

Lab 4 – Registry and Browser Forensics

Shruti Joshi

University of Maryland Baltimore County

Presented To – Gina Marie

Date – 9th July 2023

Week 4 Discussion -1:

Post the picture and give information regarding the picture this could include, device used to take the picture, GPS location, etc.



- I uploaded the above nature scenic picture on <https://fotoforensics.com> for analyzing metadata about the image and below is the link and analysis about the image:
<https://fotoforensics.com/analysis.php?id=2264b9aa5ce9555001923fc24eff7e754c1c879b.1072875>
- Digest and Metadata tab contains details about the image filehash and metadata about the image.
- The file name is 20230710_090333.jpg, file type is jpeg and image size is 1,072,875 bytes
- Device used for taking this picture is Samsung Mobile and model name is Galaxy S23 Ultra. The picture is taken on 2023:07:10 09:03:33 and modified date is same.
- The MD5 hash of file is e22a91f72b4a27b96d700f9a57809ba7
- The GPS coordinate of picture is 37 deg 34' 12.00" N, 122 deg 4' 12.00" W
GPS Latitude Ref – North
GPS Longitude Ref – West
GPS Altitude Ref – Above sea level
- The image unique ID is 6452b2d744fc55f000000000000000000
- ICC Profile Copyright - Copyright (c) 2022 Samsung Electronics Co., Ltd.
- Approximate Coordinates 37.57,-122.07
- Approximate Location 3.23 miles (5.20 km) NW of Newark, CA, US

Citations – Hany Farid. (n.d.). FotoForensics. Retrieved July 6, 2023, from

<https://fotoforensics.com/>

Introduction – In this lab, as a forensic investigator, we will simulate the process of acquiring evidence into an image file. During the analysis, we will collect registry information from evidence image file as well as collect files and metadata from an image file for analysis purpose. The registry contain configuration settings and user activity data while image file data holds details regarding the image origin and creation details which will further help in preparing the comprehensive investigation report on the case.

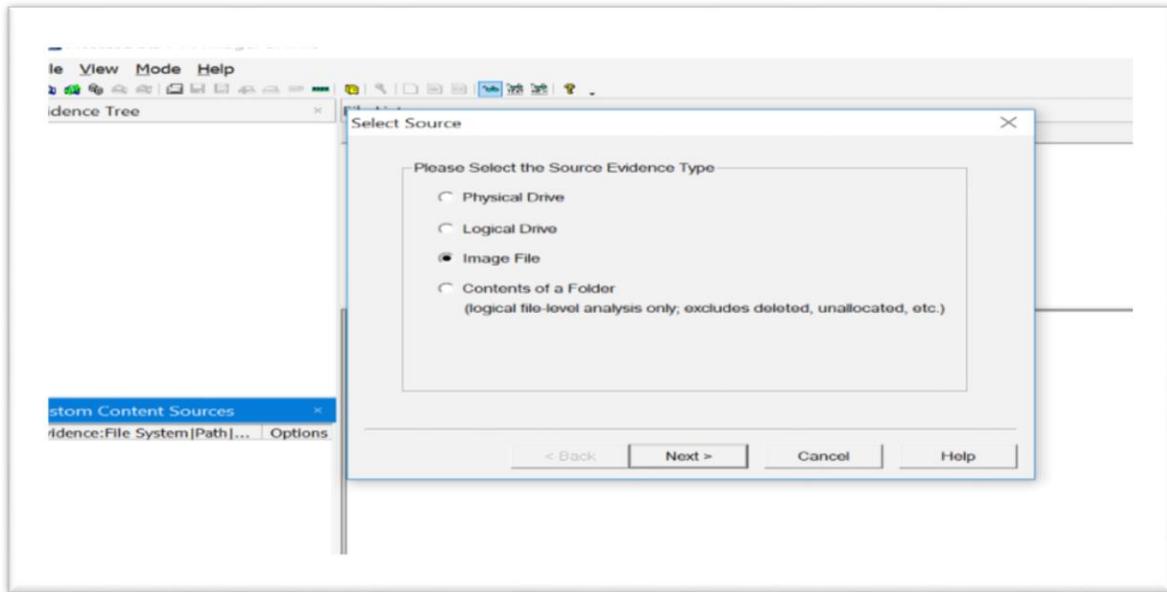
Pre-Analysis – We have created forensic images using ‘ProDiscover’ and ‘FTK Imager’. Now we will be extracting registry information from an image file using ‘FTK Imager’. Afterwards, we are going to analyze this extracted registry files using ‘Registry Forensic’ tool and will collect evidence from registry information and image file metadata.

Analysis –

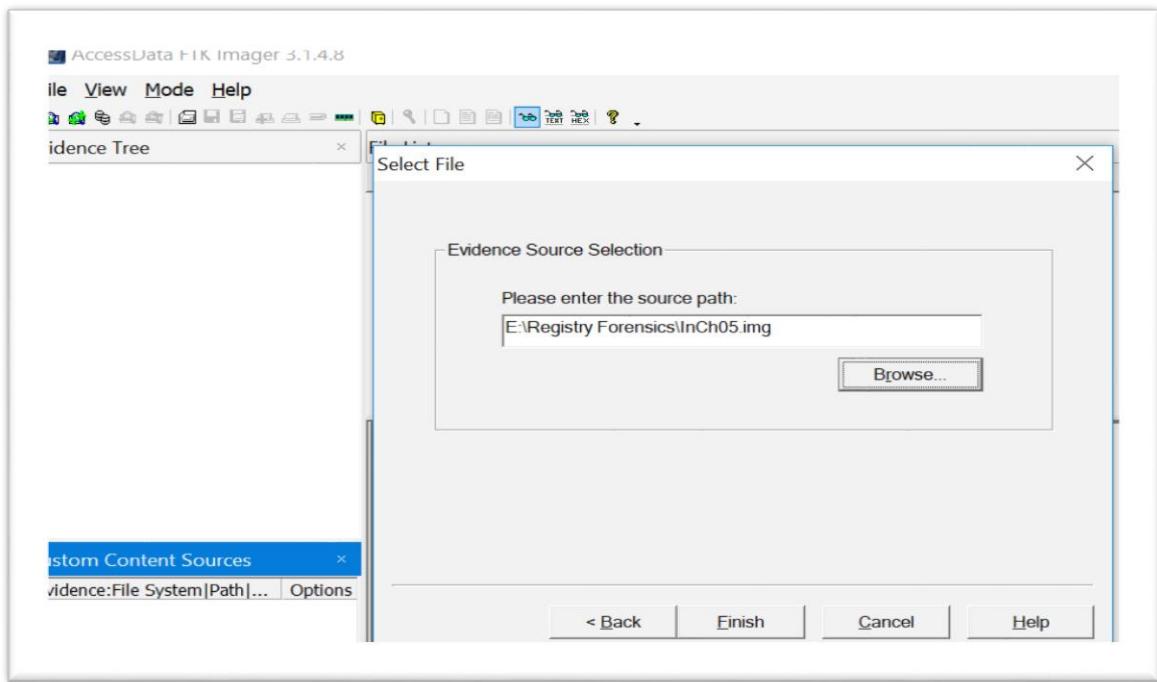
Registry Forensics

1. Extracting Registry Files from Disk Image:

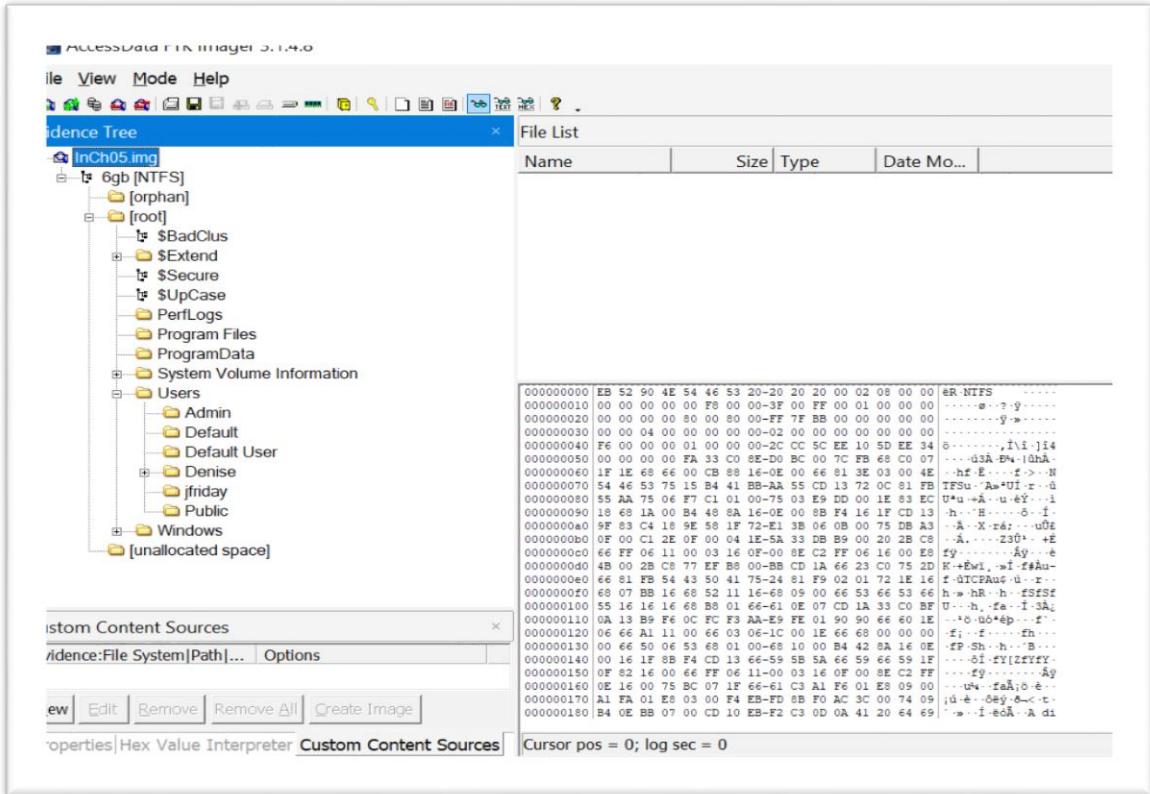
- Open FTK analyzer and click on File from the top left hand corner File → Add evidence Item. Click on image file → Next.



- Now browse to the Evidence drive → Registry Forensics and select InCh05.img and click on Finish.

