

**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 & 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

File Systems

Blue Team Level 1 Certification (Standard) > DF2) Forensics Fundamentals > File Systems

IN PROGRESS**Digital Forensics Domain
FILE SYSTEMS**

A file system (also known as a filesystem) is a critical part of any IT system. It is a means of classifying and organizing files and storing data, helping to efficiently manage the space available in a device for storing data, so that the required information can be received whenever necessary. The data and the metadata is accessed from the files and directories, using the mechanism provided by the file system. File systems are used in storage devices such as optical disks and magnetic storage disks. In short, a filesystem is a set of data types that is employed for:

- Data storage
- Hierarchical categorization
- Data management
- File navigation
- Accessing the data
- Recovery of data

During investigations you will come across different file systems, and you need to be able to identify and work with them to collect digital evidence. But first, what actually are file systems? A file system is used to control how data is stored and retrieved on a storage medium, such as a hard-disk drive. There are many different kinds of file systems, and each one has a different structure and logic, speed, flexibility, security, size, and more. In this lesson we are going to cover some of the most popular file systems;

- FAT16
- FAT32
- NTFS
- EXT3 / EXT4

FAT16

File Allocation Table is the method of using a table to mark the position of files. FAT16 is the original file system used in DOS and Windows 3. x, and was originally only designed for use on relatively small partitions. If there is an issue, and the File Allocation Table is lost or damaged, the data on the hard disk can't be used because the operating system is unable to locate the files.

FAT32

FAT32 is a revised version of **FAT16** that can be used to create much larger partitions and has native support for long filenames, and was introduced with Win98. The 32 part of its name comes from the fact that FAT32 uses 32 bits of data for identifying data clusters on the storage device. The important advantages of using **FAT32** today are:

- It is compatible with a huge variety of devices: smartphones, tablets, computers, digital cameras, gaming consoles, surveillance cameras and so on.
- It is also cross-compatible with almost all operating systems that were launched since 1995. **FAT32 works with Windows 95 OSR2, Windows 98, XP, Vista, Windows 7, 8, and 10. MacOS and Linux** also support it.

On the other hand, there are some serious disadvantages to using FAT32:

- FAT32 can only work with files that are less than 4 GB in size.
- FAT32 only works with partitions with a maximum capacity of 8 TB.
- If you have a drive that is formatted in FAT32, you do not get any data protection in case of power loss.

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
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&CK
13 Topics 2 Quizzes
BTL1 EXAM
Exam Preparation

- The FAT32 file system does not include any built-in file compression features.
- FAT32 was not designed to be secure and does not include any built-in encryption features.

NTFS

NTFS (NT File System) is a proprietary journaling file system developed by Microsoft. Starting with Windows NT 3.1, it is the default file system of the Windows NT family.

NTFS has several technical improvements over the two file systems that it superseded – File Allocation Table (FAT) and High Performance File System (HPFS) – such as improved support for metadata and advanced data structures to improve performance, reliability, and disk space use. Additional extensions are a more elaborate security system based on access control lists (ACLs) and file system journaling.

NTFS is supported in other desktop and server operating systems as well. Linux and BSD have a free and open-source NTFS driver, called NTFS-3G, with both read and write functionality. MacOS comes with read-only support for NTFS, but due to write support for NTFS being unstable, file writing is disabled by default.

EXT3 / EXT4

Linux Architecture

Before we take a look at EXT3 and EXT4, we’re going to quickly cover the architecture of Linux file systems. These filesystems are divided into three parts:

- **User Space** – The applications are located in the user space, which sends system calls to the system call interface. System call is nothing but a request that is sent to the kernel of the operating system, for a service.
- **Kernel Space** – Kernel is the core of the operating system that answers the system calls from the user space by providing the requested resources, managing the I/O (Input/output) devices, memory devices, file management etc.
- **Disk Space** – The device driver in the kernel space sends the I/O request to the hard disk of the system which contains critical file data.

