



FORENSICS LAB SERIES

Lab 1: Exploring the Windows File System

Material in this Lab Aligns to the Following Certification Domains/Objectives	
Certified Cyber Forensics Professional (CCFP) Objectives	Computer Hacking Forensic Investigator (CHFI) Objectives
4: Digital Forensics	7: Understanding Hard Disks and File Systems

Document Version: 2016-08-17

Contents

Introduction	3
Objective	3
Pod Topology	4
Lab Settings	5
1 Getting Familiar with MFT File Viewer	6
2 Identifying Attributes with MFT File Viewer	10

Introduction

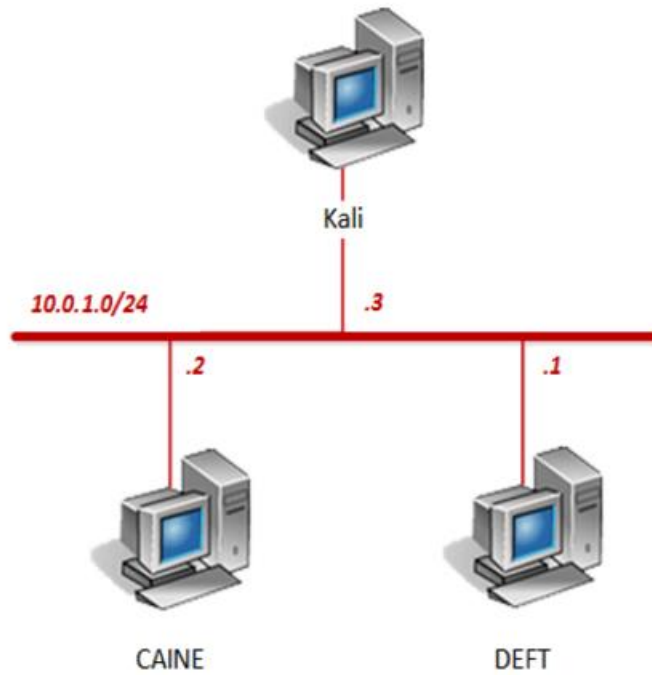
The Windows New Technology File System (NTFS) file system is commonly used to organize and handle functions such as read, write and search on most Windows Operating Systems, starting with Windows NT. In this lab, we will explore the NTFS system and how to interpret the Master File Table or MFT.

Objective

In this lab, you will be conducting forensic practices using various tools. You will be performing the following tasks:

1. Getting Familiar with MFT File Viewer
2. Identifying Attributes with MFT File Viewer

Pod Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
DEFT	10.0.1.1	deft	password
CAINE	10.0.1.2	caine	
Kali	10.0.1.3	root	toor

1 Getting Familiar with MFT File Viewer

1. Click on the **CAINE** graphic on the *topology page* to open the VM.
2. Open a new terminal by clicking on the **MATE Terminal** icon located on the bottom panel.



3. Navigate to the `/usr/local/bin` directory by typing the command below followed by pressing **Enter**.

```
cd /usr/local/bin
```

4. Launch the **MFT File Viewer** application by entering the command below.

```
MFTView.py /home/caine/Desktop/Windows\ MFT/MFT
```

```
caine@Caine01:/usr/local/bin$ MFTView.py /home/caine/Desktop/Windows\ MFT/MFT
```

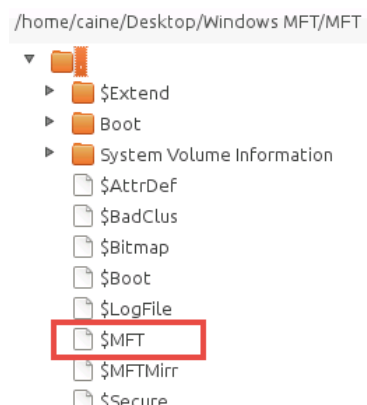
A new *MFT File Viewer* screen will appear.

5. Expand the **MFT** file by clicking on the **arrow** next to the folder icon in the left pane.

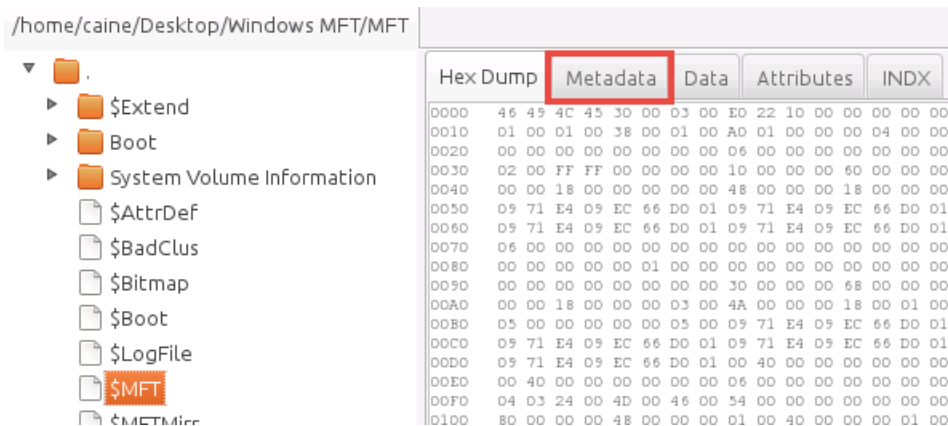


Once expanded, notice the *NTFS* metadata present for the system files.

