# UNIT-4: Understand Computer Forensics

- Digital Forensics Science
- The Need for Computer Forensics
- Cyber Forensics and Digital Evidence
- Forensics Analysis of E-Mail
- Digital Forensics Life Cycle
- Chain of Custody Concept
- Network Forensics
- Approaching a Computer Forensics Investigation
- Forensics and Social Networking Sites: The Security/Privacy Threats
- Challenges in Computer Forensics

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

# Cyber Security

## (BCC301 / BCC401/ BCC301H / BCC401H)

### Video Overview:

- Computer Forensics
- Digital Forensics Science
- The Need for Computer Forensics
- Cyber Forensics and Digital Evidence
- Forensics Analysis of E-Mail
- Digital Forensics Life Cycle
- Chain of Custody Concept
- Network Forensics
- Approaching a Computer Forensics Investigation
- Challenges in Computer Forensics

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

# UNIT 4

## Computer Forensic Science

**Computer Forensics:** It is a scientific method of investigation and analysis in order to gather evidence from digital devices or computer networks and components which is suitable for presentation in a court of law or legal body. It involves performing a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computer and who was responsible for it.

# UNIT 4

## Types of Computer Forensic

**Disk Forensics:** It deals with extracting raw data from the primary or secondary storage of the device by searching active, modified, or deleted files.

**Network Forensics:** It is a sub-branch of Computer Forensics that involves monitoring and analysing the computer network traffic.

**Database Forensics:** It deals with the study and examination of databases and their related metadata.

**Malware Forensics:** It deals with the identification of suspicious code and studying viruses, worms, etc.

**Email Forensics:** It deals with emails and their recovery and analysis, including deleted emails, calendars, and contacts.

**Memory Forensics:** Deals with collecting data from system memory (system registers, cache, RAM) in raw form and then analysing it for further investigation.

**Mobile Phone Forensics:** It mainly deals with the examination and analysis of phones and smartphones and helps to retrieve contacts, call logs, incoming, and outgoing SMS, etc., and other data present in it.

# UNIT 4

## Digital Forensic Science

- Digital Forensics is a branch of forensic science which includes the identification, collection, analysis and reporting of any valuable digital information in the digital devices related to computer crimes, as a part of the investigation.
- In simple words, Digital Forensics is the process of identifying, preserving, analysing and presenting digital evidence.
- The first computer crimes were recognized in the 1978 Florida computers act and after this,

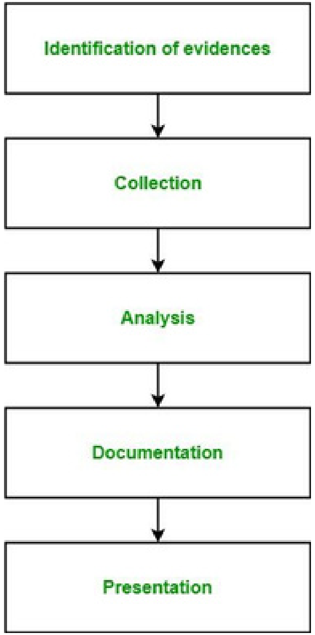
  the
- field of digital forensics grew pretty fast in the late 1980-90's.
  It includes the area of analysis like storage media, hardware, operating system, network and applications.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

# UNIT 4

## How to work Digital Forensic Science

- **Identification of evidence:** It includes identifying evidence related to the digital crime in storage media, hardware, operating system, network and/or applications. It is the most important and basic step.
- **Collection:** It includes preserving the digital evidence identified in the first step so that they don't degrade to vanish with time. Preserving the digital evidence is very important and crucial.
- **Analysis:** It includes analysing the collected digital evidence of the committed computer crime in order to trace the criminal and possible path used to breach into the system.
- **Documentation:** It includes the proper documentation of the whole digital investigation, digital evidence, loopholes of the attacked system etc. so that the case can be studied and analysed in future also and can be presented in the court in a proper format.
- **Presentation:** It includes the presentation of all the digital evidence and documentation in the court in order to prove the digital crime committed and identify the criminal.



Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

# UNIT 4

## Branches of Digital Forensic Science

- **Media forensics:** It is the branch of digital forensics which includes identification, collection, analysis and presentation of audio, video and image evidence during the investigation process.
- **Cyber forensics:** It is the branch of digital forensics which includes identification, collection, analysis and presentation of digital evidence during the investigation of a cyber crime.
- **Mobile forensics:** It is the branch of digital forensics which includes identification, collection, analysis and presentation of digital evidence during the investigation of a crime committed through a mobile device like mobile phones, GPS device, tablet, laptop.
- **Software forensics:** It is the branch of digital forensics which includes identification, collection, analysis and presentation of digital evidence during the investigation of a crime related to softwares only.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

# UNIT 4

## Cyber Forensic

Cyber forensics is a process of extracting data as proof for a crime (that involves electronic devices) while following proper investigation rules to nab the culprit by presenting the evidence to the court. Cyber forensics is also known as computer forensics. The main aim of cyber forensics is to maintain the thread of evidence and documentation to find out who did the crime digitally. Cyber forensics can do the following:

- It can recover deleted files, chat logs, emails, etc
- It can also get deleted SMS, Phone calls.
- It can get recorded audio of phone conversations.
- It can determine which user used which system and for how much time.
- It can identify which user ran which program.

# UNIT 4

## What is Digital Evidence?

- The term “ Digital Evidence” means the information that is transmitted and stored in binary form that can be found in hard disks, mobile phones etc.
- It can be used for prosecution of various crimes but it is generally associated with E-Crimes.
- Digital evidence is described as information and data kept on, received from, or transferred by an electronic device that is useful to an investigation.
- When electronic devices are taken into custody and secured for inspection, this evidence can be obtained.

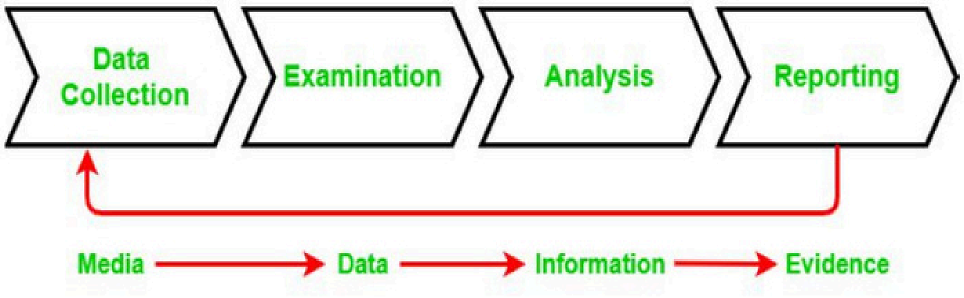
Digital proof –

1. Similar to fingerprints or DNA evidence, it is latent (hidden).
2. Swift and simple jurisdictional border crossing.
3. Can be easily changed, damaged, or destroyed.
4. Potentially time-sensitive.

# UNIT 4

## Process Involved in Digital Evidence Collection

- **Data collection:** In this process data is identified and collected for investigation.
- **Examination:** In the second step the collected data is examined carefully.
- **Analysis:** In this process, different tools and techniques are used and the collected evidence is analysed to reach some conclusion.
- **Reporting:** In this final step all the documentation, reports are compiled so that they can be submitted in court.



Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

# UNIT 4

## Forensic Analysis of E-Mail:

- Email forensics involves the systematic examination and analysis of email data to gather evidence for investigative or legal purposes.
- It plays a crucial role in cybercrime investigations, corporate incidents, and legal proceedings.

1. Collection of Email Evidence:

- **Metadata Extraction:** Collect metadata, including sender and recipient details, timestamps, and email server information.
- **Email Headers:** Examine email headers for routing information and details about the email's journey.
- **Attachments and Content:** Extract and analyse email attachments and content for potential evidence.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

# UNIT 4

## Process Involved in Digital Evidence Collection

2. Preservation of Email Evidence:

- **Original Email Preservation:** Preserve original email content, headers, and metadata to maintain authenticity.
- **Chain of Custody:** Document and maintain a secure chain of custody to track the handling of email evidence.

