CIS4810.01 Lab 2

Forensic Data Analysis

Case #CIS4810.01LAB2

Michael Andom

# Part 1 – Registry Analysis – System Hive

Answer the following questions using the SYSTEM hive:

1. Determine the current control set.

On March 30, 2023, at 10:07 pm PST, Michael Andom uploaded the evidence into EnCase under Case(E.Polytech). Michael Andom clicked ID THEFT 1 evidence file to inspect the evidence. The ID THEFT 1 evidence file has a Windows 2000+ Registry file type named system.

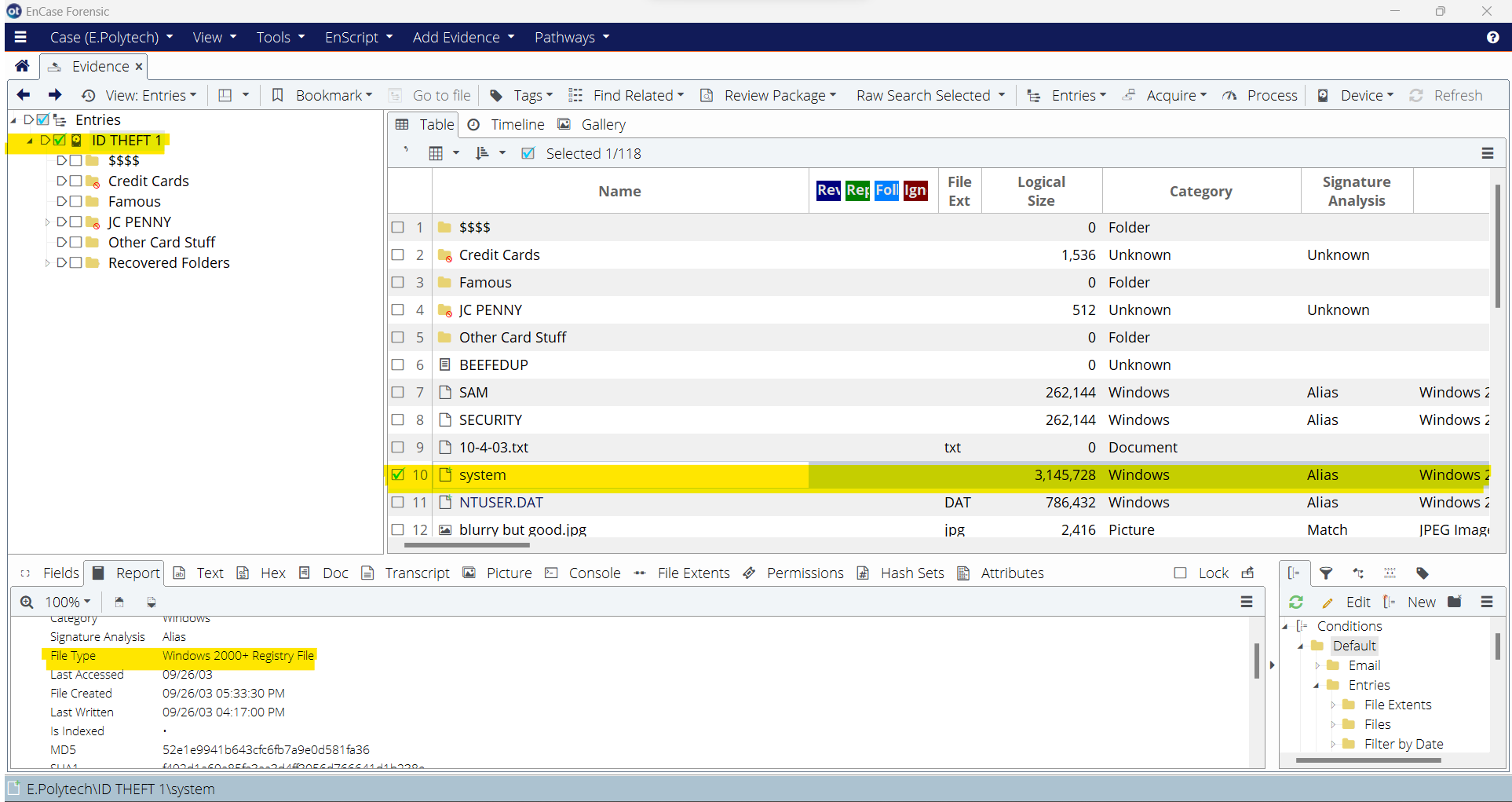


Figure 1.1 ID THEFT 1 file, Windows 2000+ Registry file type: system

On March 30, 2023, at 10:20 pm PST, Michael Andom double-clicked on the Windows 2000+ Registry file called system. In the file called system, there is a hive on the left bar starting with system → $$$PROTO.HIV.

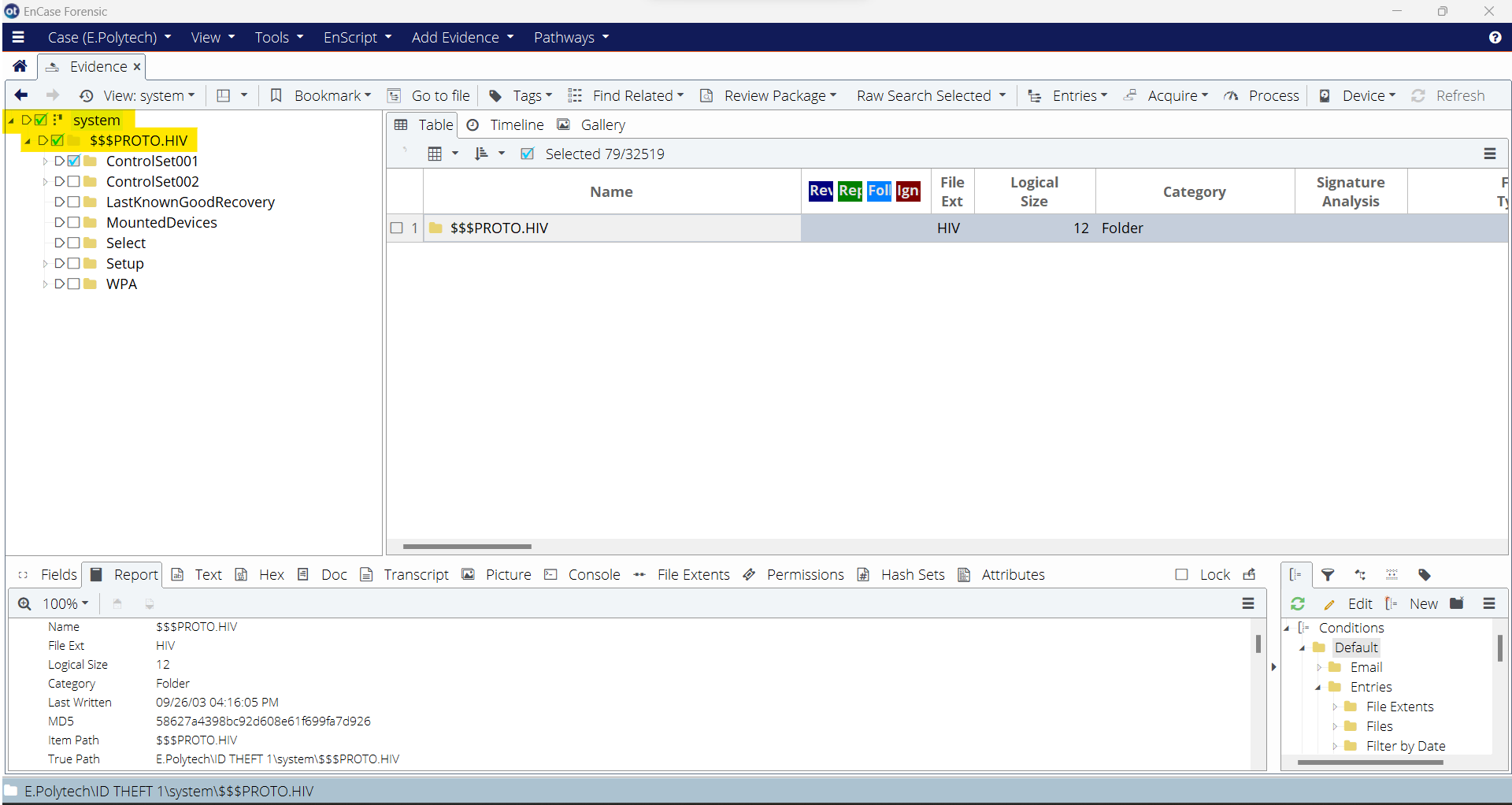


Figure 1.2 Windows 2000+ Registry File: system, hive: $$$PROTO.HIV folder on the left bar