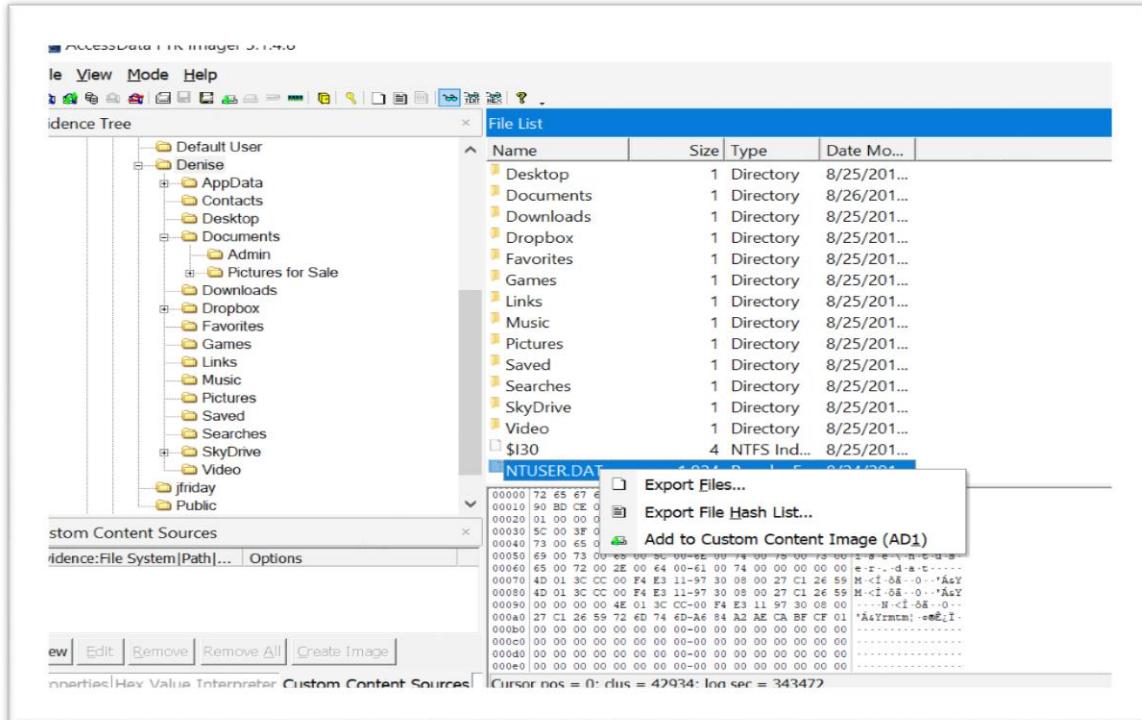


- In the left pane, expand to InCh05.img → 6gb [NTFS] → [root] → Users

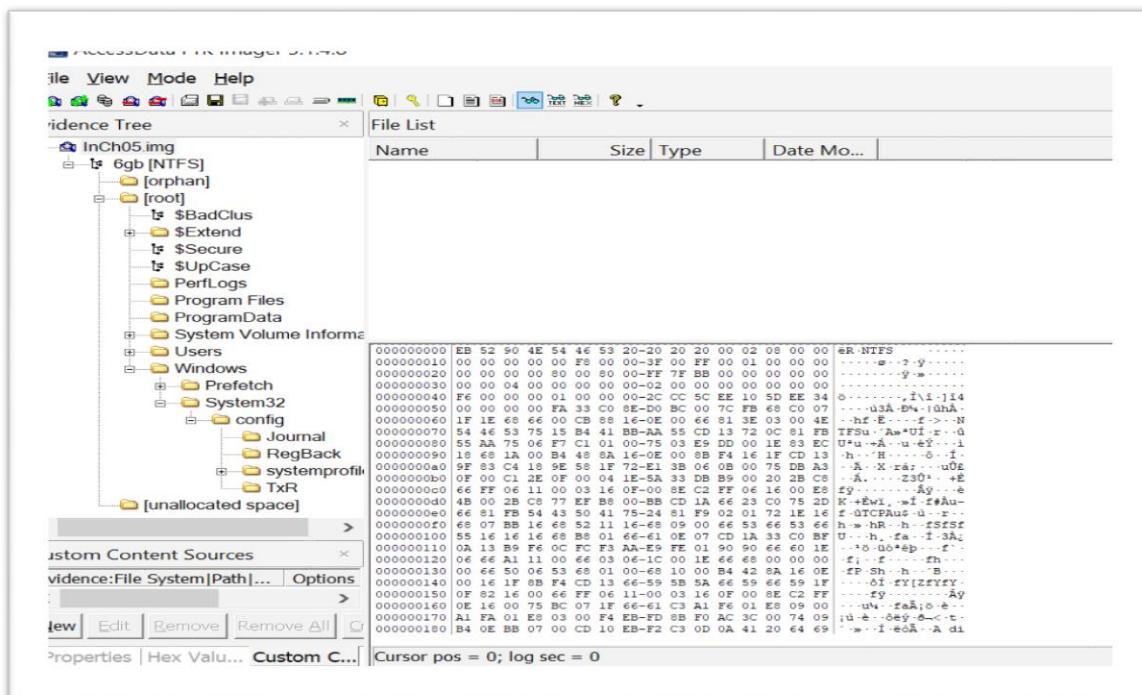


- Open the Denise folder and select NTUSER.dat, then right-click and select Export Files.

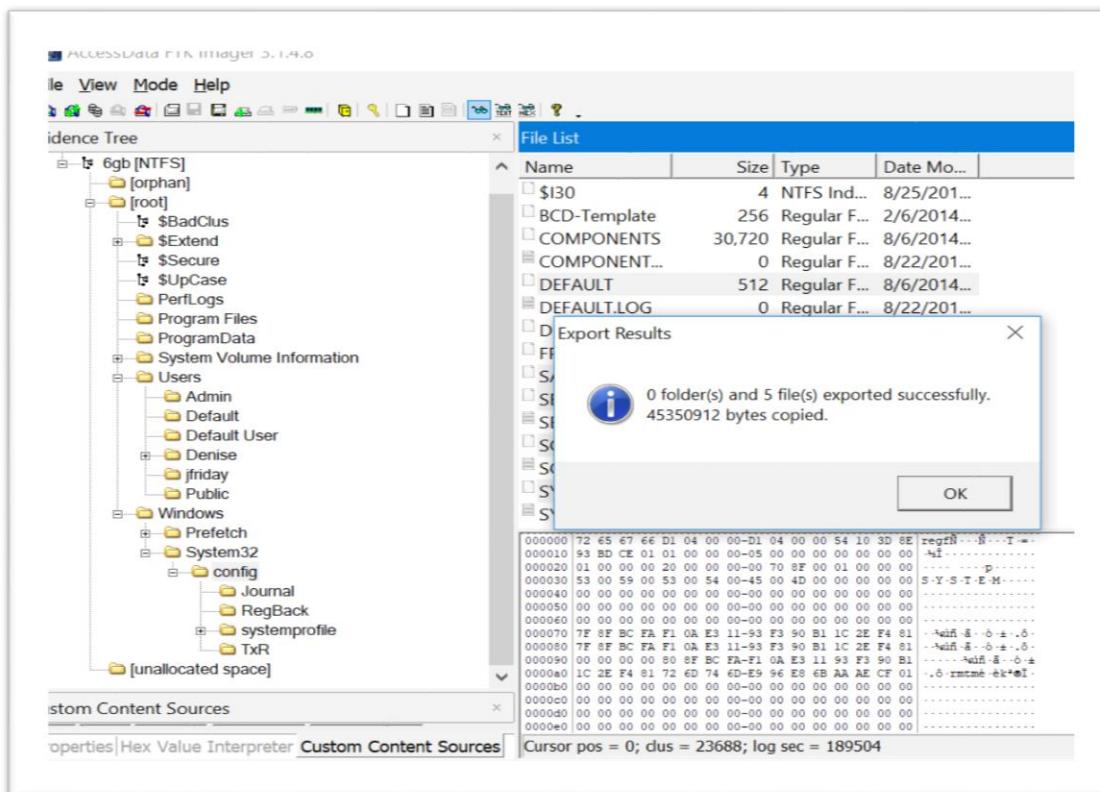
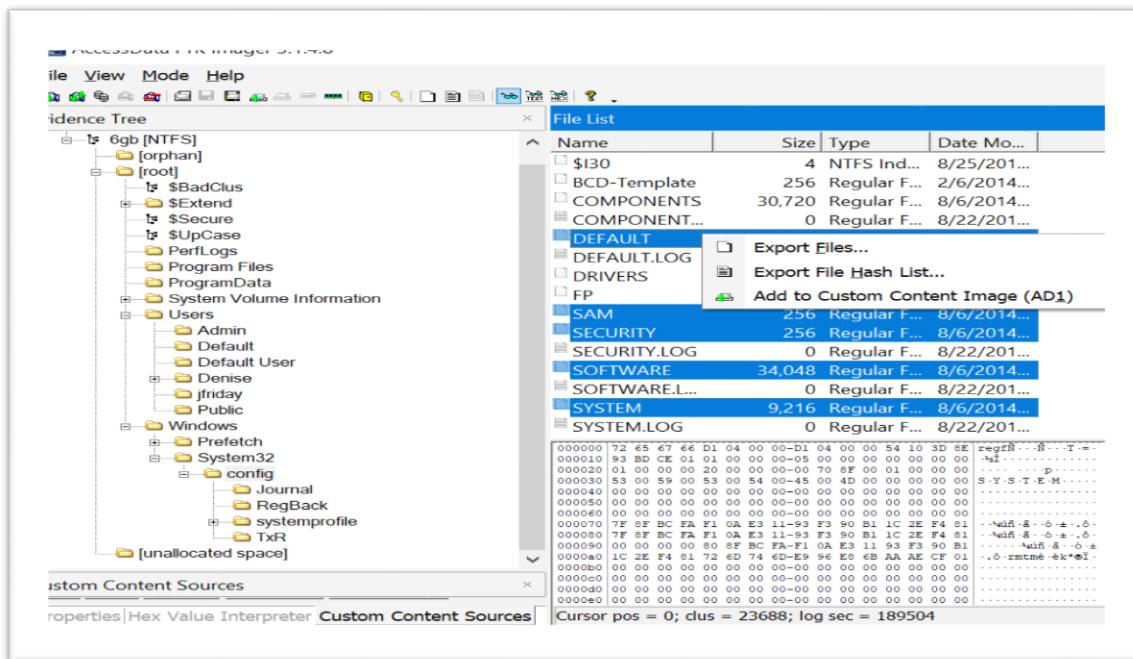
Now export the NTUSER.dat file to a windows VM for later use.



- In the left pane, expand to InCh05.img → 6gb [NTFS] →[root]→ Windows
→System32→config.

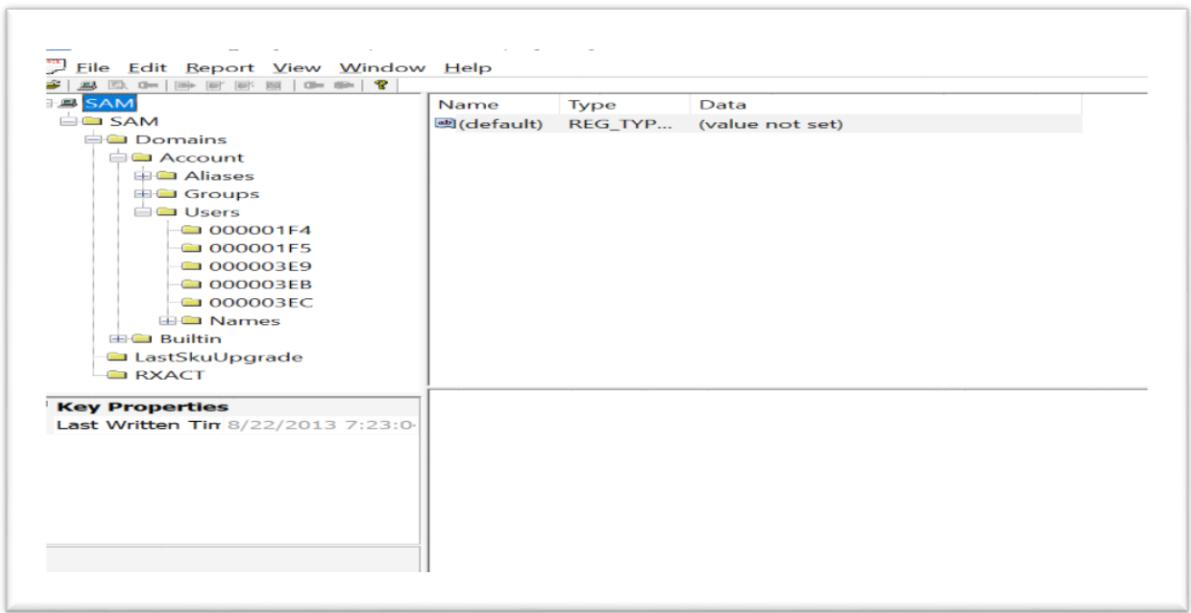


- Select SAM, DEFAULT, SYSTEM, SOFTWARE, SECURITY folders and export it to the same location as NTUSER.dat. [1]



2. Examining the SAM Hive:

- SAM hive is a database file in the Microsoft Operating System that contains username and passwords. The main purpose of SAM is to make system more secure and protect from data breach. [3]
- It is located on HKEY_LOCAL_MACHINE\SAM : \system32\config\sam [1]
- Open the registry viewer in the Demo Mode for that click “No” and “Okay” to the resulting pop-ups referencing a Security licensing dongle.
- Now click File → Open and navigate to the folder where registry files are extracted and select SAM registry file. Now expand SAM → Domains → Account → Users folders.



- After exploring the user details under the user's folder below is the analysis:
 1. Which account logged into the system the most?
 - Jfriday was logon to the account the most. His logon count is Count 7 times.

