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

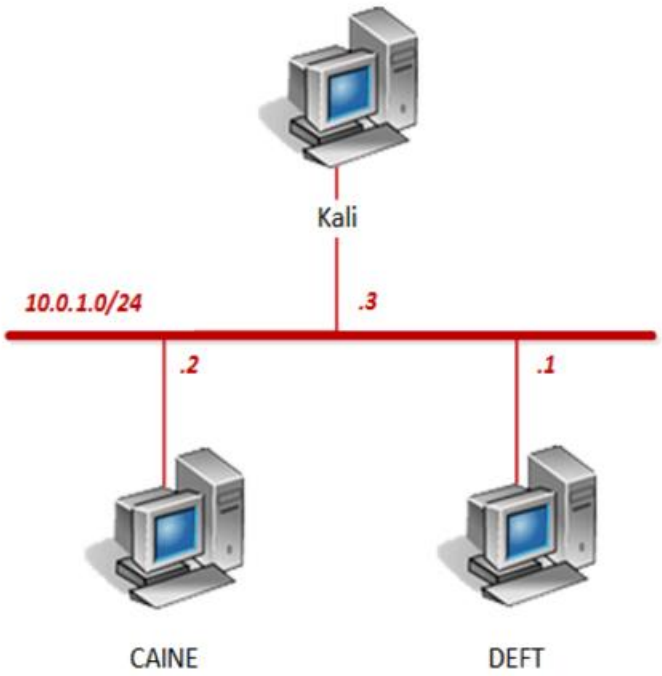
The Windows New Technology File System (NTFS) file system is commonly used to organize and handle functions such as read, write and search on most Windows Operating Systems, starting with Windows NT. In this lab, we will explore the NTFS system and how to interpret the Master File Table or MFT.

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**.

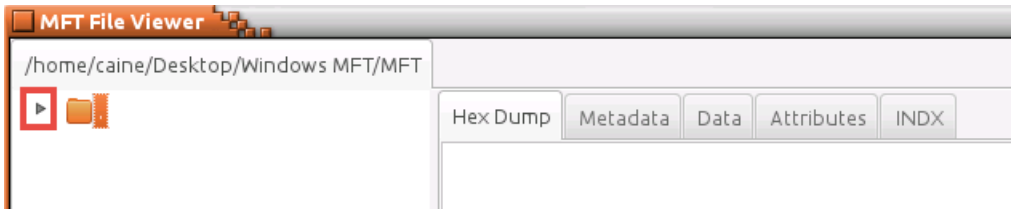
```
cd /usr/local/bin
```

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

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

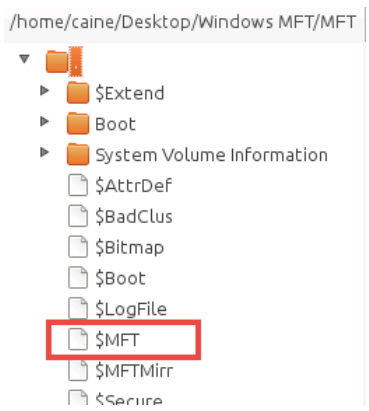
A new *MFT File Viewer* screen will appear.

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

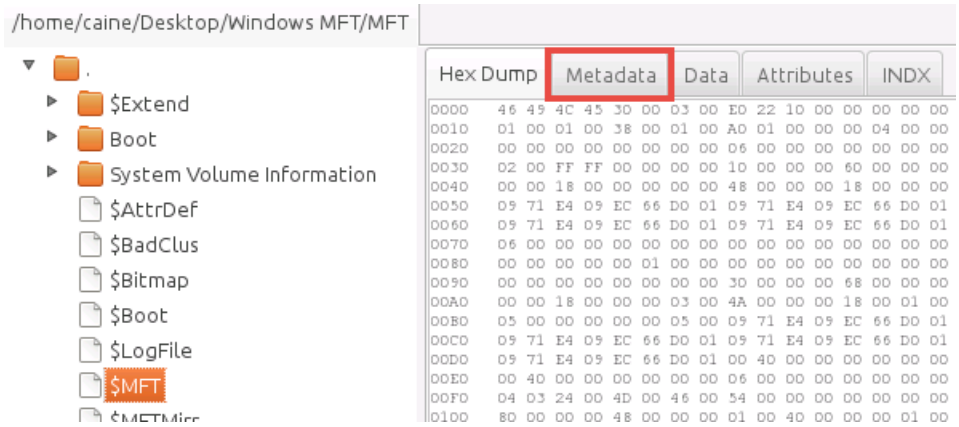


Once expanded, notice the *NTFS* metadata present for the system files.

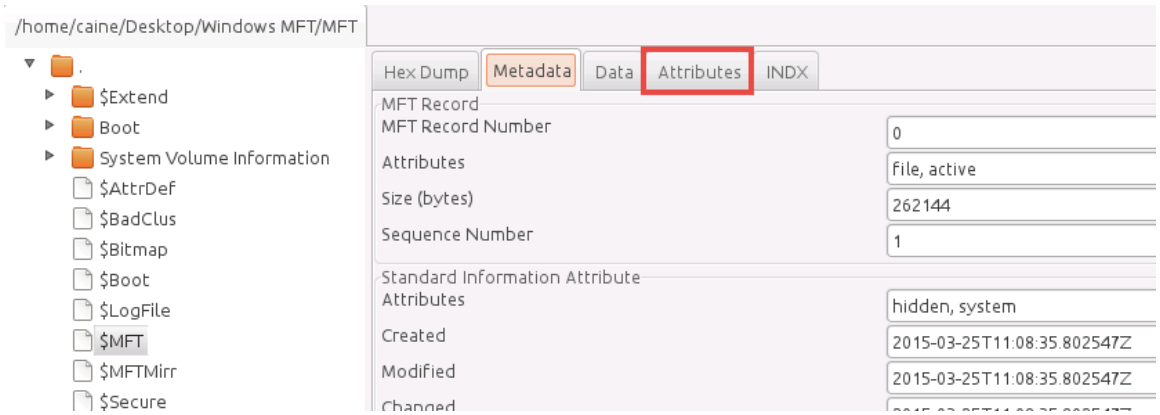
6. In the left pane, click on the **$MFT** file to explore the metadata.