Under the hive, $$$PROTO.HIV, are keys of ControlSet001, ControlSet002, LastKnownGoodRecovery, MountedDevices, Select, Setup, and WPA. On March 30, 2023, at 11:04 pm, the key titled ControlSet1, has subkeys of Control, Enum, Hardware Profiles, and Services. Under the subkeys of the subkey ControlSet1 called Hardware Profiles, there are two subkeys called 0000 and 0001. In subkey 0001, are subkeys of Software and System. Under the subkey System is a subkey called CurrentControlSet.

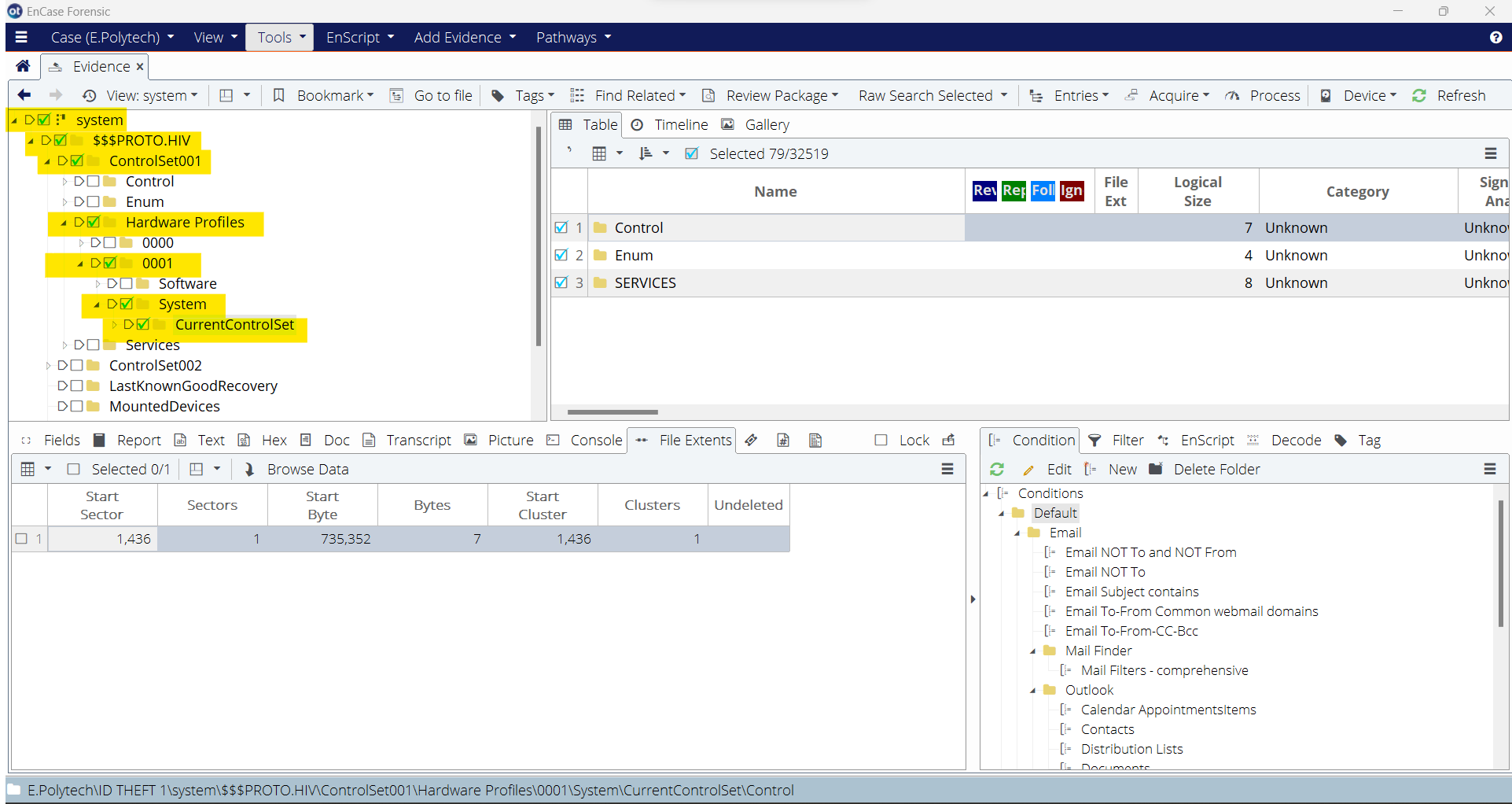


Figure 1.3 True Path: E.Polytech\ID THEFT 1\system\$$$PROTO.HIV\ControlSet001\Hardware Profiles\0001\System\CurrentControlSet\

In the Windows 2000+ Registry file, system, the Start Sector is 1,436, Sectors 1, and Start Cluster is 1,436, Clusters 1.

1. Determine the time zone bias of the suspect’s computer

On March 30, 2023, at 11:14 pm, Michael Andom went back to the right-clicked on the Windows 2000+ Registry file called system and went to Entries to Copy Files. On March 30, 2023, at 11:20 pm, Michael Andom saved Windows 2000+ Registry File under Export.