6. In the left pane, click on the **\$MFT** file to explore the metadata.

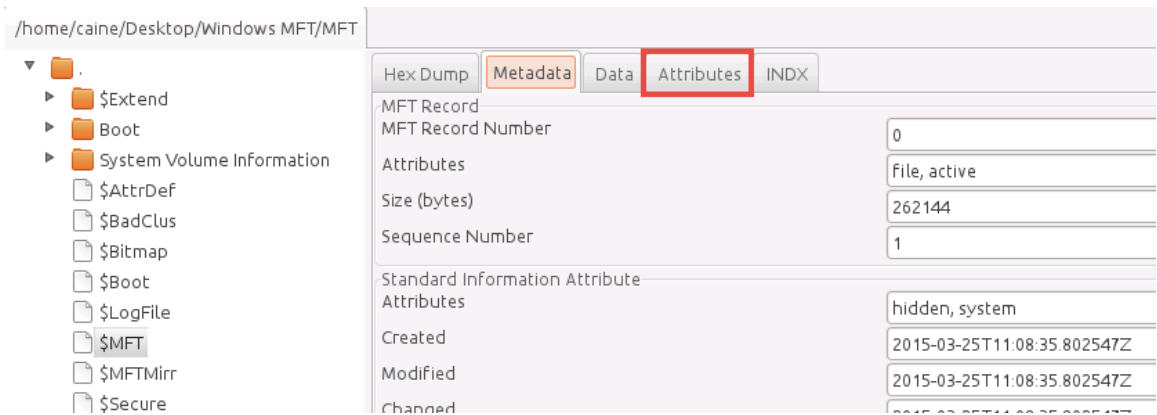


7. Once *\$MFT* is selected, click on the **Metadata** tab in the middle pane.



The screenshot shows the Windows File System Explorer with the path `/home/caine/Desktop/Windows MFT/MFT`. The left pane displays a tree view of files, including `$Extend`, `Boot`, `System Volume Information`, `$AttrDef`, `$BadClus`, `$Bitmap`, `$Boot`, `$LogFile`, `$MFT` (selected), `$MFTMirr`, and `$Secure`. The right pane shows the **Metadata** tab, which displays a hex dump of the file's contents. The hex dump shows a series of bytes, including `0000 46 49 4C 45 30 00 03 00 E0 22 10 00 00 00 00 00` and `0010 01 00 01 00 38 00 01 00 A0 01 00 00 00 04 00 00`.

8. On the *Metadata* tab, this is the first record or “Record 0” for the file system. Found within the *MFT* record are various attributes. Click on the **Attributes** tab.

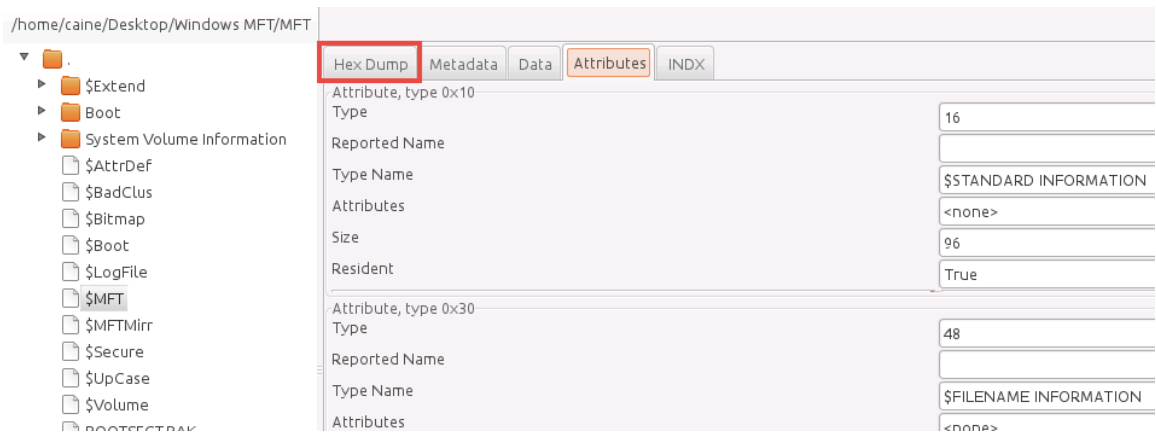


The screenshot shows the Windows File System Explorer with the path `/home/caine/Desktop/Windows MFT/MFT`. The left pane displays a tree view of files, including `$Extend`, `Boot`, `System Volume Information`, `$AttrDef`, `$BadClus`, `$Bitmap`, `$Boot`, `$LogFile`, `$MFT` (selected), `$MFTMirr`, and `$Secure`. The right pane shows the **Attributes** tab, which displays details for the first record (Record 0). The details include:

