INTERNSETU

Code. Secure. Succeed.

BUILD SKILLS
SOLVE REAL INCIDENTS
SHAPE YOUR FUTURE

CYBER FORENSICS

INVESTIGATE • ANALYZE • UNCOVER

From Devices to the Cloud — Follow the Evidence Everywhere



ANALYZE EVIDENCE

RECONSTRUCT TIMELINES

TRACE CONNECTIONS

SOLVE CASES

CYBER FORENSICS - TRAINING

INVESTIGATE / ANALYZE / UNCOVER



You start here

Cyber Forensics – Tools

- FTK Imager
- Autopsy
- Volatility
- EnCase Forensic
- Wireshark
- Magnet AXIOM
- X-Ways Forensics
- Sleuth Kit
- CAINE / SANS SIFT Workstation
- Eric Zimmerman's Tools (EZ Tools)
- Oxygen Forensic Detective
- Registry Viewer / FTK Registry Viewer

Domain 1:
Fundamentals of Digital Forensics & Chain of Custody

Domain 2:
Disk, File System & Artifact Analysis
(FAT, NTFS, EXT, APFS)

Domain 3:
Memory Forensics & RAM Analysis

Domain 4:
Network, Cloud & Mobile Forensics

Certified Cyber Forensics Expert

DIGITAL EVIDENCE BUILDS JUSTICE

INTERNSETU

Code. Secure. Succeed.



COURSE

CYBER FORENSICS TRAINING COURSE

Cyber Forensics Training course is designed to equip security professionals, incident responders, and law enforcement personnel with the technical skills needed to investigate digital crimes and cyber incidents.

INVESTIGATE
ANALYZE
RECONSTRUCT
MAKE AN IMPACT

WHO IS THIS COURSE FOR?

Security professionals, incident responders, and law enforcement personnel who want to build expertise in digital investigations and cyber crime analysis.

HANDS-ON LEARNING AND REAL-WORLD SCENARIOS

Gain practical skills through hands-on labs and real-world incident scenarios, covering the complete digital investigation lifecycle.

THE DIGITAL INVESTIGATION LIFECYCLE

Learn from initial evidence acquisition and volatile memory extraction to deep file system analysis and network traffic inspection.

INDUSTRY-STANDARD TOOLS

Get hands-on experience with FTK Imager, Autopsy, Volatility, and Magnet AXIOM to analyze disk images, registry artifacts, mobile devices, and cloud environments.

CHAIN OF CUSTODY

Follow strict procedures to maintain the integrity and admissibility of digital evidence throughout the investigation process.

COMPLEX INCIDENT ANALYSIS & REPORTING

Reconstruct cyber incidents, uncover hidden artifacts, and create court-ready forensic reports.

THE END RESULT

By the end of the program, learners will possess the knowledge and practical skills to investigate cyber incidents, and earn the **Certified Cyber Frorensics Expert** credential.



INTERNSETU

Code. Secure. Succeed.



COURSE OBJECTIVES

This course provides the core technical skills and legal frameworks required to excel in digital forensics and incident response. Designed for aspiring analysts and IT professionals, the program bridges theoretical principles with practical industry execution.

By completing this training, participants will be able to:

01

MASTER FORENSIC ACQUISITION

Learn to identify, isolate, and preserve digital evidence across storage media, memory, and mobile devices while maintaining a strict chain of custody.

02

ANALYZE FILE SYSTEMS & ARTIFACTS

Decode Windows, Linux, and macOS file systems to reconstruct user activity, extract hidden data, and recover deleted files.

03

EXECUTE RAM & VOLATILE MEMORY ANALYSIS

Capture and analyze live memory dumps to detect hidden processes, malware execution, and unencrypted credentials using tools like Volatility.

04

PERFORM NETWORK & CLOUD INVESTIGATIONS

Trace malicious network traffic, analyze packet captures with Wireshark, and investigate cloud-based security incidents.

05

UTILIZE INDUSTRY-STANDARD TOOLS

Gain hands-on experience with leading forensic suites, including FTK Imager, Autopsy, and Magnet AXIOM.