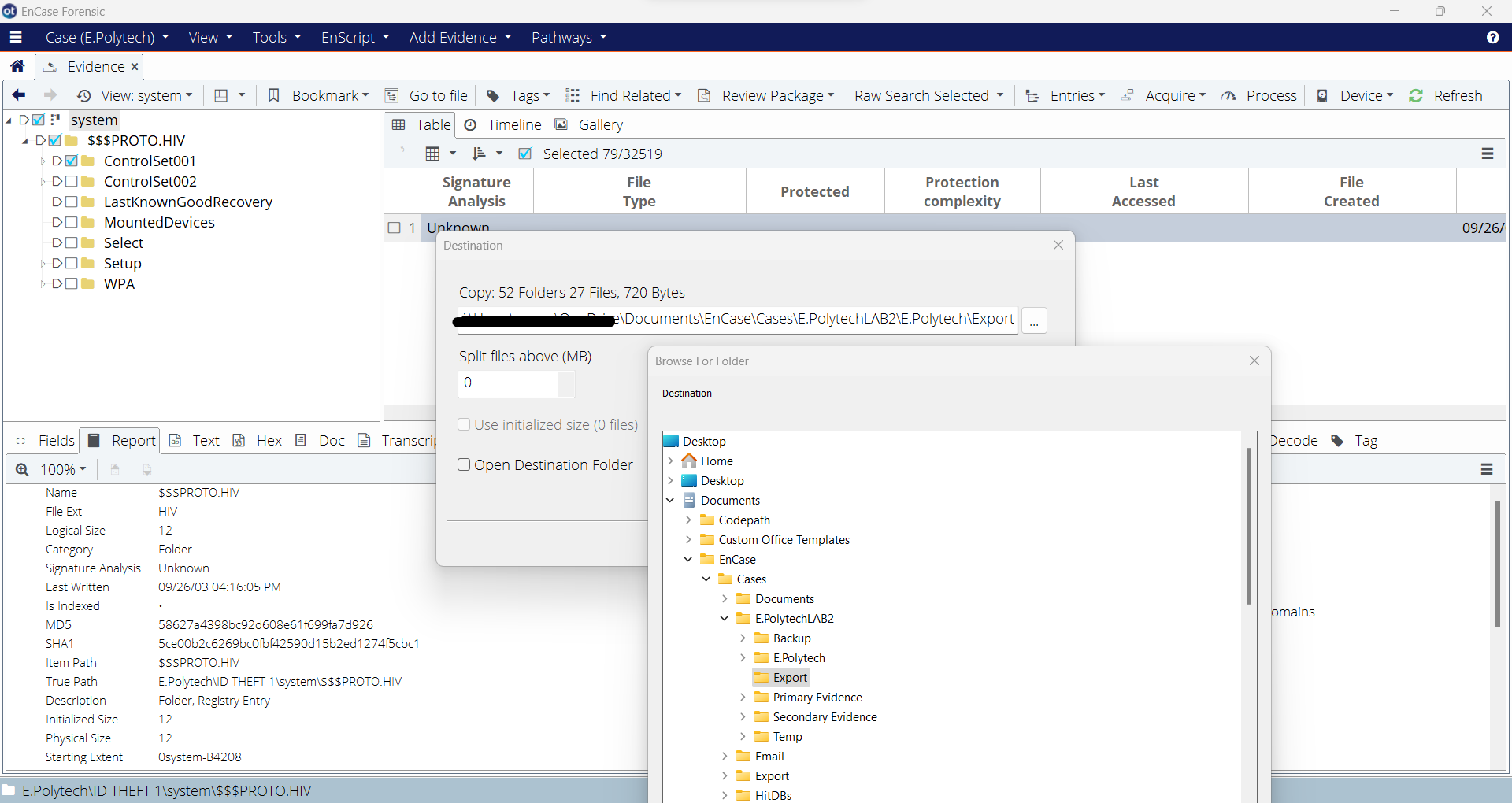


Figure 2.1 True Path: …\Documents\EnCase\Cases\E.PolytechLAB2\Export

On March 30, 2023, at 11:26 pm, Michael Andom opened a software, RegRipper v3.0, to extract the Windows registry hive file called system.

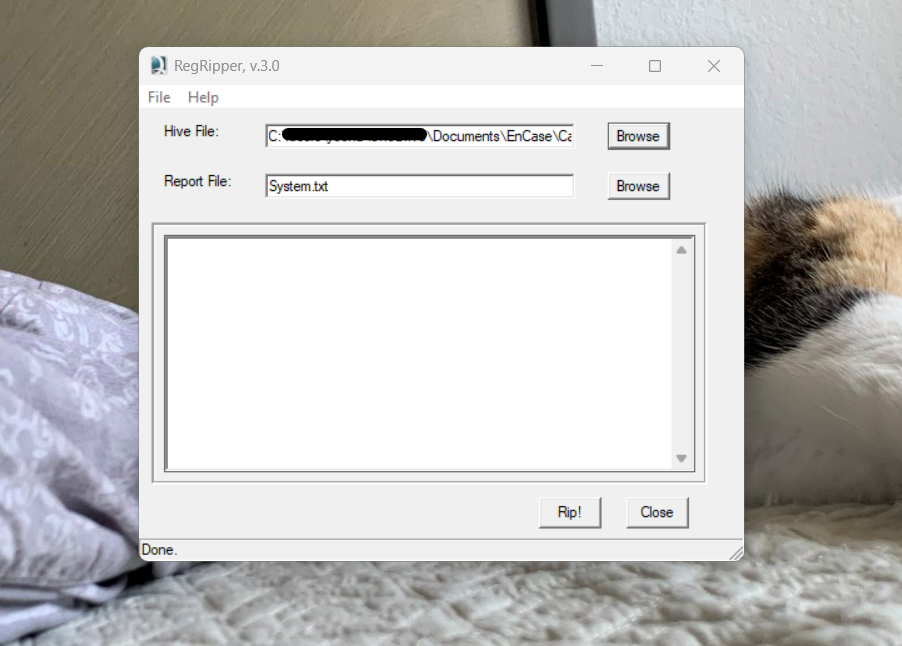


Figure 2.2 RegRipper v3.0

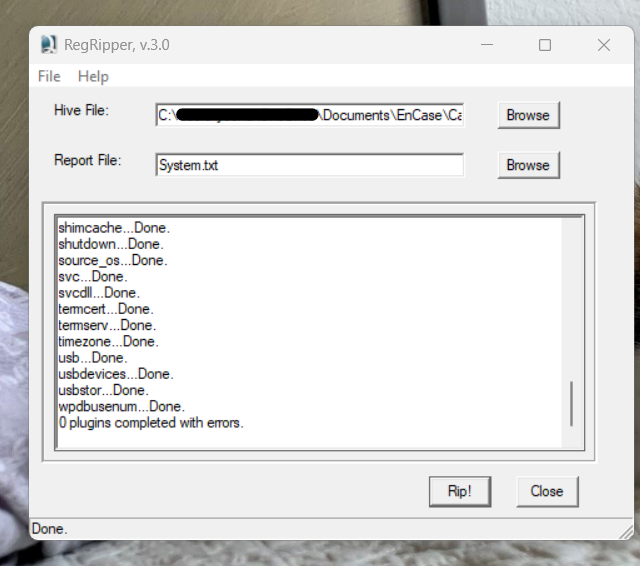


Figure 2.3 RegRipper v3.0 successful Rip!

After successfully extracting the Windows 2000+ Registry file, system, Michael Andom saved the text file called System.txt. March 30, 2023, at 11:43 pm, Michael Andom opened the System.txt file and searched timezone. The time zone bias of the suspect’s computer was set to Mountain Standard.