- MFT Record Number: 0
- Attributes: File, active
- Size (bytes): 262144
- Sequence Number: 1
- Standard Information Attribute: hidden, system
- Created: 2015-03-25T11:08:35.802547Z
- Modified: 2015-03-25T11:08:35.802547Z
- Changed: 2015-03-25T11:08:35.802547Z

In each *Record*, there are attributes. The first attribute type `0x10` is called *\$Standard Information*. Its type is `16` which is the decimal equivalent to hex value of `0x10`. Its respective size is 96 bytes and the file is *Resident* (True) in the MFT. Resident means its size is less than 512 bytes, so it can reside in the MFT and does not have to be outside of the MFT located on the disk.

9. Click on the **Hex Dump** tab to view the hex values.



10. Notice that the *MFT* header fields all start with *File 0* at offset *0x00*.

Hex Dump	Metadata	Data	Attributes	INDX
0000 46 49 4C 45 30 00 03 00 E0 22 10 00 00 00 00 00	FILE0...."	ASCII		
0010 01 00 01 00 38 00 01 00 A0 01 00 00 00 04 00 00	...B.....	-----		
0020 00 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00	...FILE0	FILE0		
0030 02 00 FF FF 00 00 00 00 10 00 00 00 60 00 00 00	...!@U!	!@U!		
0040 00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00	...!@U!	!@U!		
0050 09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	...H.....			
0060 09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	..q...f...q...f..			
0070 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00	..q...f...q...f..			
0080 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00	UTF-16		
0090 00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 00	-----		
00A0 00 00 18 00 00 00 03 00 4A 00 00 00 18 00 01 00O...h..	\$MFT		
00B0 03 00 00 00 00 00 05 00 09 71 E4 09 EC 66 D0 01J.....			
00C0 09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01q...f..			
00D0 09 71 E4 09 EC 66 D0 01 00 40 00 00 00 00 00 00	..q...f...q...f..			
00E0 00 40 00 00 00 00 00 00 06 00 00 00 00 00 00	..q...f...@.....			
00F0 04 03 24 00 4D 00 46 00 54 00 00 00 00 00 00	..@.....			
0100 80 00 00 00 48 00 00 00 01 00 40 00 00 00 01 00	..\$.M.F.T.....			
0110 00 00 00 00 00 00 00 00 3F 00 00 00 00 00 00	...H.....@.....			
0120 40 00 00 00 00 00 00 00 00 00 04 00 00 00 00?.....			
0130 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00	@.....			
0140 21 40 55 21 00 F8 FF FF B0 00 00 00 50 00 00 00P...			
0150 01 00 40 00 00 00 05 00 00 00 00 00 00 00 00	..@.....			

11. Note that the size of the *MFT* record located at offset *0x1c* to *0x1f* is the default size of *0x400* or 262144 bytes.

Hex Dump	Metadata	Data	Attributes	INDX	
0000 46 49 4C 45 30 00 03 00 E0 22 10 00 00 00 00 00				FILE0....".....	ASCII
0010 01 00 01 00 38 00 01 00 A0 01 00 00 00 04 00 00			8.....	-----
0020 00 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00				FILE0
0030 02 00 FF FF 00 00 00 00 10 00 00 00 60 00 00 00			`.....	!@U!
0040 00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00			H.....	!@U!
0050 09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01				.q...f...q...f..	
0060 09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01				.q...f...q...f..	
0070 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00				UTF-16
0080 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00				-----
0090 00 00 00 00 00 00 00 00 30 00 00 00 68 00 00			0...h...	\$MFT
00A0 00 00 18 00 00 00 03 00 4A 00 00 00 18 00 01 00			J.....	
00B0 05 00 00 00 00 00 05 00 09 71 E4 09 EC 66 D0 01			q...f..	
00C0 09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01				.q...f...q...f..	
00D0 09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01				.q...f...q...f..	

12. Locate the length of the header at offset *0x14* and is *0x38* or 56 bytes.

Hex Dump	Metadata	Data	Attributes	INDX	
0000 46 49 4C 45 30 00 03 00 E0 22 10 00 00 00 00 00				FILE0....".....	ASCII
0010 01 00 01 00 38 00 01 00 A0 01 00 00 00 04 00 00			8.....	-----
0020 00 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00				FILE0
0030 02 00 FF FF 00 00 00 00 10 00 00 00 60 00 00 00			`.....	!@U!
0040 00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00			H.....	!@U!
0050 09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01				.q...f...q...f..	
0060 09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01				.q...f...q...f..	
0070 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00				UTF-16
0080 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00				-----
0090 00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 00			0...h...	\$MFT
00A0 00 00 18 00 00 00 03 00 4A 00 00 00 18 00 01 00			J.....	
00B0 05 00 00 00 00 00 05 00 09 71 E4 09 EC 66 D0 01			q...f..	

