Lab 3: File Headers and Hive

CNIT42000-001

Ethan Hammond

Prof. Tahir Khan

Date Submitted: 3/2/23

Date Due: 3/4/23

Table of Contents

Abstract

During the forensic investigation of InCh05.img and some created test files, it was demonstrated how to use software like WinHex to examine file hexadecimal data, OSForensics to examine user account and password data, and FTK Imager to examine user and Windows registry data. All of these forensic investigation tools are critical to a cyber forensics specialist. User data as shown in files like SAM.dat can be used to see when users were logged in, when they changed passwords, and when they modified their accounts. Tools like OSForensics can be used to extract important confidential data out of drives to find the most amount of relevant data off of data sources as well as capture passwords to access more of a user's encrypted drives. All of these methods can be used to investigate a user's digital data and be used in court or given to higher up officials to further an investigation.

Report

Task 1

In order to examine the contents of an MFT, a file was created to be examined in the file. This file was created with sample text provided by the Lab Manual. The contents of the file can be seen in Figure 1 below.

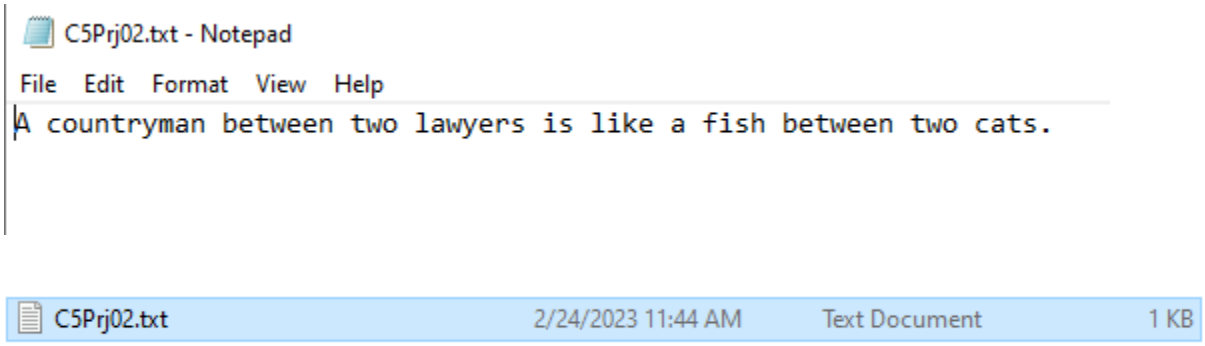

Figure 1: Creation of Text file to be viewed in the MFT

WinHex was put into Read-only mode to prevent the digital forensic professional from accidentally writing data to the file that should not be there. This could alter the hash of the drive image and make it no longer usable as evidence or falsely convict somebody. The setting change can be seen in Figure 2 below.

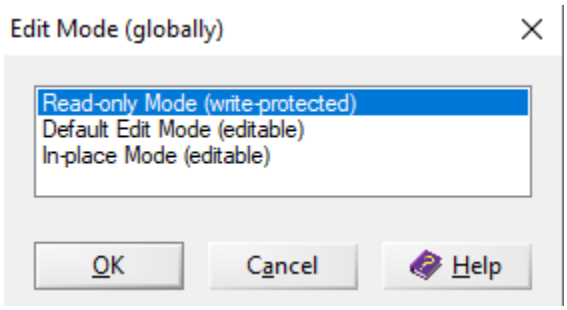

Figure 2: Putting the WinHex program in Read-only Mode

Within WinHex, the data interpreter window allows forensic specialists to view specific data from the extracted hex text. In this case, Windows FILETIME was to be selected to be able to see dates and times that files were created and modified. This setting can be seen in Figure 3 below.

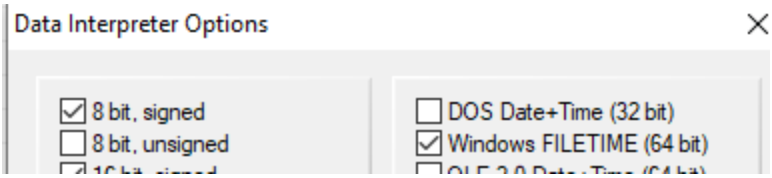

Figure 3: Adjusting the Data interpreter settings

After the file was selected in WinHex, the hex values were analyzed from the MFT. The data interpreter Window on the top right shows all of the filetime contents to the examiner. The hex files were translated to Filetime dates by offsetting the hex values by a certain amount. The first 50 hex values show the file creation time, the next 8 show the file altered date, and the next 2 show the last access time. From the next offset to 0xB8, 0xC0, 0xC8, and 0xD0 show the file creation, file alter time, file read time, and MFT change from a specific file name. These examinations can be seen in Figures 1-9.

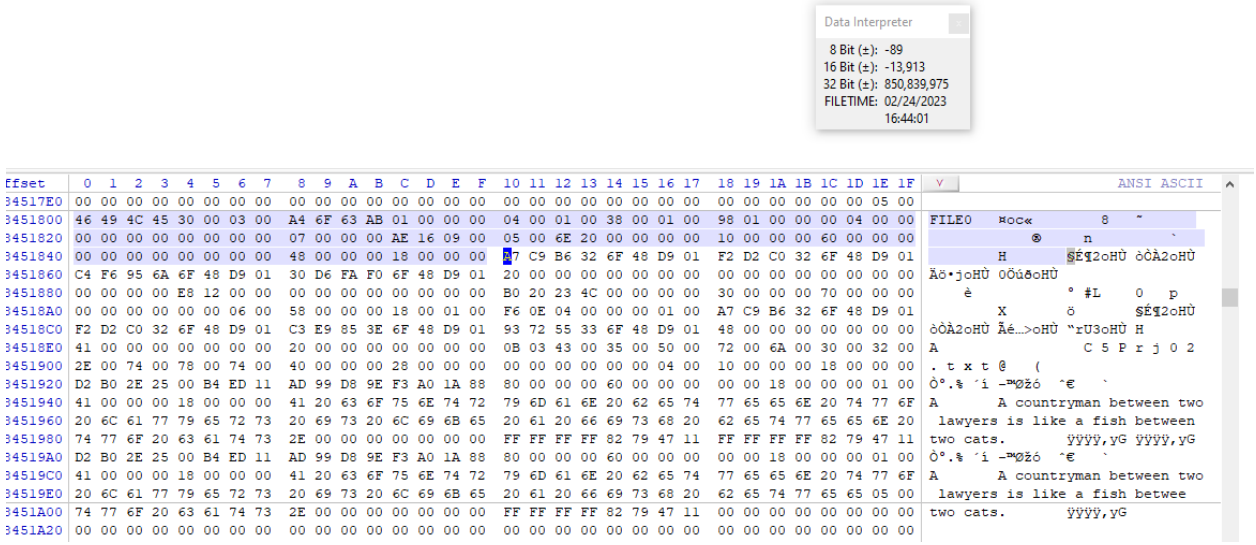

Figure 4: File creation time offset 0x50.

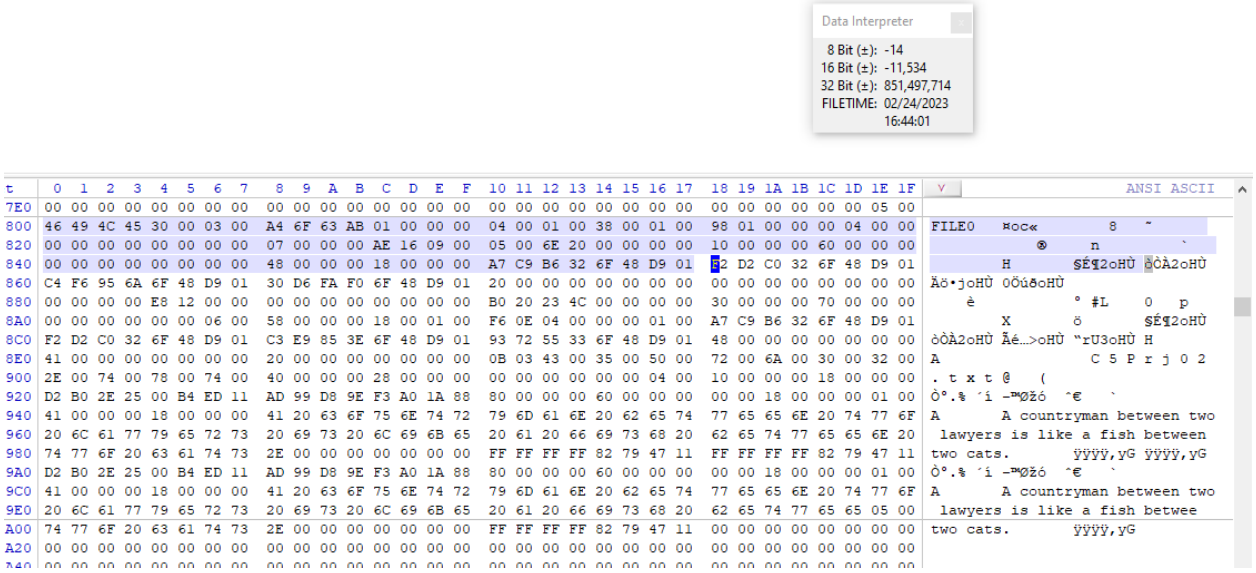

Figure 5: File alter time with offset 0x58.

