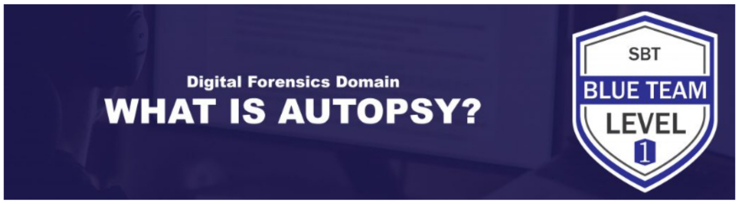
# What is Autopsy?

Blue Team Level 1 Certification (Standard) > DF7) Autopsy > 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.

Previous Topic
Mark Complete ✓
Next Topic
Back to Lesson

○ How to Start Your Exam

Privacy & Cookies Policy

Privacy - Terms