Cyber Forensics

CS 4241

Dr. Anand Kumar Mishra

NIIT University

01 Aug 2022

Who am I?

- Anand
  - or Dr. Anand
- Assistant Professor, NIIT University
- Specialization: Cloud Computing, Cyber Forensics
- Former:
  - Faculty, Dept. of CSE, National Institute of Technology Sikkim
  - Research Scholar, Malaviya National Institute of Technology Jaipur
  - Researcher @ IT Lab, National

Topic -1

- Computer Forensics and Investigation
- Understanding Computer Forensics,
- Preparing for Computer Investigations,
- Maintaining Professional Conduct,
- Preparing a Computer Investigation,
- Taking a Systematic Approach, Procedures for Corporate High-Tech Investigations, Understanding Data Recovery Workstations and Software, Conducting an Investigation

Topic - 2

- Data Acquisition and Processing Crime and Incident Scenes
- Understanding Storage Formats for Digital Evidence,
- Determining the Best Acquisition Method,
- Contingency Planning for Image Acquisitions,
- Using Acquisition Tools,
- Validating Data Acquisitions Performing RAID Data Acquisitions,
- Identifying Digital Evidence Collecting Evidence in Private-Sector Incident Scenes, Processing Law Enforcement Crime Scenes, Preparing for a Search, Securing a Computer Incident or Crime Scene, Seizing Digital Evidence at the

Topic - 3

- Operating system forensics:
- Working with Windows and DOS systems- understanding file systems, exploring Microsoft file structures examining NTFS disks,
- understanding whole disk encryption, windows registry, Microsoft start-up tasks,
- MS Dos start-up tasks, virtual machines Macintosh and Linux Boot Processes and File Systems- Understanding the Macintosh File Structure and Boot Process, Examining UNIX and Linux Disk Structures and Boot Processes.

Topic – 4

- Computer forensic analysis and validation and Current Computer Forensic Tools:
- Determining what data to collect and analyze,
- validating forensic data, addressing data-hiding techniques,
- performing remote acquisitions, evaluating computer forensic tool needs, computer forensic software tools, computer forensic hardware tools,
- validating and testing forensic software.

Topic – 5

- Virtual Machine,
- Network Forensics and Live Acquisition and Email Investigation:
- Network forensic overview, performing live acquisitions, developing standard procedures for network forensics, using network tools,
- examining the honey net project,
- Exploring the role of email in investigations, exploring the role of client and server in email, investigating email crimes and violations,
- understanding email servers, using specialized email forensic tools.

02 Aug 2022

Cyber Forensics

- An electronic discovery technique used to determine and reveal technical criminal evidence
- Computer forensics
- Cross-driven analysis that correlates data from multiple hard drives

Cyber Crime - A Criminal activity

- Committed against- individuals, companies, institutions
- Involves - computer, network, digital devices, mobile technology, Internet
- By cybercriminals or hackers
- Email and internet fraud, Identity fraud, theft of financial data, Malware attacks, Phishing, Distributed DoS attacks
- Cyberextortion - demanding money to prevent a threatened attack
- Cryptojacking - mine cryptocurrency

Cyber Crime - Common Ways

- Email Spoofing - Mail from untrusted IDs
- Sending Malicious File Applications - direct message, gaming, websites, etc.
- Social Engineering - to gain confidence to get information
- Cyber Bullying - harassment
- Identity Theft - using someone’s ID
- Job Frauds - fraudulent representation
- Banking Frauds - fraudulently obtaining money

The Need for Forensics

- Over the last decade, the number of crimes that involve computers has grown
- Aim to assist law enforcement in using computer-based evidence to determine the -
- who
- what
- where
- when
- how for crimes

The Need for Forensics

- Result - Computer and Network Forensics
  - To assure proper presentation of computer crime evidentiary data into court
- Forensic tools and techniques
  - Criminal investigations
  - Computer security incident handling

Forensic tools and techniques

- Operational Troubleshooting
  - Finding the virtual and physical location of a host with an incorrect network configuration
  - Resolving a functional problem with an application
- Log Monitoring - analyzing log entries and correlating log entries across multiple systems
- Data Recovery
- Data Acquisition
- Due Diligence/Regulatory Compliance
  - To protect sensitive information
  - Maintain certain records for audit purposes