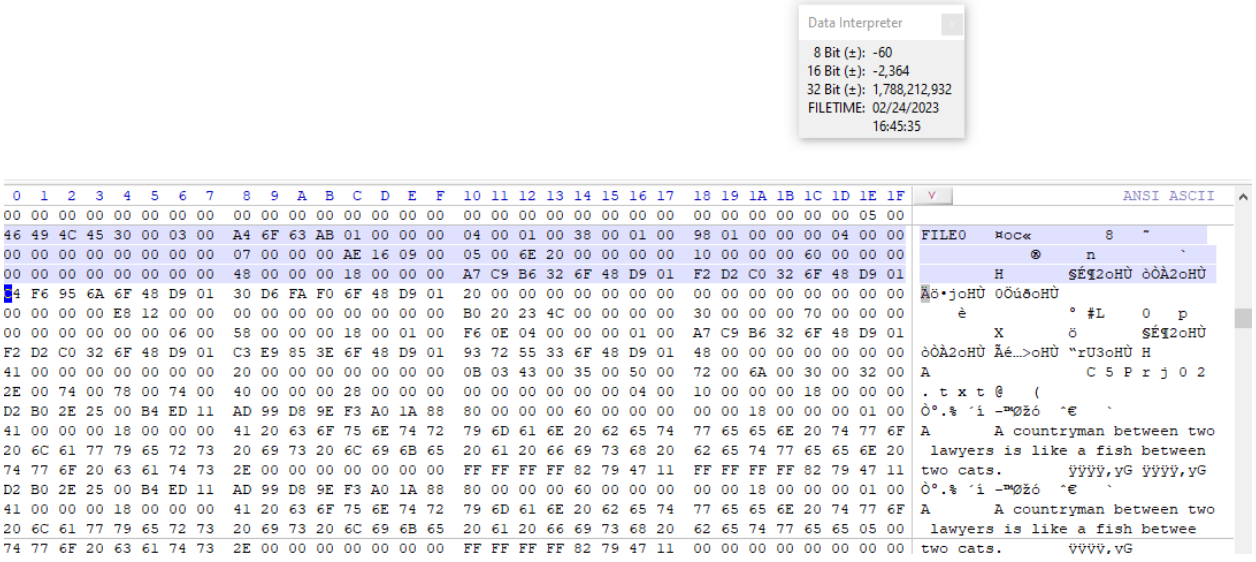

Figure 6: File last access time with offset 0x60.

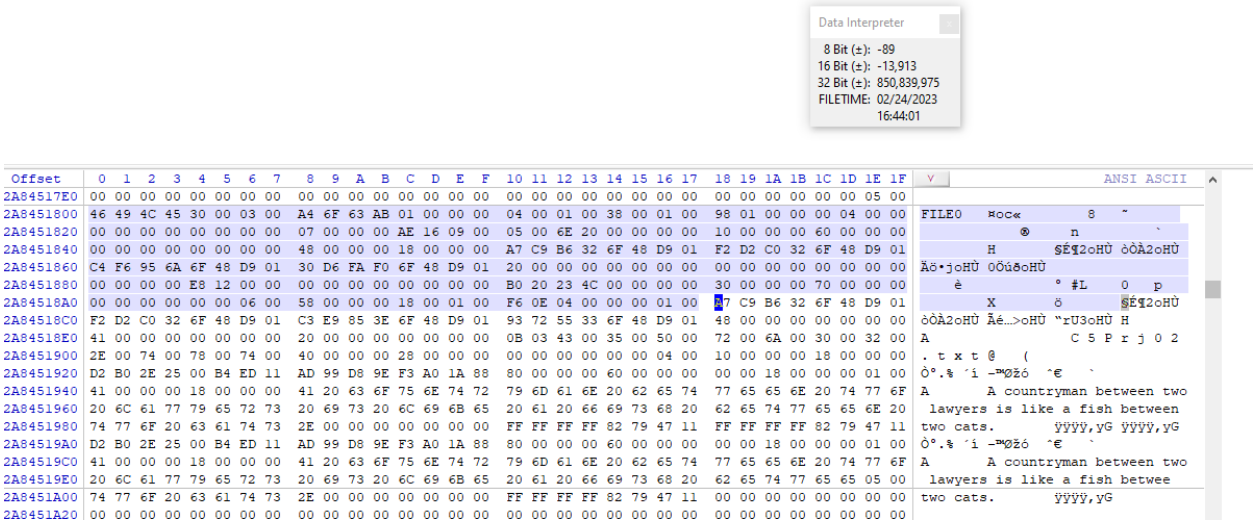

Figure 7: File creation time with offset 0xB8.

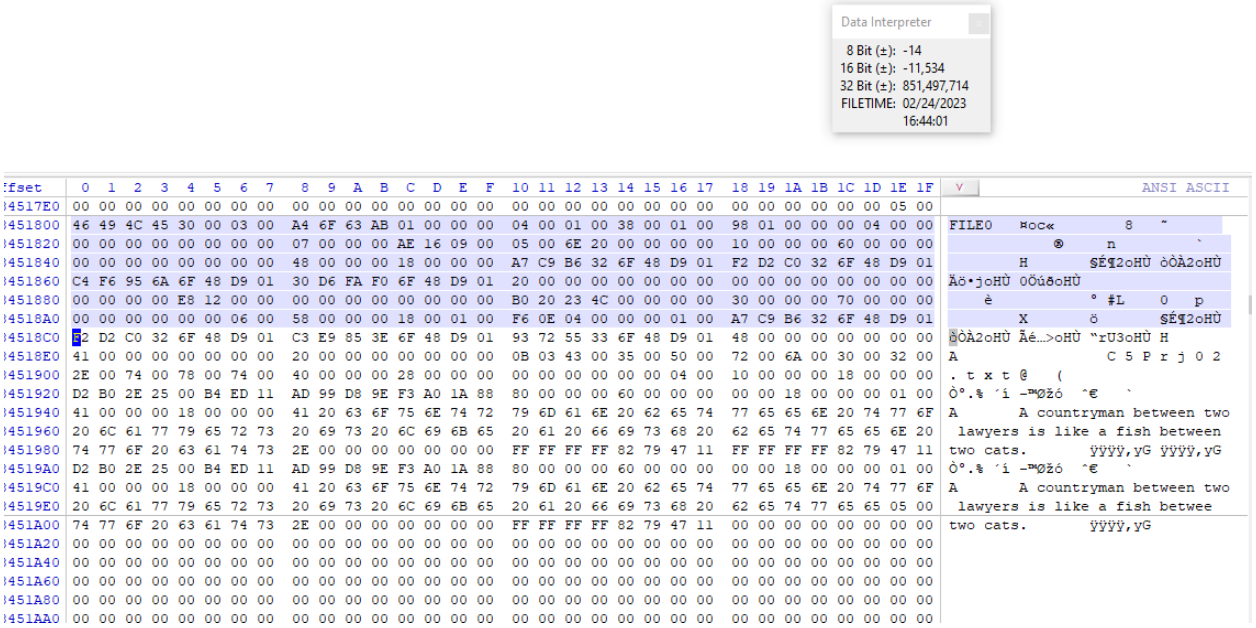

Figure 8: File alter time with offset 0xC0.

