Forebrain — Digital Forensics & Malware Analysis (3 Months / 12 Weeks)

Duration: 3 Months (12 Weeks / 60 instructional days)

Format: 1 hour class + 1 hour lab practice (Monday–Friday). Saturday = Activity Day (practical session based on weekly topics).

Focus: Practical digital forensics, memory and disk analysis, malware behavior analysis, and incident handling.

Outcome: A forensic case report, memory and disk artifacts, malware analysis reports, and a capstone investigation exercise.

Phase-wise Curriculum Overview

Phase 1 — Foundations & Evidence Collection (Weeks 1–3)

- Introduction to digital forensics: principles, disciplines, and legal considerations

- Forensic readiness: chain-of-custody, imaging, documentation and lab setup

- Disk imaging and acquisition: FTK Imager, dd, DC3 tools, write blockers

- File systems and artifact locations (NTFS, FAT, ext4): common forensic artifacts

- Basic memory fundamentals and volatile data collection methods

- Initial triage: timeline creation, triage checklists, and evidence preservation

Deliverable: Acquired disk images and chain-of-custody documentation

Phase 2 — Memory Analysis & Static Malware Analysis (Weeks 4–6)

- Memory forensics concepts and capturing live memory (Volatility, Dumpit)

- Process, network, and DLL analysis from memory dumps

- Static malware analysis: PE headers, strings, imports, and basic unpacking

- Using YARA for malware identification and classification

- Automated sandbox analysis (Cuckoo) and behavioral overview

- Safe handling of samples in isolated lab environments

Deliverable: Memory analysis report + YARA rules for detected samples

Phase 3 — Network Forensics & Threat Attribution (Weeks 7–9)

- PCAP analysis fundamentals with Wireshark and tcpdump

- Network timeline correlation: combining host and network artifacts

- Protocol analysis, DNS, HTTP, SMTP, and command-and-control patterns

- Traffic carving and extraction of transferred artifacts from PCAPs

- Threat attribution basics and open-source intelligence correlation

- Integration with SIEM for forensic data ingestion and historical searches

Deliverable: PCAP analysis report with extracted artifacts and timeline

Phase 4 — Advanced Malware Analysis & Incident Reporting (Weeks 10–12)

- Dynamic malware analysis: sandbox instrumentation, API monitoring, and behavior graphs

- Reverse engineering basics: IDA/Ghidra intro (static code walkthroughs)

- Advanced unpacking, deobfuscation and persistence mechanism analysis

- Correlating forensic findings to produce incident reports and remediation guidance

- Legal and ethical considerations for disclosure and evidence sharing

- Capstone: full investigation from triage to final forensic report

Deliverable: Final forensic investigation report + malware analysis artifacts

Tools & Technologies Covered

Disk & Imaging:

- FTK Imager
- dd
- Sleuth Kit
- Autopsy

Memory & Malware:

- Volatility

- Rekall
- DumpIt
- Cuckoo Sandbox
- YARA

Network Analysis:

- Wireshark
- tcpdump
- Zeek (Bro)

Reverse Engineering:

- Ghidra
- IDA Pro (conceptual)
- radare2

Forensic Workflow:

- Write blockers, FTK, Autopsy, timeline tools (plaso)

Threat Intel & Correlation:

- VirusTotal
- MISP
- OSINT tools

Deliverables & Assessment

- Weekly lab evidence: images, memory dumps, PCAPs, analysis notes
- Memory analysis report and YARA signatures
- Disk forensics case report using Autopsy/Sleuth Kit
- PCAP analysis deliverable and extracted artifacts
- Final capstone forensic investigation report and presentation