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

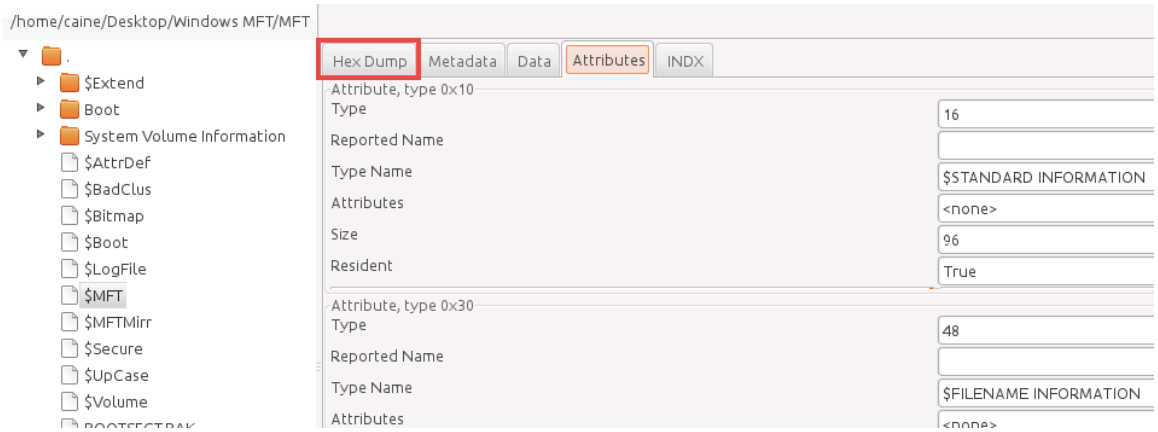


8. On the *Metadata* tab, this is the first record or "Record 0" for the file system. Found within the *MFT* record are various attributes. Click on the **Attributes** tab.

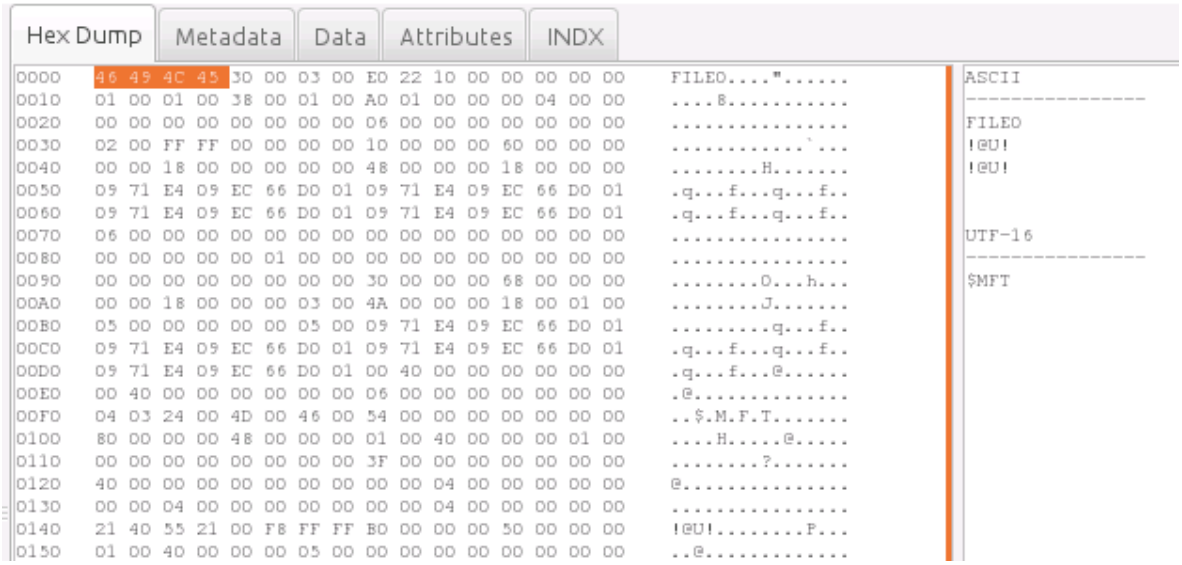


In each *Record*, there are attributes. The first attribute type *0x10* is called *$Standard Information*. Its type is *16* which is the decimal equivalent to hex value of *0x10*. Its respective size is *96* bytes and the file is *Resident* (True) in the MFT. Resident means its size is less than 512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

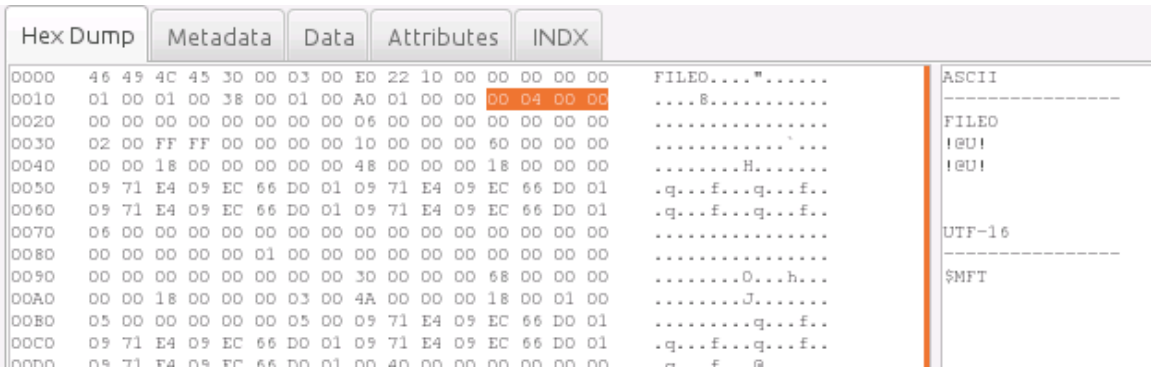
9. Click on the **Hex Dump** tab to view the hex values.