06

DRAFT COURT-READY REPORTS

Document findings accurately and compile comprehensive forensic audit reports suitable for legal proceedings, internal investigations, and compliance requirements.

BUILD SKILLS. SOLVE REAL CASES.

MAKE A SAFER DIGITAL WORLD.



INTERNSETU

Code. Secure. Succeed.



WHY GET CERTIFIED CYBER FORENSIC EXPERT?

More than a certification — it's your gateway to a secure career, global opportunities, and the skills to make a real impact.

SKILLS
CREDIBILITY
OPPORTUNITY
IMPACT

1 HIGH-DEMAND, FUTURE-PROOF CAREER

Rising Cybercrime
With global cyberattacks, ransomware, and corporate data breaches at an all-time high, organizations urgently need specialists who can investigate how incidents occurred and who was responsible.

Specialized Job Roles
Opens direct pathways to high-paying positions such as Digital Forensics Investigator, Incident Response Specialist, Malware Analyst, and Cyber Crime Investigator.

2 BRIDGE THE GAP BETWEEN IT AND LAW

Court-Admissible Evidence
Technical knowledge alone isn't enough; certified professionals learn strict Chain of Custody protocols to ensure digital evidence is legally valid in court.

Regulatory Compliance
Helps organizations satisfy legal and industry compliance standards (such as ISO 27001, GDPR, HIPAA, and PCI-DSS) during audit and incident investigations.

3 MASTER ADVANCED TECHNICAL & FORENSIC SKILLS

Deep Systems Visibility
Go beyond basic cybersecurity to recover deleted, encrypted, or hidden files across file systems, volatile memory (RAM), mobile devices, and cloud environments.

Hands-On Tool Expertise
Validates practical experience with enterprise forensic tools like FTK Imager, Autopsy, Volatility, EnCase, and Magnet AXIOM.

4 GLOBAL RECOGNITION & PROFESSIONAL CREDIBILITY

Industry Trust
A recognized certification serves as proof of expertise to employers, law enforcement agencies, and corporate clients.

Expert Witness Authority
Provides the foundational credibility required to testify as an expert witness in legal proceedings and corporate disputes.

CERTIFIED CYBER FORENSIC EXPERT

INVESTIGATE / ANALYZE / MAKE AN IMPACT

INTERNSETU

Code. Secure. Succeed.



PREREQUISITES

Build the foundation. Be ready for the challenge.

THE RIGHT FOUNDATION LEADS TO REAL EXPERTISE.



BASIC COMPUTER & NETWORKING FUNDAMENTALS

Understanding of basic operating system concepts (Windows/Linux) and fundamental networking principles (TCP/IP, IP addressing, and common ports).

FUNDAMENTAL SECURITY KNOWLEDGE

A foundational understanding of general cybersecurity concepts, threat types, and basic IT security principles.

BASIC COMMAND-LINE FAMILIARITY

Comfort with navigating command-line interfaces (such as Windows Command Prompt/PowerShell or Linux Terminal) for running basic scripts and tools.

TARGET AUDIENCE

Who Should Enroll?

DIFFERENT BACKGROUNDS.
ONE MISSION.
A SAFER DIGITAL WORLD.

01



CYBERSECURITY PROFESSIONALS & SOC ANALYSTS

Security analysts, incident responders, and IT administrators looking to specialize in digital evidence collection, threat hunting, and deep forensic investigations.

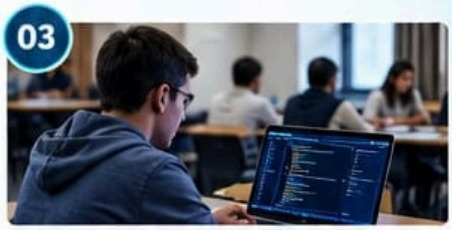
02



LAW ENFORCEMENT & LEGAL PROFESSIONALS

Investigators, law enforcement personnel, and legal auditors who need to understand digital evidence handling, chain of custody, and forensic reporting for court cases.

