Case Name: The NTFS File System

Couse Name: IST402

Instructor: Robert Price

Date: 02/27/2025

Examiner Name: Jaspreet Singh

Table of Contents

**LIST OF ILLUSTRATIVE MATERIALS3**

TABLES3

FIGURES3

**EXECUTIVE SUMMARY4**

BACKGROUND4

EVIDENCE4

**COLLECTION AND ANALYSIS4**

COLLECTION5

ANALYSIS 5

NTFS File System5

HxD Application12

Autopsy 4.2.015

**CONCLISION16**

NTFS17

HxD Application17

Autopsy 4.2.017

List of Illustrative Materials

**Tables1**

Table 1: Evidence4

**Figures5**

NTFS File System

Figure 1: Viewing Local Drive (C: ) Properties5

Figure 2: Viewing SAMPLEFLAG:999818 Drive Directory6

Figure 3: Creating ADS in Command Prompt7

Figure 4: Viewing ADS in Command Prompt7

Figure 5: Timestomp analysis in Command Prompt8

Figure 6: Timestomp on .txt file8

Figure 7: Creating new private directory and SSN.txt file9

Figure 8: Encrypting private folder in drive (C:) 10

Figure 9: Creating New User10

Figure 10: Adding new user as administrator11

Figure 11: Denied access to file SSN.txt12

HxD Application

Figure 12: Loading disk image on HxD Application12

Figure 13: Rest of ASCII Message 13

Figure 14: Switching Offset from h to d 13

Figure 15: First Partition of Disk Image14

Figure 16: Second Partition of Disk Image 14

Figure 17: Third Partition of Disk Image14

Figure 18: Fourth Partition of Disk Image14

Figure 19: Full partition explanation 14

Figure 20: New disk image NTFS message15

Autopsy 4.2.0

Figure 21: Verifying hash values16

Figure 22: Autopsy File Partition16

# EXECUTIVE SUMMARY

## Background

The primary file system for Windows is the New Technology File System, also known as (NTFS), and is the primary focus of this lab's analysis. The main goal was to understand its structure, security characteristics, and forensic value. NTFS's primary purpose is to provide the ability to store large files efficiently and provide advanced security features, making this a strong focus in forensic investigations examining NTFS and exploring raw disk data using a HEX editor. This forensic tool allows the examiner to view and analyze the raw data of a file in a hexadecimal format. Hashing to confirm image integrity, which plays a vital role in verifying the authentication of images, and utilizing Autopsy, an open-source forensic tool whose purpose is to analyze disk images, recover deleted files, and extract artifacts from NTFS partitions to analyze an NTFS partition, were among the examiner's primary activities.

In addition, in this lab, the examiner looks at the following characteristics of NTFS: Alternate Data Streams (ADS), a feature in the NTFS file system that allows compatibility with older versions of Mac OS. ADS can also be used to determine whether an individual is trying to hide data on their system. Encryption file system (EFS) is another NTFS feature that allows one to encrypt files and folders. Timestomp is used in the command prompt to change files, such as Modified, Access, and Created times.

Overall, by utilizing these NTFS features and forensic tools, the examiner can detect hidden data or files, verify a file's integrity, and track any modifications made to data or files.

### Evidence

|  |  |  |  |
| --- | --- | --- | --- |
| Description | Hash Algorithm | Hash Value | Examiner |
| Evidence | CRC32 | 93644201 | Jaspreet Singh |
| Evidence | MD5 | A2BA635AAF7AEEF814C6EA41A968E5DB | Jaspreet Singh |
| Evidence | SHA-1 | CF27F528D469012B59EC6440D3A4085261176FD | Jaspreet Singh |

# COLLECTION AND ANALYSIS

### Collection

Through this process, the examiner could acquire and retrieve information from an NTFS partition without modifying the original evidence by looking at a disk image. This would then allow the integrity of the original evidence to remain intact when extracting data. Imaging and hashing the NTFS file system in this way would ensure that data is not altered and remains consistent when the examiner executes a forensic analysis. The examiner will use forensic tools to verify, interpret, and analyze the NTFS partition and the respective artifacts during this forensic analysis of the Windows file system, such as the HEX editor, command prompts, and Autopsy. Through hashing, the examiner will ensure that the image obtained can be trusted and has not been altered for forensic analysis.

### Analysis

#### Local Drive NTFS File System

The examiner examined the local drive (C:) called SAMPLEFLAG:999818(C:) and from there the examiner opened the properties and saw the file system was NTFS meaning that the local drive supports advanced security permissions, features, encryption, ACLs and ADS.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 1: Viewing Local Drive (C: ) Properties

#### Command Prompt showing the Directory

In the command prompt the examiner is looking at the directory of the local drive (C:) by using the command “dir” the examiner can see the entire directory of SAMPLEFLAG:999818.