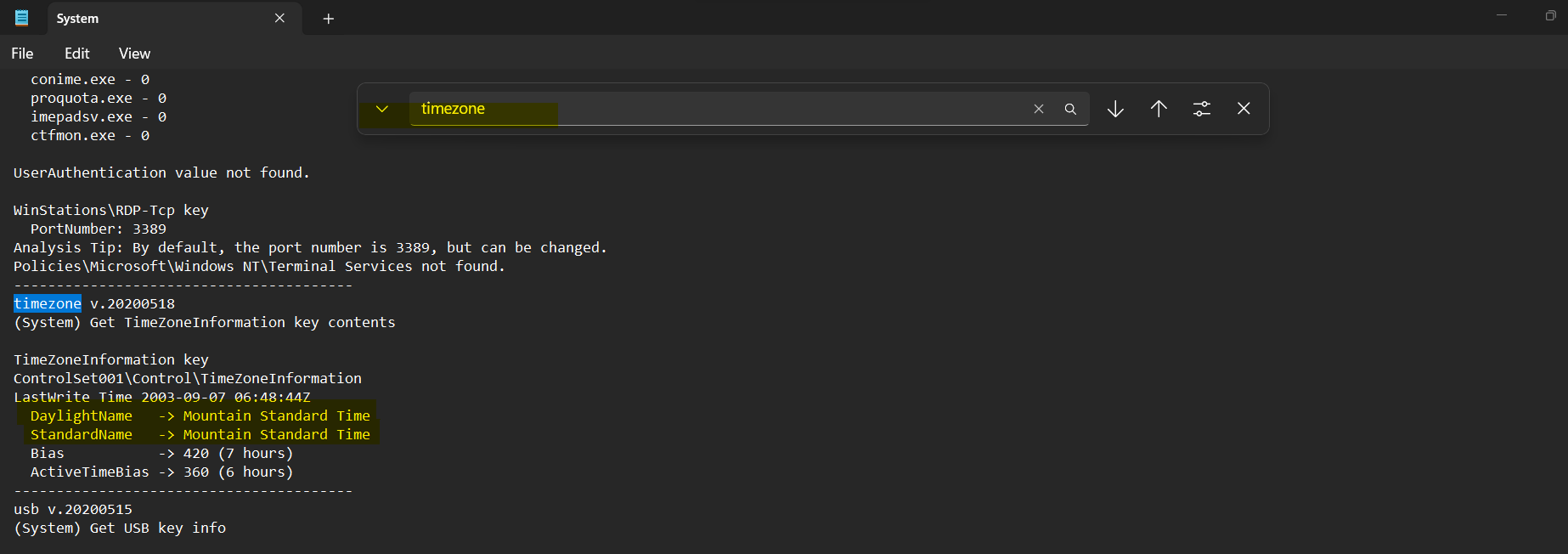


Figure 2.4 Timezone: Mountain Standard

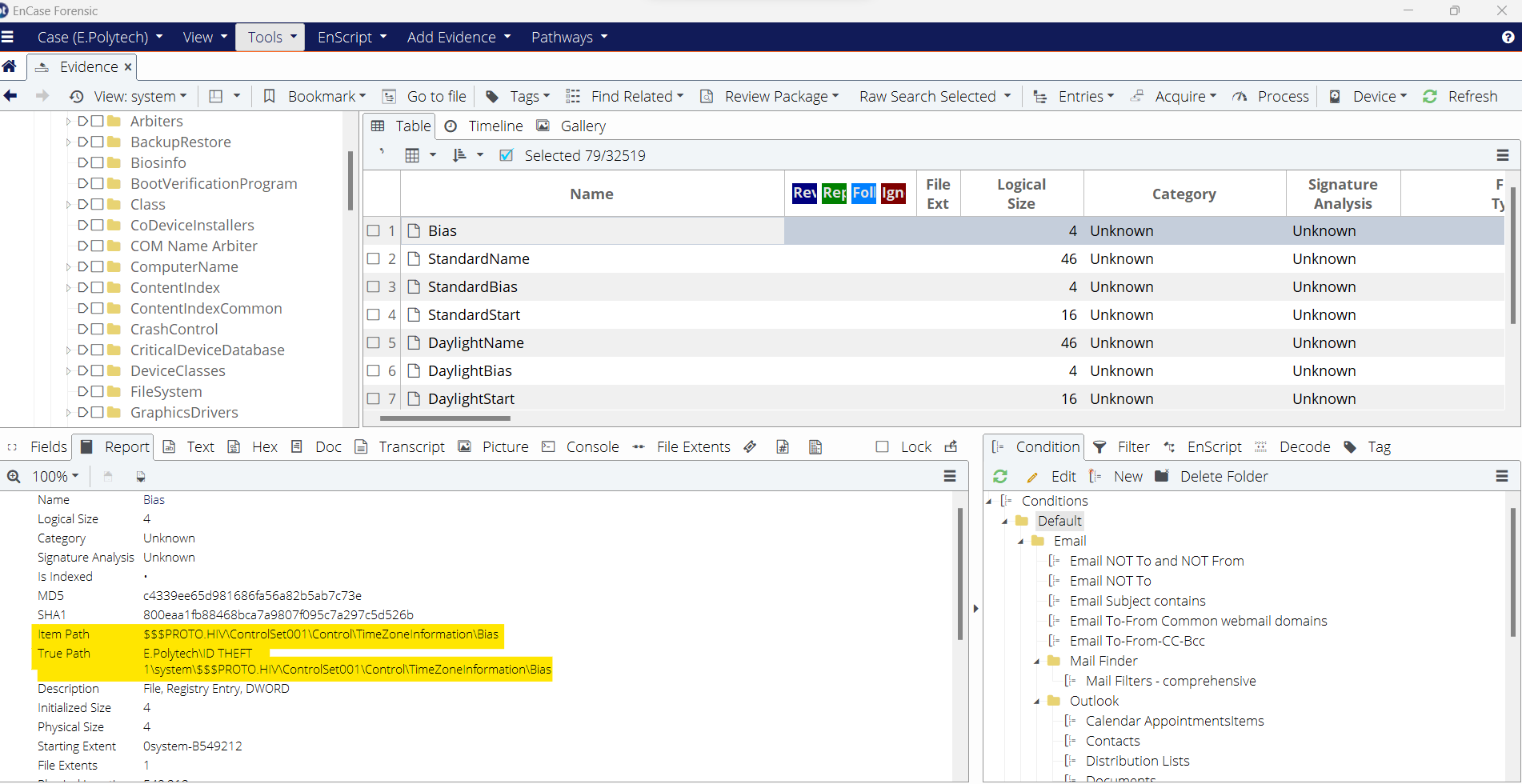


Figure 2.5 True Path: E.Polytech\ID THEFT 1\system\$$$PROTO.HIV\ControlSet001\Control\TimeZoneInformationBias