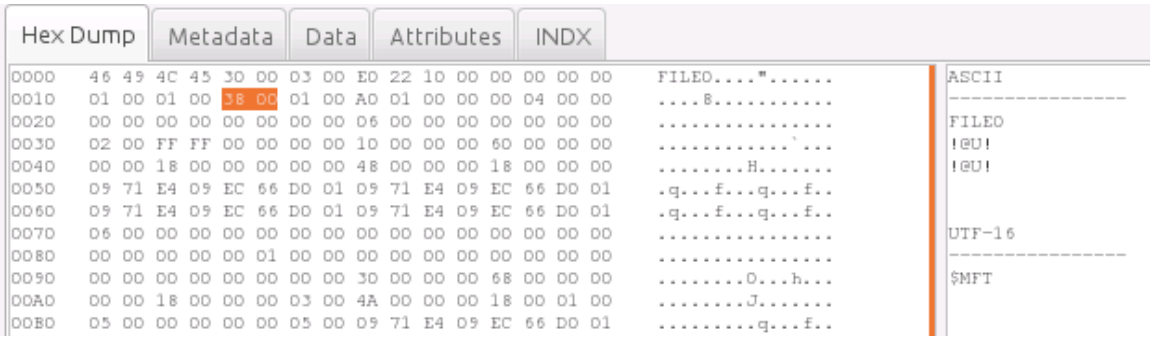
10. Notice that the *MFT* header fields all start with *File 0* at offset *0x00*.



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

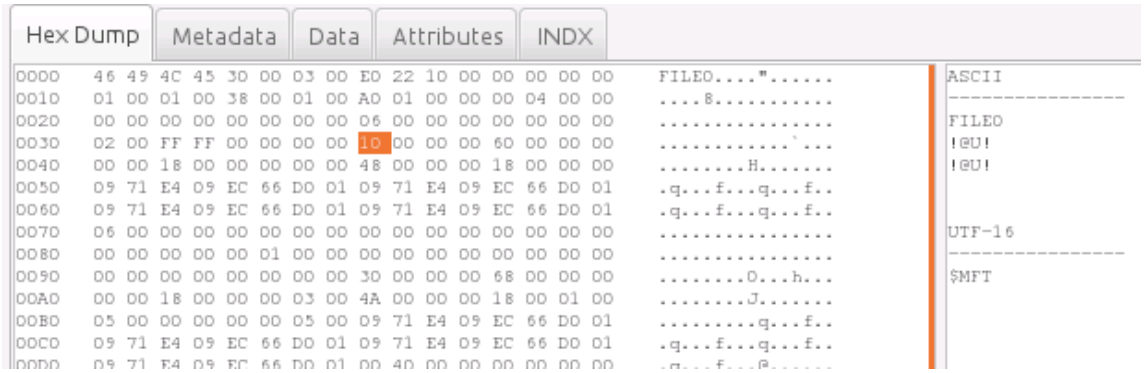


12. Locate the length of the header at offset *0x14* and is 0x38 or 56 bytes.

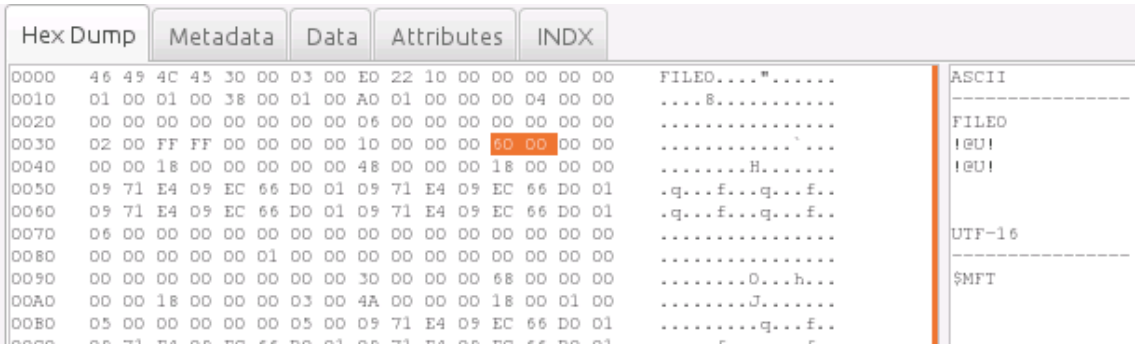


2 Identifying Attributes with MFT File Viewer

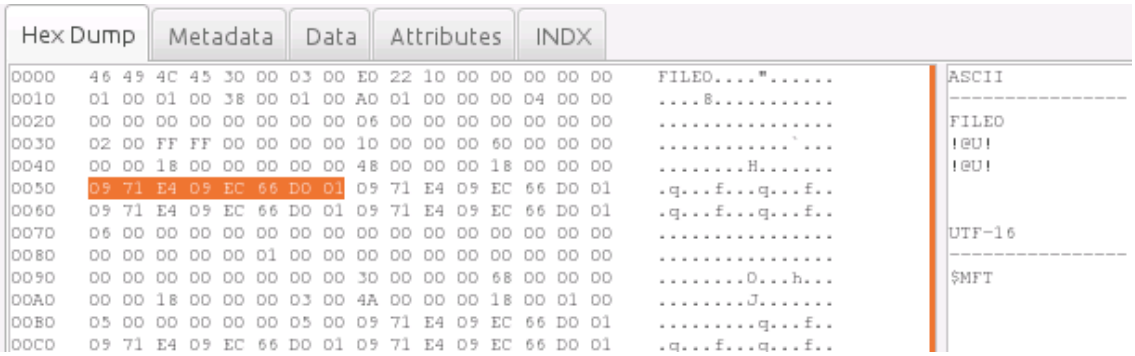
1. While on the *Hex Dump* tab, locate where the *Standard Information* attribute *0x10* starts on offset 0x38.