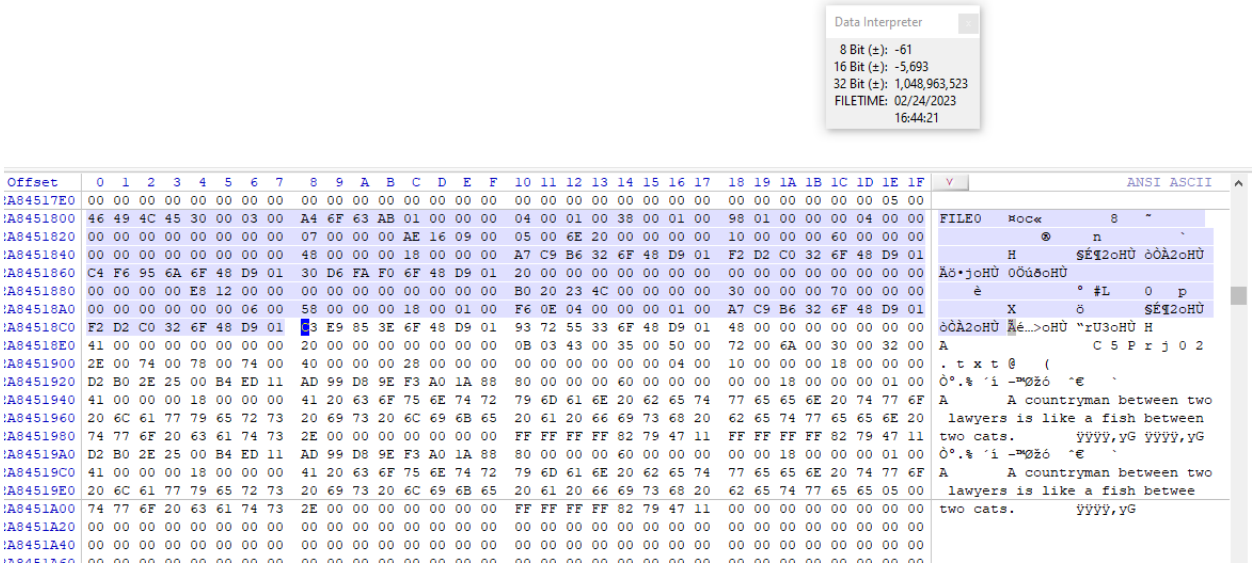

Figure 8: File read time with offset 0xC8.

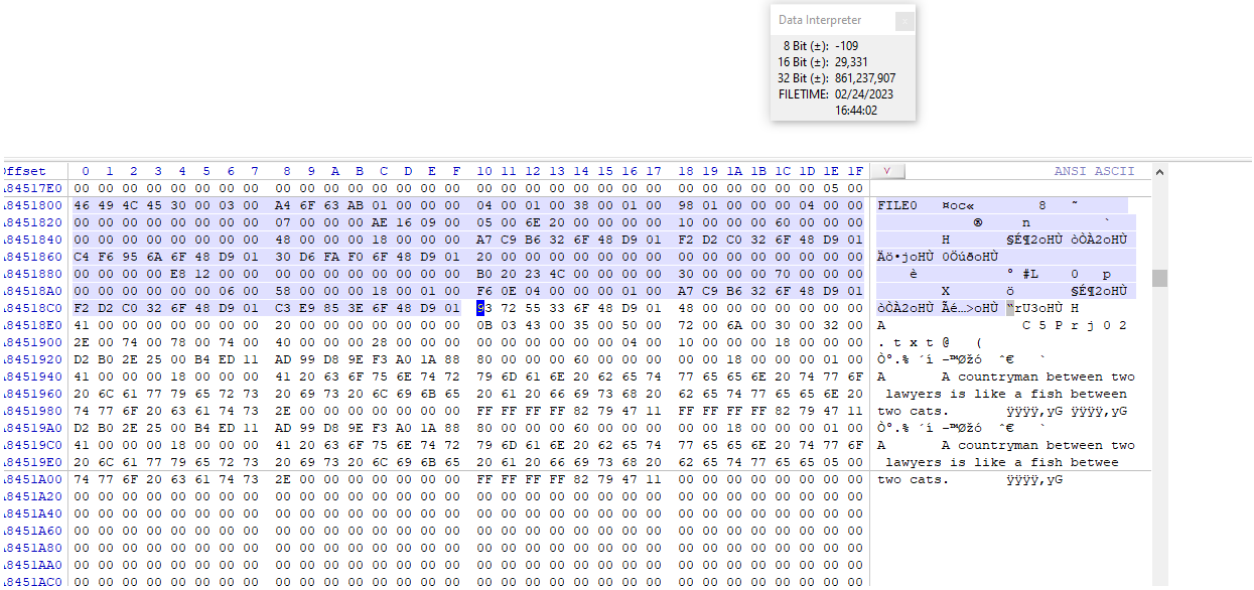

Figure 9: MFT Change time with offset 0xD0.

Task 2:

Several files were created to be examined in WinHex. These files consisted of .xlsx, .gif, .jpg, .mp3, and .docx files seen in Figure 10 below.

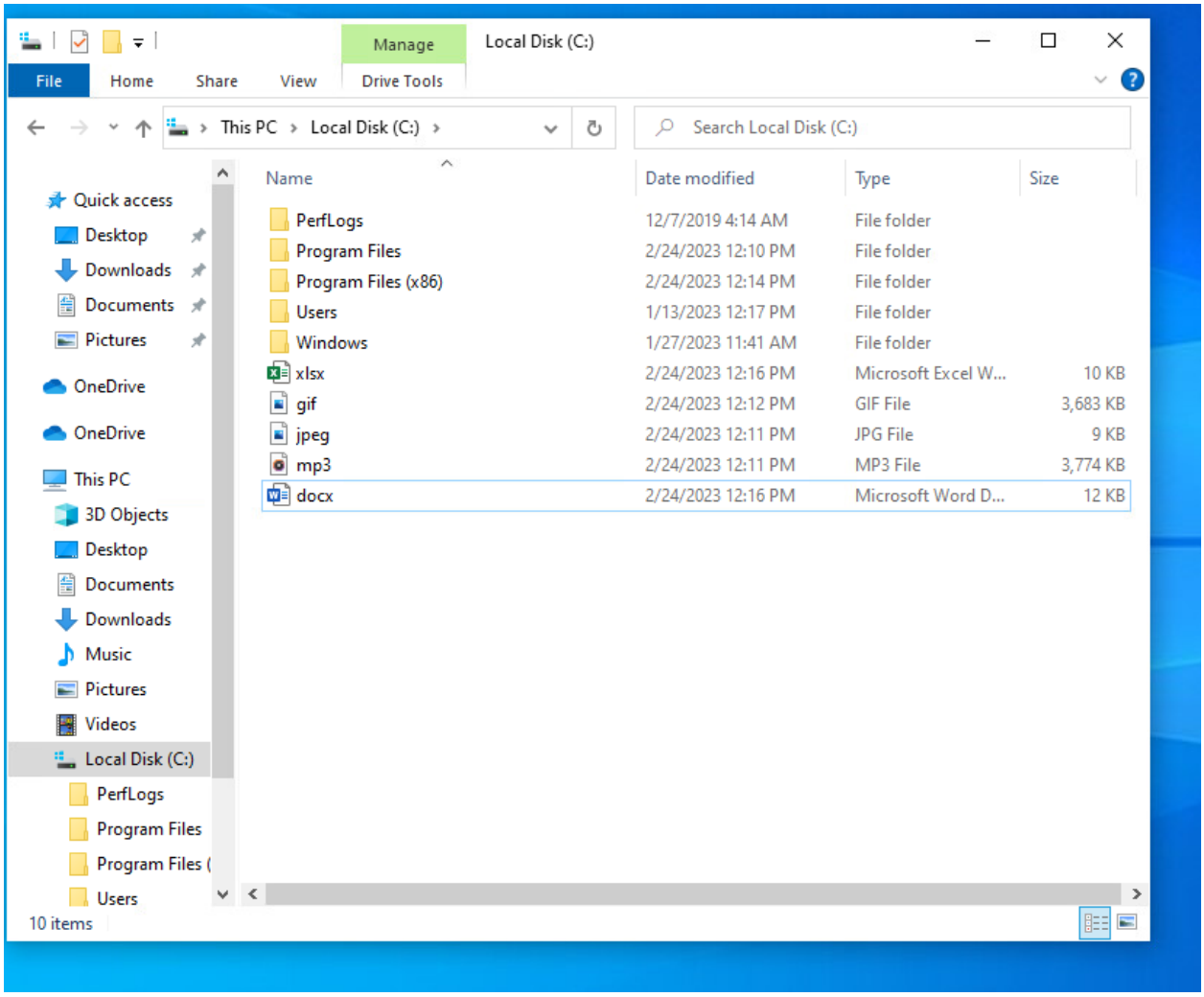

Figure 10: Creation of Excel, Word, JPG, MP3, and GIF Files for examination.