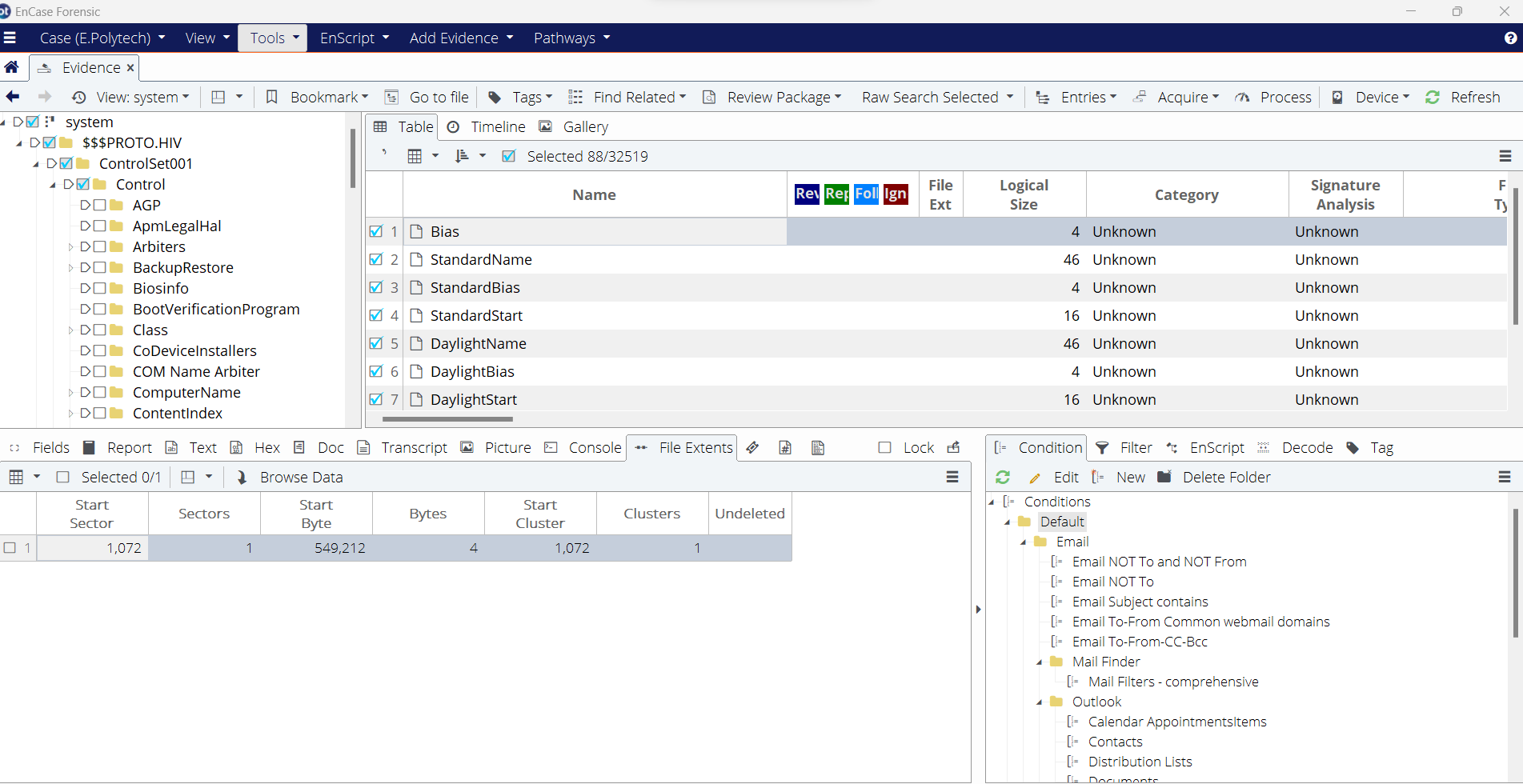


Figure 2.6 Start Sector 1,072, Sectors 1, Start Cluster 1,072, Clusters 1 for TimeZoneInformation

1. Elvis is known to transport illicit files on portable storage devices. The Pomona PD has several portable storage devices in their possession from Elvis’ school locker. Can you give them any information that can help them determine if Elvis has connected to these portable storage devices? If so, be sure to provide the friendly names of each portable storage device.

On March 31, 2023, at 12:12 AM, Michael Andom looked at the Windows 2000+ Registry File, system, under the Hive, $$$PROTO.HIV, under the key, ControlSet001, under the subkey, Enum, to find the portable devices that the suspect connected. Under the subkey, Enum was the subkey, USBSTOR, which provided the devices.

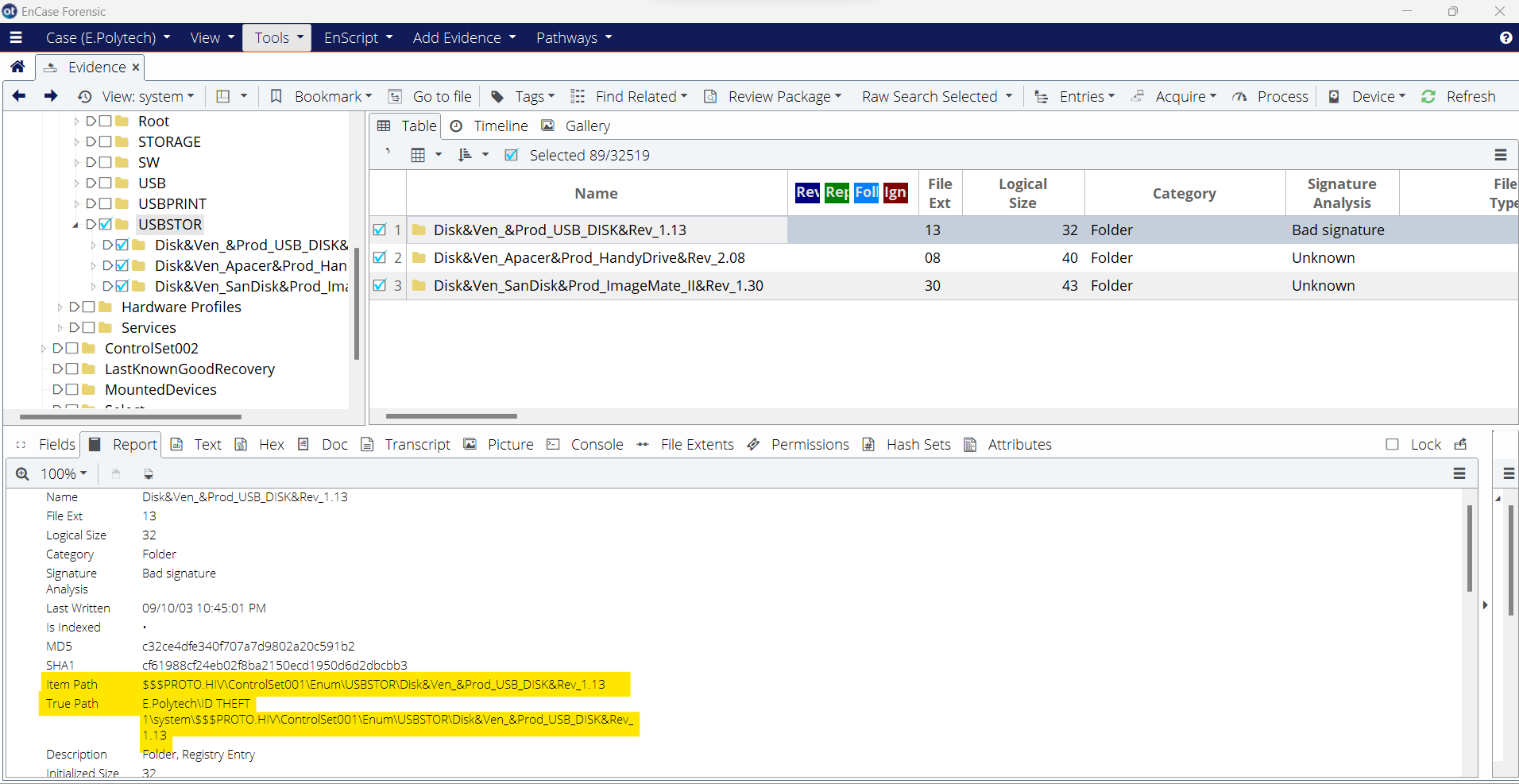


Figure 3.1 True Path: E.Polytech\ID THEFT 1\system\$$$PROTO.HIV\ControlSet001\Enum\USBSTOR\



Figure 3.2 Start Sector 1,424, Sector 1, Start Cluster 1,424, Cluster 1 for Subkey Enum, Subkey USBSTOR

On March 31, 2023, at 12:29 AM, Michael Andom used the same text file, System.txt, to look up more information.

