Definitions
- Responsible Disclosure
- Key Principles of Disclosure
- Goals of Incident Response

❑ Digital Forensic Investigation

- Definitions
- Crime Scene Examples
- Crime Scene Characteristic

Response and Responsible Disclosure

What is a Response ?

- A coordinated and structured approach to manage a Digital Incident from detection to resolution.

What is a Response Disclosure ?

- Ethical practice of reporting security vulnerabilities or issues discovered during digital forensic investigations to the relevant parties, such as software developers, hardware manufacturers, law enforcement agencies or other affected entities, in a manner that allows them to address the issue before it is publicly disclosed or exploited.

Responsible Disclosure - Key Principles



Privacy

Ensuring that sensitive information related to the vulnerability is shared only with the entity responsible for addressing it, protecting the details from potential misuse.



Timeliness

Reporting the vulnerability promptly after discovery, allowing for a reasonable timeframe for the issue to be fixed before any public disclosure.



Collaboration

Working together with the affected entity to understand the severity of the issue, validate the vulnerability, and assist in mitigating any potential impacts..



Transparency

Following up with the affected entity to monitor the progress and, if agreed upon, publicly disclosing the vulnerability details in a way that benefits the wider community, once a fix has been implemented..



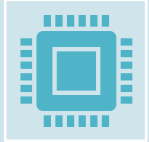
Posturing

Presenting stance or readiness to address vulnerabilities and engage with the ethical disclosure process. Positioning itself to respond to disclosures, plays a crucial role in building trust.

Incident Response



Goals of an Incident Response



Investigate: A systematic way to collect and process information about an incident.

Attack Vector

Malware and Tools

Affected Systems

Damage Assessment

State of Attack

Time Frame



Present: Presenting evidences to a competitive authority.