File signatures can be recorded by clicking on a file in WinHex and examining the first bits. These bits can tell the viewer what file extension this is. This is how the Windows operating system knows what files types are. File signatures for all files shown in Figure 10 are shown below in Figure 11.

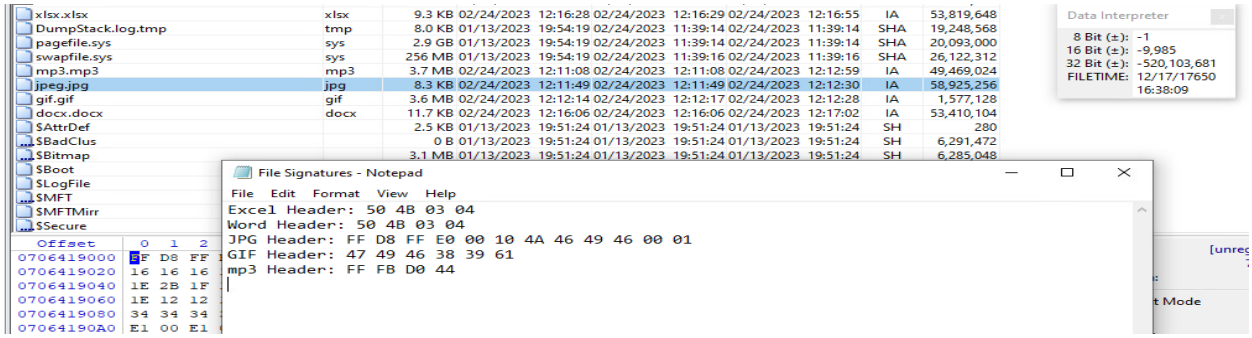

Figure 11: File signatures recorded for all created files in Figure 10.

Task 3

Before anything can be done within OSForensics, it is necessary to create a new case with the software. This is shown below in Figure 12.

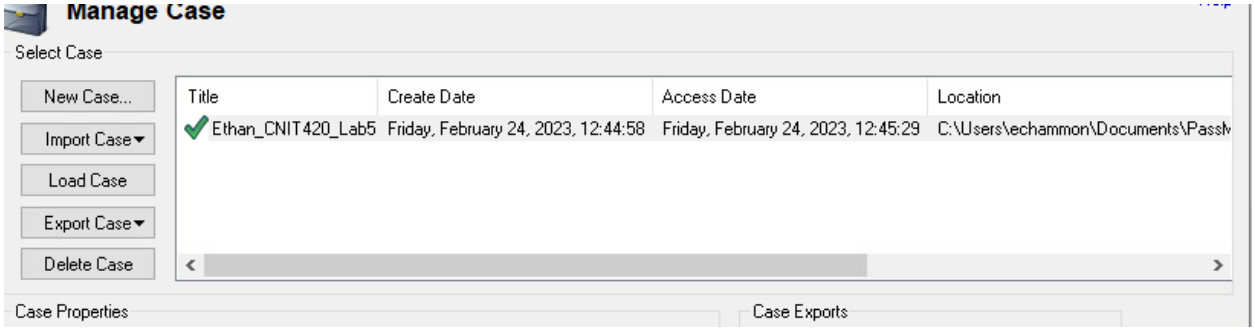

Figure 12: Creation of case in OSForensics

As with other forensic recording software, the data source is added as an image file provided on Brightspace to be examined. This can be seen below in Figure 13.

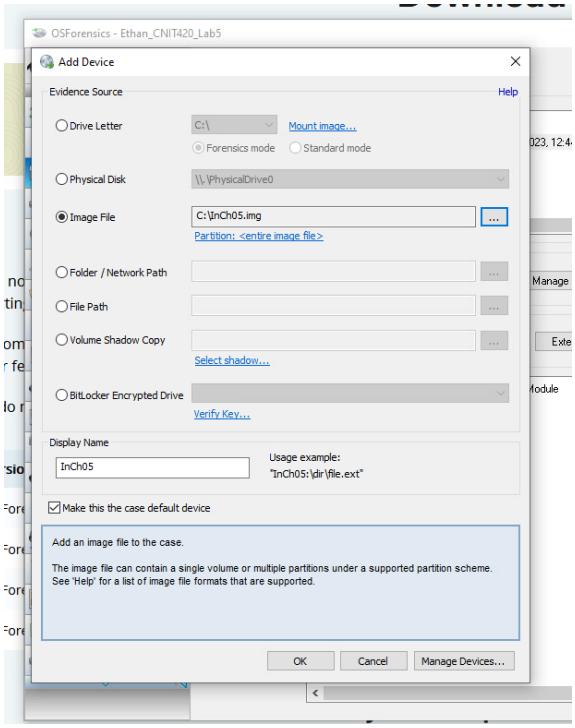

Figure 13: Input of data source InCH05.img.

OSForensics contains a tool that can allow the drive or image to be scanned for passwords and usernames. The passwords captured were for user ‘jfriday’ and were ‘thunder’. The capture can be seen below in Figure 14.

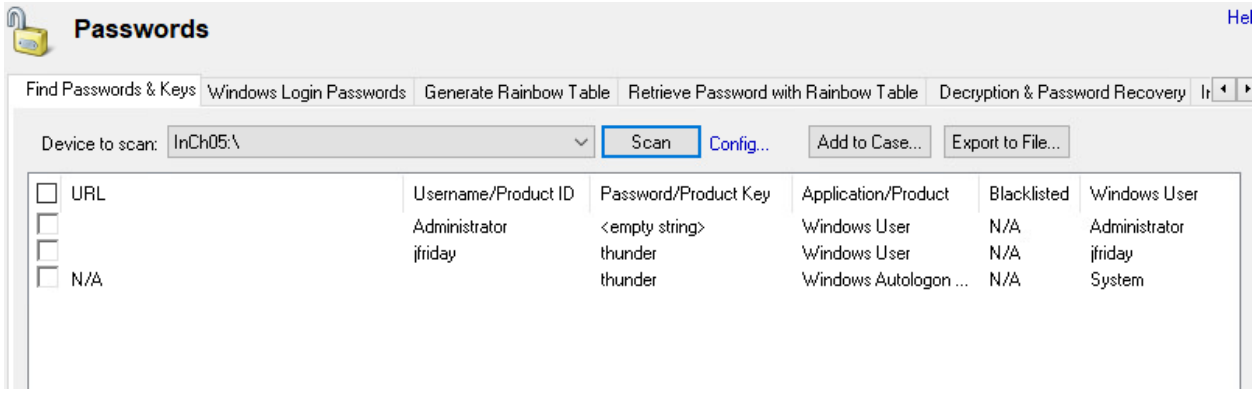

Figure 14: All scanned passwords from OSForensics

Scans can also be completed for Windows logins. Only 1 password was able to be scanned off of the drive and can be seen in Figure 15 below.