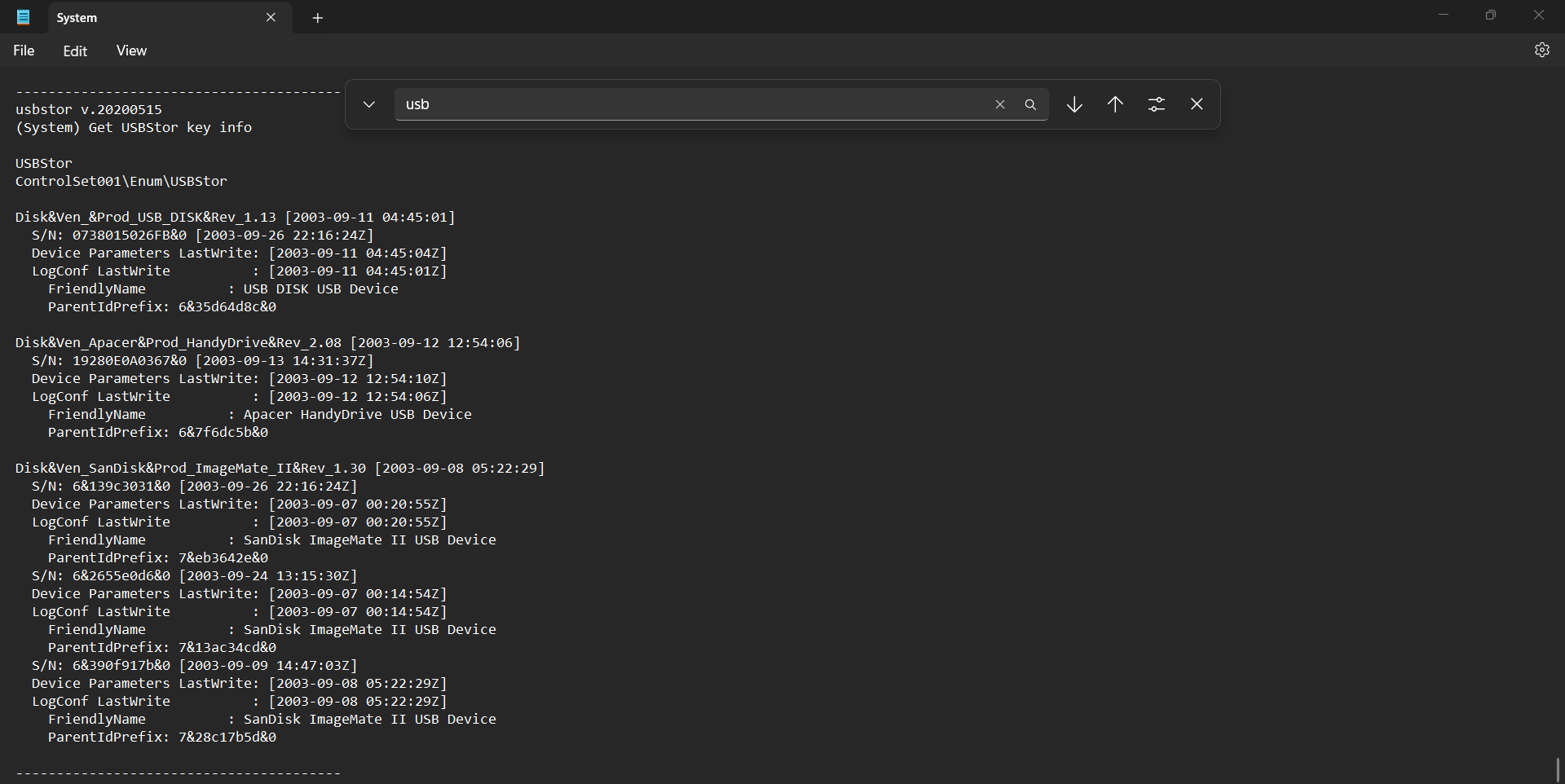


Figure 3.3 System.txt file for USB devices that the suspect connected.

Based on the System.txt file, the suspect connected to several USB devices. The USB devices’ friendly names are USB DISK USB Device, Apacer HandyDrive USB Device, and SanDisk ImageMate II USB Device. The suspect connected with USB Disk USB Device on September 11, 2003, with serial numbers: 0738015026FB&0. The suspect connected with Apacer HandyDrive USB Device on September 12, 2003, with serial number: 19280E0A0367&0. The suspect connected with a USB device, SanDisk ImageMate II, three times with September 8, 2003, being the last connection. The SanDisk ImageMate II USB device has serial numbers: 6&139c3031&0.

1. Elvis’ computer has been attempting to hack several Salt Lake City credit card sites. The event logs continually show a reference to KAL as an incoming computer name. Look for information that supports this and list a location that could be used to corroborate it.

On March 31, 2023, at 12:25 PM (PST), Michael Andom found the computer name and TCP/IP name that states KAL in the System.txt file.

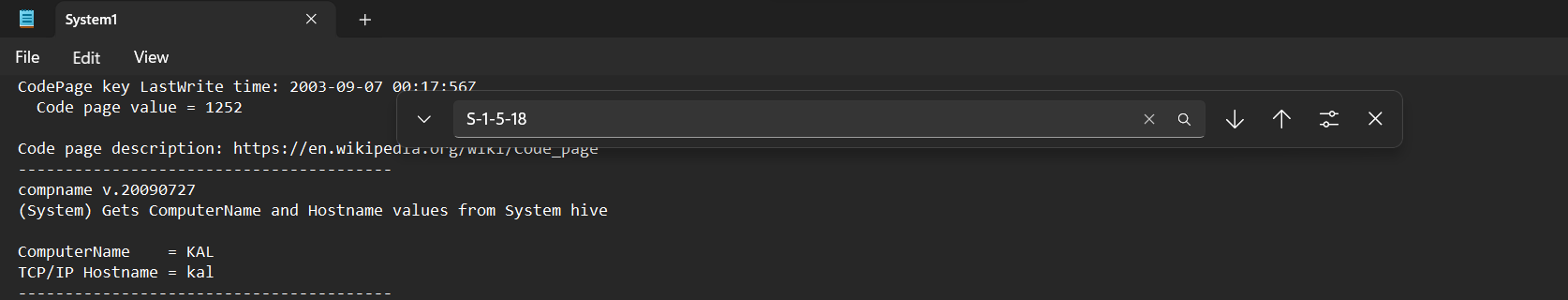


Figure 4.1 System.txt file that shows ComputerName and TCP/IP Hostname as KAL.

March 31, 2023, at 12:40 PM(PST), Michael Andom used EnCase to confirm the path. Michael Andom clicked on the $$$PROTO.HIV to go into the key, ControlSet001. In the key, ControlSet001, Michael Andom clicked on the subkey, Services, to inspect the subkey, Tcpip. In the subkey Tcpip, Michael Andom clicked on the subkey, Parameters, and found the Hostname. To confirm, Michael Andom right-clicked on the subkey, Parameters, and copied the folder.

