Blue Team Level 1 Certification (Standard)
TI5) Strategic Threat Intelligence
5 Topics | 1 Quiz
TI6) Malware and Global Campaigns
6 Topics | 1 Quiz
DIGITAL FORENSICS DOMAIN
DF1) Introduction to Digital Forensics
5 Topics
DF2) Forensics Fundamentals
10 Topics | 5 Quizzes
DF3) Digital Evidence Collection
8 Topics | 1 Quiz
Section Introduction, Evidence Collection
Equipment
ACPO Principles of Digital Evidence Collection & Preservation
Chain of Custody
Disk Imaging: FTK Imager
Live Forensics
Live Acquisition: KAPE
Evidence Destruction
Activity) End of Section Review, Evidence Collection
DF4) Windows Investigations
3 Topics | 3 Quizzes
DF5) Linux Investigations
4 Topics | 2 Quizzes
DF6) Volatility
3 Topics | 1 Quiz
DF7) Autopsy
4 Topics | 1 Quiz
SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN
SI1) Introduction to SIEM
7 Topics | 1 Quiz
SI2) Logging
6 Topics | 2 Quizzes
SI3) Aggregation
2 Topics | 1 Quiz
SI4) Correlation
6 Topics | 1 Quiz

Live Forensics

This lesson will cover what live forensics means, and why evidence may be collected in this way. Live forensics is a branch of digital forensics that focuses specifically on computers and other IT systems that are powered on. As we've previously covered, volatile artifacts often only exist while a system is turned on, and shutting the system off would cause these artifacts to be lost. This volatile data could be extremely important to an investigation, so it's crucial to collect it, but not jeopardize other data that could be affected by aspects such as SSDs that use Garbage Collection or TRIM. To acquire volatile data, but not leave the system running for extended periods of time where unnecessary, live forensics techniques can be used to quickly acquire evidence.

WHY IS IT IMPORTANT?

Higher amounts of Random Access Memory (RAM) are being used in modern computers, and the 64-bit operating systems use the whole array of this quick storage to cache and serve data more quickly, so the possibility that evidence is stored in this area is very high. Data stored in RAM quickly fades once a system is powered off, and while there are ways to preserve it, acquiring this information while the system is online is the most effective.

Live forensics can work to battle methods criminals use to prevent analysis such as full disk encryption, using live CDs instead of an installed operating system, and cloud storage is commonly used. Encryption can sometimes be reversed by extracting the encryption key from RAM, and cloud or other internet-based storage can be detected and downloaded while the machine is still running and connected to the service provider.

Live forensics isn't just about acquiring volatile data before it's lost. Having a global organization that has offices in different continents can cause major issues if digital forensics work needs to be carried out at offices where there are not trained individuals with the skills that are needed to conduct such tasks. Live forensics gives a centralized security team the ability to remotely connect into a system while it is powered on and conduct actions such as; viewing any running processes, view active network connections, and take a snapshot of the RAM for later analysis.