A screenshot of a computer program

AI-generated content may be incorrect.

Figure 2: Viewing SAMPLEFLAG:999818 Drive Directory

#### Creating ADS

The examiner in the command prompt is creating an Alternate Data Stream (ADS) to allow files to store hidden data. So, in this the examiner created a file called regular.txt and then hid that file within another file called hidden.txt.

A screenshot of a computer program

AI-generated content may be incorrect.

Figure 3: Creating ADS in Command Prompt

#### Viewing ADS

The examiner used the command prompt to view the content within the hidden.txt file created to reveal the information in regular.txt in a notepad file.

A computer screen with white text

AI-generated content may be incorrect.

Figure 4: Viewing ADS in command prompt.

#### Timestomp in Command Prompt

In the command prompt the examiner can view a files timestomps data. It allows for the manipulation of file data such as modified, accessed, created, and MFT entry modified. It’s often used by hackers to change timestamps, so it makes it difficult for forensic analysis.

A screenshot of a computer program

AI-generated content may be incorrect.

Figure 5: Timestomp analysis in Command Prompt

#### Using Timestomp on a .txt file.

In the command prompt the examiner is using the Timestomp tool to manipulate the file ht.txt and copies timestomps from config.sys into the txt file.

A computer screen with white text

AI-generated content may be incorrect.

Figure 6: Timestomp on .txt file

#### Creating a new Directory and File then Testing

The examiner created a new directory in drive C: called private and created a new file called SSN.txt with an inputter SSN. Then the examiner checked the C:\privat directory and verified that the new SSN.txt file created was present and viewed the files contents.

A screenshot of a computer program

AI-generated content may be incorrect.

Figure 7: Creating new private directory and SSN.txt file

#### Viewing drive (C:) Private Folder

The examiner went into the local drive (C:) and saw the private folders properties and went to advanced. From there the examiner encrypted the contents and applied the changes to the entire private folder and its contents and now the folder has green text to show that it’s encrypted.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 8: Encrypting private folder in drive (C:)

#### Creating new User in command prompt

The examiner in the command prompt is adding a new user called Jesse James with the password cowboy and then verifying after creating the user if it’s in the system.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 9: Creating new user

#### Adding New User as Administrator

The examiner after verifying that jessejames has been added will then add jessejames as an administrator and once that is completed. The examiner can verify that both jessejames and student are the two administrators on the device.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 10: Adding new user as administrator

#### Switching users to test accessibility to the encrypted private folder

The examiner logged out of student’s profile and logged into the new administrator file jessejames. The examiner let the environment boot up fully then went into the local drive (C:) on jessejames to try to open the encrypted file in private folder called SSN.txt. But the user was denied access to the file since the file is encrypted. The user does not have proper authority or key to open the file therefore cannot access the file.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 11: Denied access to file SSN.txt

#### Using HxD Application

The examiner opened the HxD application and went to the computer’s local drive (C:) to open a disk image called 10-ntfs-disk.dd-shortcut on the application. From there the examiner selected the sector size of 512 bytes and highlighted from bytes 00000000 to 00000162 to show the following message on the ASCII table on the right “Error loading operating system”.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 12: Loading disk image on HxD Application

#### Examining ASCII table

The examiner highlights the following bytes from 00000163 to 000001B2 to show the rest of the message which shows “Missing operating system” on the ASCII table.

A blue and white grid with numbers

AI-generated content may be incorrect.

Figure 13: Rest of ASCII Message

#### Viewing from h to d

The examiner changes the offset located on the upper left from h to d which is decimal values. The examiner switches from hexadecimal to decimal because it is more natural for people to understand and that also makes it easier to understand partitions.

A screenshot of a computer screen

AI-generated content may be incorrect.

Figure 14: Switching Offset from h to d

#### Viewing the first partition

The examiner looks at each partition of the disk image which has a total of 64 bytes in the HxD application. First the examiner starts with the first partition which is from 1BE to 1CD. This first partition shows that it’s a non-bootable partition with the entry of 00 at the beginning.



Figure 15: First Partition of Disk Image

#### Viewing the second partition

The examiner looks at the next 16-byte partition from 1CE to 1DD.



Figure 16: Second Partition of Disk Image

#### Viewing the third partition

The examiner looks at the third 16-byte partition from 1DE to 1ED.



Figure 17: Third Partition of Disk Image

#### Viewing the fourth partition

The examiner looks at the last 16-byte partition of the 64-byte disk image from m 1EE to 1FD.