03



COMPUTER SCIENCE STUDENTS & IT GRADUATES

Aspiring tech professionals and computer science graduates aiming to build a high-demand career in digital forensics, incident response, and cyber crime investigation.

INTERNSETU
Code. Secure. Succeed.



INVESTIGATE
ANALYZE
RECOVER
PROTECT

DIGITAL FORENSICS TOOLS & TECHNOLOGIES

Industry-Standard Tools for Real-World Investigations

RIGHT TOOLS.
DEEPER INSIGHTS.
STRONGER EVIDENCE.

01 ALL-IN-ONE FORENSIC SUITES

Autopsy
A popular open-source, GUI-based digital forensics platform used by law enforcement and corporate investigators to analyze hard drives, mobile devices, and media cards.

FTK (Forensic Toolkit)
An industry-standard court-accepted suite built for fast index searching, heavy data processing, and complex multi-device investigations.

MAGNET AXIOM
A leading forensic platform that recovers, analyzes, and reports on digital evidence from mobile devices, computers, cloud services, and IoT devices in a single case file.

EnCase Forensic
A long-standing enterprise investigation tool known for deep disk analysis, encrypted drive decryption, and court-admissible evidence reporting.

02 DISK ACQUISITION & FILE SYSTEM ANALYSIS

FTK Imager
A free tool designed for creating bit-stream forensic images of hard drives and media without altering original evidence, while also allowing quick previewing of file systems.

The Sleuth Kit (TSK)
A collection of command-line tools that allow investigators to inspect volume and file system data (NTFS, FAT, EXT, APFS) to recover deleted files and hidden artifacts.

X-Ways Forensics
A lightweight, highly efficient forensic environment favoured for its speed, low resource usage, and deep raw disk editing capabilities.

03 MEMORY (RAM) FORENSICS

Volatility Framework
The world's most widely used open-source memory forensics framework for extracting artifact data from volatile RAM (e.g., active network connections, running malware, process trees).

WinPmem / LiME
Lightweight tools used to capture live RAM dumps from Windows and Linux operating systems without corrupting volatile evidence.

04 WINDOWS ARTIFACT & REGISTRY ANALYSIS

Eric Zimmerman's Tools (EZ Tools)
A collection of specialized utilities (such as KAPE, AmcacheParser, and Registry Explorer) designed to quickly parse Windows system artifacts like Prefetch, Shimcache, and Registry hives.

Registry Viewer / FTK Registry Viewer
Specialized tools used to open and inspect Windows Registry files to identify logged-in users, connected USB devices, and auto-start applications.

05 NETWORK & CLOUD FORENSICS

Wireshark
The standard open-source packet analyzer used to capture network traffic, inspect packet details, and reconstruct unencrypted communications during an incident response.

NetworkMiner
A Network Forensic Analysis Tool (NFAT) that extracts files, images, credentials, and session details directly from network packet capture (PCAP) files.

06 MOBILE & SPECIALIST FORENSICS

Cellebrite UFED
The premier hardware and software solution used by law enforcement globally to extract and bypass security on iOS and Android devices.

Oxygen Forensic Detective
A multi-platform forensic software specializing in extracting data from mobile devices, cloud backups, and IoT logs.

CAINE / SANS SIFT Workstation
Dedicated Linux distributions pre-packaged with hundreds of incident response and digital forensic tools for immediate deployment.

THE RIGHT TOOLS UNLOCK
THE TRUTH

FIND EVIDENCE | ANALYZE DATA | BUILD CASES | MAKE AN IMPACT

INTERNSETU

Code. Secure. Succeed.



DOMAIN 1
FUNDAMENTALS OF DIGITAL FORENSICS & CHAIN OF CUSTODY

This foundational domain introduces the core principles, legal guidelines, and operational procedures required to handle digital evidence correctly from the moment an incident is discovered.

RIGHT PROCESS.
LEGAL STANDARDS.
ADMISSIBLE EVIDENCE.

KEY TOPICS COVERED

01 INTRODUCTION TO DIGITAL FORENSICS

Understanding the scope of digital forensics, the role of an investigator, and the fundamental rules governing digital evidence.