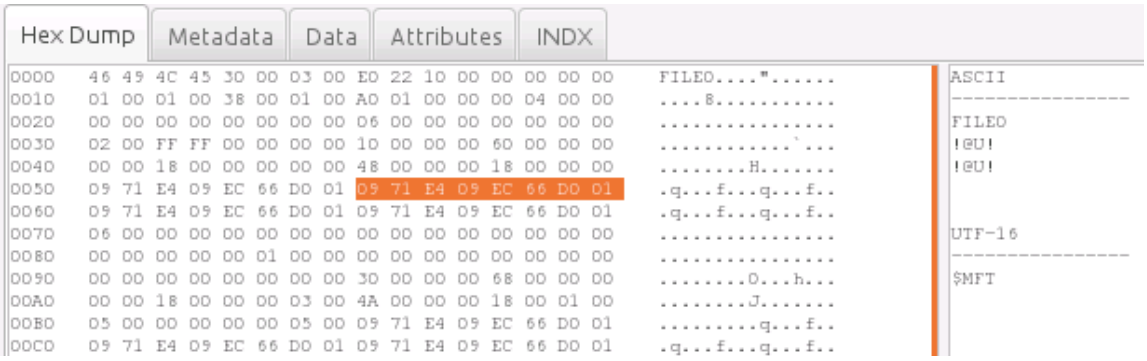
2. The size of the *Standard Information* attribute is at offset *0x04* and *0x05* from the beginning of the attribute. Its size is 0x60 or 96 bytes.



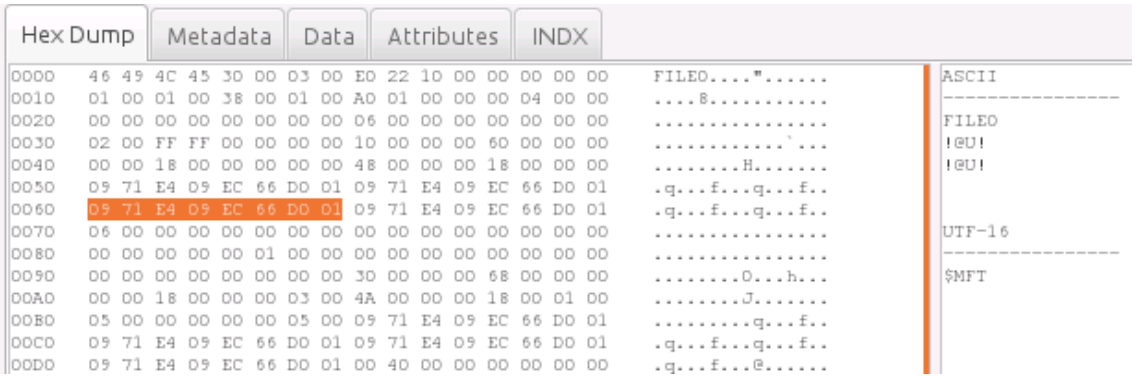
3. Identify the creation date and time at *0x18* to *0x1F*. When decoded, it can be concluded that this is stored in a Windows 64 bit hex format – Little Endian.



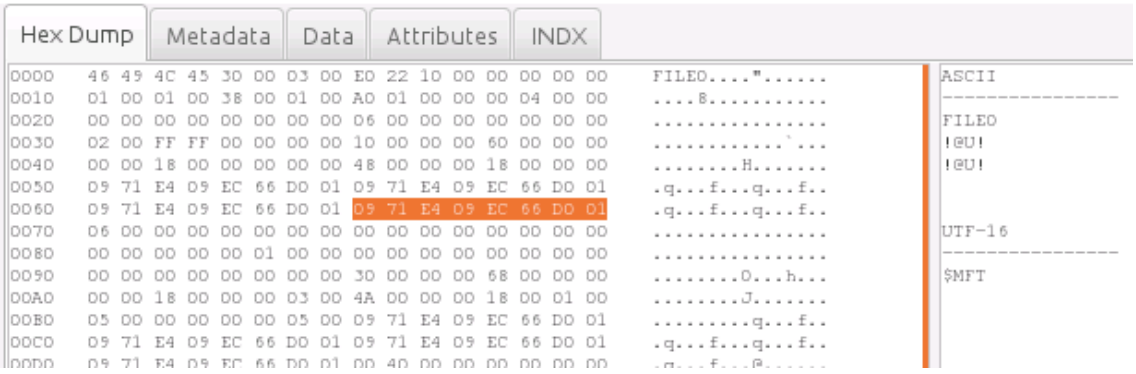
4. The last modified date and time for the file is next. Notice that the value is the same as the previous creation date and time.