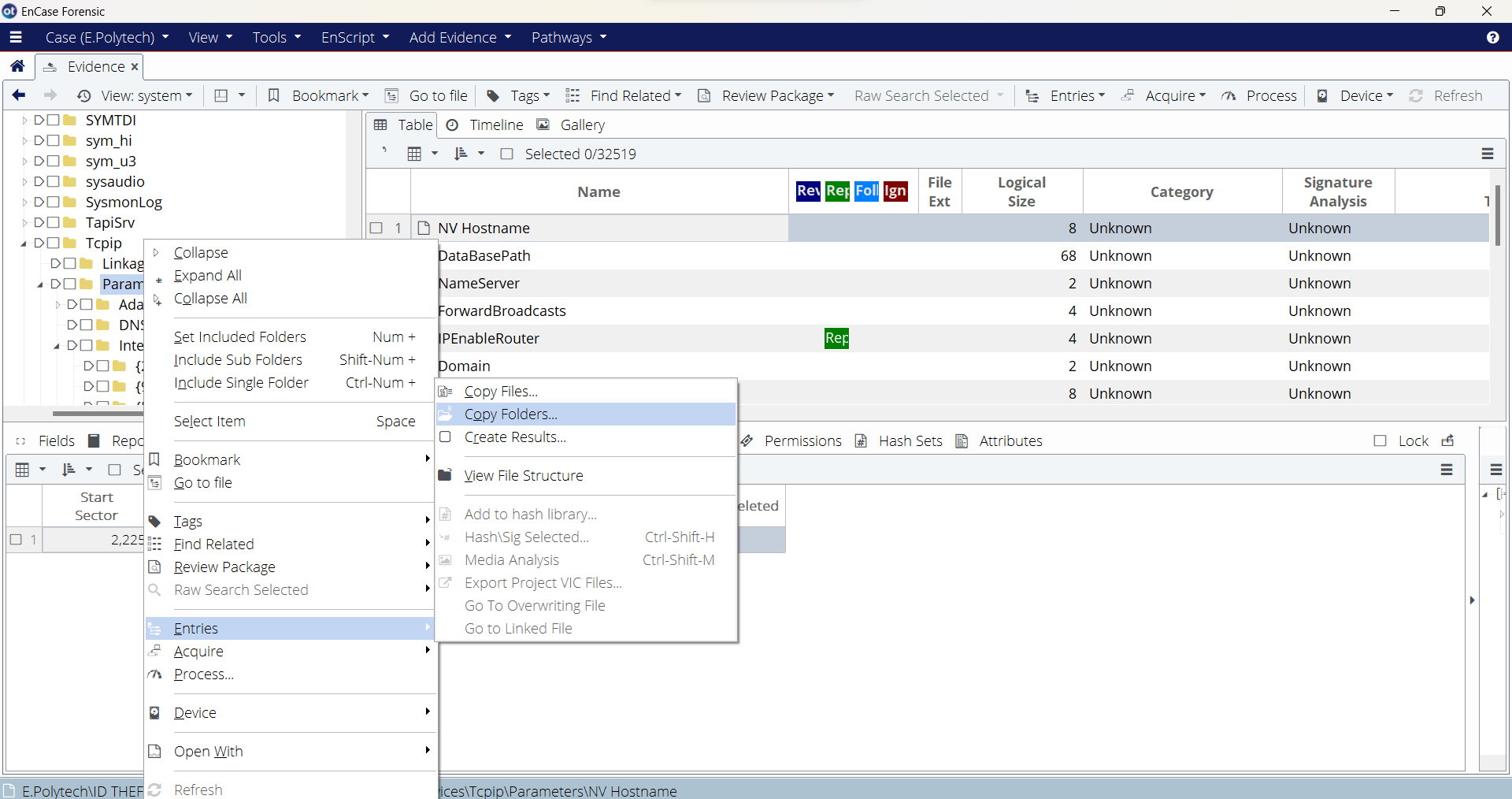


Figure 4.2 Copying the subkey, Parameter, to inspect.



Figure 4.3 Path: …\Documents\EnCase\Cases\E.PolytechLAB2\E.Polytech\Export

Michael Andom confirmed that the Hostname is kal by opening the Hostname file using Notepad.

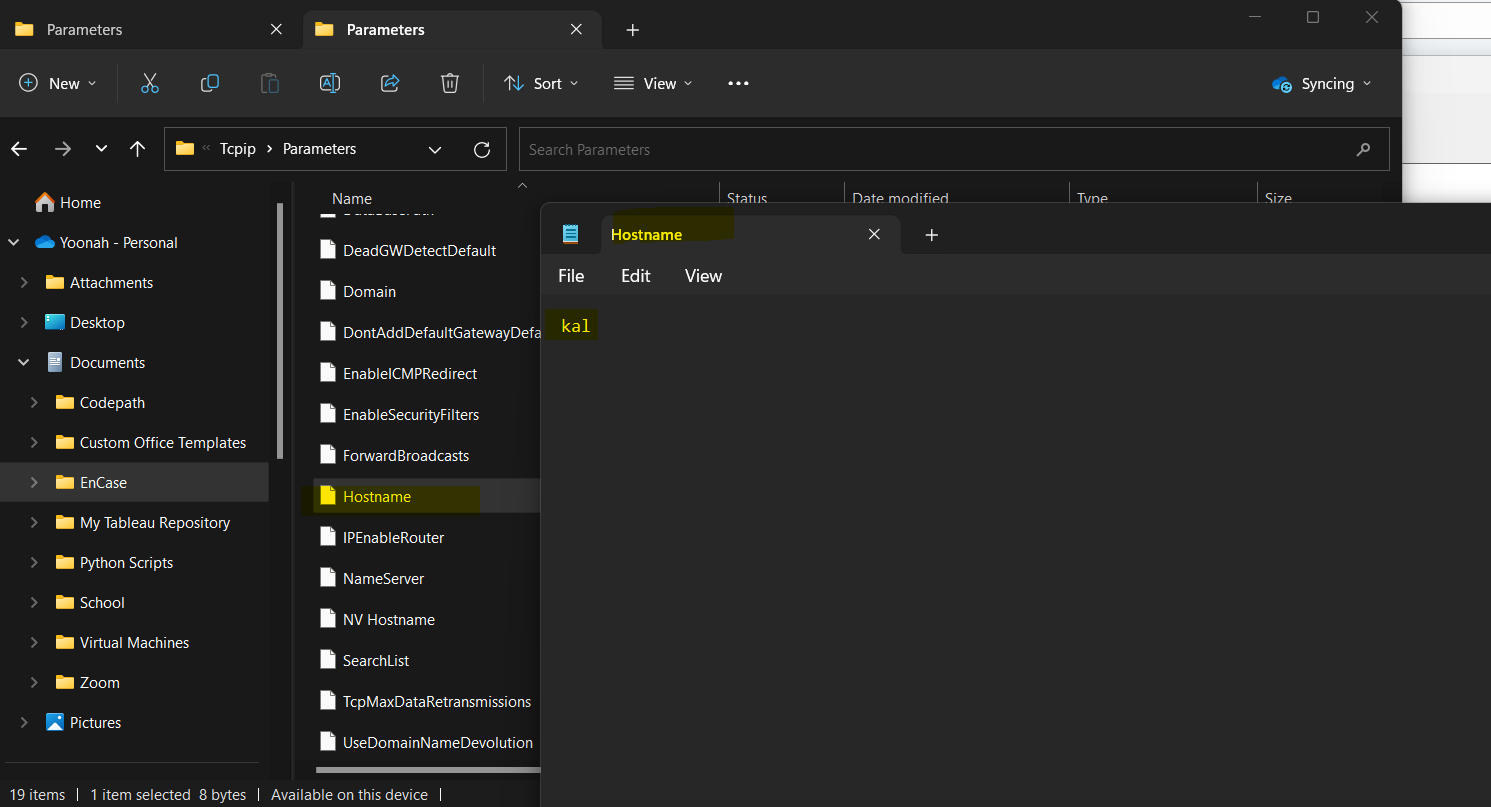


Figure 4.4 Hostname file using Notepad stating that the Hostname is kal.