Last Written Time	3/4/2014 11:50:27 UTC
SID unique identifier	1001
User Name	jfriday
Full Name	jfriday
Logon Count	7
Last Logon Time	3/4/2014 10:41:08 UTC
Last Password Change Time	2/6/2014 18:44:26 UTC
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	2/25/2014 20:04:53 UTC
Account Disabled	false
Password Required	false
Country Code	0 (System Default)
Has LAN Manager Password	false

2. Has Denise Robinson logged in?

- Denise Robinson was never login to the account as his logon count is ‘Zero’ and

Last logon time is ‘Never’

Last Written Time	3/4/2014 11:53:29 UTC
SID unique identifier	1004
User Name	Denise
Full Name	Denise Robinson
Logon Count	0
Last Logon Time	Never
Last Password Change Time	3/4/2014 11:53:06 UTC
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	Never
Account Disabled	false
Password Required	true
Country Code	0 (System Default)
Has LAN Manager Password	false

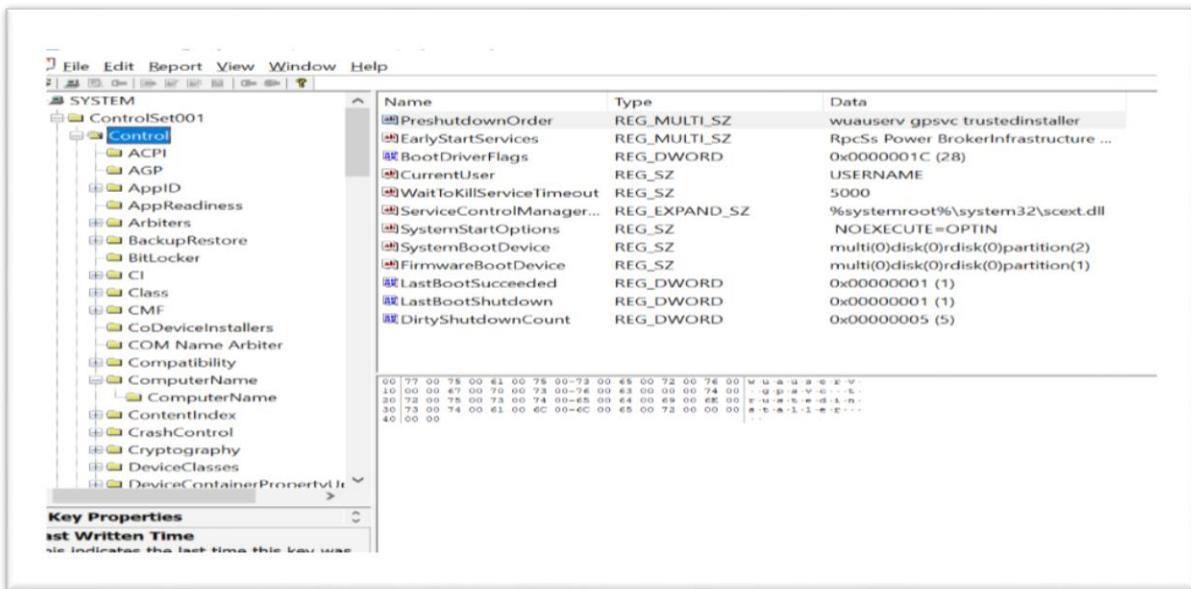
3. Expand SAM --> Domains --> Accounts --> Users --> Names and identify when jfriday’s account password was last set?

- Jfriday’s account password was last set at ‘02-06-2014 18:44:26 UTC’

Last Written Time	3/4/2014 11:50:27 UTC
SID unique identifier	1001
User Name	jfriday
Full Name	jfriday
Logon Count	7
Last Logon Time	3/4/2014 10:41:08 UTC
Last Password Change Time	2/6/2014 18:44:26 UTC
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	2/25/2014 20:04:53 UTC
Account Disabled	false
Password Required	false
Country Code	0 (System Default)
Has LAN Manager Password	false
Has NTLMv2 Password	true

3. Examining the SYSTEM Hive:

- It is located on path HKEY_LOCAL_MACHINE\SYSTEM : \system32\config\system [1]
- Now open the System registry file from the extracted registry files to examine the System Hive. Expand SYSTEM → ControlSet001 → Control



- Below are the analysis after exploring details from the above folder.
 1. What is the computer name this image is from?
➤ Now navigate to the ComputerName → ComputerName folder to find computer name details. ComputerName : GCFI5E

	Name	Type	Data
	(default)	REG_SZ	mnmsrvrc
	ComputerName	REG_SZ	GCFI5E

2. Scroll down to TimeZoneInformation to identify the computer's time zone.
➤ To get the Time Zone details navigate to the TimeZoneInformation folder

Computer's time zone is in 'Pacific Standard Time'

DaylightBias	REG_DWORD	0xFFFFFFF4 (4294967236)
DaylightName	REG_SZ	@tzres.dll_-211
StandardStart	REG_BINARY	00 00 08 00 01 00 02 00 00 00 00
StandardBias	REG_DWORD	0x00000000 (0)
StandardName	REG_SZ	@tzres.dll_-212
Bias	REG_DWORD	0x000001E0 (480)
DaylightStart	REG_BINARY	00 00 03 00 02 00 02 00 00 00 00
TimeZoneKeyName	REG_SZ	Pacific Standard Time
DynamicDaylightTimeDl...	REG_DWORD	0x00000000 (0)

3. Expand the Enum folder and then IDE and USB to view the IDE and USB based storage devices plugged into the computer, and when they were last accessed.
 - Navigate to the Enum → IDE folder to check the storage devices which were connected to the computer and when they were last accessed

Last access Time – 02/06/2014 10:35:09 UTC

DeviceDesc	REG_SZ	@cdrom.inf,%gendrom_devdesc%;CD-ROM Drive
LocationInformation	REG_SZ	Channel 1, Target 0, Lun 0
Capabilities	REG_DWORD	0x00000000 (0)
UINumber	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{00000000-0000-0000-ffff-ffffffffff}
HardwareID	REG_MULTI_SZ	IDE\CdRomVBOX_CD-ROM_1.0__IDE\VBOX_CD-ROM
CompatibleIDs	REG_MULTI_SZ	GenCdRom
ClassGUID	REG_SZ	{4d36e965-e325-11ce-bfc1-08002be10318}
Service	REG_SZ	cdrom
Driver	REG_SZ	{4d36e965-e325-11ce-bfc1-08002be10318}\0000
Mfg	REG_SZ	@cdrom.inf,%genmanufacturer%{Standard CD-ROM drives}
FriendlyName	REG_SZ	VBOX CD-ROM ATA Device

4. Click on System-MountedDevices to see the list of every storage device that was mounted into the Windows OS and its associated drive letter/GUID value.
 - Similarly, can check storage device details from USB folder.

Navigate to Enum → USB folder to check the storage devices which were connected to the computer and when they were last accessed

Below are the list of storage devices and last connected date:

ROOT_HUB: 8/6/2014 2:54:48 UTC

VID_08C2&PID_50A5: 3/4/2014 14:17:28 UTC

VID_08DA&PID_0158: 7/24/2014 2:37:57 UTC

VID_1058&PID_10A2: 7/24/2014 2:37:36 UTC

VID_1241&PID_1203: 7/23/2014 10:20:27 UTC

VID_1241&PID_1203&MI_00: 8/6/2014 2:54:49 UTC

VID_1241&PID_1203&MI_01: 8/6/2014 2:54:49 UTC

VID_152D&PID_0539: 7/23/2014 10:27:12 UTC

VID_4146&PID_BA67: 3/4/2014 14:25:03 UTC

VID_80EE&PID_0021: 8/6/2014 2:54:48 UTC

Key Properties																																						
Last Written Time		8/6/2014 2:54:48 UTC																																				
		<table border="1"><thead><tr><th>Name</th><th>Type</th><th>Data</th></tr></thead><tbody><tr><td>Capabilities</td><td>REG_DWORD</td><td>0x00000080 (128)</td></tr><tr><td>ContainerID</td><td>REG_SZ</td><td>{00000000-0000-0000-ffff-ffffffffffff}</td></tr><tr><td>HardwareID</td><td>REG_MULTI_SZ</td><td>USB\ROOT_HUB&VID1068&PID003F&REV0000 USB\ROOT_HUB&VID1068&PID003F USB\ROOT_HUB</td></tr><tr><td>ClassGUID</td><td>REG_SZ</td><td>{36fc9e60-c465-11cf-8056-444553540000}</td></tr><tr><td>Service</td><td>REG_SZ</td><td>usbhub</td></tr><tr><td>DeviceDesc</td><td>REG_SZ</td><td>@usbport.inf.%usb\root_hub.devcidesc%USB Root Hub</td></tr><tr><td>Driver</td><td>REG_SZ</td><td>{36fc9e60-c465-11cf-8056-444553540000}\0001</td></tr><tr><td>Mfg</td><td>REG_SZ</td><td>@usbport.inf.%generic.mfg%(Standard USB Host Controller)</td></tr><tr><td>ConfigFlags</td><td>REG_DWORD</td><td>0x00000000 (0)</td></tr><tr><td>ParentIdPrefix</td><td>REG_SZ</td><td>5&2d7ae1ff&0</td></tr></tbody></table>	Name	Type	Data	Capabilities	REG_DWORD	0x00000080 (128)	ContainerID	REG_SZ	{00000000-0000-0000-ffff-ffffffffffff}	HardwareID	REG_MULTI_SZ	USB\ROOT_HUB&VID1068&PID003F&REV0000 USB\ROOT_HUB&VID1068&PID003F USB\ROOT_HUB	ClassGUID	REG_SZ	{36fc9e60-c465-11cf-8056-444553540000}	Service	REG_SZ	usbhub	DeviceDesc	REG_SZ	@usbport.inf.%usb\root_hub.devcidesc%USB Root Hub	Driver	REG_SZ	{36fc9e60-c465-11cf-8056-444553540000}\0001	Mfg	REG_SZ	@usbport.inf.%generic.mfg%(Standard USB Host Controller)	ConfigFlags	REG_DWORD	0x00000000 (0)	ParentIdPrefix	REG_SZ	5&2d7ae1ff&0			
Name	Type	Data																																				
Capabilities	REG_DWORD	0x00000080 (128)																																				
ContainerID	REG_SZ	{00000000-0000-0000-ffff-ffffffffffff}																																				
HardwareID	REG_MULTI_SZ	USB\ROOT_HUB&VID1068&PID003F&REV0000 USB\ROOT_HUB&VID1068&PID003F USB\ROOT_HUB																																				
ClassGUID	REG_SZ	{36fc9e60-c465-11cf-8056-444553540000}																																				
Service	REG_SZ	usbhub																																				
DeviceDesc	REG_SZ	@usbport.inf.%usb\root_hub.devcidesc%USB Root Hub																																				
Driver	REG_SZ	{36fc9e60-c465-11cf-8056-444553540000}\0001																																				
Mfg	REG_SZ	@usbport.inf.%generic.mfg%(Standard USB Host Controller)																																				
ConfigFlags	REG_DWORD	0x00000000 (0)																																				
ParentIdPrefix	REG_SZ	5&2d7ae1ff&0																																				
		<table border="1"><thead><tr><th>Name</th><th>Type</th><th>Data</th></tr></thead><tbody><tr><td>DeviceDesc</td><td>REG_SZ</td><td>@usbstor.inf.%genericbulkonly.devcidesc%USB Mass Storage Device</td></tr><tr><td>LocationInformation</td><td>REG_SZ</td><td>Port_\#0002.Hub_\#0001</td></tr><tr><td>Capabilities</td><td>REG_DWORD</td><td>0x00000014 (20)</td></tr><tr><td>ContainerID</td><td>REG_SZ</td><td>{b79ef8d5-5bc0-51e1-b12e-26e55c1bec05}</td></tr><tr><td>HardwareID</td><td>REG_MULTI_SZ</td><td>USB\VID_0BC2&PID_50A5&REV_0100 USB\VID_0BC2&PID_50A5</td></tr><tr><td>CompatibleIDs</td><td>REG_MULTI_SZ</td><td>USB\Class_08&SubClass_06&Prot_50 USB\Class_08&SubClass_06 USB\Class_08</td></tr><tr><td>ClassGUID</td><td>REG_SZ</td><td>{36fc9e60-c465-11cf-8056-444553540000}</td></tr><tr><td>Service</td><td>REG_SZ</td><td>USBSTOR</td></tr><tr><td>Driver</td><td>REG_SZ</td><td>{36fc9e60-c465-11cf-8056-444553540000}\0004</td></tr><tr><td>Mfg</td><td>REG_SZ</td><td>@usbstor.inf.%generic.mfg%Compatible USB storage device</td></tr><tr><td>ConfigFlags</td><td>REG_DWORD</td><td>0x00000000 (0)</td></tr></tbody></table>	Name	Type	Data	DeviceDesc	REG_SZ	@usbstor.inf.%genericbulkonly.devcidesc%USB Mass Storage Device	LocationInformation	REG_SZ	Port_\#0002.Hub_\#0001	Capabilities	REG_DWORD	0x00000014 (20)	ContainerID	REG_SZ	{b79ef8d5-5bc0-51e1-b12e-26e55c1bec05}	HardwareID	REG_MULTI_SZ	USB\VID_0BC2&PID_50A5&REV_0100 USB\VID_0BC2&PID_50A5	CompatibleIDs	REG_MULTI_SZ	USB\Class_08&SubClass_06&Prot_50 USB\Class_08&SubClass_06 USB\Class_08	ClassGUID	REG_SZ	{36fc9e60-c465-11cf-8056-444553540000}	Service	REG_SZ	USBSTOR	Driver	REG_SZ	{36fc9e60-c465-11cf-8056-444553540000}\0004	Mfg	REG_SZ	@usbstor.inf.%generic.mfg%Compatible USB storage device	ConfigFlags	REG_DWORD	0x00000000 (0)
Name	Type	Data																																				
DeviceDesc	REG_SZ	@usbstor.inf.%genericbulkonly.devcidesc%USB Mass Storage Device																																				
LocationInformation	REG_SZ	Port_\#0002.Hub_\#0001																																				
Capabilities	REG_DWORD	0x00000014 (20)																																				
ContainerID	REG_SZ	{b79ef8d5-5bc0-51e1-b12e-26e55c1bec05}																																				
HardwareID	REG_MULTI_SZ	USB\VID_0BC2&PID_50A5&REV_0100 USB\VID_0BC2&PID_50A5																																				
CompatibleIDs	REG_MULTI_SZ	USB\Class_08&SubClass_06&Prot_50 USB\Class_08&SubClass_06 USB\Class_08																																				
ClassGUID	REG_SZ	{36fc9e60-c465-11cf-8056-444553540000}																																				
Service	REG_SZ	USBSTOR																																				
Driver	REG_SZ	{36fc9e60-c465-11cf-8056-444553540000}\0004																																				
Mfg	REG_SZ	@usbstor.inf.%generic.mfg%Compatible USB storage device																																				
ConfigFlags	REG_DWORD	0x00000000 (0)																																				
		<table border="1"><thead><tr><th>Name</th><th>Type</th><th>Data</th></tr></thead><tbody><tr><td>DeviceDesc</td><td>REG_SZ</td><td>@usbstor.inf.%genericbulkonly.devcidesc%USB Mass Storage Device</td></tr><tr><td>LocationInformation</td><td>REG_SZ</td><td>Port_\#0006.Hub_\#0001</td></tr><tr><td>Capabilities</td><td>REG_DWORD</td><td>0x00000014 (20)</td></tr><tr><td>ContainerID</td><td>REG_SZ</td><td>{b757f9b0-6543-51ae-a4c9-88e9e05cea1a}</td></tr><tr><td>HardwareID</td><td>REG_MULTI_SZ</td><td>USB\VID_0BDA&PID_0158&REV_5899 USB\VID_0BDA&PID_0158</td></tr><tr><td>CompatibleIDs</td><td>REG_MULTI_SZ</td><td>USB\Class_08&SubClass_06&Prot_50 USB\Class_08&SubClass_06 USB\Class_08</td></tr><tr><td>ClassGUID</td><td>REG_SZ</td><td>{36fc9e60-c465-11cf-8056-444553540000}</td></tr><tr><td>Service</td><td>REG_SZ</td><td>USBSTOR</td></tr><tr><td>Driver</td><td>REG_SZ</td><td>{36fc9e60-c465-11cf-8056-444553540000}\0009</td></tr><tr><td>Mfg</td><td>REG_SZ</td><td>@usbstor.inf.%generic.mfg%Compatible USB storage device</td></tr><tr><td>ConfigFlags</td><td>REG_DWORD</td><td>0x00000000 (0)</td></tr></tbody></table>	Name	Type	Data	DeviceDesc	REG_SZ	@usbstor.inf.%genericbulkonly.devcidesc%USB Mass Storage Device	LocationInformation	REG_SZ	Port_\#0006.Hub_\#0001	Capabilities	REG_DWORD	0x00000014 (20)	ContainerID	REG_SZ	{b757f9b0-6543-51ae-a4c9-88e9e05cea1a}	HardwareID	REG_MULTI_SZ	USB\VID_0BDA&PID_0158&REV_5899 USB\VID_0BDA&PID_0158	CompatibleIDs	REG_MULTI_SZ	USB\Class_08&SubClass_06&Prot_50 USB\Class_08&SubClass_06 USB\Class_08	ClassGUID	REG_SZ	{36fc9e60-c465-11cf-8056-444553540000}	Service	REG_SZ	USBSTOR	Driver	REG_SZ	{36fc9e60-c465-11cf-8056-444553540000}\0009	Mfg	REG_SZ	@usbstor.inf.%generic.mfg%Compatible USB storage device	ConfigFlags	REG_DWORD	0x00000000 (0)
Name	Type	Data																																				
DeviceDesc	REG_SZ	@usbstor.inf.%genericbulkonly.devcidesc%USB Mass Storage Device																																				
LocationInformation	REG_SZ	Port_\#0006.Hub_\#0001																																				
Capabilities	REG_DWORD	0x00000014 (20)																																				
ContainerID	REG_SZ	{b757f9b0-6543-51ae-a4c9-88e9e05cea1a}																																				
HardwareID	REG_MULTI_SZ	USB\VID_0BDA&PID_0158&REV_5899 USB\VID_0BDA&PID_0158																																				
CompatibleIDs	REG_MULTI_SZ	USB\Class_08&SubClass_06&Prot_50 USB\Class_08&SubClass_06 USB\Class_08																																				
ClassGUID	REG_SZ	{36fc9e60-c465-11cf-8056-444553540000}																																				
Service	REG_SZ	USBSTOR																																				
Driver	REG_SZ	{36fc9e60-c465-11cf-8056-444553540000}\0009																																				
Mfg	REG_SZ	@usbstor.inf.%generic.mfg%Compatible USB storage device																																				
ConfigFlags	REG_DWORD	0x00000000 (0)																																				

Name	Type	Data
DeviceDesc	REG_SZ	@usbstor.inf%\genericbulkonly.devidesc%USB Mass Storage Device
LocationInformation	REG_SZ	Port_#0005.Hub_#0001
Capabilities	REG_DWORD	0x00000014 (20)
ContainerID	REG_SZ	{d7cbc01-b319-5c3d-8ec9-c6256a1ce047}
HardwareID	REG_MULTI_SZ	USB\VID_1058&PID_10A2&REV_1033 USB\VID_1058&PID_10A2
CompatibleIDs	REG_MULTI_SZ	USB\Class_08&SubClass_06&Prot_50 USB\Class_08&SubClass_06 USB\Class_08
ClassGUID	REG_SZ	{36fc9e60-c465-11cf-8056-444553540000}
Service	REG_SZ	USBSTOR
Driver	REG_SZ	{36fc9e60-c465-11cf-8056-444553540000}\0006
IMfg	REG_SZ	@usbstor.inf%\generic.mfg%;Compatible USB storage device
ConfigFlags	REG_DWORD	0x00000000 (0)

Name	Type	Data
LocationInformation	REG_SZ	Port_#0002.Hub_#0001
Capabilities	REG_DWORD	0x00000084 (132)
ContainerID	REG_SZ	{eddb0889-1252-11e4-9736-806e6f6e6963}
HardwareID	REG_MULTI_SZ	USB\VID_1241&PID_1203&REV_0230 USB\VID_1241&PID_1203
CompatibleIDs	REG_MULTI_SZ	USB\DevClass_00&SubClass_00&Prot_00 USB\DevClass_00&SubClass_00 USB\DevClass_00 USB\COMP...
ClassGUID	REG_SZ	{36fc9e60-c465-11cf-8056-444553540000}
Service	REG_SZ	usbccp
DeviceDesc	REG_SZ	@usb.inf%\usb\composite.devidesc%USB Composite Device
Driver	REG_SZ	{36fc9e60-c465-11cf-8056-444553540000}\0010
IMfg	REG_SZ	@usb.inf%\generic.mfg%;(Standard USB Host Controller)
ConfigFlags	REG_DWORD	0x00000000 (0)
ParentIDPrefix	REG_SZ	6&3023beff&0

Name	Type	Data
Locatio...	REG_SZ	0000.0006.0000.003.000.000.000....
Capabili...	REG_DW...	0x00000080 (128)
Contain...	REG_SZ	{9938829b-11bf-11e4-9732-0800...
Hardwa...	REG_MUL...	USB\VID_1241&PID_1203&REV_02...
Compat...	REG_MUL...	USB\Class_03&SubClass_01&Prot_...
ClassGU...	REG_SZ	{745a17a0-74d3-11d0-b6fe-00a0c...
Service	REG_SZ	HidUsb
Device...	REG_SZ	@input.inf%\hid.devidesc%USB ...
Driver	REG_SZ	{745a17a0-74d3-11d0-b6fe-00a0c...
IMfg	REG_SZ	@input.inf%\stdmfg%;(Standard sy...
ConfigF...	REG_DW...	0x00000000 (0)
Parentl...	REG_SZ	7&28312db2&0

Name	Type	Data
Locatio...	REG_SZ	0000.0006.0000.003.000.000.000....
Capabili...	REG_DW...	0x00000080 (128)
Contain...	REG_SZ	{9938829b-11bf-11e4-9732-0800...
Hardwa...	REG_MUL...	USB\VID_1241&PID_1203&REV_02...
Compat...	REG_MUL...	USB\Class_03&SubClass_00&Prot_...
ClassGU...	REG_SZ	{745a17a0-74d3-11d0-b6fe-00a0c...
Service	REG_SZ	HidUsb
Device...	REG_SZ	@input.inf%\hid.devidesc%USB ...
Driver	REG_SZ	{745a17a0-74d3-11d0-b6fe-00a0c...
IMfg	REG_SZ	@input.inf%\stdmfg%;(Standard sy...
ConfigF...	REG_DW...	0x00000000 (0)
Parentl...	REG_SZ	7&106da16d&0

Name	Type	Data
Device...	REG_SZ	@usbstor.inf%\genericbulkonly.de...
Locatio...	REG_SZ	Port_#0004.Hub_#0001
Capabili...	REG_DW...	0x00000014 (20)
Contain...	REG_SZ	{03020100-0504-0706-0800-0000...
Hardwa...	REG_MUL...	USB\VID_152D&PID_0539&REV_0...
Compat...	REG_MUL...	USB\Class_08&SubClass_06&Prot_...
ClassGU...	REG_SZ	{36fc9e60-c465-11cf-8056-44455...
Service	REG_SZ	USBSTOR
Driver	REG_SZ	{36fc9e60-c465-11cf-8056-44455...
IMfg	REG_SZ	@usbstor.inf%\generic.mfg%;Com...
ConfigF...	REG_DW...	0x00000000 (0)

The screenshot shows two registry keys in the Windows Registry Editor:

- Key 1 (Top):** `HKLM\Device\Hubs\VID_4146&PID_BA6\{d225e4040545c5}`
- Key 2 (Bottom):** `HKLM\Device\Hubs\VID_80EE&PID_0002\5&2d7ae1ff&0&`

Key Properties:

- Key 1 Last Written T 3/4/2014 14:25:
- Key 2 Last Written T 8/6/2014 2:54:4

Table Data (Key 1):

Name	Type	Data
DeviceName	REG_SZ	@usbstor.inf,%genericbulkonly.de...
LocationName	REG_SZ	Port_#0003.Hub_#0001
Capabilities	REG_DWORD	0x00000014 (20)
ContainerID	REG_SZ	{cfe61601-e2dc-56a4-86f7-e9719...
HardwareClass	REG_MULTI_SZ	USB\VID_4146&PID_BA67&REV_0...
CompatList	REG_MULTI_SZ	{36fc9e60-c465-11cf-8056-44455...
ClassGUID	REG_SZ	{36fc9e60-c465-11cf-8056-44455...
Service	REG_SZ	USBSTOR
Driver	REG_SZ	{36fc9e60-c465-11cf-8056-44455...
Mfg	REG_SZ	@usbstor.inf,%generic.mfg%;Com...
ConfigFlags	REG_DWORD	0x00000000 (0)

Table Data (Key 2):

Name	Type	Data
DeviceName	REG_SZ	@input.inf,%hid.devicedesc%;USB ...
LocationName	REG_SZ	Port_#0001.Hub_#0001
Capabilities	REG_DWORD	0x00000084 (132)
ContainerID	REG_SZ	{538e1959-8f1a-11e3-9716-806e6...
HardwareClass	REG_MULTI_SZ	USB\VID_80EE&PID_0021&REV_01...
CompatList	REG_MULTI_SZ	{745a17a0-74d3-11d0-b6fe-00a0c...
ClassGUID	REG_SZ	{745a17a0-74d3-11d0-b6fe-00a0c...
Service	REG_SZ	HidUsb
Driver	REG_SZ	{745a17a0-74d3-11d0-b6fe-00a0c...
Mfg	REG_SZ	@input.inf,%stdmfg%;(Standard sy...
ConfigFlags	REG_DWORD	0x00000000 (0)
ParentID	REG_SZ	6&156f3ba&0

- How many mounted devices on the system have an assigned drive letter?
 - There are 5 mounted devices attached to the computer and out of which 2 devices on the system have an attached a drive letter

\DosDevices\C: , \DosDevices\D:

The screenshot shows the `HKLM\HardwareConfig\MountedDevices` key in the Windows Registry Editor.