# UNIT 4

## Process Involved in Digital Evidence Collection

3. Email Analysis Techniques:

- **Keyword Search:** Conduct keyword searches to identify relevant information within email content.
- **Link Analysis:** Analyse relationships between email senders, recipients, and other entities to uncover patterns or connections.
- **Timeline Reconstruction:** Reconstruct timelines of email exchanges to understand the sequence of events.
- **Content Analysis:** Analyse the content of emails for contextual clues, threats, or indications of malicious activity.

# UNIT 4

## Process Involved in Digital Evidence Collection

4. Authentication and Verification:

- **Email Source Verification:** Verify the authenticity of emails by examining the source, SPF/DKIM signatures, and sender information.
- **Sender Authentication:** Validate the identity of the sender through forensic analysis to prevent email spoofing.

5. Investigation of Email Attachments:

- **Malware Analysis:** Conduct analysis on email attachments to identify and characterise potential malware.
- **File Metadata Examination:** Examine metadata of attached files for additional insights into their origin and history.

# UNIT 4

## Process Involved in Digital Evidence Collection

6. Email Header Examination:

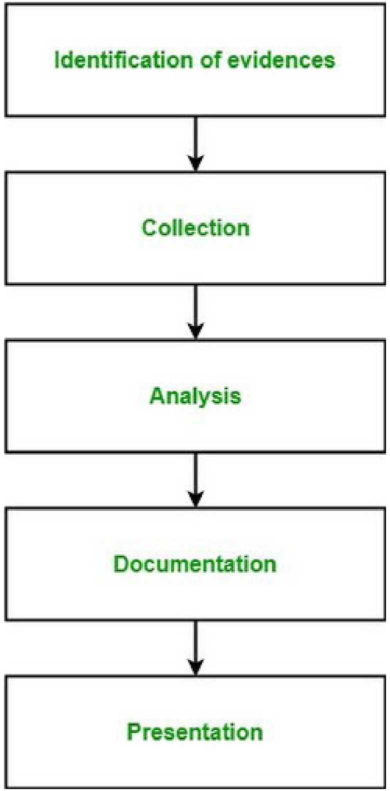
- **IP Address Analysis:** Analyse IP addresses in email headers to trace the geographic location or identify potential malicious activities.
- **Email Routing Analysis:** Examine email routing paths to understand the journey of the email through different servers.

**7. Recovering Deleted Emails:** Employ forensic techniques to recover deleted emails, including examining email server logs and backup systems.

**8. Reporting:** Generate comprehensive reports documenting the findings of the email forensics analysis, including key evidence, methodologies used, and conclusions drawn.

# UNIT 4

## Digital Evidence Life Cycle



- The digital forensics cycle consists of a series of systematic, steps and processes aimed at identifying, collecting, analysing, and preserving digital evidence in a forensically sound manner.
- This life cycle is followed in the investigation of cyber crimes, incidents, or any digital-related legal matters.

# UNIT 4

## Chain of Custody Concept in Digital Forensics

The chain of custody in digital cyber forensics is also known as the paper trail or forensic link, chronological documentation of the evidence.

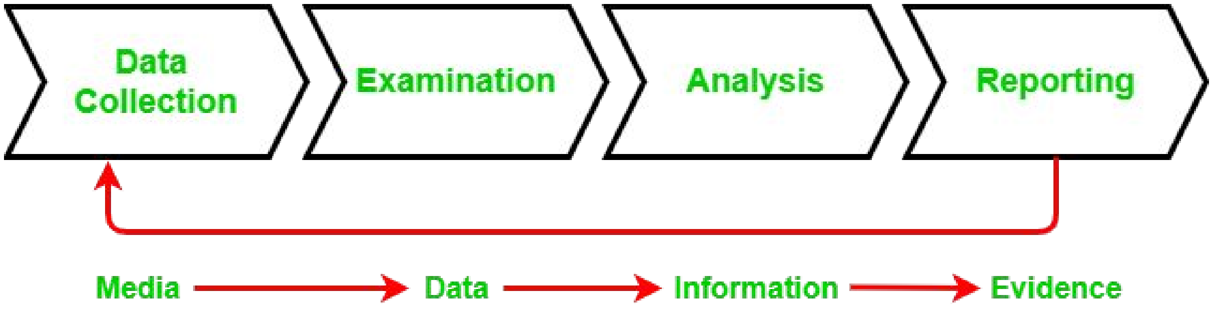
- Chain of custody indicates the collection, sequence of control, transfer and analysis.
- It also documents details of each person who handled the evidence, date and time it was collected or transferred, and the purpose of the transfer.
- It demonstrates trust to the courts and to the client that the evidence has not tampered.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