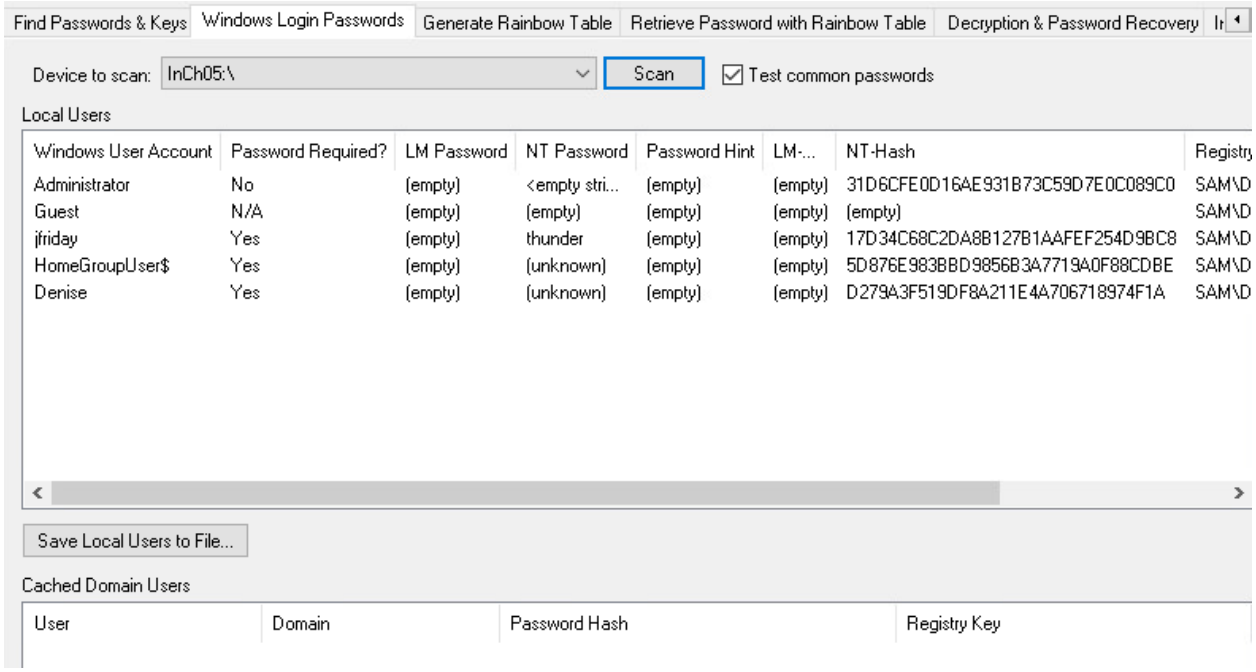

Figure 15: Scanned Windows Login Passwords.

It was necessary to attach the Windows passwords to the case before the report was generated so that all relevant information to the case is included in the OSForensics report. The attachment can be seen below in Figure 16.

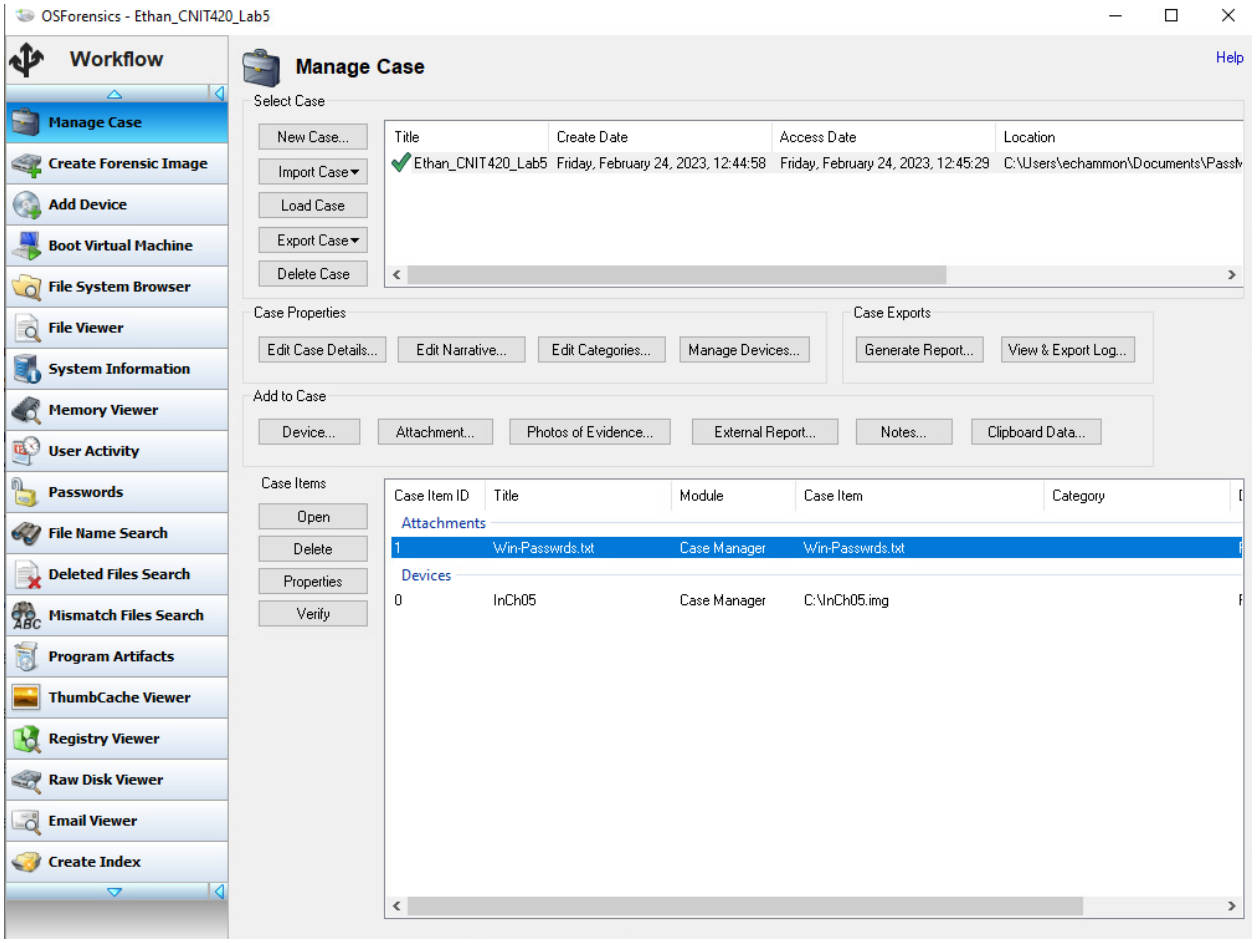

Figure 16: Attachment of found Windows passwords.

After forensic reports are concluded, reports always need to be generated to present the information found to the investigators. The report for this OSForensics investigation can be seen below in Figure 17.

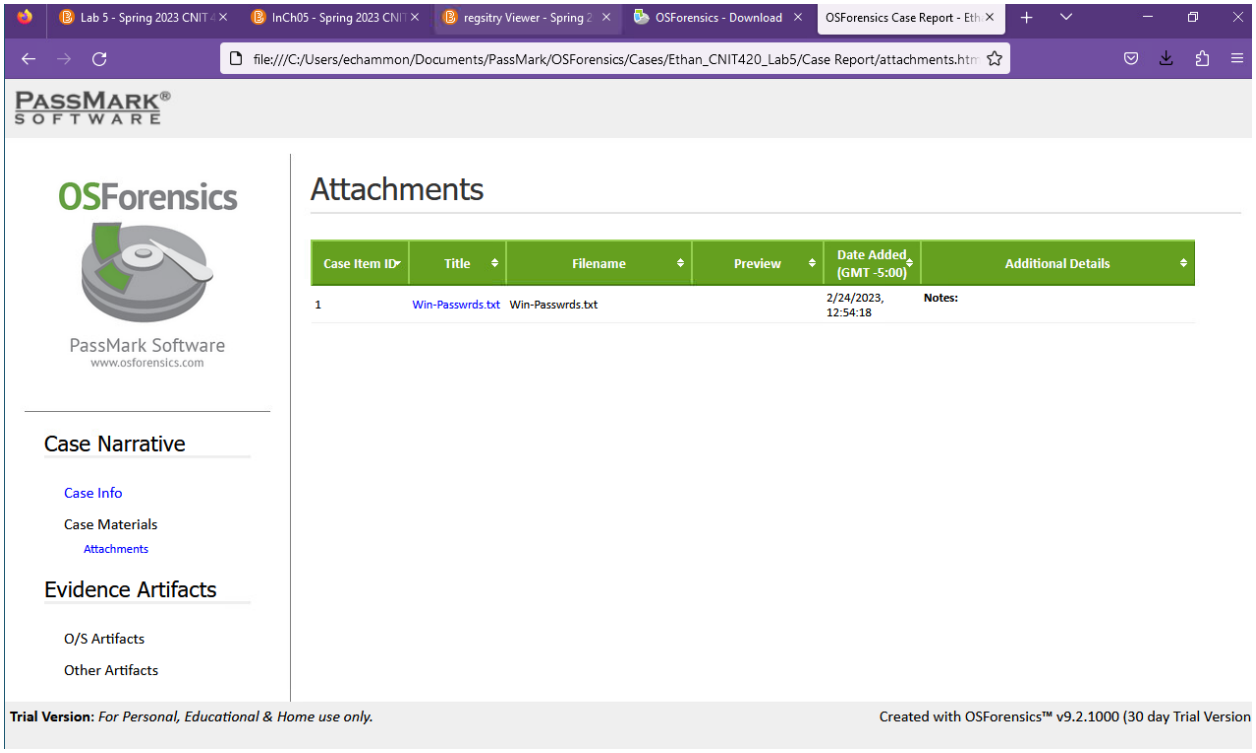

Figure 17: Generated report of OSForensics case analysis

Task 4

To access the registry files of the image, it was put into FTK Imager for analysis. The hex text can be seen below in Figure 18.