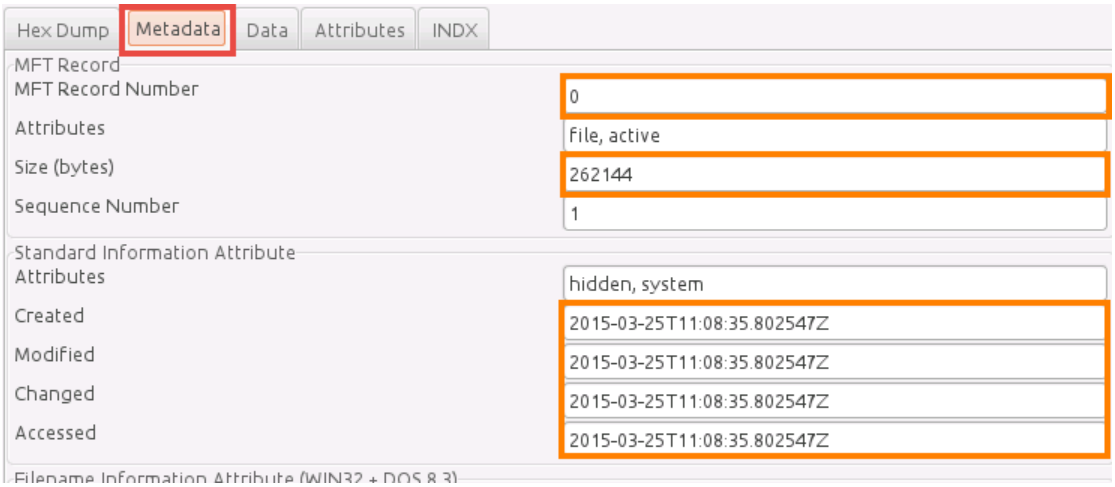
5. Next is the last access date and time. Notice the same value again.



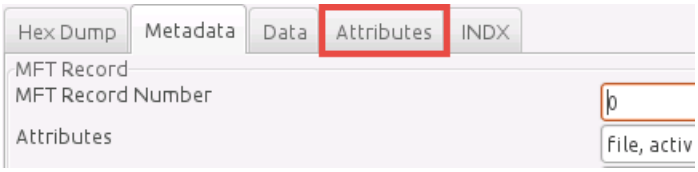
6. The next line of hex is the record access date and time. Notice the dates are the same.



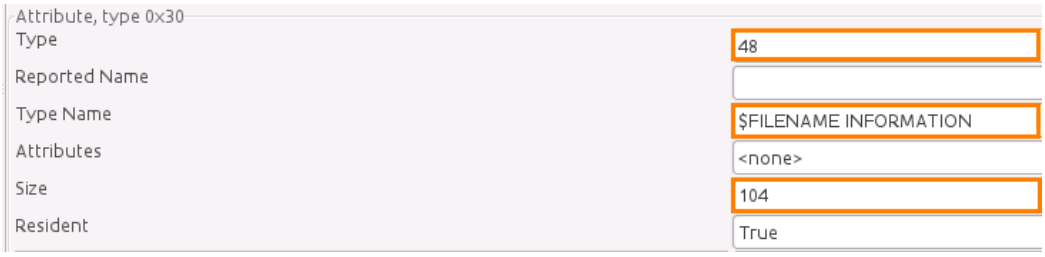
7. Navigate to the **Metadata** tab and compare the values to the actual values. The hex values should match.



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

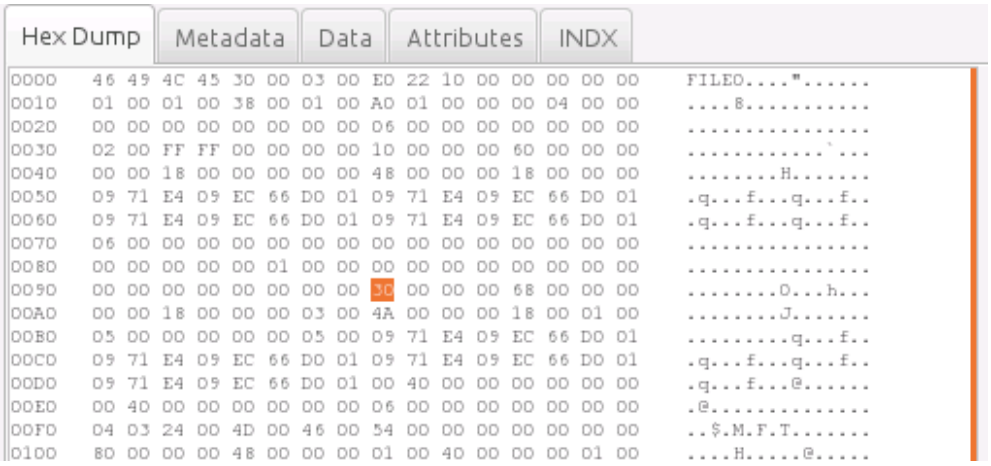


9. Identify the next attribute, *0x30 $Filename Information*. Its type is 48, which is decimal for *0x30*. Its respective size is 104 bytes and its resident.

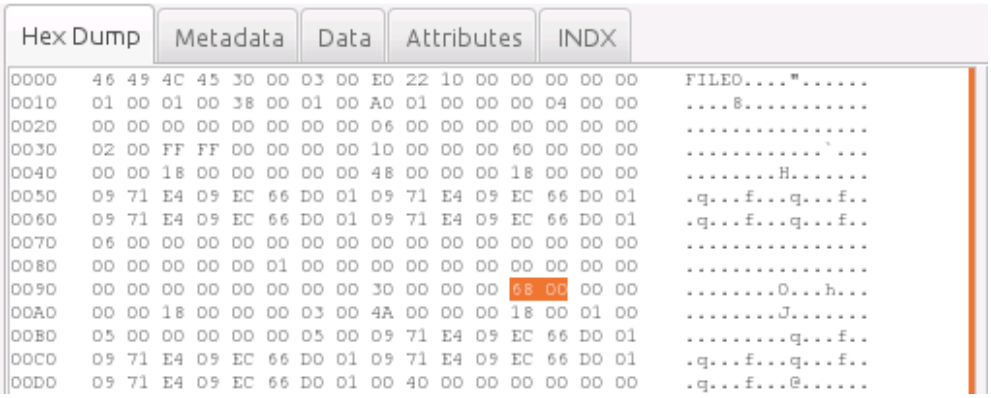


10. Click on the **Hex Dump** tab.

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

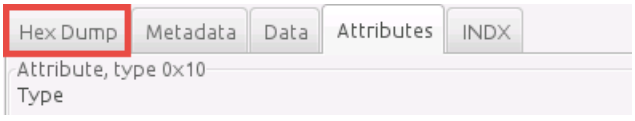


12. Identify the size by locating bytes *0x04* and *0x05* from the *0x30*. Notice the size is 68 bytes in hex, which is 104 bytes in decimal. It is also a resident record.