# UNIT 4

## Chain of Custody Process

In order to preserve digital evidence, the chain of custody should span from the first step of data collection to examination, analysis, reporting, and the time of presentation to the Courts. This is very important to avoid the possibility of any suggestion that the evidence has been compromised in any way.



- **Data Collection:** This is where the chain of custody process is initiated. It involves identification, labelling, recording, and the acquisition of data from all the possible relevant sources that preserve the integrity of the data and evidence collected.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

# UNIT 4

## Chain of Custody Process

- **Examination:** During this process, the chain of custody information is documented outlining the forensic process undertaken. It is important to capture screenshots throughout the process to show the tasks that are completed and the evidence uncovered.
- **Analysis:** This stage is the result of the examination stage. In the Analysis stage, legally justifiable methods and techniques are used to derive useful information to address questions posed in the particular case.
- **Reporting:** This is the documentation phase of the Examination and Analysis stage. Reporting includes the following:

  a. Statement regarding Chain of Custody.
  b. Explanation of the various tools used.
  c. A description of the analysis of various data sources.
  d. Issues identified.
  e. Vulnerabilities identified.

# UNIT 4

## Network Forensics

- Network forensics is a subcategory of digital forensics that essentially deals with the examination of the network and its traffic going across a network that is suspected to be involved in malicious activities, and its investigation for example a network that is spreading malware for stealing credentials or for the purpose analysing the cyber-attacks.
- As the internet grew cyber crimes also grew along with it and so did the significance of network forensics, with the development and acceptance of network-based services such as the World Wide Web, e-mails, and others.
- With the help of network forensics, the entire data can be retrieved including messages, file transfers, e-mails, and, web browsing history, and reconstructed to expose the original transaction.
- It is also possible that the payload in the uppermost layer packet might wind up on the disc, but the envelopes used for delivering it are only captured in network traffic.

# UNIT 4

## Processes Involved in Network Forensics

- **Identification:** In this process, investigators identify and evaluate the incident based on the network pointers.
- **Safeguarding:** In this process, the investigators preserve and secure the data so that the tempering can be prevented.
- **Accumulation:** In this step, a detailed report of the crime scene is documented and all the collected digital shreds of evidence are duplicated.
- **Observation:** In this process, all the visible data is tracked along with the metadata.
- **Investigation:** In this process, a final conclusion is drawn from the collected shreds of evidence.
- **Documentation:** In this process, all the shreds of evidence, reports, conclusions are documented and presented in court.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

# UNIT 4

## Approaching a computer Forensics investigation

The phases in a computer forensics investigation are:

- Secure the subject system
- Take a copy of hard drive/disk
- Identify and recover all files
- Access/view/copy hidden, protected, and temp files
- Study special areas on the drive
- Investigate the settings and any data from programs on the system
- Consider the system from various perspectives
- Create detailed report containing an assessment of the data and information collected

# UNIT 4

## General Steps in Solving computer Forensics case are

- Prepare for the forensic examination
- Talk to key people about the case and what you are looking for
- Start assembling tools to collect the data and identify the target media
- Collect the data from the target media
- Use a write blocking tool while performing imaging of the disk
- Check emails records too while collecting evidence
- Examine the collected evidence on the image that is created
- Analyse the evidence
- Report your finding to your client

# UNIT 4

## Challenges in computer Forensics

1. **Data Encryption:** Encryption can make it difficult to access the data on a device or network, making it harder for forensic investigators to collect evidence. This can require specialised decryption tools and techniques.
2. **Data Destruction:** Criminals may attempt to destroy digital evidence by wiping or destroying devices. This can require specialised data recovery techniques.
3. **Data Storage:** The sheer amount of data that can be stored on modern digital devices can make it difficult for forensic investigators to locate relevant information. This can require