02 THE FORENSIC PROCESS LIFE CYCLE

Master the standard step-by-step workflow:

- **Identification** – Locating digital devices and potential sources of evidence.
- **Preservation** – Isolating and securing devices to prevent data alteration or destruction.
- **Collection & Acquisition** – Creating forensically sound, bit-stream copies (forensic images) of target media.
- **Analysis** – Extracting, searching, and evaluating data to reconstruct events.
- **Reporting** – Documenting findings and generating legal-grade technical reports.

03 CHAIN OF CUSTODY (CoC)

Creating and maintaining rigorous evidence logs that document who collected, accessed, transferred, and stored evidence to ensure it remains admissible in a court of law.

04 LOCARD'S EXCHANGE PRINCIPLE IN CYBERSPACE

Understanding how digital interactions leave traces and how to identify digital footprints left by attackers.

05 LEGAL FRAMEWORKS & ETHICS

Navigating search warrants, privacy laws, regulatory standards, and professional codes of ethics during an investigation.

06 EVIDENCE HANDLING & ANTI-STATIC SAFETY

Physical handling of storage devices, write-blockers (hardware and software), write-protection techniques, and secure storage practices.

BUILD THE SKILLS. FOLLOW THE PROCESS.

PRESERVE THE TRUTH.

INTERNSETU
Code. Secure. Succeed.



DOMAIN 2

DISK, FILE SYSTEM & ARTIFACT ANALYSIS

PAGE 1: CORE DISK CONCEPTS & FILE SYSTEM ARCHITECTURES

UNDERSTAND THE STORAGE. UNCOVER THE EVIDENCE.

MODULE OVERVIEW

Domain 2 forms the technical backbone of digital forensics. Investigations rarely rely on simple file browsing; attackers often hide, alter, or delete evidence at the drive level. This module equips students with the skills to decode physical storage structures, analyze file system metadata, and extract artifacts hidden deep within media.



1 STORAGE ARCHITECTURE & DISK STRUCTURE

Before examining file systems, investigators must understand how data is physically and logically stored on non-volatile media.

Physical vs. Logical Drives
Understanding sectors, tracks, cylinders, clusters, and drive partitioning formats (MBR vs. GPT).

Hexadecimal & Binary Analysis
Navigating raw drive images using hex editors to identify file headers, trailers, and sector signatures.

Unallocated Space vs. Slack Space

- **Unallocated Space:** Regions of the drive not assigned to active files, frequently containing deleted data.
- **File Slack & RAM Slack:** The unused bytes within an allocated cluster that can hide remnants of previous data or concealed payloads.

2 DEEP-DIVE INTO MAJOR FILE SYSTEMS

A. FAT (FAT16, FAT32, exFAT)

- **Structure:** File Allocation Table, Boot Sector, Directory Entries, and Data Area.
- **Forensic Significance:**
  - Simple architecture makes manual recovery straightforward.
  - Examination of directory entries to retrieve deleted file markers (e.g., 0xE5).
  - Analysis of timestamp handling and file attributes.

B. NTFS (New Technology File System)

- **The Master File Table (MFT):** The heart of NTFS where every file and folder is tracked as ta record.
- **MFT Attributes:** $STANDARD_INFORMATION (SI) and $FILE_NAME (FN).
- **Timestomping Detection:** Comparing SI and FN timestamps to identify anti-forensic manipulation.
- **Alternate Data Streams (ADS):** Hide malicious payloads (filename.txt:hidden.exe).
- **NTFS Log Files:** Analyzing $LogFile and $UsnJrnl (Change Journal).

3 EXT (EXT3 / EXT4 - LINUX SYSTEMS)

- **Inodes & Superblocks:** How Linux systems organize data structures, file permissions, ownership (UID/GID), and pointers to data blocks.
- **Inode Tables:** Analyzing creation time (crtime), access time (atime), modification time (mtime), and status change time (ctime).
- **Journaling Forensics:** Utilizing JBD2 logs to track uncommitted changes and recently deleted files.