Key Properties:

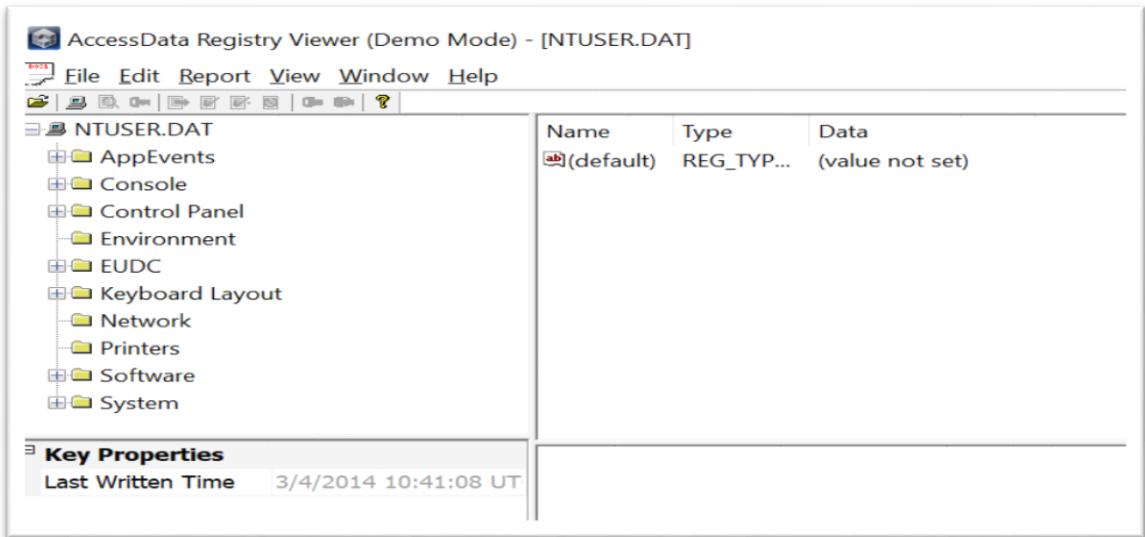
- Last Written Time 2/6/2014 10:35:06 UTC

Table Data:

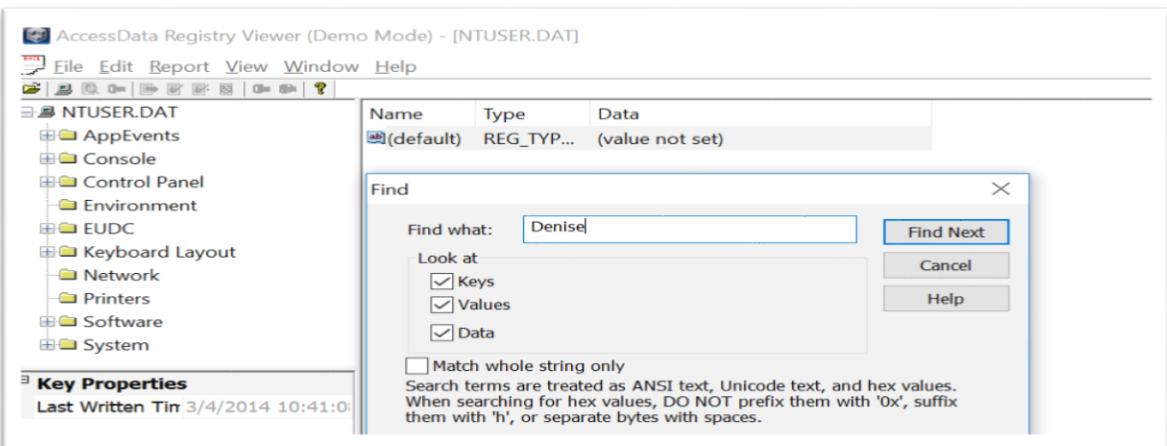
Name	Type	Data
\DosDevices\C:	REG_BINARY	7B 30 A1 3C 00 00 F0 15 00 00 00 00
\Volume{538e1951-8f1a-11e3-9716-806e6f6e6963}	REG_BINARY	7B 30 A1 3C 00 00 10 00 00 00 00 00
\Volume{538e1952-8f1a-11e3-9716-806e6f6e6963}	REG_BINARY	7B 30 A1 3C 00 00 F0 15 00 00 00 00
\Volume{538e1956-8f1a-11e3-9716-806e6f6e6963}	REG_BINARY	5C 00 3F 00 3F 00 5C 00 49 00 44 00 45 00 23 00 43 00 64 00 52 0
\DosDevices\D:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 49 00 44 00 45 00 23 00 43 00 64 00 52 0

4. Examining the NTUSER.DAT File

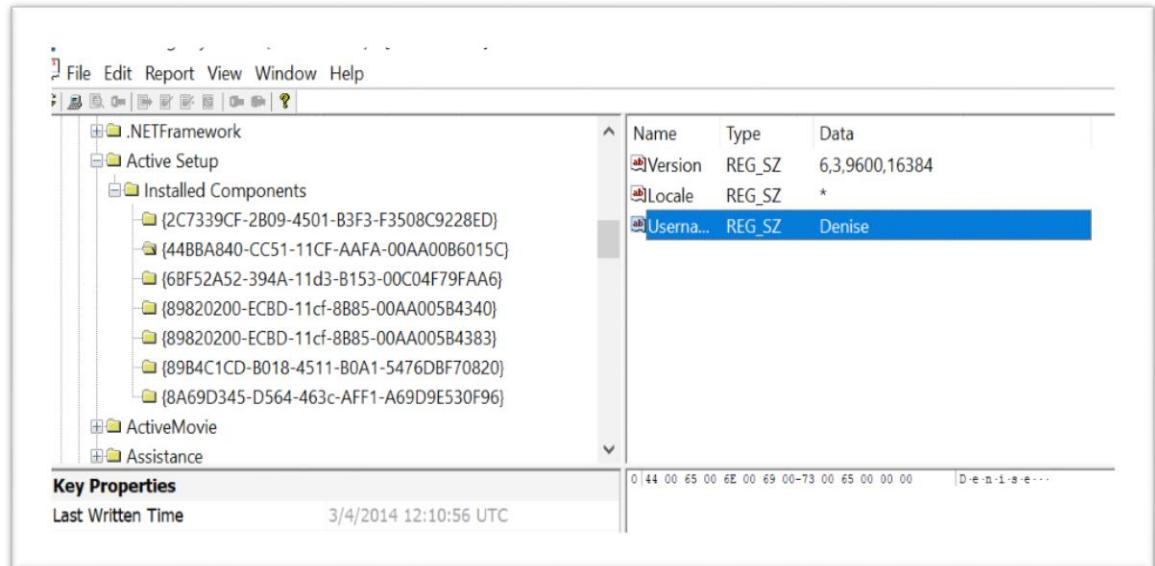
- NTUSER.DAT is a windows generated file and contains information about user account settings. Each user has their own NTUSER.DAT file in user's profile. [2]
- Open the NTUSER.DAT file from the extracted registry files for analysis



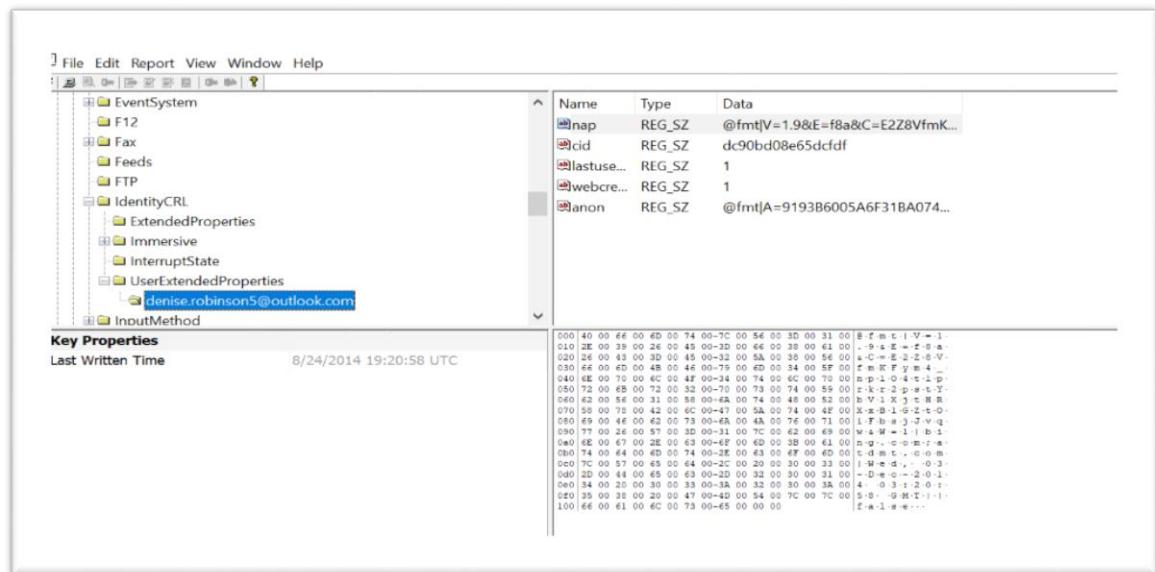
- Click Edit → Find and type Denise into the search bar, click Next and Iterate through the search (by pressing F3) to identify information related to the Denise user account:



1. GUID associated with the username



2. Email account information



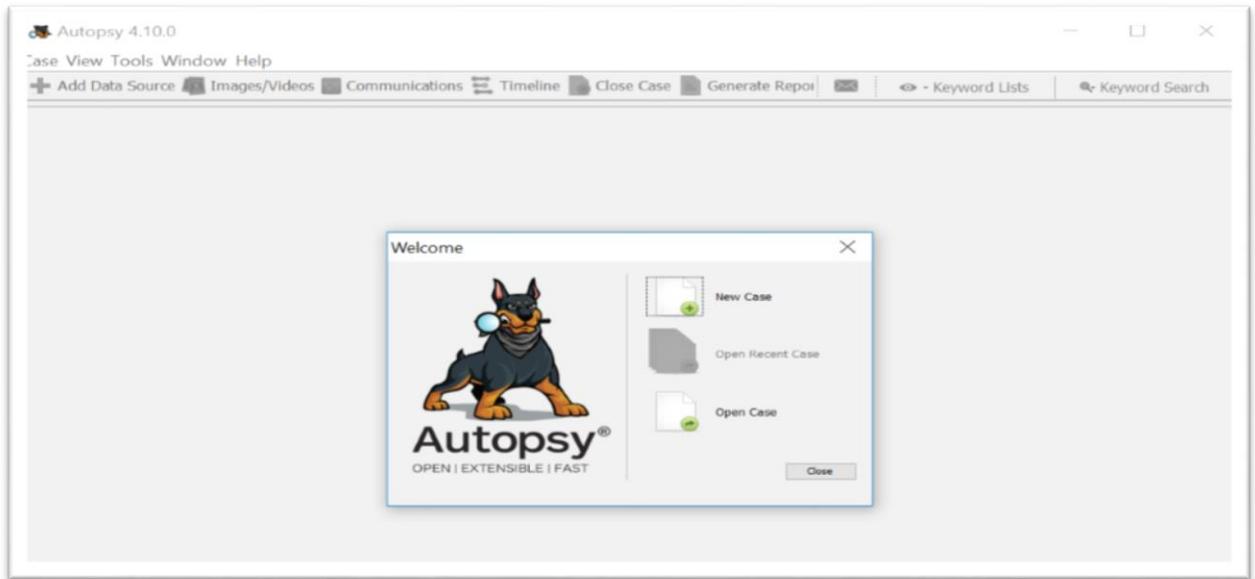
- Click Edit-Find, and type “jfriday” in the resulting search box.
 1. What information can you find for jfriday? Why?
 - There is no information available for user jfriday after searching. Because while extracting NTUSER.DAT file, I have only extracted file from Denise user profile
 - NTUSER.DAT is a windows generated file and contains information about user account settings. Each user has their own NTUSER.DAT file in user's profile.