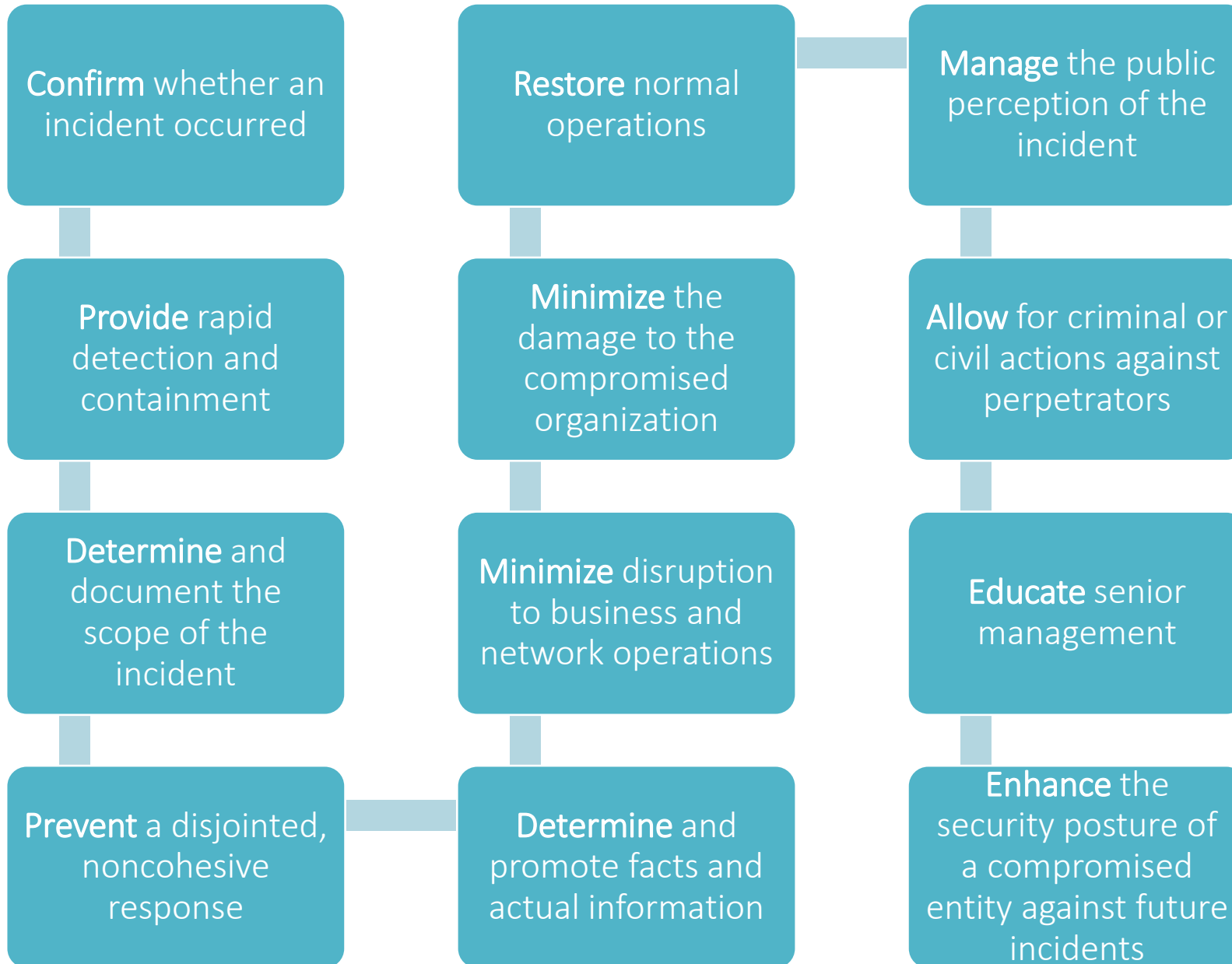


Remediate: A systematic way to manage an incident and its aftereffects.

Developing a plan

Implementing a plan

Activities of an Incident Response



Incident Response Team Structure





Investigation Process

Part 5: Investigation Specific Processes

Book Chapter: 3

Applying Digital Forensics to Investigations



Three Vital Aspects of Digital Forensics

- **Digital Forensic Data: contain information that help with:**
 - Chain of incidents leading to a crime
 - Evidence that can lead to a conviction
 - Evidence that can lead to a acquittal
- **Digital Forensic Tools: may be necessary in investigation as:**
 - Evidence (information might be protected or encrypted)
 - Evidence that can lead to a acquittal
- **Digital Forensic Process: may be necessary in investigation as:**
 - Law enforcement need to follow proper procedure to acquire evidence
 - Digital evidence can be easily altered by an overeager investigator

Taking a Systematic Approach

- ☐ Make an initial assessment about the nature of the case
- ☐ Determine a preliminary design or approach to the case
- ☐ Determine the resources you need
- ☐ Obtain and copy an evidence drive
- ☐ Create a detailed checklist/report
- ☐ Present your analysis/investigation

Systematic Approach - Initial Assessment

☐ Understand the nature of the incident or crime

- Cyber Theft, Attack , Espionage, Terrorism

☐ Identify potential sources of digital evidence

- Stored data, transient data, logs, communications

☐ Determine the scope of the investigation

- Timeframe, involved parties, etc.

☐ Assess the potential complexities of the case

- Types of devices involved, encryption, data volume, etc.

Systematic Approach - Preliminary Design

- ❑ Develop a strategy tailored to the specificities of the case.
- ❑ Select tools for data collection, preservation, and analysis.
- ❑ Plan the sequence of actions to minimize data loss/contamination.
- ❑ Plan to handle challenges like encrypted data or large data sets.

Systematic Approach - Resource Determination

☐ Identify the human resources required

- Software/security engineer, forensic analysts, legal advisors, etc.

☐ Determine the technical resources needed

- Forensic software, hardware, and specialized tools

☐ Evaluate the need for additional resources

- Cloud storage access or expertise in specific software/hardware.

Systematic Approach - Evidence Drive

- ❑ **Securely acquire the physical or logical storage media**
 - Hard drives, SSDs, mobile devices, cloud storage, etc.
- ❑ **Create forensic images of the media**
 - Ensure that they are exact bit-by-bit copies
- ❑ **Use write blockers to prevent any modifications**
 - Original evidence during the copying process must be preserved
- ❑ **Verify the integrity of the forensic images through hash values**
 - MD5, SHA 1, SHA 2

Systematic Approach - Detailed Checklists

- ☐ **List every step of the forensic process**
 - Initial assessment to final reporting
- ☐ **Include specific actions for evidence handling**
 - Documentation, and analysis
- ☐ **Create sub-checklists for different phases**
 - Collection, examination, and analysis
- ☐ **Ensure that the checklist covers legal compliance**
 - Chain of custody, and quality control measures

Types of Checklists



Digital Forensic Checklist - Generic

☐ Date and time of the incident

- Hard drives, SSDs, mobile devices, cloud storage, etc.

