

# Kurumbapalayam (Po), Coimbatore - 641 107

# AN AUTONOMOUS INSTITUTION

# Accredited by NAAC-UGC with 'A' Grade, Accredited by NBA Approved by AICTE & Affiliated to Anna University, Chennai.

#### Forensic Technologies and Their Applications in Computer Investigations

#### Introduction

- Objective:
  - o To provide an overview of different forensic technologies and their applications throughout the various stages of a computer investigation.
- Importance:
  - Understanding these technologies helps forensic professionals effectively collect, analyze, and preserve digital evidence.

### 1. Stages of a Computer Investigation

- 1. Preparation and Planning
- 2. Evidence Collection
- 3. Evidence Preservation
- 4. Evidence Analysis
- 5. Presentation and Reporting

# 2. Forensic Technologies and Their Applications

#### 2.1. Preparation and Planning

- Incident Response Tools
  - o Role:
    - Tools and frameworks used to plan and prepare for potential incidents and to manage the initial response.
  - Examples:
    - **IR Frameworks:** NIST Cybersecurity Framework, SANS Critical Security Controls.
  - o Applications:
    - Developing incident response plans, conducting risk assessments, and preparing response toolkits.

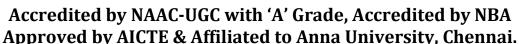
#### 2.2. Evidence Collection

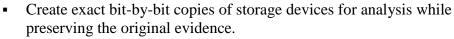
- Disk Imaging Tools
  - o Role:



# Kurumbapalayam (Po), Coimbatore – 641 107

# AN AUTONOMOUS INSTITUTION





- Examples:
  - **FTK Imager:** Captures disk images and provides preview functionality.
  - **dd** (Unix/Linux): A command-line tool for creating disk images.
- Applications:
  - Collecting data from hard drives, SSDs, and other storage media.

# • Memory Dump Tools

- o Role:
  - Capture the contents of volatile memory (RAM) for analysis of active processes and system state.
- Examples:
  - Volatility: An open-source framework for analyzing memory dumps.
  - **FTK Imager:** Also used for capturing memory images.
- Applications:
  - Analyzing running processes, network connections, and system artifacts.

#### • Network Forensics Tools

- o Role:
  - Capture and analyze network traffic to detect and investigate suspicious activities.
- Examples:
  - **Wireshark:** A network protocol analyzer for capturing and examining network packets.
  - **tcpdump:** A command-line tool for network traffic analysis.
- Applications:
  - Investigating network intrusions, analyzing traffic patterns, and detecting anomalies.

#### 2.3. Evidence Preservation

- Write-Blocking Tools
  - o Role:
    - Prevent modification of data during the evidence collection process.
  - Examples:
    - Hardware Write-Blockers: Devices that allow read-only access to storage media.
    - **Software Write-Blockers:** Tools that provide write-blocking functionality at the software level.
  - Applications:
    - Ensuring the integrity of digital evidence during collection.
- Hashing Tools
  - o Role:
    - Generate cryptographic hash values to verify the integrity of data.



# Kurumbapalayam (Po), Coimbatore – 641 107

# AN AUTONOMOUS INSTITUTION

# Accredited by NAAC-UGC with 'A' Grade, Accredited by NBA Approved by AICTE & Affiliated to Anna University, Chennai.



- MD5/SHA-1/SHA-256: Hash algorithms used for integrity checks.
- **HashCalc:** A tool for computing hash values of files.

#### Applications:

 Verifying that evidence has not been altered and maintaining the chain of custody.

#### 2.4. Evidence Analysis

#### Forensic Analysis Software

- o Role:
  - Analyze disk images, memory dumps, and other data to uncover relevant evidence.

#### Examples:

- **EnCase:** A comprehensive forensic analysis tool for examining file systems, emails, and more.
- **Cellebrite UFED:** Specialized in mobile device forensics.

#### Applications:

 Data recovery, file analysis, and identifying artifacts related to criminal activities.

#### Malware Analysis Tools

- o Role:
  - Analyze and understand malicious software to determine its behavior and impact.

#### Examples:

- **IDA Pro:** A disassembler and debugger for reverse engineering malware.
- Cuckoo Sandbox: An open-source automated malware analysis system.

### o Applications:

 Understanding malware behavior, identifying indicators of compromise, and developing mitigation strategies.

#### • Data Carving Tools

- o Role:
  - Recover deleted or fragmented files from disk images or raw data.

#### Examples:

- **PhotoRec:** A tool for recovering lost files from various file systems.
- **Scalpel:** A file carving tool for recovering files from disk images.

#### Applications:

 Recovering files that have been deleted or fragmented, which may contain critical evidence.

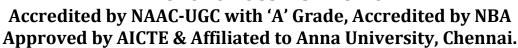
#### 2.5. Presentation and Reporting

• Reporting Tools



# Kurumbapalayam (Po), Coimbatore – 641 107

#### AN AUTONOMOUS INSTITUTION



#### o Role:

• Generate comprehensive reports detailing findings and evidence for legal and investigative purposes.

#### • Examples:

- **X1 Social Discovery:** Provides reporting and analysis capabilities for social media and online content.
- Case Management Systems: Tools for documenting evidence and managing case details.

#### Applications:

 Creating detailed reports of findings, supporting legal proceedings, and communicating results to stakeholders.

#### • Visualization Tools

- o Role:
  - Create visual representations of data to aid in the understanding and presentation of findings.

#### Examples:

- Maltego: A tool for link analysis and visualization of relationships between entities.
- **i2 Analyst's Notebook:** A tool for visualizing and analyzing complex data sets.

#### Applications:

 Presenting evidence in a clear and understandable manner for courtrooms or investigations.

#### Conclusion

#### **Summary:**

- **Preparation and Planning:** Use incident response frameworks to prepare for and manage incidents.
- **Evidence Collection:** Utilize disk imaging, memory dump, and network forensics tools to gather evidence.
- Evidence Preservation: Apply write-blocking and hashing tools to maintain evidence integrity.
- Evidence Analysis: Employ forensic analysis software, malware analysis tools, and data carving techniques to investigate data.
- **Presentation and Reporting:** Generate comprehensive reports and use visualization tools to effectively present findings.

#### **Key Takeaway:**



# Kurumbapalayam (Po), Coimbatore - 641 107

# AN AUTONOMOUS INSTITUTION

# Accredited by NAAC-UGC with 'A' Grade, Accredited by NBA Approved by AICTE & Affiliated to Anna University, Chennai.

• A range of forensic technologies supports each stage of a computer investigation, from initial preparation to final presentation. Leveraging these technologies effectively ensures a thorough and successful investigation.

These notes provide an overview of the forensic technologies available and their specific applications across the stages of a computer investigation. Understanding these tools and their uses is essential for effective digital forensic practices.