2 Identifying Attributes with MFT File Viewer

1. While on the *Hex Dump* tab, locate where the *Standard Information* attribute *0x10* starts on offset *0x38*.

Hex Dump	Metadata	Data	Attributes	INDX
0000	46 49 4C 45 30 00 03 00 E0 22 10 00 00 00 00 00	FILE0...."	ASCII	
0010	01 00 01 00 38 00 01 00 A0 01 00 00 00 04 00 008.....	-----	
0020	00 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00	FILE0	
0030	02 00 FF FF 00 00 00 00 10 00 00 00 60 00 00 00`.....	!@U!	
0040	00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00H.....	!@U!	
0050	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		
0060	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		
0070	06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	UTF-16	
0080	00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00	-----	
0090	00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 000...h...	\$MFT	
00A0	00 00 18 00 00 00 03 00 4A 00 00 00 18 00 01 00J.....		
00B0	05 00 00 00 00 00 05 00 09 71 E4 09 EC 66 D0 01q...f..		
00C0	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		
00D0	09 71 E4 09 EC 66 D0 01 00 40 00 00 00 00 00 00	.q...f...P.....		

2. The size of the *Standard Information* attribute is at offset *0x04* and *0x05* from the beginning of the attribute. Its size is *0x60* or 96 bytes.

Hex Dump	Metadata	Data	Attributes	INDX
0000	46 49 4C 45 30 00 03 00 E0 22 10 00 00 00 00 00	FILE0...."	ASCII	
0010	01 00 01 00 38 00 01 00 A0 01 00 00 00 04 00 008.....	-----	
0020	00 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00	FILE0	
0030	02 00 FF FF 00 00 00 00 10 00 00 00 60 00 00 00`.....	!@U!	
0040	00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00H.....	!@U!	
0050	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		
0060	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		
0070	06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	UTF-16	
0080	00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00	-----	
0090	00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 000...h...	\$MFT	
00A0	00 00 18 00 00 00 03 00 4A 00 00 00 18 00 01 00J.....		
00B0	05 00 00 00 00 00 05 00 09 71 E4 09 EC 66 D0 01q...f..		
00C0	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		

3. Identify the creation date and time at *0x18* to *0x1F*. When decoded, it can be concluded that this is stored in a Windows 64 bit hex format – Little Endian.

Hex Dump	Metadata	Data	Attributes	INDX
0000	46 49 4C 45 30 00 03 00 E0 22 10 00 00 00 00 00	FILE0...."	ASCII	
0010	01 00 01 00 38 00 01 00 A0 01 00 00 00 04 00 008.....	-----	
0020	00 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00	FILE0	
0030	02 00 FF FF 00 00 00 00 10 00 00 00 60 00 00 00`.....	!@U!	
0040	00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00H.....	!@U!	
0050	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		
0060	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		
0070	06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	UTF-16	
0080	00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00	-----	
0090	00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 000...h...	\$MFT	
00A0	00 00 18 00 00 00 03 00 4A 00 00 00 18 00 01 00J.....		
00B0	05 00 00 00 00 00 05 00 09 71 E4 09 EC 66 D0 01q...f..		
00C0	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		

4. The last modified date and time for the file is next. Notice that the value is the same as the previous creation date and time.

Hex Dump	Metadata	Data	Attributes	INDX
0000	46 49 4C 45 30 00 03 00 E0 22 10 00 00 00 00 00	FILE0....".		ASCII
0010	01 00 01 00 38 00 01 00 A0 01 00 00 00 04 00 00	...8.....		-----
0020	00 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00		FILE0
0030	02 00 FF FF 00 00 00 00 10 00 00 00 60 00 00 00^...		!@U!
0040	00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00H.....		!@U!
0050	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		
0060	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		
0070	06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		UTF-16
0080	00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00		-----
0090	00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 000...h...		\$MFT
00A0	00 00 18 00 00 00 03 00 4A 00 00 00 18 00 01 00J.....		
00B0	05 00 00 00 00 00 05 00 09 71 E4 09 EC 66 D0 01q...f..		
00C0	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		

5. Next is the last access date and time. Notice the same value again.

Hex Dump	Metadata	Data	Attributes	INDX
0000	46 49 4C 45 30 00 03 00 E0 22 10 00 00 00 00 00	FILE0....".		ASCII
0010	01 00 01 00 38 00 01 00 A0 01 00 00 00 04 00 00	...8.....		-----
0020	00 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00		FILE0
0030	02 00 FF FF 00 00 00 00 10 00 00 00 60 00 00 00^...		!@U!
0040	00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00H.....		!@U!
0050	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		
0060	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		
0070	06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		UTF-16
0080	00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00		-----
0090	00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 000...h...		\$MFT
00A0	00 00 18 00 00 00 03 00 4A 00 00 00 18 00 01 00J.....		
00B0	05 00 00 00 00 00 05 00 09 71 E4 09 EC 66 D0 01q...f..		
00C0	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		
00D0	09 71 E4 09 EC 66 D0 01 00 40 00 00 00 00 00 00	.q...f...@.....		