CASE STUDY 1- Part A

- Alice is a successful businesswoman who runs a shopping website in cloud. The site serves a number of customers every day and her organization generates a significant amount of profit from it.
  - Therefore, if the site is down even for a few minutes, it will seriously hamper not only their profit but also the goodwill.
- Mallory, a malicious attacker decided to attack Alice's shopping website. She rented some machines in cloud and launched a Distributed Denial of Service (DDoS) attack to the shopping website using those rented machines.
- As a result, the site was down for an hour, which had quite negative impact on Alice's business.

CASE STUDY 1- Part B

- Consequently, Alice asked a forensic investigator to investigate the case. The investigator found that Alice's website records the visiting customer's IP address.
- Analyzing the visiting customers records, the investigator found that Alice's website was flooded by some IP addresses which are owned by a cloud service provider.
- Eventually, the investigator issued a subpoena to the corresponding cloud provider to provide him the network logs for those particular IP addresses.
- On the other hand, Mallory managed to collude with the cloud provider after the attack.
  - Therefore, while providing the logs to the investigator, the cloud provider supplied tampered log to the investigator, who had no way to verify the correctness of the logs.

CASE STUDY 1- Part C

- Under this circumstance, Mallory will remain undetected. Even if the cloud provider was honest, Mallory could terminate her rented machines and left no traces of the attack. Hence, the cloud provider could not give any useful logs to the investigator.

CASE STUDY 2 - Part A

- Mallory worked in a software development company BISoft and there she developed a business analysis algorithm and a business intelligence system for high volume business data.
- The software proved popular among in industry and BISoft reaped large profits from the system.
- Though the company maintains strict rules to protect their intellectual property, Mallory managed to export the code of the developed system to CloudCo’s storage, an arms-length 3rd party CSP.

CASE STUDY 2 - Part B

- Later, Mallory formed her own company and used substantially the same designs and code to develop a business intelligence system.
- BISoft filed a case against Mallory accusing her and her company of stealing intellectual property and Bob, a digital forensics investigator, was assigned to determine the facts.

04 Aug 2022

Computer Forensics Fundamentals

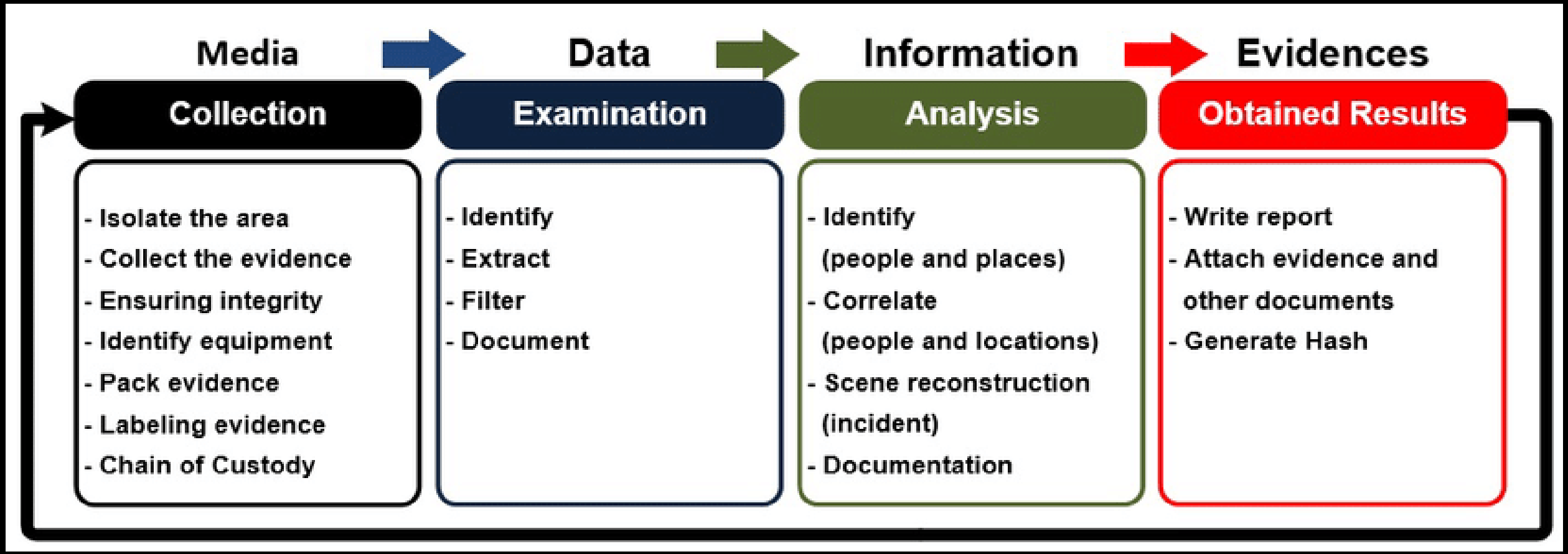
- Basic Methodology
    1. Acquire the evidence without altering or damaging the original
    2. Authenticate that your recovered evidence is the same as the originally seized data
    3. Analyze the data without modifying it.