4 APFS (APPLE FILE SYSTEM)

- **Copy-on-Write Architecture:** Understanding how APFS avoids metadata overwrite during updates, preserving historical sanpshots.
- **Containers & Volumes:** Analyzing dynamic space allocation across multiple logical volumes inside a single container.
- **Decryption & FileVault:** Techniques for mounting and decrypting encrypted APFS volumes using recovery keys or user credentials.

FROM BITS TO BREAKTHROUGHS

ANALYZE • RECONSTRUCT • DELIVER



INTERNSETU
Code. Secure. Succeed.



DOMAIN 2

DISK, FILE SYSTEM & ARTIFACT ANALYSIS

PAGE 1: CORE DISK CONCEPTS & FILE SYSTEM ARCHITECTURES

UNDERSTAND THE STORAGE. UNCOVER THE EVIDENCE.

MODULE OVERVIEW

Domain 2 forms the technical backbone of digital forensics. Investigations rarely rely on simple file browsing; attackers often hide, alter, or delete evidence at the drive level. This module equips students with the skills to decode physical storage structures, analyze file system metadata, and extract artifacts hidden deep within media.



1 STORAGE ARCHITECTURE & DISK STRUCTURE

Before examining file systems, investigators must understand how data is physically and logically stored on non-volatile media.

Physical vs. Logical Drives
Understanding sectors, tracks, cylinders, clusters, and drive partitioning formats (MBR vs. GPT).

Hexadecimal & Binary Analysis
Navigating raw drive images using hex editors to identify file headers, trailers, and sector signatures.

Unallocated Space vs. Slack Space

- **Unallocated Space:** Regions of the drive not assigned to active files, frequently containing deleted data.
- **File Slack & RAM Slack:** The unused bytes within an allocated cluster that can hide remnants of previous data or concealed payloads.

2 DEEP-DIVE INTO MAJOR FILE SYSTEMS

A. FAT (FAT16, FAT32, exFAT)

- **Structure:** File Allocation Table, Boot Sector, Directory Entries, and Data Area.
- **Forensic Significance:**
  - Simple architecture makes manual recovery straightforward.
  - Examination of directory entries to retrieve deleted file markers (e.g., 0xE5).
  - Analysis of timestamp handling and file attributes.

B. NTFS (New Technology File System)

- **The Master File Table (MFT):** The heart of NTFS where every file and folder is tracked as ta record.
- **MFT Attributes:** $STANDARD_INFORMATION (SI) and $FILE_NAME (FN).
- **Timestomping Detection:** Comparing SI and FN timestamps to identify anti-forensic manipulation.
- **Alternate Data Streams (ADS):** Hide malicious payloads (filename.txt:hidden.exe).
- **NTFS Log Files:** Analyzing $LogFile and $UsnJrnl (Change Journal).

3 EXT (EXT3 / EXT4 - LINUX SYSTEMS)

- **Inodes & Superblocks:** How Linux systems organize data structures, file permissions, ownership (UID/GID), and pointers to data blocks.
- **Inode Tables:** Analyzing creation time (crtime), access time (atime), modification time (mtime), and status change time (ctime).
- **Journaling Forensics:** Utilizing JBD2 logs to track uncommitted changes and recently deleted files.

4 APFS (APPLE FILE SYSTEM)

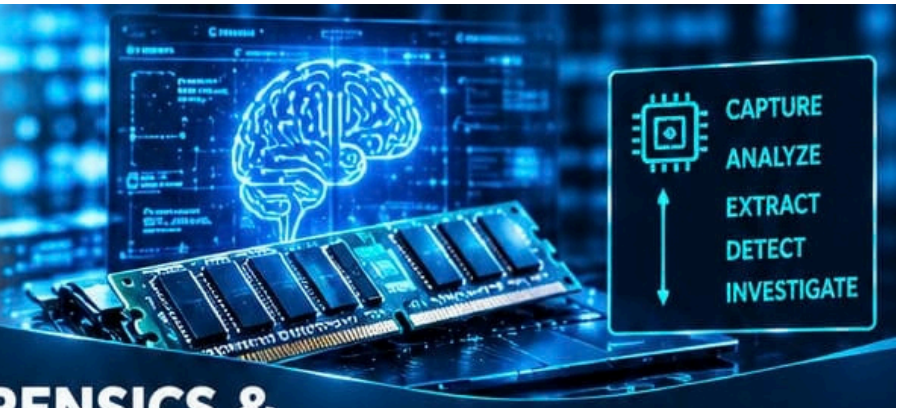
- **Copy-on-Write Architecture:** Understanding how APFS avoids metadata overwrite during updates, preserving historical sanpshots.
- **Containers & Volumes:** Analyzing dynamic space allocation across multiple logical volumes inside a single container.
- **Decryption & FileVault:** Techniques for mounting and decrypting encrypted APFS volumes using recovery keys or user credentials.