6. The next line of hex is the record access date and time. Notice the dates are the same.

Hex Dump	Metadata	Data	Attributes	INDX
0000	46 49 4C 45 30 00 03 00 E0 22 10 00 00 00 00 00	FILE0....".		ASCII
0010	01 00 01 00 38 00 01 00 A0 01 00 00 00 04 00 00	...8.....		-----
0020	00 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00		FILE0
0030	02 00 FF FF 00 00 00 00 10 00 00 00 60 00 00 00^...		!@U!
0040	00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00H.....		!@U!
0050	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		
0060	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		
0070	06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		UTF-16
0080	00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00		-----
0090	00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 000...h...		\$MFT
00A0	00 00 18 00 00 00 03 00 4A 00 00 00 18 00 01 00J.....		
00B0	05 00 00 00 00 00 05 00 09 71 E4 09 EC 66 D0 01q...f..		
00C0	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		
00D0	09 71 E4 09 EC 66 D0 01 00 40 00 00 00 00 00 00	.q...f...@.....		

7. Navigate to the **Metadata** tab and compare the values to the actual values. The hex values should match.

Hex Dump	Metadata	Data	Attributes	INDX
MFT Record				
MFT Record Number		0		
Attributes		File, active		
Size (bytes)		262144		
Sequence Number		1		
Standard Information Attribute				
Attributes		hidden, system		
Created		2015-03-25T11:08:35.802547Z		
Modified		2015-03-25T11:08:35.802547Z		
Changed		2015-03-25T11:08:35.802547Z		
Accessed		2015-03-25T11:08:35.802547Z		
Filename Information Attribute (WIN32 + DOS 8.3)				

8. Click on the **Attributes** tab.

Hex Dump	Metadata	Data	Attributes	INDX
MFT Record				
MFT Record Number		0		
Attributes		File, active		

9. Identify the next attribute, *0x30 \$Filename Information*. Its type is 48, which is decimal for *0x30*. Its respective size is 104 bytes and its resident.

Attribute, type 0x30	
Type	48
Reported Name	
Type Name	\$FILENAME INFORMATION
Attributes	<none>
Size	104
Resident	True

10. Click on the **Hex Dump** tab.

Hex Dump	Metadata	Data	Attributes	INDX
Reported Name				
Type Name				
Attributes				

11. At offset 0x98, the attribute 0x30 can be located.

Hex Dump	Metadata	Data	Attributes	INDX
0000	46 49 4C 45 30 00 03 00 E0 22 10 00 00 00 00 00	FILED....*		
0010	01 00 01 00 38 00 01 00 A0 01 00 00 00 04 00 008.....		
0020	00 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00		
0030	02 00 FF FF 00 00 00 00 10 00 00 00 60 00 00 00		
0040	00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00H.....		
0050	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		
0060	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		
0070	06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
0080	00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00		
0090	00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 00O...h...		
00A0	00 00 18 00 00 00 03 00 4A 00 00 00 18 00 01 00J.....		
00B0	05 00 00 00 00 00 05 00 09 71 E4 09 EC 66 D0 01q...f..		
00C0	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		
00D0	09 71 E4 09 EC 66 D0 01 00 40 00 00 00 00 00 00	.q...f...@.....		
00E0	00 40 00 00 00 00 00 00 06 00 00 00 00 00 00 00	.@.....		
00F0	04 03 24 00 4D 00 46 00 54 00 00 00 00 00 00 00	..\$.M.F.T.....		
0100	80 00 00 00 48 00 00 00 01 00 40 00 00 00 01 00H.....@.....		

12. Identify the size by locating bytes 0x04 and 0x05 from the 0x30. Notice the size is 68 bytes in hex, which is 104 bytes in decimal. It is also a resident record.

Hex Dump	Metadata	Data	Attributes	INDX
0000	46 49 4C 45 30 00 03 00 E0 22 10 00 00 00 00 00	FILED....*		
0010	01 00 01 00 38 00 01 00 A0 01 00 00 00 04 00 008.....		
0020	00 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00		
0030	02 00 FF FF 00 00 00 00 10 00 00 00 60 00 00 00		
0040	00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00H.....		
0050	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		
0060	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		
0070	06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
0080	00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00		
0090	00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 00O...h...		
00A0	00 00 18 00 00 00 03 00 4A 00 00 00 18 00 01 00J.....		
00B0	05 00 00 00 00 00 05 00 09 71 E4 09 EC 66 D0 01q...f..		
00C0	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		
00D0	09 71 E4 09 EC 66 D0 01 00 40 00 00 00 00 00 00	.q...f...@.....		

