**Chapter 3**

**File System Forensics**

**V1**

**A blue outline of a bird with a crown and text

Description automatically generatedSID: 2103022**

**Anglia Ruskin Final Project**

**Table of Contents**

[**Introduction** 2](#_Toc160808147)

[**Objective** 2](#_Toc160808148)

[**1.0** **Using HxD to identify filesystem type** 3](#_Toc160808149)

# **Introduction**

This third chapter covers the file system on Windows 10. It will also cover the limitations and advantages while identifying the differences.

# **Objective**

* Explore different filesystems and learn how to identify each type via hex.
* Explore volume serial numbers (S/N) and how to decode them and their creation dates and times.

1. **Using HxD to identify filesystem type**

1.Login as Digital-Forensics and use the password **‘password’** to login to the VM.

A login screen with a beach and rocks

Description automatically generated

2. Launch FTK imager found in the tools folder on the Desktop. **Desktop>Tools> HxD Hex Editor**.

A close up of a computer screen

Description automatically generated

3. Enable data inspector by going **View>Data** inspector or pressing **Ctrl+Alt+D.**

**A screenshot of a computer

Description automatically generated**

4. If you have done this correctly you should see a pop up on the right-hand side like the figure below.

**A screenshot of a computer

Description automatically generated**

5. Go Tools> Open disk image..

A screenshot of a computer

Description automatically generated

6. Locate the FileSystemForensics.001 file in the Evidence folder on the desktop and click open this is a formatted evidence file that we need to determine the file system type.

**A screenshot of a computer

Description automatically generated**

7. A popup will appear click OK.

**A screenshot of a computer error

Description automatically generated**

8. Alter the view to decimal via **Tools> Offset base>Decimal.**

A screenshot of a computer

Description automatically generated

9. Now go to **Search>Go to…**

A screenshot of a computer program

Description automatically generated

10. As we want to look at the Partition table, we must look at Decimal 446-509 Hex 1BE-1FD and length in bytes 64 so enter 446 in the offset as ‘dec’ is already selected.

A screenshot of a computer

Description automatically generated

11. Highlight the 16 bytes including the bit you landed on, so it looks like the figure below.

A screenshot of a computer

Description automatically generated

12. The table below explains what each byte means.

|  |  |  |  |
| --- | --- | --- | --- |
| **Byte** | **Offset** | **Byte Length** | **Description** |
| 1 | 80 | 1 | If first character is 0 the partition is not bootable if 80 partition is bootable. |
| 2-4 | 01 01 00 | 3 | Starting sector read in little-endian (read from right to left) and located at 00 01 01 |
| 5 | 07 | 1 | Represents the filesystem type 07 means NTFS/exFAT, 0E means FAT |
| 6-8 | FE 3F 04 | 3 | Ending sector read in little-endian located at 04 3F FE |
| 9-12 | 3F 00 00 00 | 4 | Stating sector in Hex also read in little-endian. |
| 13-16 | 86 39 01 00 | 4 | Number of sectors in partition also stored in little-endian |

13. The chapter is now complete, and you can now identify the File system of a formatted evidence file. You can close all applications and return to the desktop for Chapter 4 or shutdown if you wish to continue later.