Since I have only extracted NTUSER.DAT file from Denise profile, there is no details available for user jfriday. [2]

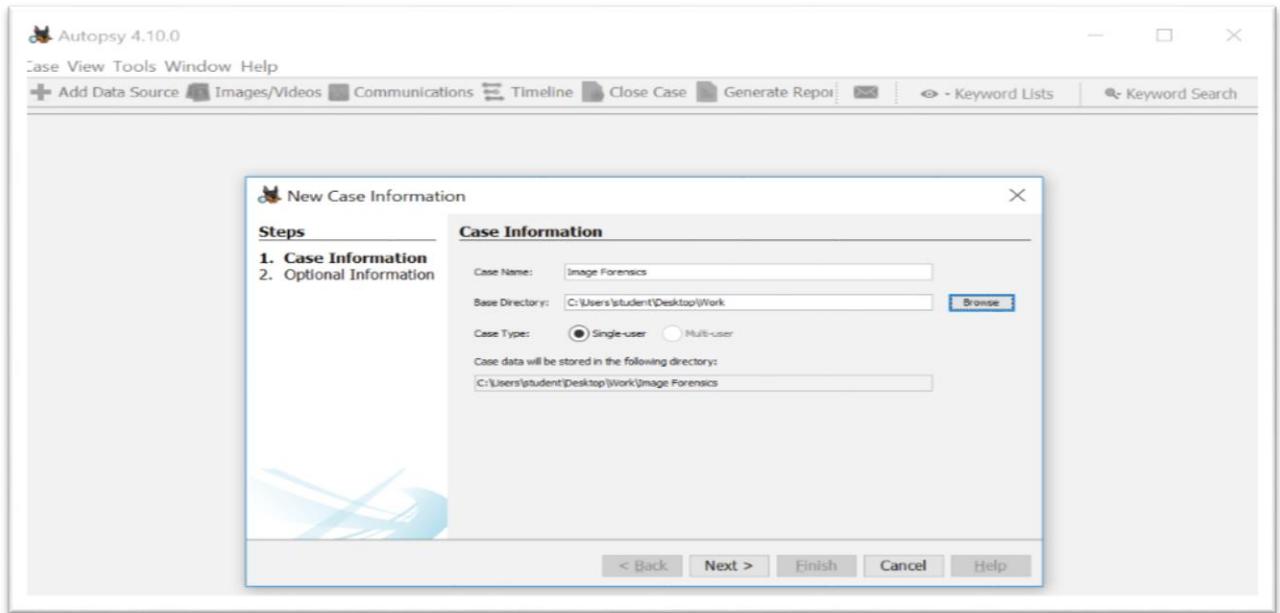
Image Forensics

1. Analysis of Image Files

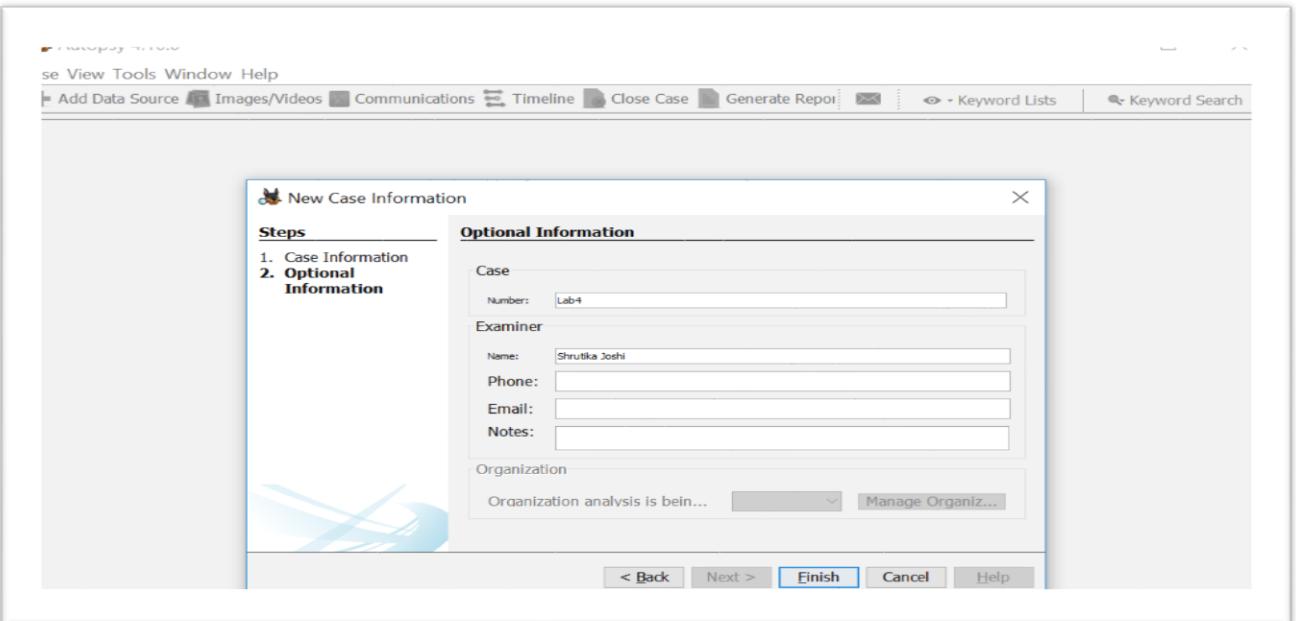
- Open Autopsy and create new case



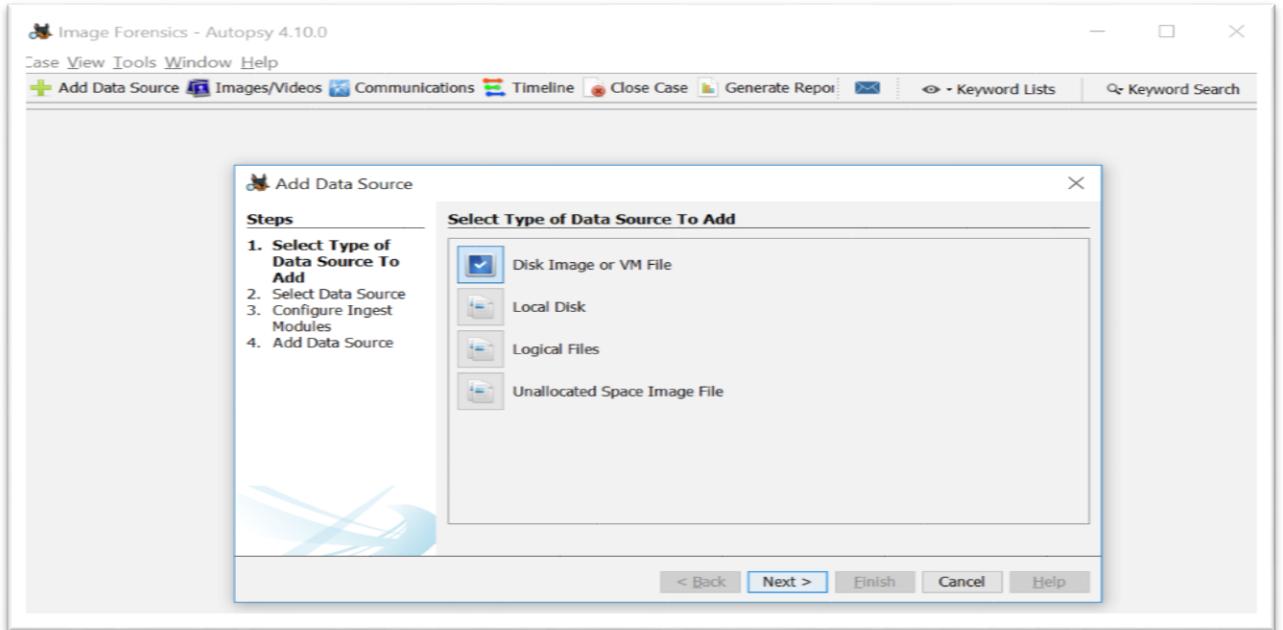
- Run through the new case wizard, add Case name and file destination location and click Next



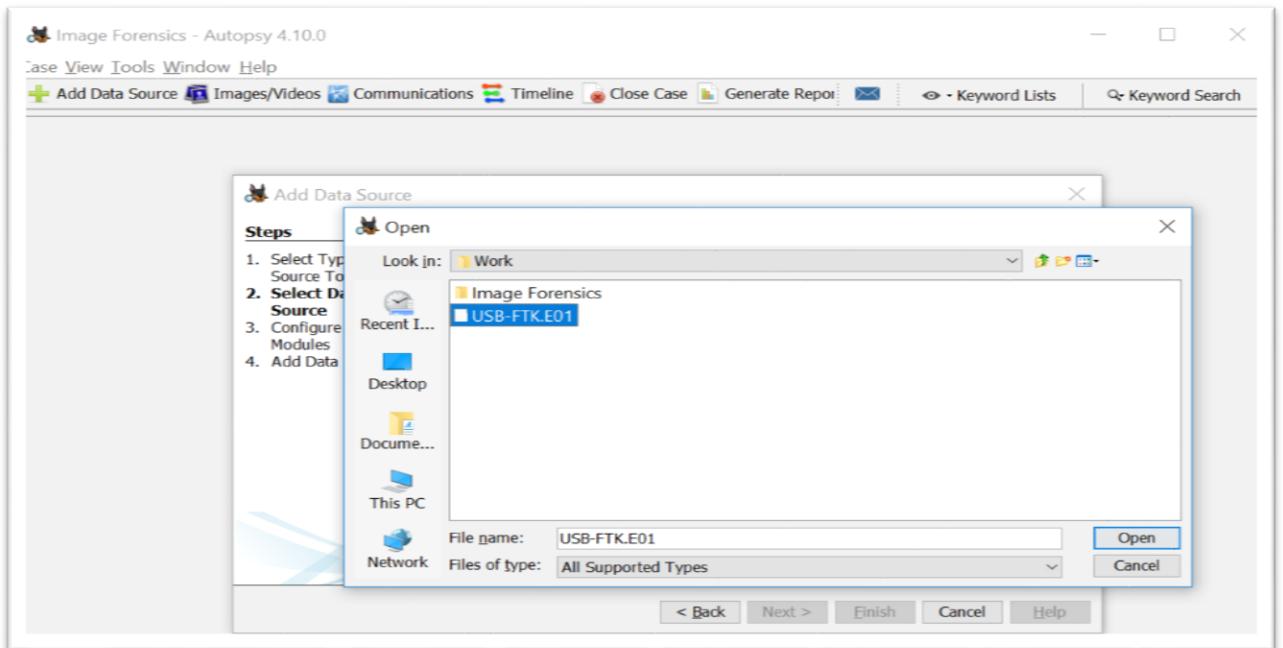
- Now add Case Number and Examiner name in the pop-up window and click Finish



- In the Add Data Source panel, click on Disk Image or VM File option and click Next.