13. Click on the **Attributes** tab and identify the 0x80 attribute.

Hex Dump	Metadata	Data	Attributes	INDX
0000	46 49 4C 45 30 00 03 00 E0 22 10 00 00 00 00 00	FILED....*		
0010	01 00 01 00 38 00 01 00 A0 01 00 00 00 04 00 008.....		
0020	00 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00		
0030	02 00 FF FF 00 00 00 00 10 00 00 00 60 00 00 00		



14. Notice the attribute is the \$Data attribute, which is type 0x80 or 128. Its size is 72 bytes and its non-resident.

15. Click on the **Hex Dump** tab to analyze the \$Data attribute more closely.

Hex Dump	Metadata	Data	Attributes	INDX
Attribute, type 0x10				
Type				

16. Identify offset *0x100* to locate attribute *0x80*. Move to bytes 0x04 and 0x05 from there to find the size.

Hex Dump	Metadata	Data	Attributes	INDX
0000	46 49 4C 45 30 00 03 00	ED 22 10 00 00 00 00 00	FILE0...."	
0010	01 00 01 00 38 00 01 00	A0 01 00 00 00 04 00 008.....	
0020	00 00 00 00 00 00 00 00	06 00 00 00 00 00 00 00	
0030	02 00 FF FF 00 00 00 00	10 00 00 00 60 00 00 00'	
0040	00 00 18 00 00 00 00 00	48 00 00 00 18 00 00 00H.....	
0050	09 71 E4 09 EC 66 D0 01 09	71 E4 09 EC 66 D0 01	.q...f...q...f..	
0060	09 71 E4 09 EC 66 D0 01 09	71 E4 09 EC 66 D0 01	.q...f...q...f..	
0070	06 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0080	00 00 00 00 00 01 00 00	00 00 00 00 00 00 00 00	
0090	00 00 00 00 00 00 00 00	30 00 00 00 68 00 00 000...h...	
00A0	00 00 18 00 00 00 03 00	4A 00 00 00 18 00 01 00J.....	
00B0	03 00 00 00 00 00 05 00	09 71 E4 09 EC 66 D0 01q...f..	
00C0	09 71 E4 09 EC 66 D0 01 09	71 E4 09 EC 66 D0 01	.q...f...q...f..	
00D0	09 71 E4 09 EC 66 D0 01 00	40 00 00 00 00 00 00 00	.q...f...@.....	
00E0	00 40 00 00 00 00 00 00	06 00 00 00 00 00 00 00	.@.....	
00F0	04 03 24 00 4D 00 46 00	54 00 00 00 00 00 00 00	..\$.M.F.T.....	
0100	80 00 00 00 48 00 00 01	00 40 00 00 00 01 00H.....@.....	
0110	00 00 00 00 00 00 00 00	3F 00 00 00 00 00 00 00?.....	
0120	40 00 00 00 00 00 00 00	00 00 04 00 00 00 00 00	@.....	
0130	00 00 04 00 00 00 00 00	00 00 04 00 00 00 00 00	

17. Notice that it is 48 in hex or 72 bytes in decimal. Move three more bytes to find the non-resident flag set.

Hex Dump	Metadata	Data	Attributes	INDX
0000	46 49 4C 45 30 00 03 00	ED 22 10 00 00 00 00 00	FILE0...."	
0010	01 00 01 00 38 00 01 00	A0 01 00 00 00 04 00 008.....	
0020	00 00 00 00 00 00 00 00	06 00 00 00 00 00 00 00	
0030	02 00 FF FF 00 00 00 00	10 00 00 00 60 00 00 00'	
0040	00 00 18 00 00 00 00 00	48 00 00 00 18 00 00 00H.....	
0050	09 71 E4 09 EC 66 D0 01 09	71 E4 09 EC 66 D0 01	.q...f...q...f..	
0060	09 71 E4 09 EC 66 D0 01 09	71 E4 09 EC 66 D0 01	.q...f...q...f..	
0070	06 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0080	00 00 00 00 00 01 00 00	00 00 00 00 00 00 00 00	
0090	00 00 00 00 00 00 00 00	30 00 00 00 68 00 00 000...h...	
00A0	00 00 18 00 00 00 03 00	4A 00 00 00 18 00 01 00J.....	
00B0	03 00 00 00 00 00 05 00	09 71 E4 09 EC 66 D0 01q...f..	
00C0	09 71 E4 09 EC 66 D0 01 09	71 E4 09 EC 66 D0 01	.q...f...q...f..	
00D0	09 71 E4 09 EC 66 D0 01 00	40 00 00 00 00 00 00 00	.q...f...@.....	
00E0	00 40 00 00 00 00 00 00	06 00 00 00 00 00 00 00	.@.....	
00F0	04 03 24 00 4D 00 46 00	54 00 00 00 00 00 00 00	..\$.M.F.T.....	
0100	80 00 00 00 48 00 00 00	04 00 40 00 00 00 01 00H.....@.....	
0110	00 00 00 00 00 00 00 00	3F 00 00 00 00 00 00 00?.....	
0120	40 00 00 00 00 00 00 00	00 00 04 00 00 00 00 00	@.....	
0130	00 00 04 00 00 00 00 00	00 00 04 00 00 00 00 00	
0140	21 40 55 21 00 F8 FF FF	BD 00 00 00 5D 00 00 00	1/2/11 P	

