

Blue Team Level 1 Certification
(Standard)

✓ Networking 101

6 Topics 1 Quiz

✓ Management Principles

4 Topics 1 Quiz

PHISHING ANALYSIS DOMAIN

✓ PA1) Introduction to Emails and Phishing

7 Topics 1 Quiz

✓ PA2) Types of Phishing Emails

10 Topics 2 Quizzes

✓ PA3) Tactics and Techniques Used

12 Topics 2 Quizzes

✓ PA4) Investigating a Phishing Email

8 Topics 2 Quizzes

✓ PA5) Analysing URLs, Attachments, and Artifacts

8 Topics 1 Quiz

○ PA6) Taking Defensive Actions

12 Topics 1 Quiz

○ PA7) Report Writing

7 Topics 1 Quiz

○ PA8) Phishing Response Challenge

3 Topics 1 Quiz

THREAT INTELLIGENCE DOMAIN

○ 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

○ 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

SSD Drive Basics

Blue Team Level 1 Certification (Standard) > DF2) Forensics Fundamentals > SSD Drive Basics

IN PROGRESS

Digital Forensics Domain
SOLID STATE DISK
DRIVE BASICS

Similar to hard disk drives, solid state disk drives (SSDs) are typically where a lot of digital evidence is stored and collected, so understanding how they work and where data can be hidden is important, allowing you to collect artifacts in future lessons. This lesson will cover the following SSD basics:

- Garbage Collection
- Trim
- Wear Leveling

WHAT ARE SSDs?

A solid-state drive (SSD) is a new generation of storage device. SSDs have evolved beyond traditional mechanical hard disks by using flash-based memory which is significantly faster, allowing SSDs to speed up computers significantly because of their low read-access times and fast throughputs. Instead of writing data to a magnetic disk, solid-state disks instead data is written to "pages", and once there's enough, it's written to a "block" on the actual drive.



GARBAGE

Garbage collection is a process used by solid-state drives to optimize space and improve efficiency. The goal of garbage collection is to keep as many empty blocks as possible, so that when the SSD needs to write data, it can do so without waiting for a block to be erased. The SSD's controller looks for any pages that are no longer being used, such as deleted data and modified data. It then moves used pages to new blocks, leaving behind the data that is no

<input checked="" type="radio"/> Lab) Metadata and File Carving
<input type="radio"/> Memory, Pagefile and Hibernation File
<input type="radio"/> Hashing and Integrity
<input checked="" type="radio"/> Lab) Hashing and Integrity
<input checked="" type="radio"/> Activity) End of Section Review, Forensics Fundamentals
<input type="radio"/> DF3) Digital Evidence Collection
<input checked="" type="radio"/> 8 Topics 1 Quiz
<input type="radio"/> DF4) Windows Investigations
<input checked="" type="radio"/> 3 Topics 3 Quizzes
<input type="radio"/> DF5) Linux Investigations
<input checked="" type="radio"/> 4 Topics 2 Quizzes
<input type="radio"/> DF6) Volatility
<input checked="" type="radio"/> 3 Topics 1 Quiz
<input type="radio"/> DF7) Autopsy
<input checked="" type="radio"/> 4 Topics 1 Quiz
SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN
<input type="radio"/> SI1) Introduction to SIEM
<input checked="" type="radio"/> 7 Topics 1 Quiz
<input type="radio"/> SI2) Logging
<input checked="" type="radio"/> 6 Topics 2 Quizzes
<input type="radio"/> SI3) Aggregation
<input checked="" type="radio"/> 2 Topics 1 Quiz
<input type="radio"/> SI4) Correlation
<input checked="" type="radio"/> 6 Topics 1 Quiz
<input type="radio"/> SI5) Using Splunk
<input checked="" type="radio"/> 5 Topics 2 Quizzes
INCIDENT RESPONSE DOMAIN
<input type="radio"/> IR1) Introduction to Incident Response
<input checked="" type="radio"/> 8 Topics 1 Quiz
<input type="radio"/> IR2) Preparation Phase
<input checked="" type="radio"/> 10 Topics 2 Quizzes
<input type="radio"/> IR3) Detection and Analysis Phase
<input checked="" type="radio"/> 7 Topics 4 Quizzes
<input type="radio"/> IR4) Containment, Eradication, and Recovery Phase
<input checked="" type="radio"/> 5 Topics 1 Quiz
<input type="radio"/> IR5) Lessons Learned and Reporting
<input checked="" type="radio"/> 7 Topics
<input type="radio"/> IR6) MITRE ATT&CK
<input checked="" type="radio"/> 13 Topics 2 Quizzes
BTL1 EXAM
<input type="radio"/> Exam Preparation
<input type="radio"/> Using RDP and SSH
<input type="radio"/> How to Start Your Exam

such as deleted data and modified data. It then moves used pages to new blocks, leaving behind the data that is no longer needed. The controller then erases the block so that it's ready for use. This is a background process, handled by the SSD controller and the operating system.

Why is garbage collection important in regard to digital forensics? If we have crucial evidence on a system, there's always the risk that garbage collection will identify the blocks either legitimately or illegitimately as unwanted, and the controller will erase the blocks in order to free up space. If a computer is using solid-state drives, it needs to be powered off immediately to prevent this from happening, either with a hard shut-down (holding the power button until the system turns off), or pulling the plug so the power supply unit (PSU) receives no electricity. Shutting down the system via the operating system could execute a malicious script that works to destroy data contained on any attached drives, and could ruin an investigation (but we need to remember volatile evidence, which we'll cover later!).

TRIM

When files are sent to locations such as the Recycle Bin, they are not immediately deleted. Moving them to this location tells the operating system that it is ok to overwrite these files, as they are no longer wanted by the user. If a deleted file is 174192 bytes, and a new file is only 121 bytes, then there will still be 174071 bytes of the deleted file available, so we can recover this and attempt to fix the file so we can see what it was, even with some missing data. However, TRIM operates similarly to Garbage Collection, and instead of telling the SSD to make the size of the deleted file unallocated (available for overwriting), TRIM on an SSD will simply select the data and clear it, removing any chance of forensic investigations recovering the file, or parts of the file.

To counter this, we should take the same actions when dealing with Garbage Collection, as they work together. Power the system off with a hard shut-down or pull the plug (again, we need to remember volatile evidence, which we'll cover later!).

WEAR LEVELLING

Wear leveling is a technique that some SSDs utilize to increase the lifetime of the memory using a very simple approach: evenly distribute writing on all blocks of an SSD so they wear evenly. Using this method, all physical cells in the SSD receive the same number of writes, to avoid writing too often on the same blocks, causing damage over time.

Wear leveling is performed by the micro-controller or the firmware of the SSD device. The process of wear leveling is conducted by algorithms, of which there are two basic varieties.

- **Dynamic wear leveling** – When dynamic wear leveling is used blocks that undergo rewriting are repositioned to new blocks. The algorithm selects an empty block on which to write the data. The number of writes to each block are kept track of by the controller. A downside to dynamic leveling is that data blocks that are not frequently updated are not moved which can lead to uneven block wear.
- **Static wear leveling** – The same techniques are employed by static wear leveling with one important difference. Blocks of static data are moved when their block erase count falls below a certain threshold. This leads to more effective leveling which results in slightly slower write performance countered with enhanced longevity of the device.