☐ Date and time the incident detection

- Ensure that they are exact bit-by-bit copies

☐ Personnel documenting the incident

- Original evidence during the copying process must be preserved

☐ Personnel reporting the incident

- MD5, SHA I, SHA 2

☐ Personnel detecting the incident

- MD5, SHA I, SHA 2

Digital Forensic Checklist - Generic

☐ Personnel aware of the incident

- Monitor the activities

☐ State of the incident

- Currently ongoing or stopped

☐ Affected resources

- Data or resources that may have been affected

☐ Requirement to share the incident

- Share on a “need-to-know” basis

☐ Personnel accessing the affected resources

- Monitor their activities

Digital Forensic Checklist - Generic

☐ Unique identifiers and locations

- Affected resources' IP addresses may not be unique

☐ Categorization of the incident

- Malware, phishing, failed logins, unauthorized access

☐ Incident detection method

- Antivirus alert, an IDS alert, user reported behavior

☐ Anything else

- MD5, SHA I, SHA 2

☐ Anything else

- MD5, SHA I, SHA 2

Summary - Digital Forensic Checklist - Generic

- | | | |
|---|---|--|
| 1. Date and time of the incident | currently ongoing/stopped | 11. Unique identifier and location of affected resources - IP address may not be unique |
| 2. Date and time the incident detection | 8. Affected resources - data or resources that may have been affected | 12. Categorization of the incident - malware, phishing, failed logins, unauthorized access |
| 3. Personnel documenting the incident | 9. Requirement to keep knowledge of the incident on a “need-to-know” basis | 13. Incident detection method - antivirus alert, an IDS alert, user reported suspicious behavior |
| 4. Personnel reporting the incident | 10. Personnel accessing affected resources (since the detection) and their activities | |
| 5. Personnel detecting the incident | | |
| 6. Personnel aware of the incident | | |
| 7. State of incident - | | |

Digital Forensic Checklist - Individual System

☐ Physical Location

- Maintains the context: chain of study, jurisdiction, environment

☐ The asset tag number

- Ensures proper identification and maintaining chain of custody

☐ The system's make and model

- Ensures proper identification and maintaining chain of custody

☐ The operating system installed

- Knowing the OS is essential for the forensic investigation process

☐ Primary function of the system

- Helps identify relevant data, potential attack vectors, access patterns

Digital Forensic Checklist - Individual System

☐ **The responsible system administrator or user**

- Ensures proper access, preserving the integrity of evidence

☐ **The assigned IP addresses**

- Trace network activity, identify users, correlate log data

☐ **The system's host name and domain**

- Ensures proper identification and maintaining chain of custody

☐ **Malware detected and any remediations taken**

- Knowing malware is essential for the forensic investigation

☐ **Existing backups for the system**

- Helps identify relevant data, potential attack vectors, access patterns

Digital Forensic Checklist - Individual System

1. Physical location
2. The asset tag number
3. The system's make and model
4. The operating system installed
5. Primary function of the system
6. The responsible system administrator or user
7. The assigned IP addresses
8. The system's host name and domain
9. The critical information stored on the system
10. Whether backups exist for the system
11. Whether the system is still connected to the network
12. A list of malware detected, from the time of investigation back to the beginning of logs
13. A list of any remediation steps that have been taken
14. Data being preserved - what process is being used and where it is being stored