18. Notice that the end of the MFT record is at offset 0x200.

Hex Dump	Metadata	Data	Attributes	INDX
0000	46 49 4C 45 30 00 03 00 E0 22 10 00 00 00 00 00	FILED....".		
0010	01 00 01 00 38 00 01 00 A0 01 00 00 00 04 00 008.....		
0020	00 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00		
0030	02 00 FF FF 00 00 00 00 10 00 00 00 60 00 00 00^.....		
0040	00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00H.....		
0050	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		
0060	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		
0070	06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
0080	00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00		
0090	00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 00O...h...		
00A0	00 00 18 00 00 00 03 00 4A 00 00 00 18 00 01 00J.....		
00B0	05 00 00 00 00 00 05 00 09 71 E4 09 EC 66 D0 01q...f..		
00C0	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		
00D0	09 71 E4 09 EC 66 D0 01 00 40 00 00 00 00 00 00	.q...f...@.....		
00E0	00 40 00 00 00 00 00 00 06 00 00 00 00 00 00 00	.@.....		
00F0	04 03 24 00 4D 00 46 00 54 00 00 00 00 00 00 00	..\$.M.F.T.....		
0100	80 00 00 00 48 00 00 00 01 00 40 00 00 00 01 00H.....@.....		
0110	00 00 00 00 00 00 00 00 3F 00 00 00 00 00 00 00?.....		
0120	40 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00	@.....		
0130	00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00		
0140	21 40 55 21 00 F8 FF FF B0 00 00 00 50 00 00 00	!@U!.....P...		
0150	01 00 40 00 00 00 05 00 00 00 00 00 00 00 00 00	..@.....		
0160	01 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00@.....		
0170	00 20 00 00 00 00 00 00 08 10 00 00 00 00 00 00		
0180	08 10 00 00 00 00 00 00 21 01 54 21 21 01 FE FD!T!!.....		
0190	00 DE 8B 02 80 FA FF FF FF FF FF FF 00 00 00 00		
01A0	00 00 04 00 00 00 00 00 21 40 55 21 00 F8 FF FF!@U!.....		
01B0	B0 00 00 00 50 00 00 00 01 00 40 00 00 00 05 00P.....@.....		
01C0	00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00		
01D0	40 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00	@.....		
01E0	08 10 00 00 00 00 00 00 08 10 00 00 00 00 00 00		
01F0	21 01 54 21 21 01 FE FD 00 DE 8B 02 80 FA FF FF	!.T!!.....		
0200	FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00		
0210	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
0220	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		

19. Click on the **Attributes** tab.

Hex Dump	Metadata	Data	Attributes	INDX
0000	46 49 4C 45 30 00 03 00 E0 22 10 00 00 00 00 00	FILED....".		
0010	01 00 01 00 38 00 01 00 A0 01 00 00 00 04 00 00B.....		
0020	00 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00		
0030	02 00 FF FF 00 00 00 00 10 00 00 00 60 00 00 00		
0040	00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00H.....		

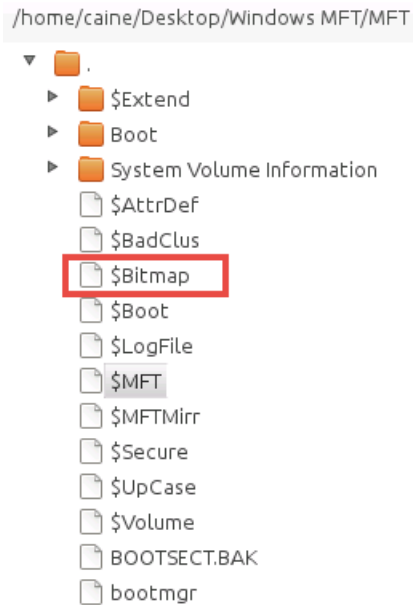
20. Compare the values found from the *Hex Dump* tab to the *Attributes* tab.

Hex Dump	Metadata	Data	Attributes	INDX
Size		96		
Resident		True		
Attribute, type 0x30				
Type		48		
Reported Name				
Type Name		\$FILENAME INFORMATION		
Attributes		<none>		
Size		104		
Resident		True		
Attribute, type 0x80				
Type		128		
Reported Name				
Type Name		\$DATA		
Attributes		<none>		
Size		72		
Resident		False		
Attribute, type 0xb0				

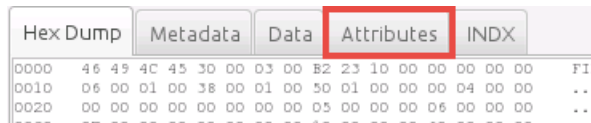
21. Click on the **Hex Dump** tab. The last record is *\$Bitmap* and its type *0xb0* is 176 bytes in decimal. Its size is 80 in hex and is non-resident.

