

Blue Team Level 1 Certification  
(Standard)

## Introduction to BTL1

✓ Welcome to Blue Team Level 1

● 4 Topics

✓ Lab and Forum Access

## SECURITY FUNDAMENTALS DOMAIN

✓ Introduction to Security Fundamentals

● 1 Topic

✓ Soft Skills

● 7 Topics

✓ Security Controls

● 5 Topics 1 Quiz

✓ 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 &amp; 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

## Evidence Destruction

Blue Team Level 1 Certification (Standard) &gt; DF3) Digital Evidence Collection &gt; Evidence Destruction

IN PROGRESS

## Digital Forensics Domain

## EVIDENCE DESTRUCTION



This lesson will focus on how digital evidence should be disposed of after the retention period has expired. It is crucial that evidence is securely destroyed, luckily there are a number of methods we can use to achieve this. We will cover:

- Degaussing
- File Shredding
- Physical Shredding
- Hydraulic Crusher
- Overwriting

## DEGAUSSING

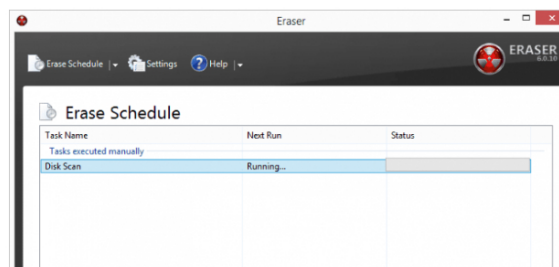
When exposed to the powerful magnetic field of a degausser, the magnetic data on a tape or hard disk is neutralized or erased. Degaussing is the guaranteed form of hard drive erasure, which means that it serves as the standard method of data destruction. Using the right degausser will guarantee that your information is no longer retrievable.



## FILE SHREDDING

File Shredding can sometimes be the same as manually deleting a file or folder, and as we covered at the start of the course, these files can be recovered unless they are overwritten. This is **not** a secure method of deleting digital evidence, as there is the possibility it can be recovered. However, some file shredding programs utilize different methods to overwrite or sanitize the data that has been selected for shredding. One method that is known as the [DoD 5220.22-M Wipe Method](#) includes 3 steps:

- **Pass 1:** Writes a zero and verifies the write.
- **Pass 2:** Writes a one and verifies the write.
- **Pass 3:** Writes a random character and verifies the write.



<input type="radio"/> DF3) Digital Evidence Collection
<div><div></div>8 Topics1 Quiz</div>
<input type="radio"/> Section Introduction, Evidence Collection
<input type="radio"/> Equipment
<input type="radio"/> ACPO Principles of Digital Evidence Collection & Preservation
<input type="radio"/> Chain of Custody
<input type="radio"/> Disk Imaging: FTK Imager
<input type="radio"/> Live Forensics
<input type="radio"/> Live Acquisition: KAPE
<input checked="" type="radio"/> Evidence Destruction
<div><div></div>Activity) End of Section Review, Evidence Collection</div>
<input type="radio"/> DF4) Windows Investigations
<div><div></div>3 Topics3 Quizzes</div>
<input type="radio"/> DF5) Linux Investigations
<div><div></div>4 Topics2 Quizzes</div>
<input type="radio"/> DF6) Volatility
<div><div></div>3 Topics1 Quiz</div>
<input type="radio"/> DF7) Autopsy
<div><div></div>4 Topics1 Quiz</div>
SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN
<input type="radio"/> SI1) Introduction to SIEM
<div><div></div>7 Topics1 Quiz</div>
<input type="radio"/> SI2) Logging
<div><div></div>6 Topics2 Quizzes</div>
<input type="radio"/> SI3) Aggregation
<div><div></div>2 Topics1 Quiz</div>
<input type="radio"/> SI4) Correlation
<div><div></div>6 Topics1 Quiz</div>
<input type="radio"/> SI5) Using Splunk
<div><div></div>5 Topics2 Quizzes</div>
INCIDENT RESPONSE DOMAIN
<input type="radio"/> IR1) Introduction to Incident Response
<div><div></div>8 Topics1 Quiz</div>
<input type="radio"/> IR2) Preparation Phase
<div><div></div>10 Topics2 Quizzes</div>
<input type="radio"/> IR3) Detection and Analysis Phase
<div><div></div>7 Topics4 Quizzes</div>
<input type="radio"/> IR4) Containment, Eradication, and Recovery Phase
<div><div></div>5 Topics1 Quiz</div>
<input type="radio"/> IR5) Lessons Learned and Reporting
<div><div></div>7 Topics</div>
<input type="radio"/> IR6) MITRE ATT&CK
<div><div></div>13 Topics2 Quizzes</div>
BTL1 EXAM
<input type="radio"/> Exam Preparation
<input type="radio"/> Using RDP and SSH
<input type="radio"/> How to Start Your Exam



# PHYSICAL SHREDDING

Physical shredding is the process of destroying physical storage media so that it can't be reassembled and accessed. A hard drive, USB, or other hardware will be shredded into small pieces using industrial-grade destruction equipment. The hard drive shredding process destroys the drive platters, mechanisms, and the electronic components rendering the data unrecoverable.



# HYDRAULIC CRUSHER

The name says it all, this method of destruction uses a hydraulic press with a metal rod that is pushed straight through the hard drive. Punching a hole with approximately 3,400 kilos of force pressure completely destroys the drive platters, rippling and fracturing the magnetic surfaces and rendering the drive data unrecoverable. Other methods can include bending the hard drives until they snap, as shown in the image below.



# OVERWRITING

Organizations may want to reuse hard drives or USBs that have been involved in forensic investigations, so overwriting may be the best option as it doesn't result in physical destruction. As covered at the start of this domain, data is typically still accessible until it has been overwritten. We can simply write zeros to a hard drive, overwriting any existing data. Windows offers a function called Diskpart that allows you to completely clear a hard drive from the command prompt.

[Back to Lesson](#)

[Privacy & Cookies Policy](#)