Third Extended Filesystem (Ext3)

Third extended filesystem (Ext3), is a journaled file system that is commonly used by the Linux kernel. It is the **default file system for many popular Linux distributions**. The changes made in the journal, which is a circular log present in the file system, is monitored by ext3 which is called journaling. Journaling filesystem is an additional feature in ext3, which was not in ext2. In a non-journaled filesystem, data recovery and detecting the errors involved more time, as we may have to go through the entire data structure of the directory. But, in a journaled filesystem, we have a journal that keeps track of the changes we do in the file system. So, to detect the errors or recover data, after a crash, it just requires reading the journal instead of processing the whole data structure.

Fourth Extended Filesystem (Ext4)

The stable version of ext4 was introduced in 2008 by Linux. The maximum volume size of data supported by ext4 is 1exbiyte and file size is up to 16 terabytes. The maximum length of the filename is 56 bytes. The fragmentation in terms of physical blocks where data is stored, is replaced by extents. This modification, which was not available in ext2 and ext3, increased the performance of the file system. Extent is a data storage area that reduces file fragmentation and file scattering.

IDENTIFYING FILE SYSTEMS

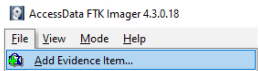
In DF3) Digital Evidence Collection we cover how to use FTK Imager for taking forensically-sound disk images during an investigation, but here we’re going to quickly cover how you can identify the file system from an existing disk image, which you’ll be doing in the file systems activity. You can download FTK Imager [here](#). Once you’ve installed it, run the program, and you’ll see the below.



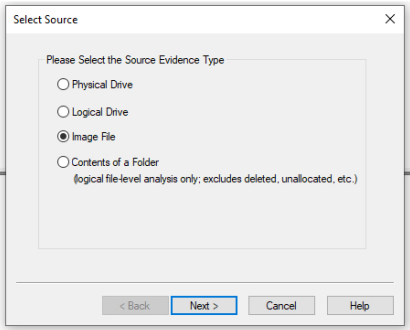
- ☐ Using RDP and SSH
- ☐ How to Start Your Exam



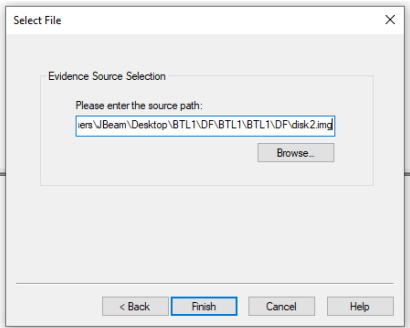
We need to click on File > Add Evidence Item.



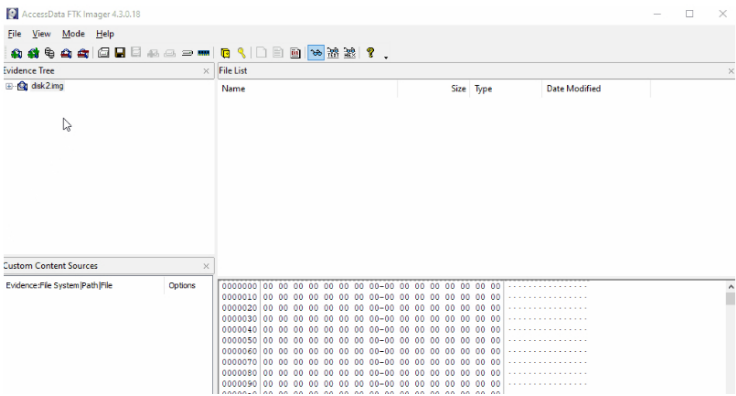
When asked for the source evidence type, we want to select Image File.

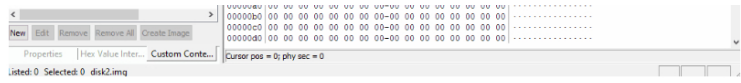


We're going to open the file disk2.img, then click Finish.



The below GIF shows how you can identify the file system using FTK Imager. The system this image file was taken from is using NTFS.





Now that you know how to identify file systems, it's time for you to have a go!

Quizzes


Lab) File Systems

Previous Topic

Back to Lesson

Next Topic

Privacy & Cookies Policy

Privacy - Terms