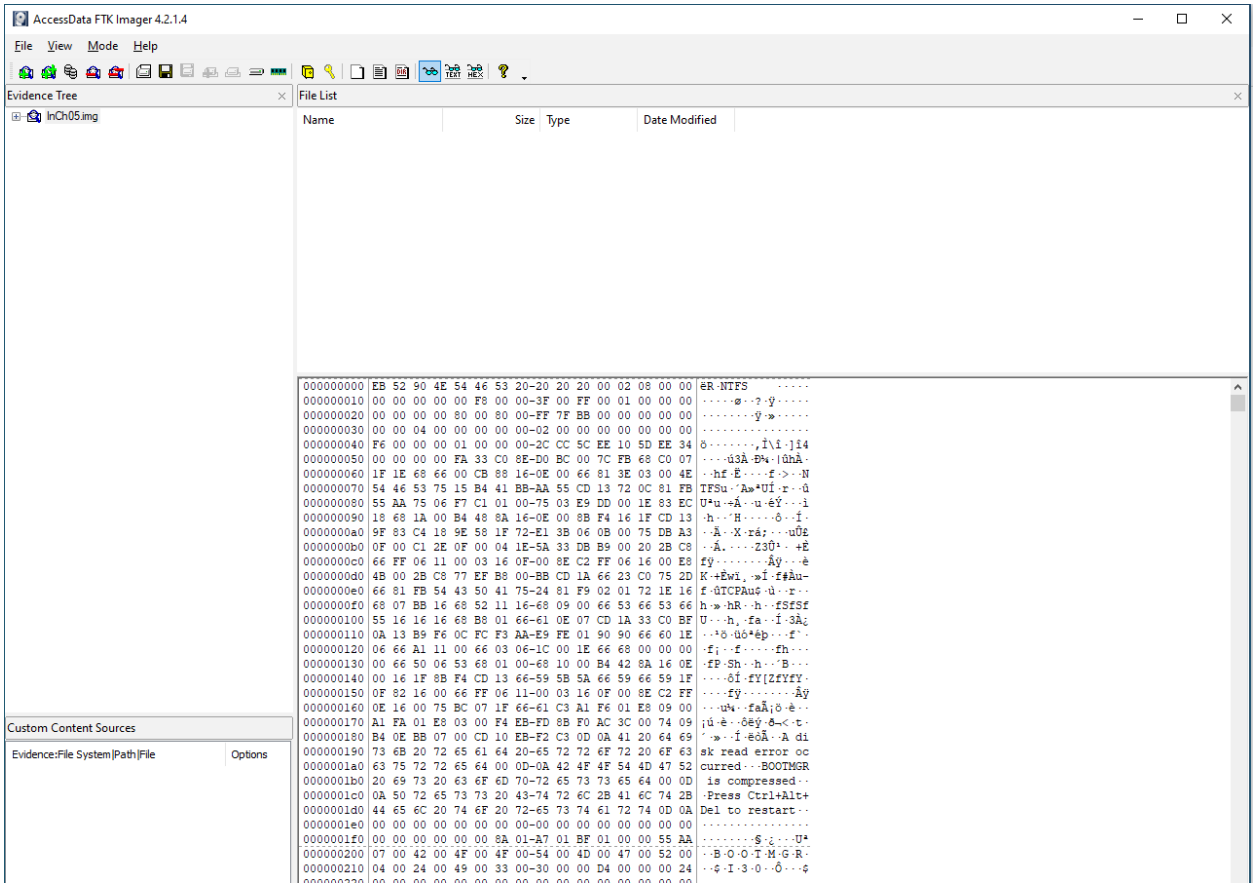

Figure 18: InCh05.img open in FTK Imager.

User data can be found in the ntuser.dat file. For further investigation purposes, this file was saved and exported to the lab computer. The extraction proof can be seen below in Figure 19.

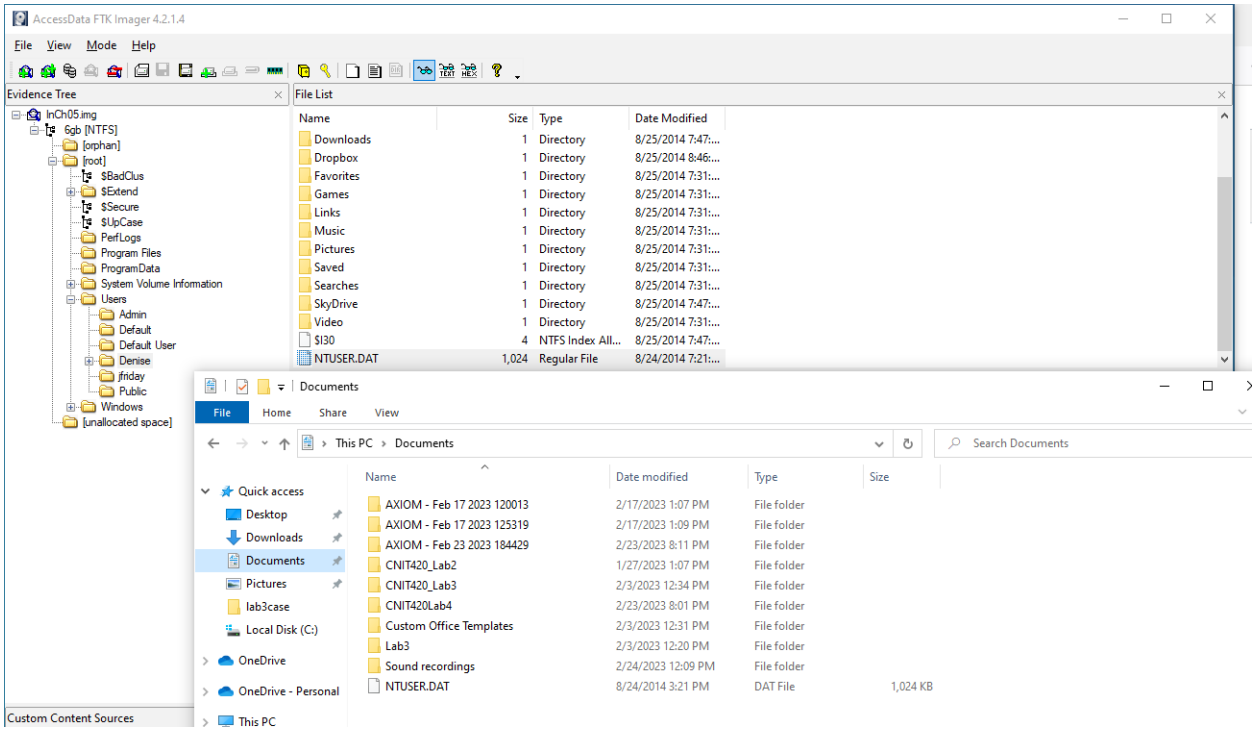

Figure 19: ntuser.dat file extraction to lab computer from InCh05.img

The rest of the registry files including DEFAULT, SAM, SECURITY, SOFTWARE, and SYSTEM were extracted to the lab computer as well for further investigation. These files can be seen in Figure 20 below.

