Blue Team Level 1 Certification (Standard) ‹

○ TI1) Introduction to Threat Intelligence
● 7 Topics

○ TI2) Threat Actors & APTs
● 6 Topics | 2 Quizzes

○ TI3) Operational Threat Intelligence
● 7 Topics | 1 Quiz

○ TI4) Tactical Threat Intelligence
● 7 Topics | 1 Quiz

○ 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

○ Section Introduction, Digital Forensics

○ What is Digital Forensics?

○ Digital Forensics Process

○ Further Reading Material, Digital Forensics

○ Digital Forensics Glossary

○ DF2) Forensics Fundamentals
● 10 Topics | 5 Quizzes

○ DF3) Digital Evidence Collection
● 8 Topics | 1 Quiz

○ 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

Digital Forensics Process

Blue Team Level 1 Certification (Standard) > DF1) Introduction to Digital Forensics > Digital For… IN PROGRESS

The **digital forensic process** is a recognized scientific and forensic process used in digital forensics investigations (mainly referring to activities conducted by law enforcement, not necessarily security teams conducting digital forensics and incident response (DFIR) activities). The process is predominantly used in computer and mobile device forensic investigations and consists of three steps: *acquisition*, *analysis* and *reporting*. This domain of BTL1 is designed to follow this process, with the sections "**Digital Evidence Collection**", "**Windows Investigations**", "**Linux Investigations**", and "**Post Investigation**".

Digital media seized for investigation is usually referred to as an "exhibit" in legal terminology. Investigators employ the scientific method to recover digital evidence to support or disprove a hypothesis, either for a court of law or in civil proceedings.

The digital forensic process has the following five basic stages:

1. **Identification** – The first stage identifies potential sources of relevant evidence or information (devices), as well as key custodians and location of data.
2. **Preservation** – The process of preserving relevant electronically stored information (ESI). This is done by protecting the crime or incident scene, capturing visual images of the scene, and documenting all relevant information about the evidence and how it was acquired.
3. **Collection** – Collecting digital information that may be relevant to the investigation. Collection may involve removing the electronic device(s) from the crime or incident scene and then imaging, copying or printing out its (their) content.
4. **Analysis** – An in-depth systematic search of evidence relating to the incident being investigated. The outputs of the examination are data objects found in the collected information. These outputs may include system and user-generated files. Analysis aims to draw conclusions based on the evidence found.
5. **Reporting** – Reports are based on proven techniques and methodology and other competent forensic examiners should be able to duplicate and reproduce the same results.

A crucial activity that accompanies the first four steps is **contemporaneous note-taking**. This is the documentation of what you have done immediately after you have completed it and should provide sufficient detail for another person to reproduce what you have done from the notes alone. The chain of custody, which we cover later in this domain, should also be followed at every stage of the investigation to ensure that evidence integrity is not compromised.

‹ Previous Topic

Mark Complete ✓

Next Topic ›

Back to Lesson