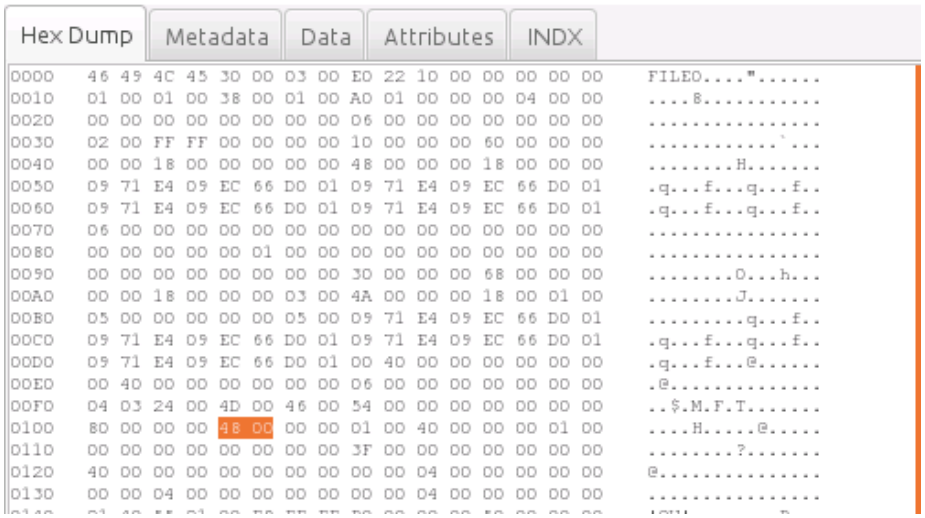


13. Click on the **Attributes** tab and identify the 0x80 attribute.

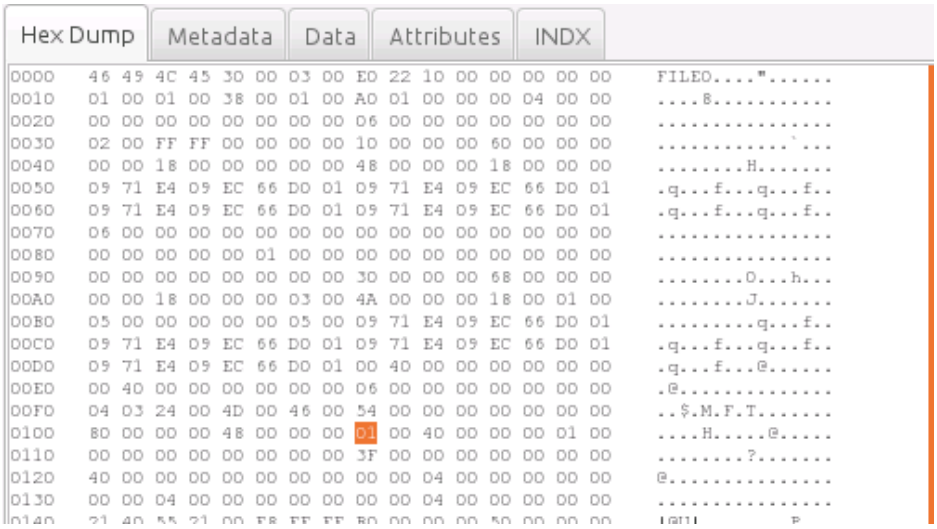
14. Notice the attribute is the *$Data* attribute, which is type *0x80* or 128. Its size is 72 bytes and its non-resident.
15. Click on the **Hex Dump** tab to analyze the *$Data* attribute more closely.



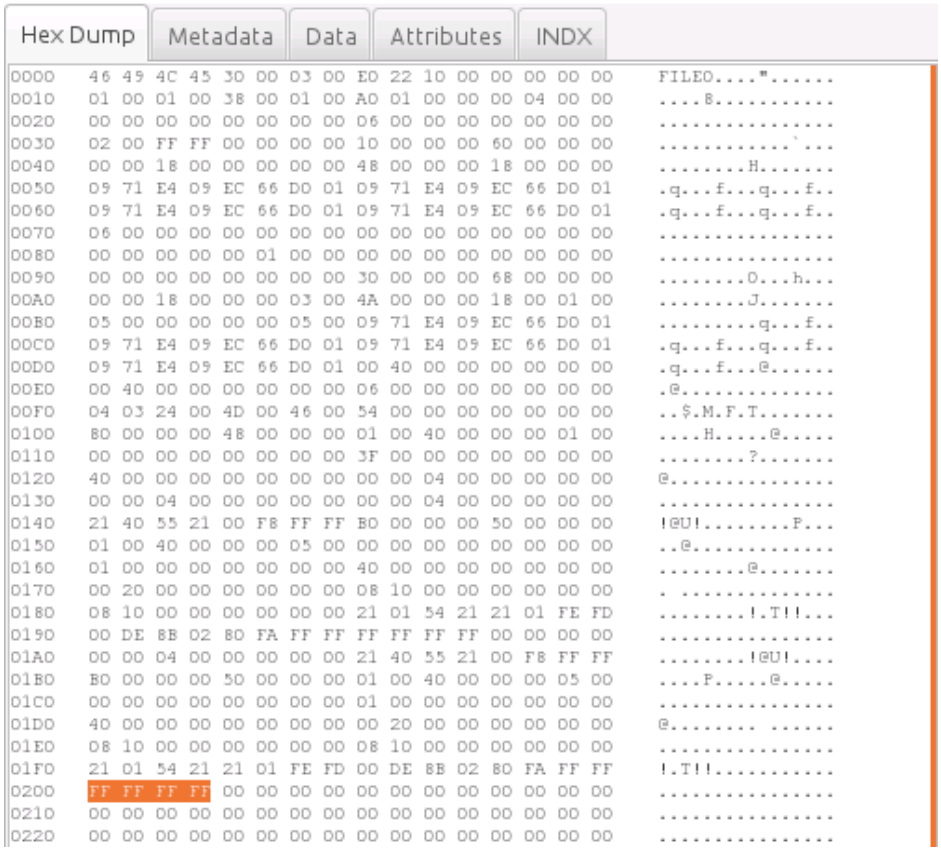
16. Identify offset *0x100* to locate attribute *0x80*. Move to bytes 0x04 and 0x05 from there to find the size.