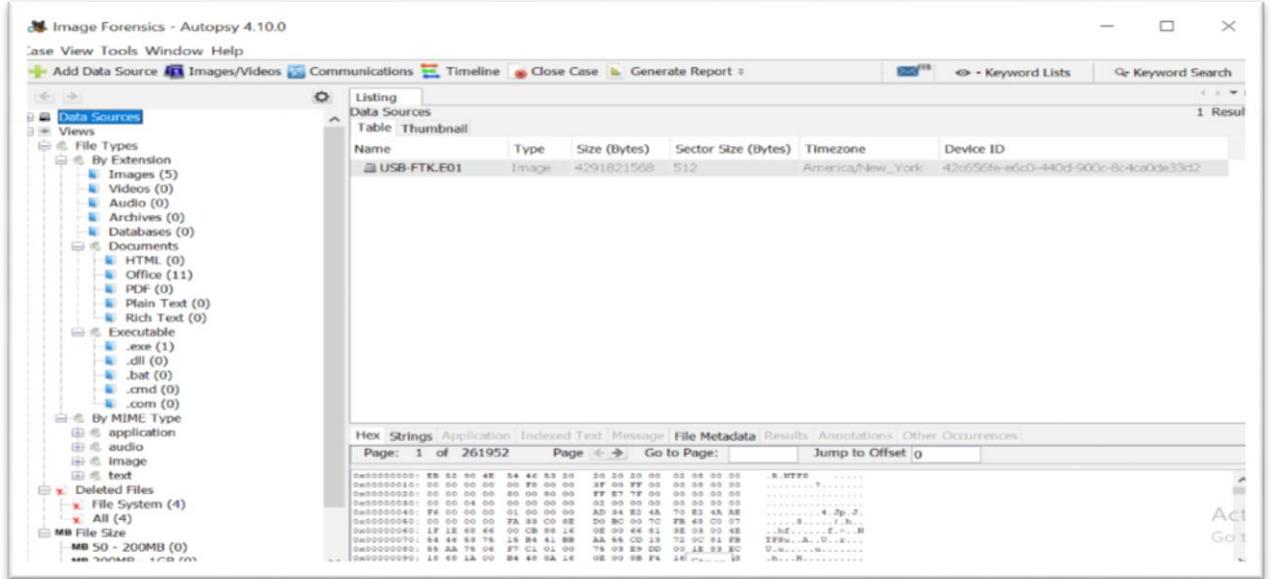


- Browse to one of the USB-FTK images you created in lab 2 (.E01 file format) and click Open.



- Let Autopsy parse through the image. When finished, expand the Views category and identify all images files. Perform an extraction of the images so you can manually review

them. (Note you can also see "Deleted Files", which is also helpful to check in a full investigation)



- Expand the Results category - Extracted Content to look at EXIF Metadata.
 1. What information can you see related to the images you identified previously?
 - From the below image, I could see details EXIF metadata like Source File, Date Created, Device Model, Device Make, Data Source, Size, Path, Latitude, Longitude, and Altitude.
 - Also, from the File Metadata tab, I am able to view important details like File Modified, Access and Change Date, MD5 hash.

e View Tools Window Help

Add Data Source Images/Videos Communications Timeline Close Case Generate Report

Listing EXIF Metadata

Table Thumbnail

Source File	S	C	O	Date Created	Device Model	Device Make	Data Source	Size	Path	Latitude
DCP_1255.jpg				2007-09-20 23:20:50 EDT	KODAK DX3600 DIGITAL CAMERA	EASTMAN KODAK COMPANY	USB-FTK.E01	271844	/Img_USB-FTK.E01/DCP_1255.jpg	
20160425_142807(0).jpg				2016-04-25 14:28:07 EDT	SAMSUNG-SM-G935A	samsung	USB-FTK.E01	2648568	/Img_USB-FTK.E01/20160425_142807... 39.248063	

Hex Strings Application Indexed Text Message File Metadata Results Annotations Other Occurrences

Name: /Img_USB-FTK.E01/DCP_1255.jpg
Type: File System
MIME Type: image/jpeg
Size: 271844
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2007-09-20 23:20:56 EDT
Accessed: 2019-08-05 18:29:29 EDT
Created: 2019-08-02 15:55:27 EDT
Changed: 2019-08-02 15:55:27 EDT
MD5: db4ebf724cdcb60fb6073c1d74720cb
Hash Lookup Results: UNKNOWN
Internal ID: 63

From The Sleuth Kit Hex Tool:
HTTP Entity Header Values:
Entry: 54 Sequence: 1
Last-Modified: 2019-08-02 15:55:27.114528000
Content-Type: image/jpeg
Content-Length: 271844
Content-MD5: db4ebf724cdcb60fb6073c1d74720cb
Content-Security-Policy: none
Content-Encoding: none
Content-Language: en-US
Content-Type: image/jpeg
Content-Length: 2648568
Content-MD5: 7c8e92e9a9a52bfb2d3e626eba844530
Content-Security-Policy: none
Content-Encoding: none
Content-Language: en-US

e View Tools Window Help

Add Data Source Images/Videos Communications Timeline Close Case Generate Report

Listing EXIF Metadata

Table Thumbnail

Source File	S	C	O	Date Created	Device Model	Device Make	Data Source	Size	Path	Latitude
DCP_1255.jpg				2007-09-20 23:20:50 EDT	KODAK DX3600 DIGITAL CAMERA	EASTMAN KODAK COMPANY	USB-FTK.E01	271844	/Img_USB-FTK.E01/DCP_1255.jpg	
20160425_142807(0).jpg				2016-04-25 14:28:07 EDT	SAMSUNG-SM-G935A	samsung	USB-FTK.E01	2648568	/Img_USB-FTK.E01/20160425_142807... 39.248063	

Hex Strings Application Indexed Text Message File Metadata Results Annotations Other Occurrences

Name: DCP_1255.jpg
Type: File System
MIME Type: image/jpeg
Size: 271844
File Name Allocation: Allocated
Metadata Allocation: Allocated
Links: 1
STANDARD_INFORMATION Attributes Values:
File: Archive
Format: ZIP
Decompress ID: 204 (13-0-12-0214340847-1800000000-027948422-1001)
Version: 1.0
File Modified: 2019-08-02 15:55:27.114528000 (EDT)
File Accessed: 2019-08-02 15:55:27.114528000 (EDT)
File Created: 2019-08-02 15:55:27.114528000 (EDT)
File Changed: 2019-08-02 15:55:27.114528000 (EDT)
Accessed: 2019-08-02 15:55:27.114528000 (EDT)
Allocation:
Name: DCP_1255.jpg
Type: STANDARD_INFORMATION (140-0) Name: N/A Resident size: 72
Name: FILE_NAME (43-0) Name: N/A Resident size: 0

Image Forensics - Autopsy 4.10.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Timeline Close Case Generate Report

Listing EXIF Metadata

Table Thumbnail

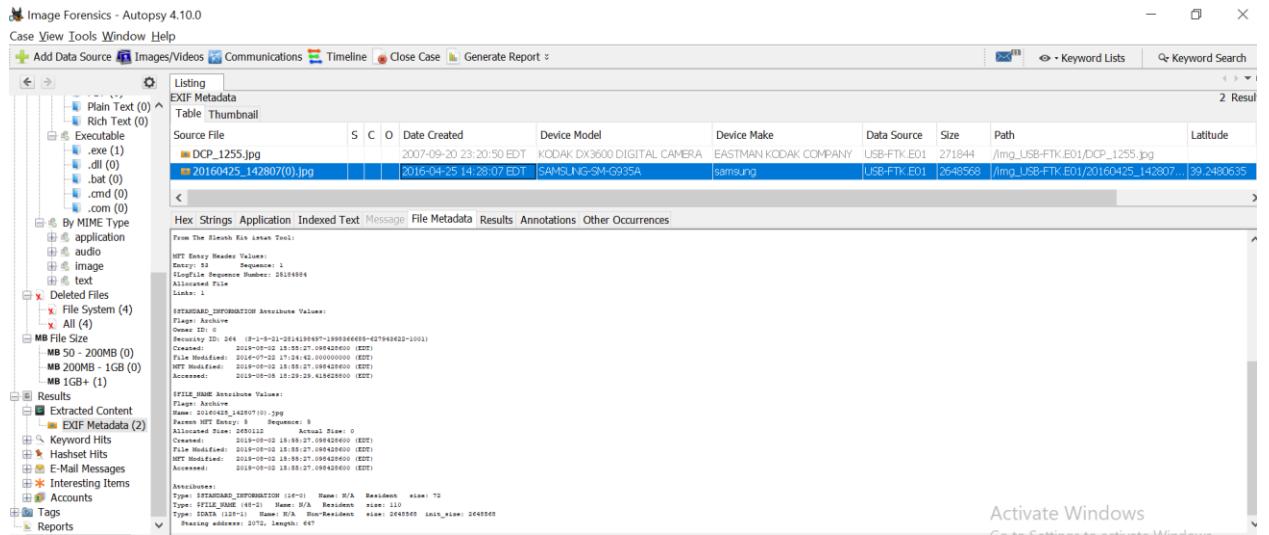
Source File	S	C	O	Date Created	Device Model	Device Make	Data Source	Size	Path	Latitude
DCP_1255.jpg				2007-09-20 23:20:50 EDT	KODAK DX3600 DIGITAL CAMERA	EASTMAN KODAK COMPANY	USB-FTK.E01	271844	/Img_USB-FTK.E01/DCP_1255.jpg	
20160425_142807(0).jpg				2016-04-25 14:28:07 EDT	SAMSUNG-SM-G935A	samsung	USB-FTK.E01	2648568	/Img_USB-FTK.E01/20160425_142807... 39.248063	

Hex Strings Application Indexed Text Message File Metadata Results Annotations Other Occurrences

Name: /Img_USB-FTK.E01/20160425_142807(0).jpg
Type: File System
MIME Type: image/jpeg
Size: 2648568
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2016-07-22 17:24:42 EDT
Accessed: 2019-08-05 18:29:29 EDT
Created: 2019-08-02 15:55:27 EDT
Changed: 2019-08-02 15:55:27 EDT
MD5: 7c8e92e9a9a52bfb2d3e626eba844530
Hash Lookup Results: UNKNOWN
Internal ID: 56

From The Sleuth Kit Hex Tool:
HTTP Entity Header Values:
Entry: 54 Sequence: 1
Last-Modified: 2019-08-02 15:55:27.114528000
Content-Type: image/jpeg
Content-Length: 2648568
Content-MD5: 7c8e92e9a9a52bfb2d3e626eba844530
Content-Security-Policy: none
Content-Encoding: none
Content-Language: en-US
Content-Type: image/jpeg
Content-Length: 2648568
Content-MD5: 7c8e92e9a9a52bfb2d3e626eba844530
Content-Security-Policy: none
Content-Encoding: none
Content-Language: en-US

Activate Windows



- To manually check the EXIF Metadata, browse to the folder you extracted the image files to previously and then Right Click-Properties on each file.
 1. Do you see any additional EXIF Metadata that wasn't present in Autopsy?
 - For both of the images, after manually checking properties I can view, image dimension details as well as more details about the camera properties set during image capture which wasn't present in Autopsy file metadata details.

DCP_1255.jpg Properties	
General Security Details Previous Versions	
Property	Value
Description	
Title	
Subject	
Rating	☆ ☆ ☆ ☆ ☆
Tags	
Comments	
Origin	
Authors	
Date taken	9/20/2007 11:20 PM
Program name	
Date acquired	
Copyright	
Image	
Image ID	
Dimensions	1800 x 1200
Width	1800 pixels
Height	1200 pixels
Horizontal resolution	230 dpi
Vertical resolution	230 dpi
Remove Properties and Personal Information	
OK Cancel Apply	

DCP_1255.jpg Properties	
General Security Details Previous Versions	
Property	Value
Vertical resolution	230 dpi
Bit depth	24
Compression	
Resolution unit	2
Color representation	sRGB
Compressed bits/pixel	
Camera	
Camera maker	EASTMAN KODAK COMPAN...
Camera model	KODAK DX3600 DIGITAL C...
F-stop	f/8
Exposure time	1/700 sec.
ISO speed	
Exposure bias	0 step
Focal length	11 mm
Max aperture	4.3
Metering mode	Average
Subject distance	1.3 m
Flash mode	No flash
Flash energy	

DCP_1255.jpg Properties	
General Security Details Previous Versions	
Property	Value
Flash energy	
35mm focal length	
Advanced photo	
Lens maker	
Lens model	
Flash maker	
Flash model	
Camera serial number	
Contrast	
Brightness	
Light source	Unknown
Exposure program	Normal
Saturation	
Sharpness	
White balance	
Photometric interpretation	
Digital zoom	
EXIF version	0210
OK Cancel Apply	

DCP_1255.jpg Properties	
General Security Details Previous Versions	
Property	Value
Sharpness	
White balance	
Photometric interpretation	
Digital zoom	
EXIF version	0210
File	
Name	DCP_1255.jpg
Item type	JPG File
Folder path	C:\Users\student\Desktop\W...
Date created	7/8/2023 8:40 PM
Date modified	7/8/2023 8:40 PM
Size	265 KB
Attributes	A
Availability	
Offline status	
Shared with	
Owner	WINDOWS10\student
Computer	WINDOWS10 (this PC)

The image displays four windows showing the properties of the file "20160425_142807(0).jpg".