Acquire the evidence without altering or damaging the original

- Handling the Evidence
- Chain of Custody -
  - Who collected it? How and where?
  - Who took possession of it? How was it stored and protected in storage?
  - Who took it out of storage and why?
- Collection
- Identification
- Transportation
- Storage
- Documenting the Investigation

Authenticate that your recovered evidence is the same as the originally seized data

- Difficult to show that evidence that you've collected is the same as what was left behind by a criminal
- When the evidence was collected - Timestamp
- Proof of integrity and timestamping - Hash Value
  - MD5 and SHA - Commonly uses
  - Create a hash of the entire drive and the individual files


Media
Data
Information
Evidences
Collection
Examination
Analysis
Obtained Results
- Isolate the area
- Collect the evidence
- Ensuring integrity
- Identify equipment
- Pack evidence
- Labeling evidence
- Chain of Custody
- Identify
- Extract
- Filter
- Document
- Identify
(people and places)
- Correlate
(people and locations)
- Scene reconstruction
(incident)
- Documentation
- Write report
- Attach evidence and
other documents
- Generate Hash

Forensic Process - Collection Phases

- To identify, label, record, and acquire data from the possible sources of relevant data
- Following guidelines and procedures
- Preserve the integrity of the data
- Performed in a timely manner because of the likelihood of losing dynamic data such as
  - current network connections
  - battery-powered devices (e.g., cell phones, PDAs)

Forensic Process - Examination Phases

- Forensically processing large amounts of collected data
- Using a combination of automated and manual methods
- To assess and extract data of particular interest
- Preserving the integrity of the data

Forensic Process - Analysis Phases

- To analyze the results of the examination
- Using legally justifiable methods and techniques
- To derive useful information that addresses the questions
- Use of a methodical approach to reach appropriate conclusions based on the available data
- It include correlating data among multiple sources.
  - For instance, a network intrusion detection system (IDS) log may link an event to a host, the host audit logs may link the event to a specific user account, and the host IDS log may indicate what actions that user performed

Forensic Process - Reporting Phases

- Reporting the results of the analysis
- Describing the actions used
  - How tools and procedures were selected,
  - Determining what other actions need to be performed
    - Forensic examination of additional data sources, Securing identified vulnerabilities, Improving existing security controls
- Providing recommendations for improvement to
  - policies, guidelines, procedures, tools, and other aspects of the forensic process
- Step varies greatly depending on the situation

Data Recovery vs Computer Forensics

- Data Recovery
  - Goal to retrieve the lost data
- Computer Forensics
  - Goal to retrieve the data and interpret as much information about it as possible

Benefits of forensics

- Possible to control cyber crime
  - Packet sniffing - sensing critical information in the data packets
  - IP address tracing - to get the address from where the criminal was accessing
  - Email address tracing - to get the details of the email server and in cases of email bombs
- To determine the cause of criminal activities

Benefits of forensics

- To reduce the risk
- To analyze potential risk factors
- Quick identification and extraction of certain risk criteria from the entire data population for further analysis
- The testing for effectiveness of the control environment and policies in place by identifying attributes that violate rules
- The identifying trends of which company personnel, consultants and forensic accountants were unaware