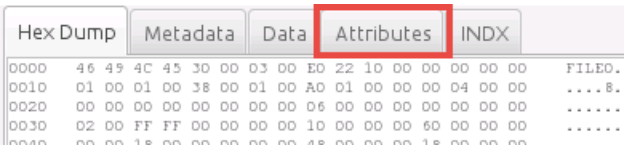
17. Notice that it is 48 in hex or 72 bytes in decimal. Move three more bytes to find the non-resident flag set.



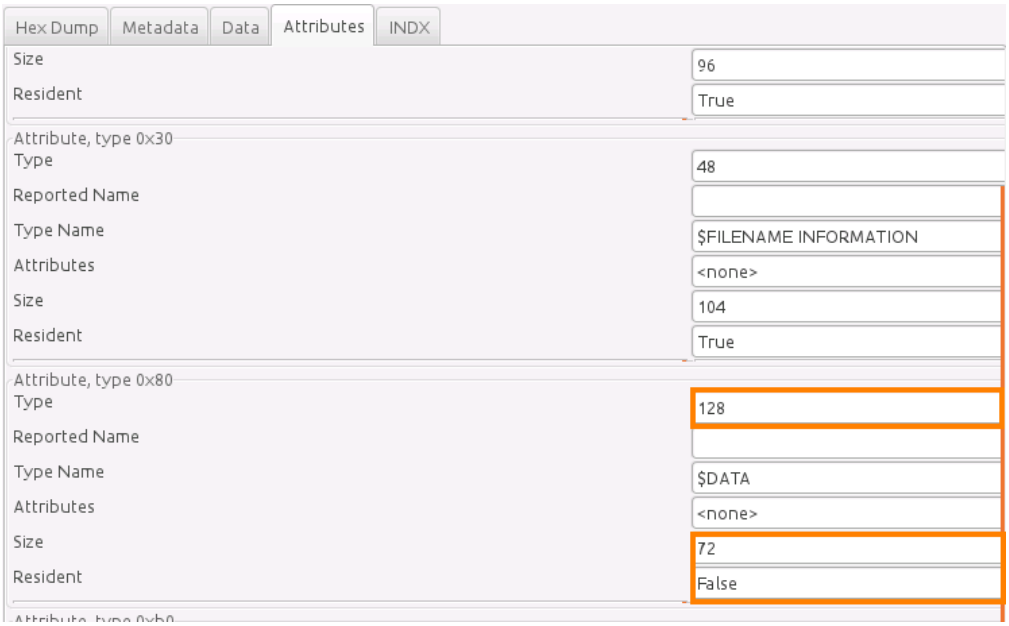
18. Notice that the end of the MFT record is at offset 0x200.



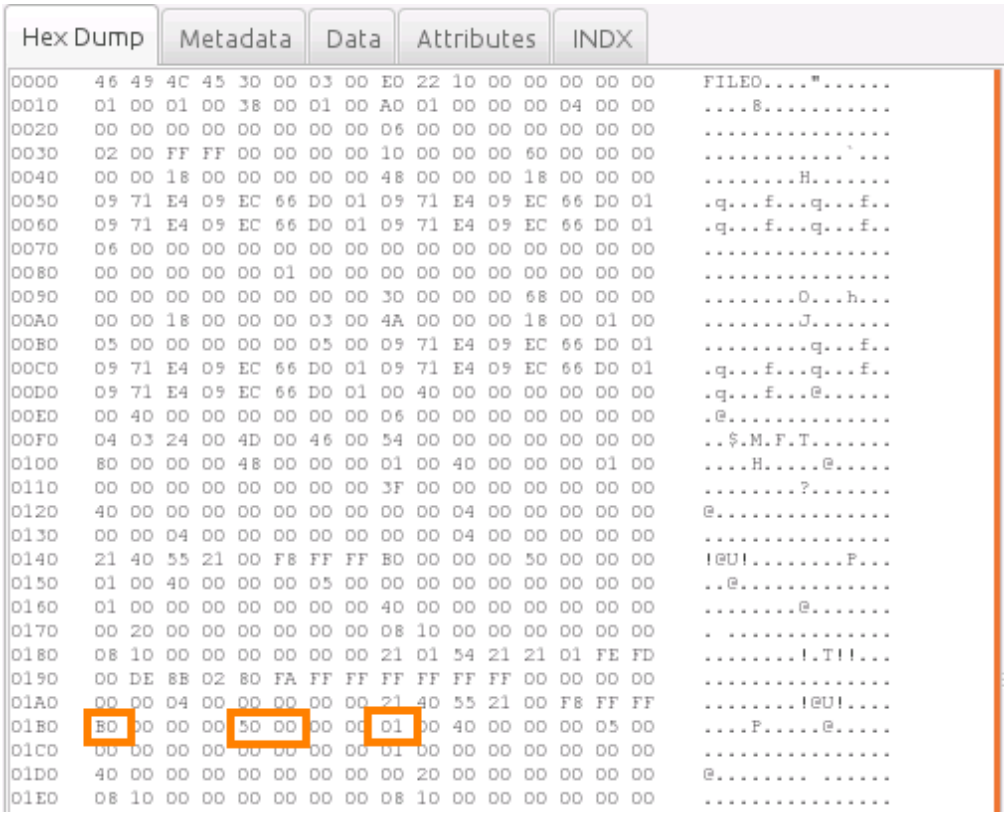
19. Click on the **Attributes** tab.