FROM BITS TO BREAKTHROUGHS

ANALYZE • RECONSTRUCT • DELIVER



INTERNSETU
Code. Secure. Succeed.



DOMAIN 3:

MEMORY FORENSICS & RAM ANALYSIS

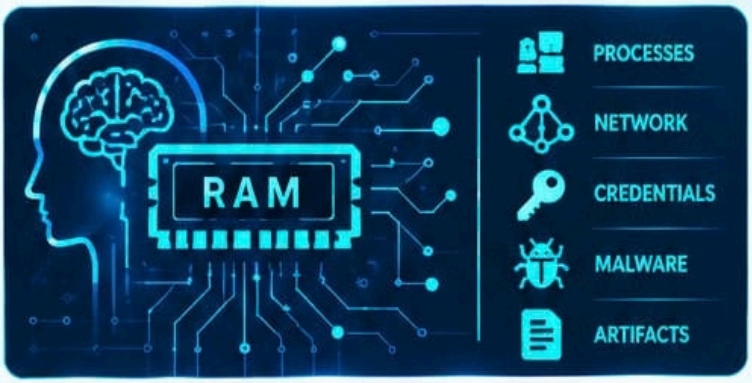
Uncover what's running. Find what's hidden.

LIVE MEMORY.
HIDDEN PROCESSES.
REAL EVIDENCE.

Module Overview

Volatile memory (RAM) holds critical operational evidence that disappears as soon as a machine powers down. While traditional disk forensics captures historical data stored on a drive, memory forensics allows investigators to inspect the live, running state of a compromise.

This domain focuses on extracting and analyzing RAM dumps to uncover fileless malware, active network connections, injected code, and unencrypted user credentials.



1 PRINCIPLES OF VOLATILE DATA ACQUISITION

Order of Volatility
- Prioritizing data capture based on life expectancy (Registers/Cache → RAM → Network State → Hard Disk).

Forensic Cleanliness
- Using lightweight, trusted acquisition tools (such as WinPmem, LiME, or FTK Imager) to dump physical RAM while minimizing the memory footprint and avoiding corruption of potential evidence.

Hibernation Files & Page Files
- Extracting volatile traces from persistent OS files, including hiberfil.sys, pagefile.sys, and swap files.

2 DEEP-DIVE PROCESS & KERNEL ANALYSIS

Process Enumeration
- Analyzing active, terminated, and hidden processes by inspecting active memory pools and doubly linked process lists (EPROCESS structures in Windows).

Identifying Process Injection
- Detecting malicious DLL injection, Process Hollowing, and Reflective DLL Loading by evaluating memory page permissions (e.g., PAGE_EXECUTE_READWRITE).

Rootkit & Hook Detection
- Uncovering stealthy rootkits that alter System Service Descriptor Tables (SSDT) or kernel function pointers to hide malicious activity from standard security software.

3 ARTIFACT EXTRACTION FROM RAM

Network Telemetry
- Extracting active TCP/UDP socket connections, listening ports, and remote IP communication logs directly from memory pools.

Credential Recovery
- Carving plaintext passwords, NTLM hashes, Kerberos tickets, and SSH keys directly from memory processes like lsass.exe.

Master Encryption Key Extraction
- Bypassing full-disk encryption by dumping volume master keys (for BitLocker, FileVault, and VeraCrypt) directly from active RAM.