08 Aug 2022

Benefits of Professional Forensics Methodology - Ensure

- No possible evidence is -
  - damaged
  - compromised by the procedures used to investigate the computer
- No possible computer virus is introduced to a subject computer during the analysis process
- Extracted and possibly relevant evidence is properly handled and protected from later mechanical damage
- A continuing chain of custody is established and maintained

Computer Crimes

- Computers can be involved
  - Terrorism, counterintelligence, economic espionage,
  - counterfeiting (to imitate something authentic), and drug dealing
  - The Internet has made targets much more accessible
    - Risks involved for the criminal are much lower than with traditional crimes

Computer Crimes

- White collar crime
  - These are high-dollar crimes made easy by technology
  - health care fraud
  - government fraud including erroneous IRS and Social Security benefit payments, and financial institution fraud
- Violent crime
  - child pornography, interstate theft
- Organized crime
  - Drug dealing, criminal enterprise

Roles of a Computer in a Crime

- A computer can be the target of the crime
- It can be the instrument of the crime
- It can serve as an evidence repository storing valuable information about the crime

Roles of a Computer in searching evidence

- If the computer was used to hack into a network password file -
  - The investigator will know to look for password cracking software and password files
- If the computer was the target of the crime, such as an intrusion -
  - Audit logs and unfamiliar programs should be checked

Computer Forensics Services

- Data seizure
  - Inspect and copy designated documents or data compilations that may contain evidence
- Data duplication and preservation
  - Duplicate of the needed data
  - Maintain the data integrity
    - data must not be altered in any way
    - the seizure must not put an undue burden on the responding party
- Data recovery
  - Forensics experts should be able to safely recover and analyze the data

Computer Forensics Services

- Document searches
  - Extract the relevant data from old and unreadable devices
  - Convert it into readable formats
  - Place it onto new storage media for analysis
- Expert witness services
  - Explain complex technical processes in an easy-to-understand fashion
  - Help judges and juries comprehend about evidence

Computer Forensics Services

- Computer evidence service options
  - Standard service - until critical electronic evidence is found
  - On-site service - evidence collection at your location
  - Emergency service - highest priority to your case
- Other miscellaneous services
  - Analysis of computers and data in criminal investigations
  - On-site seizure of computer data in criminal investigations

Use of Computer Forensics in Law Enforcement

- If there is a computer on the premises of a crime scene
  - Chances are very good that there is **valuable evidence on that computer**
- If the computer and its contents are examined (even if very briefly) by anyone **other than a trained and experienced** computer forensics specialist
  - **Usefulness and credibility of that evidence will be tainted**

Computer Forensics Computer Crime Scene Investigation(2005)

Computer Forensic Evidence

- Authentic
- Accurate
- Complete
- Convincing to juries
- In conformity with common law and legislative rules (i.e., admissible)

Use of Computer Forensics in Law Enforcement

- **Choosing a Computer Forensics Specialist** for a Criminal Case
  - Court will want to know that individual's own level of training and experience
    - Not the experience of his or her employer
  - **Expertise** and **Experience** and Stand up to **Scrutiny** and pressure **of Cross-examination**

Computer Forensic Evidence - Issues

- Computer data changes moment by moment
- Computer data is invisible to the human eye
  - It can only be viewed indirectly after appropriate procedures
- The **process of collecting computer data** may change it—in significant ways
- The processes of opening a file or printing it out are not always neutral
- Computer and telecommunications technologies are always changing so that forensic processes can seldom be fixed for very long

Computer Forensics Computer Crime Scene Investigation(2005)

Computer Forensic Evidence - General Principles

- The scene of crime has to be **frozen**
  - Evidence has to be collected **as early as possible** and without any contamination
- There must be continuity of evidence - **chain of custody**
  - It must be possible to account for all that has happened to the exhibit between its original collection and its appearance in court, preferably **unaltered**
- All procedures used in examination should be **auditable**
  - Suitably **qualified independent expert** appointed by the other side in a case should be able to track all the investigations carried out by the prosecution's experts

Computer Forensics Computer Crime Scene Investigation(2005)