- General Tab:** Shows basic file information like Title, Subject, Rating, Tags, Comments, Origin, Authors, Date taken, Program name, Date acquired, Copyright, and Image details such as Image ID, Dimensions, Width, Height, and Horizontal resolution.
- Details Tab:** Shows camera metadata including Horizontal resolution, Vertical resolution, Bit depth, Compression, Resolution unit, Color representation, Compressed bits/pixel, Camera maker, Camera model, F-stop, Exposure time, ISO speed, Exposure bias, Focal length, Max aperture, Metering mode, and Subject distance.
- Advanced photo Tab:** Shows photo-specific metadata like Flash mode, Flash energy, 35mm focal length, Lens maker, Lens model, Flash maker, Flash model, Camera serial number, Contrast, Brightness, Light source, Exposure program, Saturation, Sharpness, White balance, Photometric interpretation, and Digital zoom.
- Previous Versions Tab:** Shows EXIF version (0220), GPS coordinates (Latitude: 39° 14' 53.0285999999054, Longitude: 76° 42' 51.8280999999842..., Altitude: 0), and file details like Name, Item type, Folder path, Date created, Date modified, Size, Attributes, Availability, Offline status, Shared with, Owner, and Computer.

- Try uploading the images to online resources like fotoforensics.com or imageforensic.org.
 1. Any additional EXIF Metadata, such as a location where the image was captured?

- I uploaded image onto fotoforensics.com and I could see MORE details shown in the snapshots like approximate Geo Location, MD5 , SHA1, SHA256 hash values and below are the details.

<https://fotoforensics.com/analysis.php?id=1815b008bcc78eeb6e5e2c39fe05b3f5ebc9797a.2648568>

Make : samsung

Camera Model Name: SAMSUNG-SM-G935A

Software: G935AUCU2APD1

Device Type: Cell Phone

Date/Time Original: 2016:04:25 14:28:07

Image Unique ID: C12QSJB01SB

GPS Latitude Ref: North

GPS Longitude Ref: West

GPS Altitude Ref: Unknown (1.7)

GPS Time Stamp: 18:28:06

GPS Date Stamp: 2016:04:25

GPS Position 39 deg 14' 53.03" N, 76 deg 42' 51.83" W

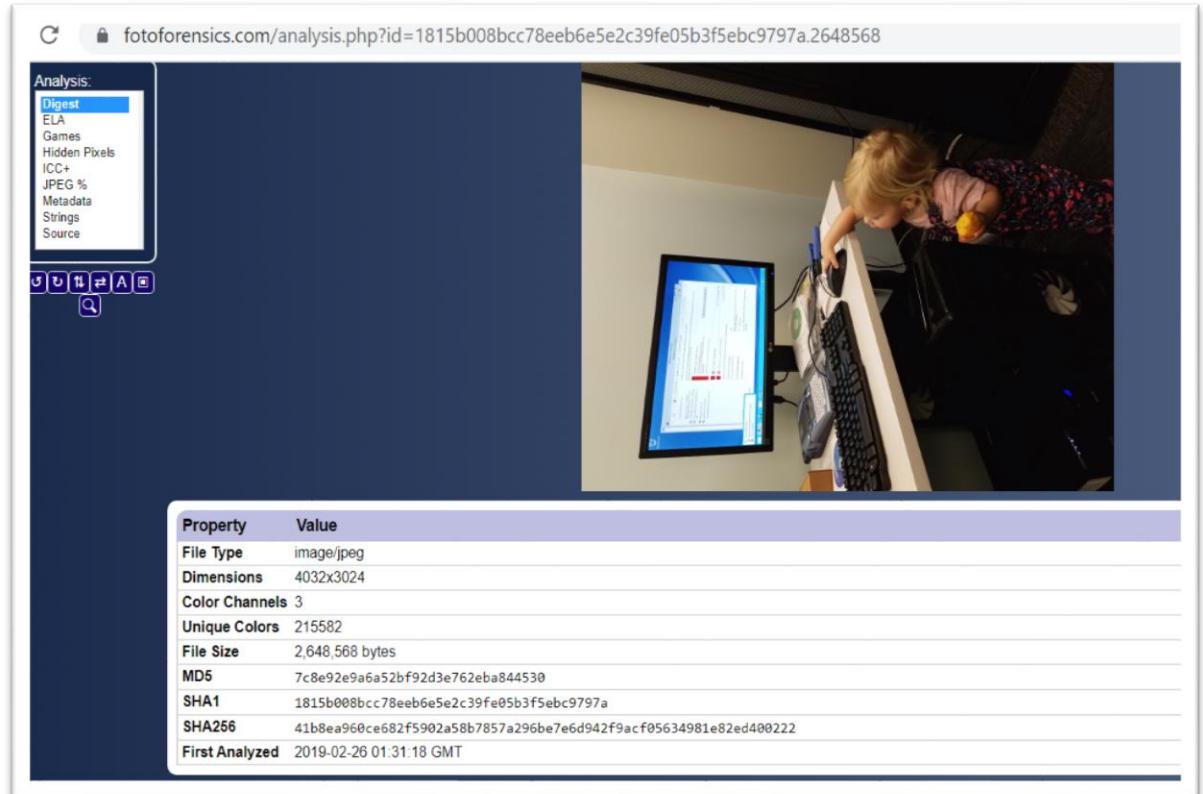
Approximate Coordinates : 39.248064,-76.714397

Approximate Location: Arbutus, MD, US

File Size: 2,648,568 bytes

MD5: 7c8e92e9a6a52bf92d3e762eba844530

- However, exposure of such metadata is harmful as it exposes all user details including the machine name, user PII details as well as geo location and hackers can take advantage of such details to design attacks or crack sensitive information. Also, it violates user privacy.



The screenshot shows a web-based forensic analysis tool. On the left, there's a sidebar with a navigation menu titled "Analysis:" containing options like "Digest", "ELA", "Games", "Hidden Pixels", "ICC+", "JPEG %", "Metadata", "Strings", and "Source". Below the menu are several small icons. The main area features a photograph of a young child with blonde hair, wearing a patterned shirt, sitting at a desk and looking at a computer monitor. The monitor displays a document with some text and a red highlight. At the bottom of the page is a table with the following data:

Property	Value
File Type	image/jpeg
Dimensions	4032x3024
Color Channels	3
Unique Colors	215582
File Size	2,648,568 bytes
MD5	7c8e92e9a6a52bf92d3e762eba844530
SHA1	1815b008bcc78eeb6e5e2c39fe05b3f5ebc9797a
SHA256	41b8ea960ce682f5902a58b7857a296be7e6d942f9acf05634981e82ed400222
First Analyzed	2019-02-26 01:31:18 GMT

File	
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Exif Byte Order	Little-endian (Intel, II)
Image Width	4032
Image Height	3024
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
Y Cb Cr Sub Sampling	YCbCr4:2:0 (2 2)
EXIF	
Make	samsung
Camera Model Name	SAMSUNG-SM-G935A
Orientation	Rotate 90 CW
X Resolution	72
Y Resolution	72
Resolution Unit	inches
Software	G935AUCL2APD1
Modify Date	2016.04.25 14:28:07
Y Cb Cr Positioning	Centered
Exposure Time	1/60
F Number	1.7
Exposure Program	Program AE
ISO	125
Exif Version	0220
Date/Time Original	2016.04.25 14:28:07
Create Date	2016.04.25 14:28:07

Activate Windows
Go to Settings to activate Windows

Shutter Speed Value	
Aperture Value	1.7
Brightness Value	2.19
Exposure Compensation	0
Max Aperture Value	1.7
Metering Mode	Center-weighted average
Light Source	Unknown
Flash	No Flash
Focal Length	4.2 mm
User Comment	-
Flashpix Version	0100
Color Space	sRGB
Exif Image Width	4032
Exif Image Height	3024
Interoperability Index	R98 - DCF basic file (sRGB)
Interoperability Version	0100
Sensing Method	One-chip color area
Scene Type	Directly photographed
Exposure Mode	Auto
White Balance	Auto
Focal Length In 35mm Format	26 mm
Scene Capture Type	Standard
Image Unique ID	C12QSJB01SB
GPS Latitude Ref	North
GPS Longitude Ref	West
GPS Altitude Ref	Unknown (1.7)
GPS Time Stamp	18:28:06
GPS Date Stamp	2016:04:25
Compression	JPEG (old-style)

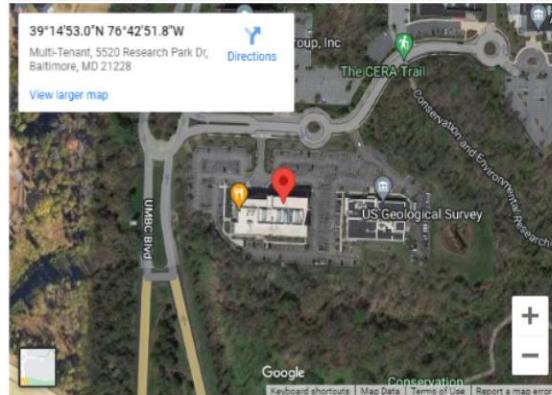
fotoforensics.com/analysis.php?id=1815b008bcc78eeb6e5e2c39fe05b3f5ebc9797a.2648568

GPS Date Stamp	2016:04:25
Compression	JPEG (old-style)
Thumbnail Offset	6150
Thumbnail Length	13480
Thumbnail Image	(Binary data 13480 bytes)
MakerNotes	
Maker Note Version	0100
Device Type	Cell Phone
Raw Data Byte Order	Little-endian (Intel, II)
Raw Data CFA Pattern	Swap
Face Detect	Off
Time Stamp	2016:04:25 18:28:07+00:00
Composite	
Aperture	1.7
Shutter Speed	1/60
GPS Altitude	0 m Above Sea Level
GPS Date/Time	2016:04:25 18:28:06Z
GPS Latitude	39 deg 14' 53.03" N
GPS Longitude	76 deg 42' 51.83" W
GPS Position	39 deg 14' 53.03" N, 76 deg 42' 51.83" W
Image Size	4032x3024
Light Value	7.1
Megapixels	12.2
Scale Factor To 35 mm Equivalent	6.2
Circle Of Confusion	0.005 mm
Field Of View	69.4 deg
Focal Length	4.2 mm (35 mm equivalent: 26.0 mm)
Hyperfocal Distance	2.14 m

Approximate GPS Location

This information is interpreted from the GPS metadata. **Locations are approximate.** Although the coordinates appear precise, mobile devices typically have low accuracy.

Approximate Coordinates	39.248064,-76.714397
Approximate Location	Arbutus, MD, US
Approximate Range	Unspecified; assume +/- 3218 meters (2 miles)



Glossary –

1. **MD5 hash** – (Message Digest Algorithm) it is a cryptographic function that takes input of any length and convert it into 128 bit hash values.
2. **GPS** – (Global Positioning System) It is navigating system using satellites, a receiver and algorithm to synchronize location, velocity and time data for air, sea and land level.
3. **Hive** – Logical group of keys, subkeys and values in registry
4. **EXIF Metadata** – (Exchangeable Image File Format) It holds information about the image itself.
5. **GUID** – (Globally unique Identifier) it is a 128 bit string that represents identification (ID)

Citations –

1. Khanse, A. (2022, October 20). Where are the Windows Registry files located in Windows 7? The Windows Club. Retrieved from <https://www.thewindowsclub.com/where-are-the-windows-registry-files-located-in-windows-7>
2. Hendrickson, J. (2019, January 18). What Is the NTUSER.DAT File? How-To Geek. Retrieved July 6, 2023, from <https://www.howtogeek.com/401365/what-is-the-ntuser.dat-file/>
3. TechTarget. (n.d.). Security Accounts Manager (SAM). SearchEnterpriseDesktop. Retrieved July 6, 2023, from <https://www.techtarget.com/searchenterprisedesktop/definition/Security-Accounts-Manager> by Katie Terrell Hanna
4. Hany Farid. (n.d.). FotoForensics. Retrieved July 6, 2023, from <https://fotoforensics.com/>

5. Heddings, L. (2019, April 30). Using Windows Admin Tools Like a Pro: Lesson 5 - Using Event Viewer to Troubleshoot Problems. How-To Geek. Retrieved from <https://www.howtogeek.com/school/using-windows-admin-tools-like-a-pro/lesson5/>