

Provide your future forensic experts with in-depth knowledge of Windows memory internals.

Training Outline

Memory Forensics Techniques

Understanding computer and operating system memory and storage structure is a crucial part of modern digital forensics. This advanced training session provides future forensics experts with in-depth knowledge of Windows memory internals, the skills required to analyze memory and system images, and the practical, hands-on experience needed to identify and access data that is critical for a successful investigation.

The training also introduces investigation techniques required for non-Windows platforms, such as OS X and Linux, and imparts live, hands-on experience in memory acquisition and analysis during various exercises in our cyberwarfare arena.



Participants

- Tier 2+3 Security Analysts
- Incident Response Team Members
- Software Developers



Prerequisites

- Understanding of basic information security concepts and tools
- Familiarity with computer and operating system architecture and internals
- Familiarity with basic programming concepts



Training Outcomes

- Acquisition of the skills, methodology and practical experience required to become a Memory Forensics expert
- Ability to expertly manage and investigate ongoing, complex cyberattacks and their consequences, in organizations of all sizes



Duration

- 24 hours (3 x 8-hour days)

#Forensics

#Qualification

#Memory