Digital Forensic Checklist - Network

☐ **Network monitoring status**

- Maintains the context: chain of study, jurisdiction, environment

☐ **Updates to network diagrams and configurations**

- Ensures proper identification and maintaining chain of custody

☐ **A list of any remediation steps that have been taken**

- Ensures proper identification and maintaining chain of custody

☐ **External malicious IP addresses or domain names involved**

- Knowing the OS is essential for the forensic investigation process

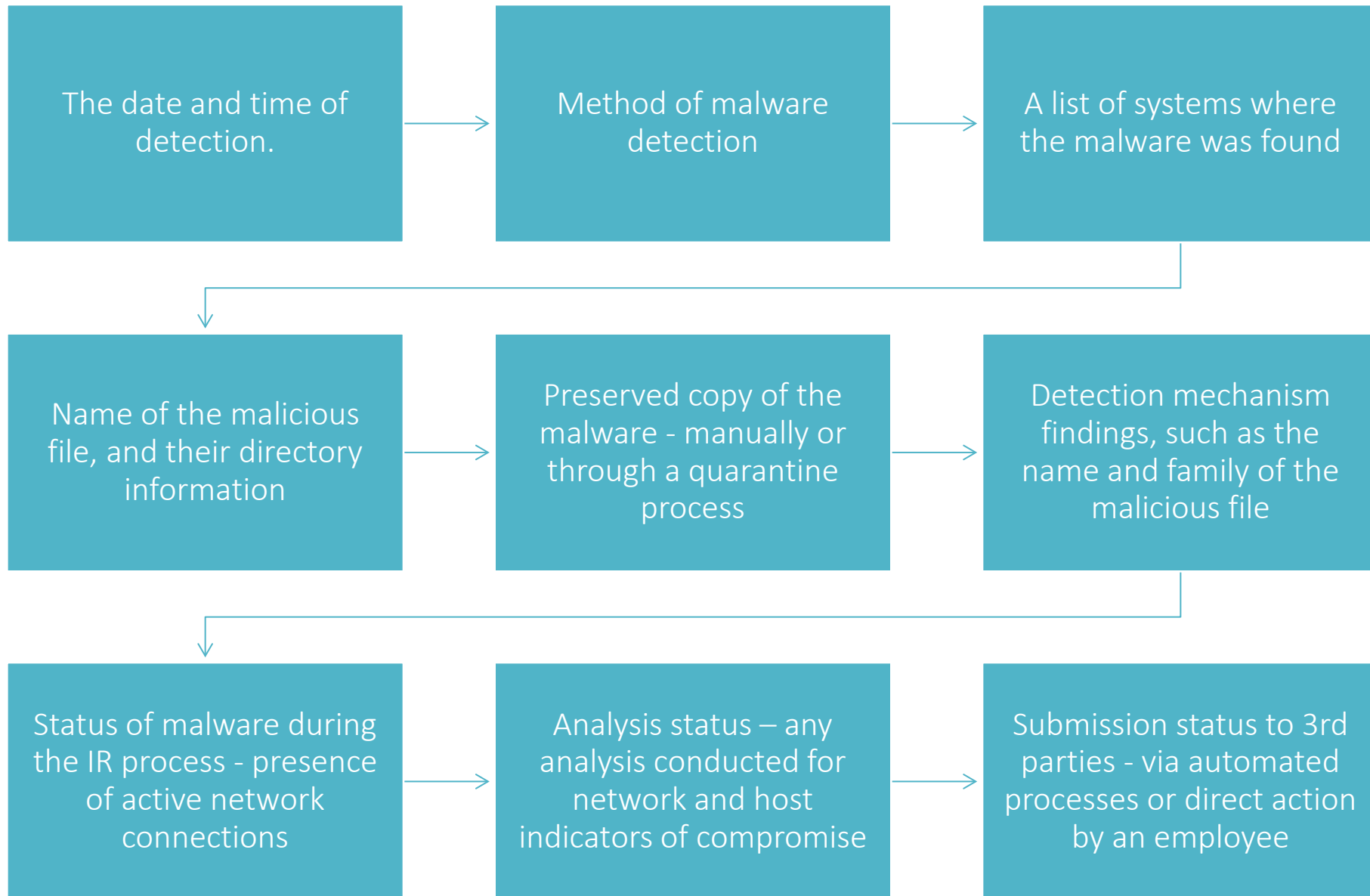
☐ **Data preserved: processes being used and stored**

- Helps identify relevant data, potential attack vectors, access patterns

Digital Forensic Checklist - Network

1. Network monitoring status
2. Updates to network diagrams and configurations
3. A list of any remediation steps that have been taken
4. A list of all external malicious IP addresses or domain names involved
5. Data preserved, what process is being used and where it is being stored

