Blue Team Level 1 Certification (Standard)

● 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

○ Section Introduction, Forensics Fundamentals

○ Introduction to Data Representation

Activity) Data Representation

○ Hard Disk Drive Basics

○ SSD Drive Basics

○ File Systems

Lab) File Systems

○ Digital Evidence and Handling

○ Order of Volatility

○ Metadata and File Carving

Lab) Metadata and File Carving

○ Memory, Pagefile and Hibernation File

○ Hashing and Integrity

Lab) Hashing and Integrity

Activity) End of Section Review, Forensics Fundamentals

○ 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

● 6 Topics | 1 Quiz

○ SI5) Using Splunk

● 5 Topics | 2 Quizzes

INCIDENT RESPONSE DOMAIN

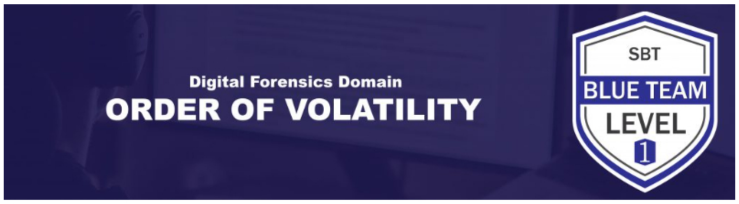
○ IR1) Introduction to Incident Response

● 8 Topics | 1 Quiz

○ IR2) Preparation Phase

Order of Volatility

Blue Team Level 1 Certification (Standard) > DF2) Forensics Fundamentals > Order of Volatility IN PROGRESS



When examining digital evidence, it is important to understand the volatile nature of some of the evidence an examiner will want to look at. Volatile evidence is evidence that can be lost when a system is powered down. For network equipment, this could include active connections or log data that is stored on the device. For laptops and desktops, volatile data includes running memory or the Address Resolution Protocol (ARP) cache.

The Internet Engineering Task Force (IETF) has put together a document titled Guidelines for Evidence Collection and Archiving (RFC 3227) that addresses the order of volatility of digital evidence. You can view and download the document here.

Below we explore the different locations where potential evidence can be retrieved, and how volatile they are, with 1 being the most volatile, and 6 being the least volatile.

1 – Registers & Cache

The contents of CPU cache and registers are extremely volatile, since they are constantly changing. An investigator needs to retrieve data from the cache and register immediately before that evidence is lost.

2 – Memory

The information located on random access memory (RAM) can be lost if there is a power spike or if the system is disconnected from power. This is a fast, temporary, type of memory in which programs, applications and data are stored. This can include very useful data about running processes, network connections, and much more.

3 – Disk (HDD and SSD)

As we covered in the hard disk drive (HDD) and solid-state disk drive (SSD) basics lessons, we know that once data has been overwritten, it is impossible to recover it, and SSDs have the additional risk of Garbage Collection or TRIM deleting files that could be used as evidence. If the system is offline then the disk space can't be overwritten and the disk is no longer considered volatile.

4 – Remote Logging and Monitoring Data

The potential for remote logging and monitoring data to change is much higher than data on a hard drive, but the information is not as vital. So, even though the volatility of the data is higher here, we still want that hard drive data first.

5 – Physical Configuration, Network Topology, Archival Media

Here we have items that are either not that vital in terms of the data or are not at all volatile. The physical configuration and network topology is information that could help an investigation, but is likely not going to have a tremendous impact. Finally, archived data is usually going to be located on a separate physical devices, such as a USB drive or external hard drive.

It is imperative that digital forensics examiners take volatility into account when starting the process of evidence collection. Methods should be employed to ensure that volatile evidence is collected and moved to a non-volatile medium, such as an external hard drive, as quickly as possible.

● 10 Topics | 2 Quizzes

○ IR3) Detection and Analysis Phase

● 7 Topics | 4 Quizzes

○ IR4) Containment, Eradication, and Recovery Phase

● 5 Topics | 1 Quiz

○ IR5) Lessons Learned and Reporting

‹ Previous Topic

Mark Complete ✓

Back to Lesson

Next Topic ›