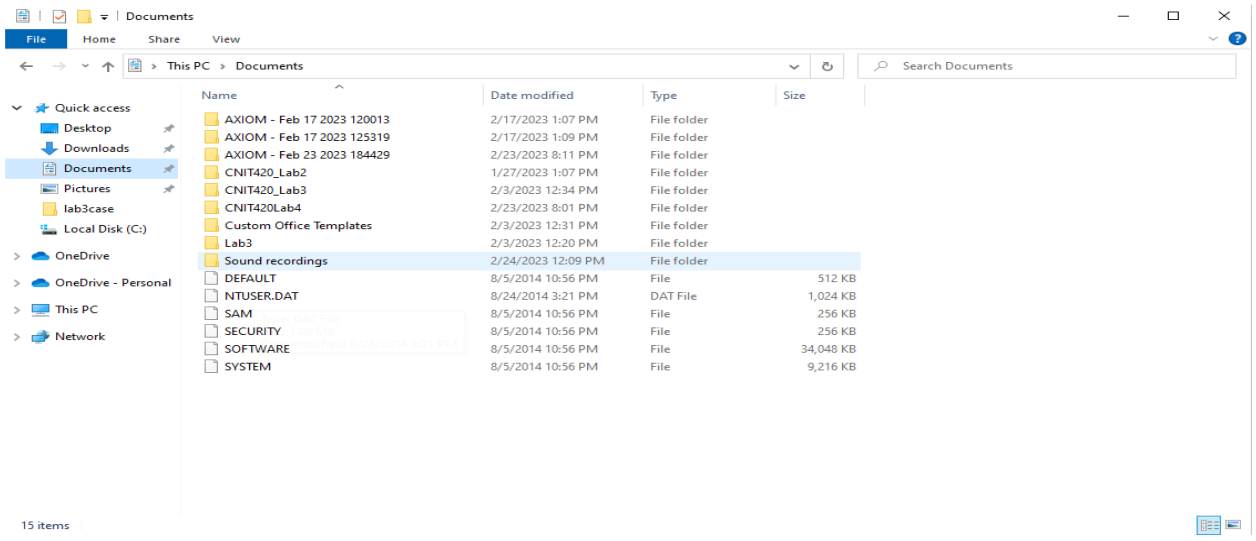

Figure 20: All registry files extracted from InCh05.img

The SAM file was examined as it has to do with user accounts. The viewing of the contents of this file can be seen in Figures 21-24.