Hex Dump	Metadata	Data	Attributes	INDX
0000	46 49 4C 45 30 00 03 00 E0 22 10 00 00 00 00 00	FILEO....".		
0010	01 00 01 00 38 00 01 00 A0 01 00 00 00 04 00 008.....		
0020	00 00 00 00 00 00 00 00 06 00 00 00 00 00 00		
0030	02 00 FF FF 00 00 00 00 10 00 00 00 60 00 00^...		
0040	00 00 18 00 00 00 00 00 48 00 00 00 18 00 00H.....		
0050	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		
0060	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		
0070	06 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
0080	00 00 00 00 00 01 00 00 00 00 00 00 00 00 00		
0090	00 00 00 00 00 00 00 00 30 00 00 00 68 00 00O...h...		
00A0	00 00 18 00 00 00 03 00 4A 00 00 00 18 00 01J.....		
00B0	05 00 00 00 00 00 03 00 09 71 E4 09 EC 66 D0 01q...f..		
00C0	09 71 E4 09 EC 66 D0 01 09 71 E4 09 EC 66 D0 01	.q...f...q...f..		
00D0	09 71 E4 09 EC 66 D0 01 00 40 00 00 00 00 00 00	.q...f...@.....		
00E0	00 40 00 00 00 00 00 00 06 00 00 00 00 00 00	.@.....		
00F0	04 03 24 00 4D 00 46 00 54 00 00 00 00 00 00	..\$.M.F.T.....		
0100	80 00 00 00 48 00 00 00 01 00 40 00 00 00 01	...H.....@.....		
0110	00 00 00 00 00 00 00 00 3F 00 00 00 00 00 00?.....		
0120	40 00 00 00 00 00 00 00 00 00 04 00 00 00 00	@.....		
0130	00 00 04 00 00 00 00 00 00 00 04 00 00 00 00		
0140	21 40 55 21 00 F8 FF FF B0 00 00 00 50 00 00	!@U!.....P...		
0150	01 00 40 00 00 00 03 00 00 00 00 00 00 00 00	..@.....		
0160	01 00 00 00 00 00 00 00 40 00 00 00 00 00 00@.....		
0170	00 20 00 00 00 00 00 00 08 10 00 00 00 00 00		
0180	08 10 00 00 00 00 00 00 21 01 54 21 21 01 FE FD!..T!!...		
0190	00 DE 8B 02 80 FA FF FF FF FF FF FF 00 00 00		
01A0	00 00 04 00 00 00 00 00 21 40 55 21 00 F8 FF FF!@U!...		
01B0	B0 00 00 00 50 00 00 00 00 40 00 00 00 03 00	...P.....@.....		
01C0	00 00 00 00 00 00 00 00 01 00 00 00 00 00 00		
01D0	40 00 00 00 00 00 00 00 20 00 00 00 00 00 00	@.....		
01E0	08 10 00 00 00 00 00 00 08 10 00 00 00 00 00		

22. Each record's respective metadata can have multiple attributes and the same techniques that were applied in this lab can be used for each NTFS System file. As an example, click on the **\$Bitmap** file in the left pane.



23. Navigate to the **Attributes** tab while having the *\$Bitmap* file selected.



24. Notice the resident and non-resident data is shown for each attribute when looking through the different *Records*.

Hex Dump	Metadata	Data	Attributes	INDX
Attribute, type 0x10				
Type			16	
Reported Name				
Type Name			\$STANDARD INFORMATION	
Attributes			<none>	
Size			96	
Resident			True	
<div> <div>0000 10 00 00 00 60 00 00 00 00 00 18 00 00 00 00 00</div> <div>0010 48 00 00 00 18 00 00 00 09 71 E4 09 EC 66 D0 01 H.....q...f..</div> </div> <div>ASCII</div>				
Attribute, type 0x30				
Type			48	
Reported Name				
Type Name			\$FILENAME INFORMATION	
Attributes			<none>	
Size			104	
Resident			True	
<div> <div>0000 30 00 00 00 68 00 00 00 00 00 18 00 00 00 02 00 O...h.....</div> <div>0010 50 00 00 00 18 00 01 00 05 00 00 00 00 00 05 00 P.....</div> </div> <div>ASCII</div>				
Attribute, type 0x80				
Type			128	
Reported Name				
Type Name			\$DATA	
Attributes			<none>	
Size			72	
Resident			False	
<div> <div>0000 80 00 00 00 48 00 00 00 01 00 40 00 00 00 04 00H....@....</div> <div>0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</div> </div> <div>ASCII</div>				

If the *Hex Dump* data cannot be seen underneath *Resident*, expand the window size so that the window takes up the entire screen. Once this is done, the *Hex Dump* data will appear.

25. Close all **PC Viewers** and end the reservation to complete the lab.