

Blue Team Level 1 Certification  
(Standard)

116) 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

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

Section Introduction, Autopsy

What is Autopsy?

Installing Autopsy

Autopsy Walkthrough

Lab) Autopsy For Disk Analysis

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

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

7 Topics

IR6) MITRE ATT&amp;CK

13 Topics 2 Quizzes

## BTL1 EXAM

Exam Preparation

Using RDP and SSH

How to Get Your Exam

## What is Autopsy?

Blue Team Level 1 Certification (Standard) &gt; DF7) Autopsy &gt; What Is Autopsy?

IN PROGRESS



Autopsy is a forensic-grade tool which is used by the military, law enforcement, and corporate examiners to investigate what had happened on a smartphone or a computer. Autopsy has a plug-in architecture which allows the user to find add-on modules or even develop custom modules written in Java or Python, providing additional functionality and automation. This awesome tool comes built-in with Kali Linux, and can also be downloaded and use on systems running the Windows operating system for free.

## Autopsy's Main Features

- **Multi-User Cases:** Collaborate with your fellow examiners on large cases.
- **Keyword Search:** Text extraction and the index searched modules allow you to find the files which mention specific terms and find the regular expression patterns.
- **Timeline Analysis:** Displays system events in a graphical interface to help identify activity. Web Artefacts: Extracts web activity from common browsers to help identify user activity.
- **LNK File Analysis:** Identifies shortcuts and accessed documents.
- **Email Analysis:** Parses MBOX format messages, such as Thunderbird. Registry Analysis: Uses RegRipper to identify recently accessed documents and USB devices. EXIF: Extracts geolocation and camera information from JPEG files.
- **File Type Sorting:** Group files by their type to find all images or documents.
- **Media Playback:** View videos and images in the application and not require an external viewer.
- **Thumbnail viewer:** Displays thumbnail of images to help quick view pictures.
- **Robust File System Analysis:** Support for common file systems, including NTFS, FAT12/FAT16/FAT32/ExFAT, HFS+, ISO9660 (CD-ROM), Ext2/Ext3/Ext4, Yaffs2, and UFS from The Sleuth Kit.
- **Hash Set Filtering:** Filter known good files using NSRL and flags known bad files using custom hash sets in HashKeeper, md5sum, and EnCase formats.
- **Tags:** Tag files with arbitrary tag names, such as 'bookmark' or 'suspicious', and add comments.
- **Unicode Strings Extraction:** Extracts strings from unallocated space and unknown file types in many languages (Arabic, Chinese, Japanese, etc.).
- **File Type Detection** based on signatures and extension mismatch detection.
- **Interesting Files Module** will flag files and folders based on name and path.
- **Android Support:** Extracts data from SMS, call logs, contacts, Tango, Words with Friends, and more.

&lt; Previous Topic

Mark Complete ✓

Back to Lesson

Next Topic &gt;