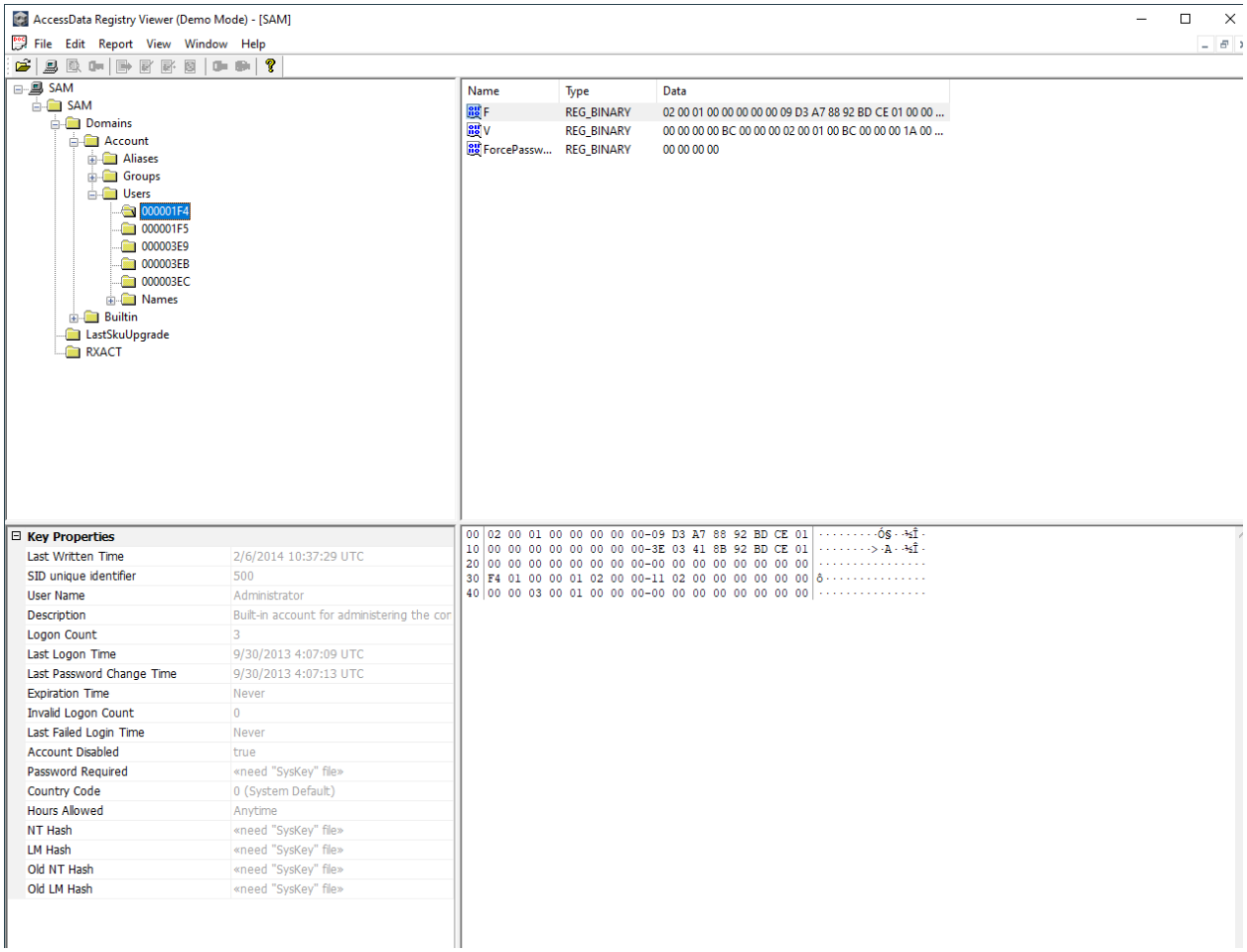

Figure 21: Administrator account details

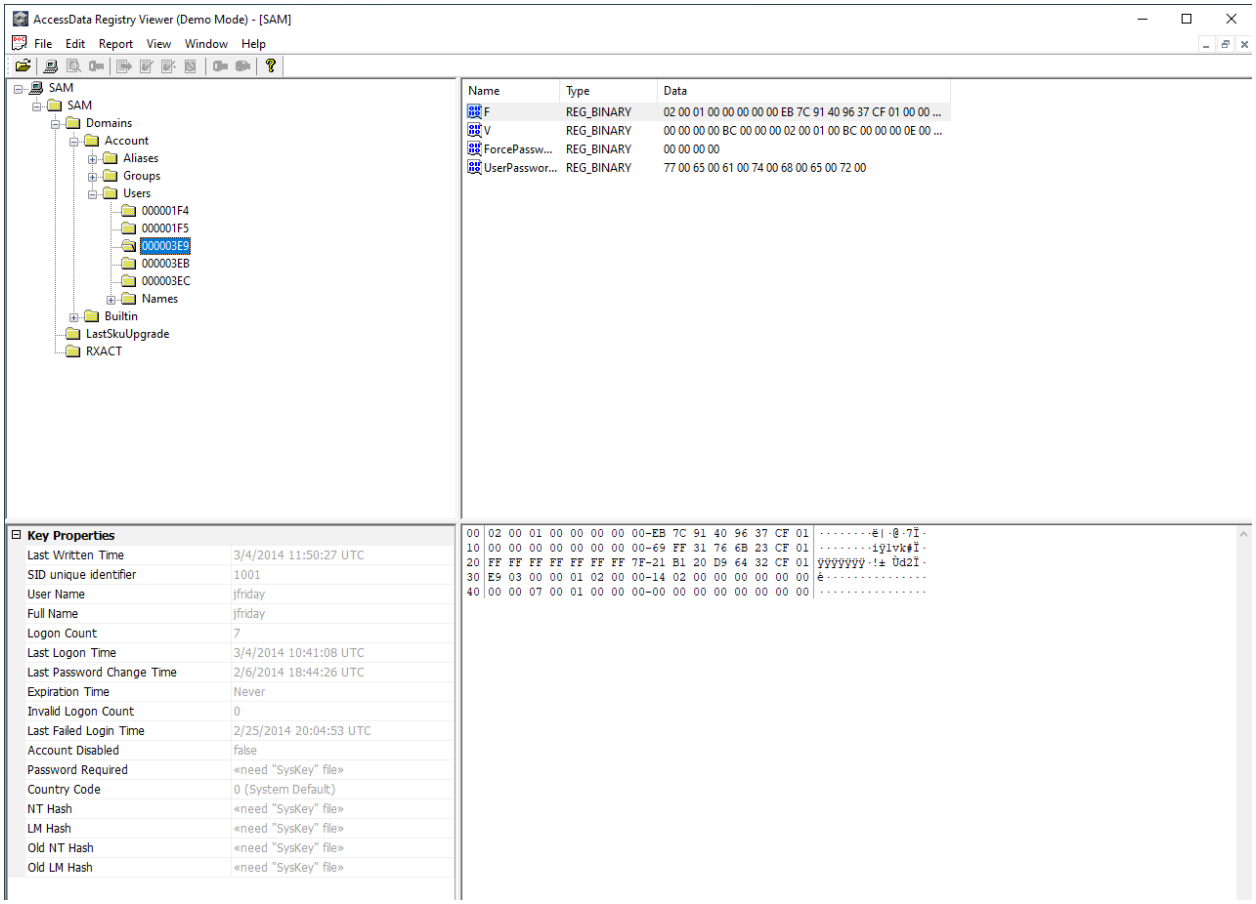

Figure 22: jfriday account details

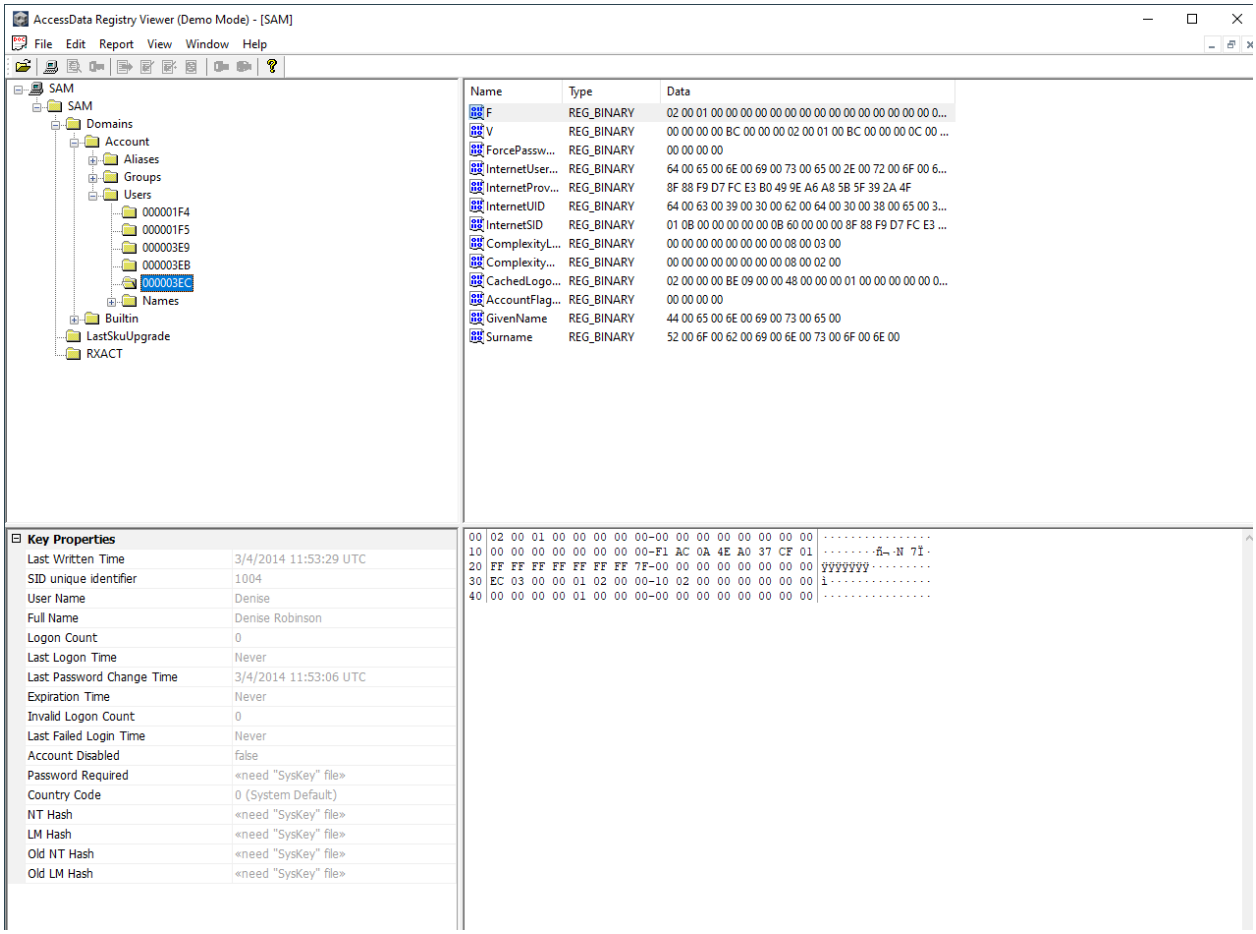

Figure 23: Denise Robinson account details

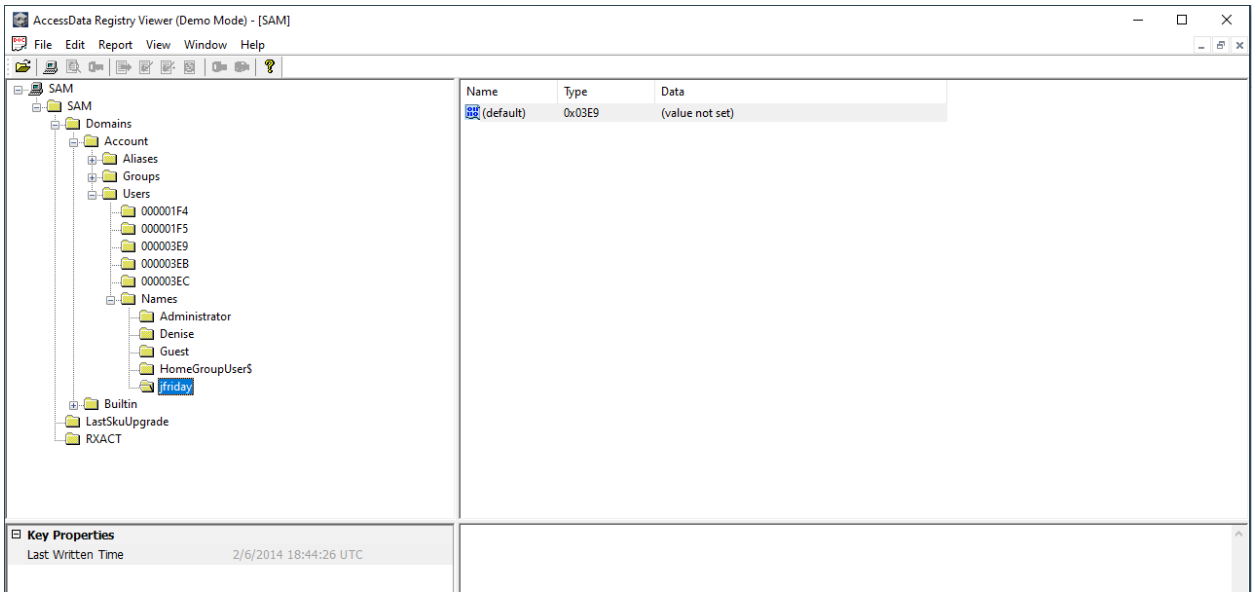

Figure 24: When the account was last accessed and when the password was changed to jfriday's account.

Conclusion

A forensic investigation was conducted on a drive image that was done to show how forensic investigators can examine MFTs to gain file and user data. The software that was used for this task was WinHex. The hex data was inspected to see data like file signatures to show how the operating system handles file types and extensions as well as file modification, creation, and reading. Next, OSForensics was used to create a case, examine files, and extract passwords from user accounts. OSForensics can be a great open source tool for extracting Windows account data as well as user account data. Lastly, FTK Imager was used to examine the registry data of a Windows account. The files ntuser, SECURITY, SAM, DEFAULT, SYSTEM, and SOFTWARE were examined as user data is present in all files. The SAM file was examined extensively as it shows user logon times, account modifications, and password modifications. These are all tools that can be important to a digital forensic investigation.

References

Khan, T. (n.d.). *Lab 5 - File Headers and Hive*. Login - Purdue University system. Retrieved March 2, 2023, from https://purdue.brightspace.com/d2l/le/content/702085/viewContent/12411274/View

Gary C. Kessler, P. D. (n.d.). File signatures. Retrieved March 2, 2023, from https://www.garykessler.net/library/file_sigs.html

Time Chart

Task Number	Time Taken
Task 1	50 Minutes
Task 2	30 Minutes
Task 3	30 Minutes
Task 4	10 Minutes
Report Writing	4 Hours
Total	6 Hours