Unencrypted File & Command Recovery
- Recovering unencrypted text, chat logs, PowerShell command-line history, and decrypted browser payloads stored temporarily in system memory.



INTERNSETU
Code. Secure. Succeed.



DOMAIN 4

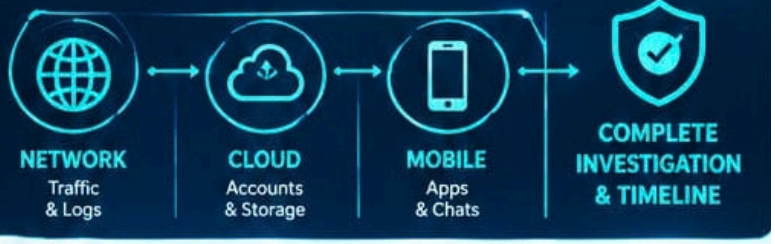
NETWORK, CLOUD & MOBILE FORENSICS

Investigate networks. Analyze the cloud. Extract mobile evidence. Build the bigger picture.

DIFFERENT PLATFORMS. SAME TRUTH.

Module Overview

Modern cybercrime rarely stays confined to a single, isolated computer. Attacks traverse corporate networks, store exfiltrated data in cloud environments, and leverage mobile devices as initial access points. Domain 4 extends forensic capabilities beyond traditional disk and memory investigation, equipping students to track network traffic, investigate multi-tenant cloud platforms, and extract critical evidence from iOS and Android devices.



1 NETWORK FORENSICS & PACKET ANALYSIS

Traffic Capture & Collection
- Promiscuous mode, TAPs, SPAN/mirror ports
- Record PCAP files

Protocol & Packet Analysis
- Wireshark & NetworkMiner
- Reconstruct HTTP/HTTPS, DNS, FTP, SMB

Detecting Covert Channels & Exfiltration
- DNS tunneling, ICMP exfiltration, TOR traffic
- C2 beaconing patterns

Log Analysis
- SIEM, firewall, proxy, IDS/IPS logs
- Track lateral movement

Wireshark | NetworkMiner | SIEM / Firewall Logs

2 CLOUD FORENSICS & INCIDENT RESPONSE

Cloud Architecture Considerations
- Shared responsibility model
- IaaS, PaaS, SaaS

AWS, Azure & Google Cloud Logging
- AWS CloudTrail, VPC Flow Logs, S3 access logs
- Azure Activity Logs, Entra ID sign-in logs
- Storage telemetry

Investigating SaaS & Identity Attacks
- Compromised accounts, API key generation
- OAuth app abuse, storage bucket exfiltration

Live Cloud Acquisition
- VM snapshots, container captures
- Docker / Kubernetes environments

aws | Microsoft Azure | Google Cloud

3 MOBILE DEVICE FORENSICS (iOS & ANDROID)

IOS Forensics
- iTunes backups, keychains
- Property list (.plist) files
- SQLite databases (location, calls, chats)

Android Forensics
- ADB extractions
- Android shared preferences
- App databasse (/data/data/)

Mobile Acquisition Types
- Logical backups
- File system extractions
- Physical (JTAG, ISP, Chip-Off)

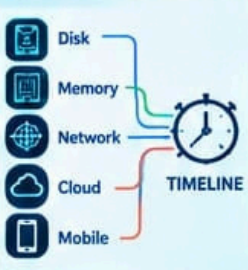
Mobile Artifact Recovery
- WhatsApp, Telegram, Signal
- Deleted SMS, GPS coordinates
- Media metadata

iOS | Android | Cellebrite UFED | Magnet AXIOM

4 ADVANCED EVIDENCE INTEGRATION & TIMELINE ANALYSIS

Cross-Source Correlation
- Merge disk, memory, network, cloud, mobile
- Use Plaso (log2timeline)

Identifying Root Cause
- Entry vector, execution timeline
- Lateral movement paths
- Data exfiltration targets



plaso | log2timeline
ONE TIMELINE. ALL EVIDENCE.

TRACK · ANALYZE · CONNECT

MORE PLATFORMS. MORE EVIDENCE. STRONGER CASES.