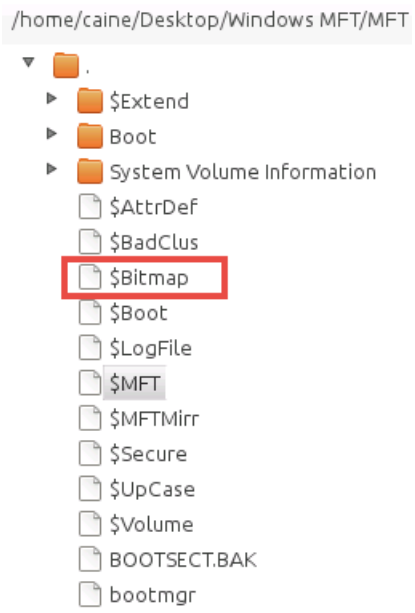
20. Compare the values found from the *Hex Dump* tab to the *Attributes* tab.



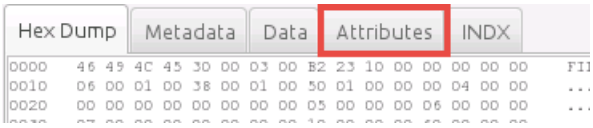
21. Click on the **Hex Dump** tab. The last record is *$Bitmap* and its type *0xb0* is 176 bytes in decimal. Its size is 80 in hex and is non-resident.



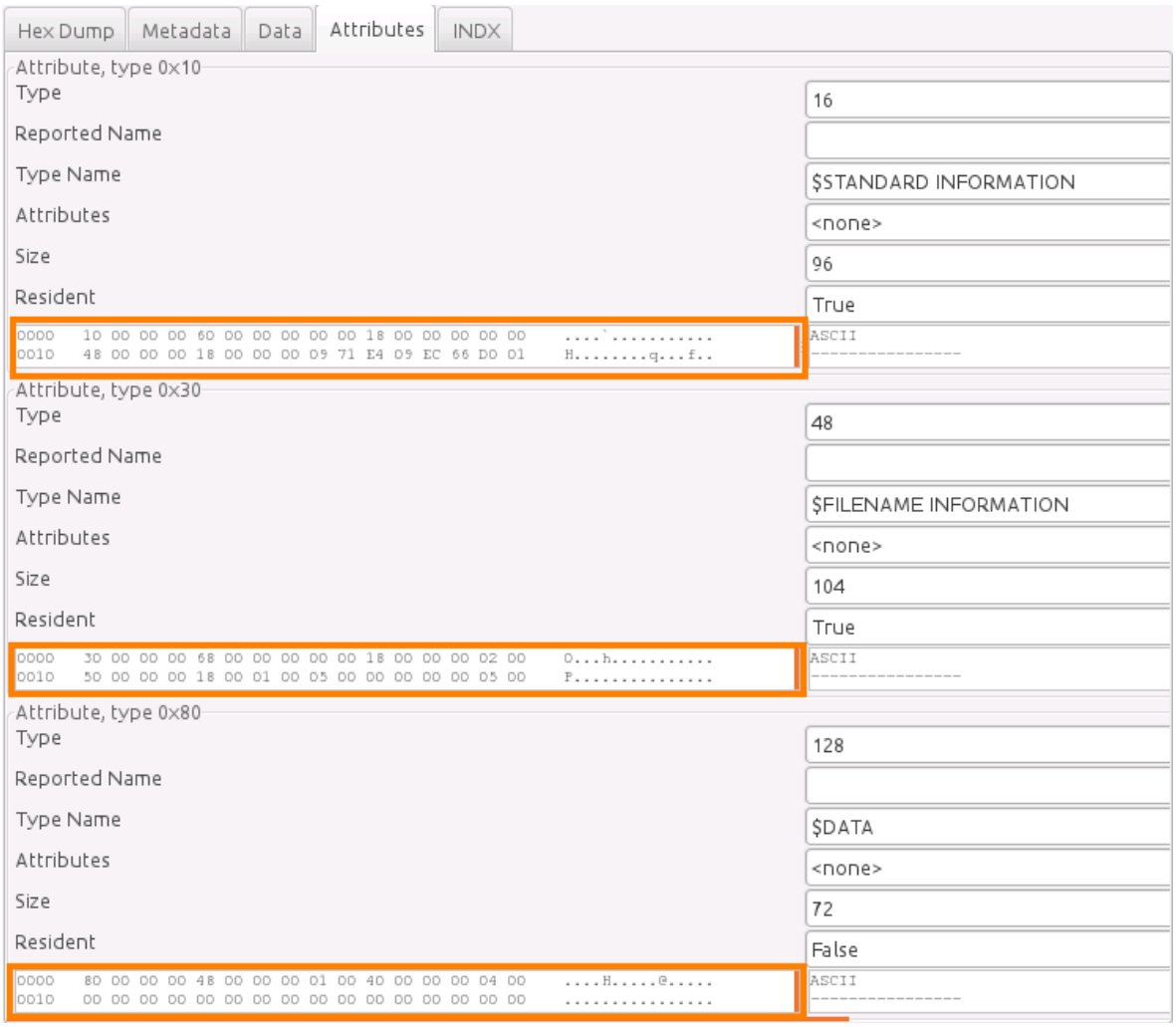
22. Each record's respective metadata can have multiple attributes and the same techniques that were applied in this lab can be used for each NTFS System file. As an example, click on the **$Bitmap** file in the left pane.



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*.



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.