Digital Forensic Checklist - Malware



Digital Forensic Checklist - Malware

- | | | |
|--|--|---|
| 1. The date and time of detection. | manually or through a quarantine process | connections |
| 2. Method of malware detection | | 8. Analysis status – any analysis conducted for network and host indicators of compromise |
| 3. A list of systems where the malware was found | 6. Detection mechanism findings, such as the name and family of the malicious file | 9. Submission status to 3rd parties - via automated processes or direct action by an employee |
| 4. Name of the malicious file, and their directory information | 7. Status of malware during the IR process - presence of active network | |
| 5. Preserved copy of the malware - | | |



Investigation Scenarios

Part 5: Investigating Specific Cases

Book Chapter: 3

Review Some Real Case Studies



Real Case Studies

William Macquarie Case Study: <http://www.youtube.com/watch?v=vJdME6vczeo>

Bin Laden Forensic Case Study: https://www.youtube.com/watch?v=4W_P_Yxhnt0

OpenText Forensic Tools: <https://www.guidancesoftware.com/encase-forensic#digital>

Case Study - Company Policy Violations



Company Policy Violations

Employees misusing resources can cost companies millions of dollars

Misuse includes:

- Surfing the Internet
- Sending personal e-mails
- Using company computers for personal tasks
- Usage of unapproved resources leading to business risks

Unapproved Resources Leading to Risks



Case Study - Employee Termination



Employee Termination

- The majority of investigative work for termination cases involves employee abuse of corporate assets
- Incidents that create a hostile work environment are the predominant types of cases investigated
 - Viewing pornography in the workplace
 - Sending inappropriate e-mails
- Organizations must have appropriate policies in place

Case Study - Internet Abuse Investigation



Internet Abuse Investigation

- 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

Internet Abuse Investigation

- Recommended steps
 - Use standard forensic analysis techniques/procedures
 - Use appropriate tools to extract all Web page URL
 - 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

Email Abuse Investigation

- **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

Email Abuse Investigation

- 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



ACP Investigations

Part 6: Attorney-Client Privileges

Book Chapter: 3

Attorney-Client Privilege Investigation

- An ACP Investigation refers to an internal or external investigation that is conducted under the protection of attorney-client privilege. Communications between an attorney and their client are kept confidential and cannot be disclosed to third parties, including in legal proceedings, without the client's consent.
- 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**
- Problems are encountered if data in the form of binary files

Attorney-Client Privilege Investigation

- **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 for each image
 - Compare hash signatures on all files on the original and re-created disks

Attorney-Client Privilege Investigation

- **Steps for conducting an ACP case (cont'd)**
 - 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
 - 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

Attorney-Client Privilege Investigation

- **Steps for conducting an ACP case (cont'd)**
 - 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 the attorney and paralegal in analyzing data

Case Study - Industrial Espionage Investigation



Industrial Espionage Investigation

- 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)

Industrial Espionage Investigation

- Guidelines when initiating an investigation
 - 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

Industrial Espionage Investigation

- Guidelines (cont'd)
 - 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 Investigation

- Planning considerations (cont'd)
 - Determine suspect location in relation to the vulnerable asset
 - Study the suspect's work habits
 - Collect all incoming and outgoing phone logs
- Steps to conducting an industrial espionage case
 - Gather all personnel assigned to the investigation and brief them on the plan
 - Gather resources to conduct the investigation

Industrial Espionage Investigation

- Steps (cont'd)
 - Place surveillance systems at key locations
 - 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

Case Study - Private Sector Investigation



Procedures for Private Sector Investigations

- As an investigator, you need to develop formal procedures and informal checklists
 - To cover all issues important to high-tech investigations
 - Ensures that correct techniques are used in an investigation

Interviews and Interrogations in Investigation

- 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**
 - Process of trying to get a suspect to confess

Interviews and Interrogations in Investigation

- 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

A person wearing a grey hoodie is seen from behind, sitting at a desk. In front of them is a computer monitor displaying some code. The background is filled with a digital aesthetic, featuring a grid of binary code (0s and 1s) in green and blue tones. The overall scene suggests a focus on digital technology and cybersecurity.

Next Class

INCS-712: Digital Forensics

Chapter 4 - Digital Forensic Tools

Baljeet Malhotra, PhD