Figure 18: Fourth Partition of Disk Image

#### Viewing the full partition

After the examiner analyzes the four separate partitions, they can now see the full 64-byte disk image and see that in the full partition the next three bytes after the 00 non-bootable indicate the head, sector, and cylinder known as the CHS address (0,1,1). Then the examiner sees 07 after the CHS address indication the partition type which is 07 hence indicating it’s a NTFS partition. Then the examiner looks at bytes 3F 00 00 00 indicating the Logical Block Addressing (LBA) which is used by computers to access and locate data in storage. Then the next four bytes the examiner sees is 47 78 01 00 which indicates the size in sectors of the partition which means that each entry is 16 bytes long. Finally at the end the examiner sees 55 AA which signifies an MBR signature.

A blue and white screen with numbers

AI-generated content may be incorrect.



Figure 19: Full partition explanation

#### Opening New Disk Image

The examiner opens new disk image from the local drive (C:) called 10-ntfs-part1.dd with a sector size of 512 bytes and in the partition the examiner analyzes the following bytes 4E 54 46 53 and sees in the message on the ASCII table on right “NTFS”.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 20: New disk image NTFS message

#### Verifying Evidence Hash Values

The examiner has now logged into windows 10 and went to the Local Drive(C:) file and opened images. Then clicked the file called ntfsdd.txt. From there the examiner can see the CRC, MD5, and SHA1 values. The examiner from there can go into the ntfsdd.txt files properties and then look at the hash values in the properties. Then the examiner can review both the hash values in notepad and properties to verify that each match is correct.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 21: Verifying hash values

#### NTFS Partition with Autopsy

The examiner used Autopsy 4.2.0 application to create a new case named Lab0 for the base directory C:\images. Then the examiner inputted the case number as ‘1’ and examiner ‘Jaspreet’. Once created the examiner added data by browsing the C:\images and clicked on the ntfs.dd file. Once this file is selected the examiner configures the ingest modules and selects all the things to search for when reviewing this ntfs.dd file. Then once the examiner selects all the things to search for and sees the results the examiner looks through the created table data on the file. Then the examiner sees that the NTFS file system includes the Master File Table ($MFT) which is used to help with file metadata in NTFS and the Master File Table Mirror ($MFTMirr) which is used to recover files and check integrity. This is important because these files are critical for the NTFS file system structure and for forensic analysis.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 22: Autopsy File Partition

# Conclusion

Overall, through this lab the examiner was able to analyze and understand the NTFS file system using the following forensic tools HxD and Autopsy as well as command prompts to examine the raw disk data, verify the data’s integrity, and reveal any hidden or deleted information. Through this process the examiner was able to gain hands-on experience in understanding the structure of NTFS file system as well as exploring how partitions worked and identifying critical system files. By using the forensic tools, it ensured that the examiner followed a structured approach when conducting the forensic analysis on the data and ensured that the integrity of the data through the investigation remained in tact through the analysis of key NTFS features such as ADS, Timestomp manipulation, and $MFT.

### NTFS File System

This is primarily used in windows operating systems to provide a secure and modern file system. This file system included advanced features such as ADS, ACLs, journaling, and file encryption, all of which is useful and impactful during a forensic investigation. THE NTFS file system also keeps a Master file Table, which stores all the metadata about all files and directories within it, making it a vital resource for digital analysis. By understanding the key features and structures of the NTFS file system the examiner can recover deleted content or files, track the modification of files, and detect any techniques or actions conducted by malicious characters during an investigation.

### HxD Application

This is a hex editor application that allows the examiner to modify and or view raw disk image data on a byte level. This tool is essential to examine the Master Boot Record (MBR) of 512 bytes in length and helps to partition the table into sections to help the examiner locate and interpret partition structures. This application utilizes the switching of offsets from hexadecimal (h) to decimal (d) to make the partitions easier to compare with other forensic tools as well as make it easier to interpret and read the data. By understanding the key features of this hex editor application, it can play a critical role in tracing deleted files, recovering hidden data, and overall providing a forensic analysis of a disk image during an investigation.

### Autopsy

Autopsy is an open-source forensic tool that is used to analyze NTFS disk images and extract any crucial artifacts within it. Through this the examiner was able to examine the disk image of the NTFS file system including the $MFT and $MFTMirr, which include stored metadata about every file on the system. This forensic tool allowed the examiner to recover any deleted files, detect possible techniques used by attackers to hide data, and inspect timestamps of files. This tool is crucial to a forensic investigation because it allows for more simplified and structured interfaces to browse a file system searching for key hidden artifacts and generating a report on the file system based on the selected prompts by an examiner.