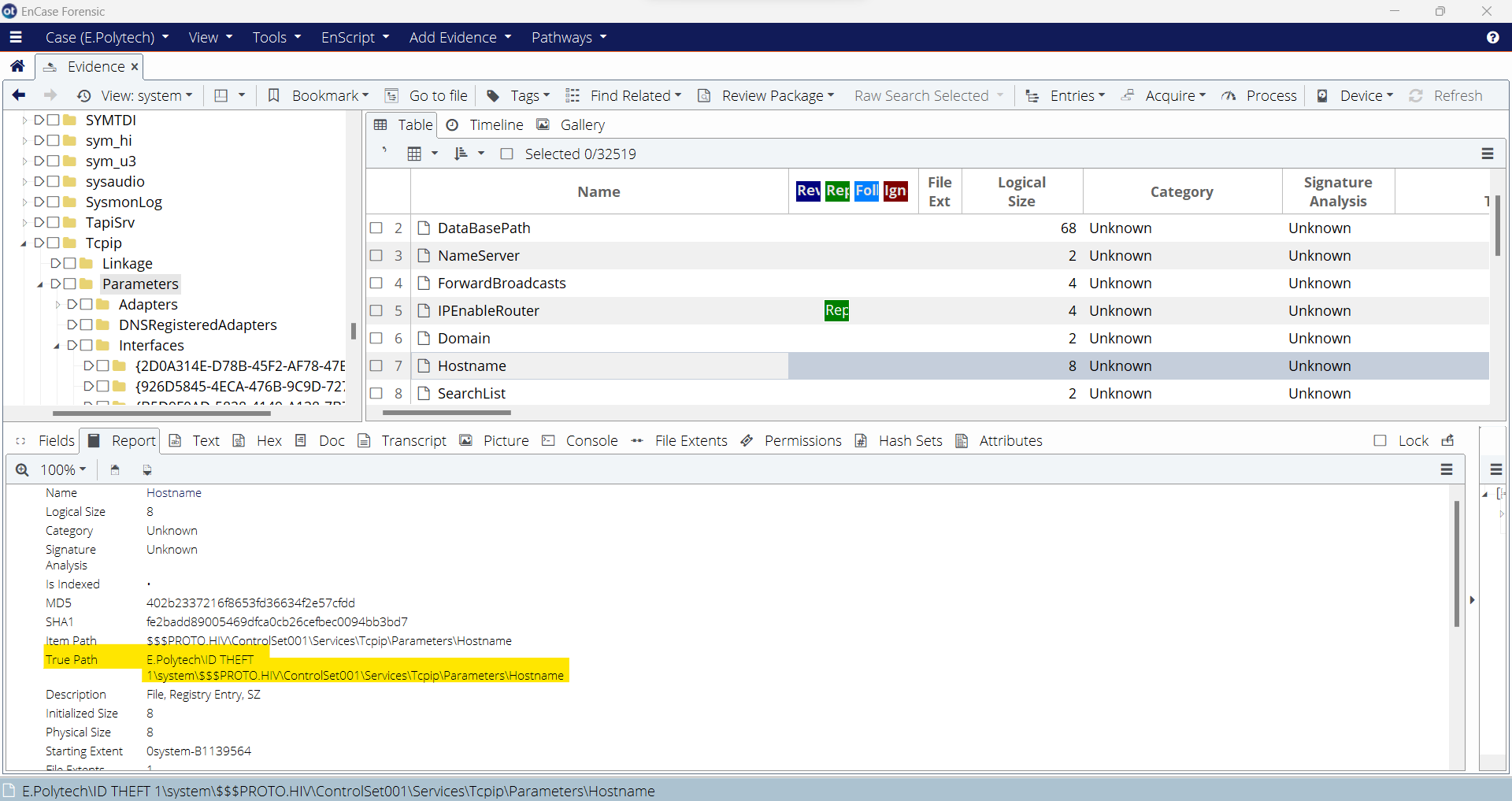


Figure 4.5 True Path: E.Polytech\ID THEFT 1\system\$$$PROTO.HIV\ControlSet001\Services\Tcpip\Paramters\Hostname

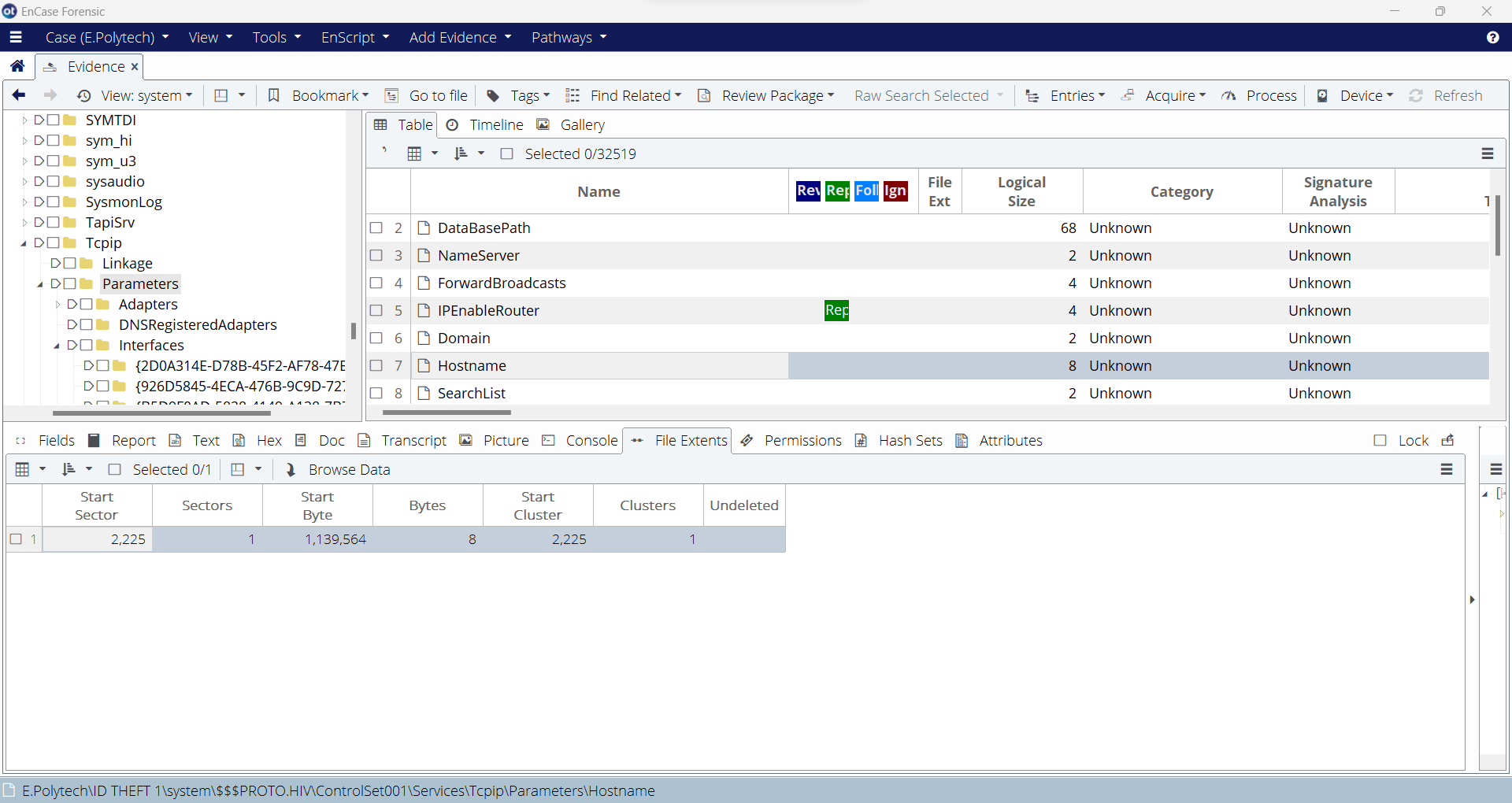


Figure 4.6 Start Sector 2,225, Sectors 1, Start Cluster 2,225, Clusters 1 for the Hostname

March 31, 2023, at 1:24 PM(PST), Michael Andom found the ComputerName under the hive $$$PROTO.HIV. Michael Andom clicked the key, ControlSet001. In the key, ControlSet001, Michael Andom clicked on the subkey, Control. Under the subkey, Control, there is a subkey, ComputerName. Michael Andom right-clicked the subkey, ComputerName, and copied the folder.

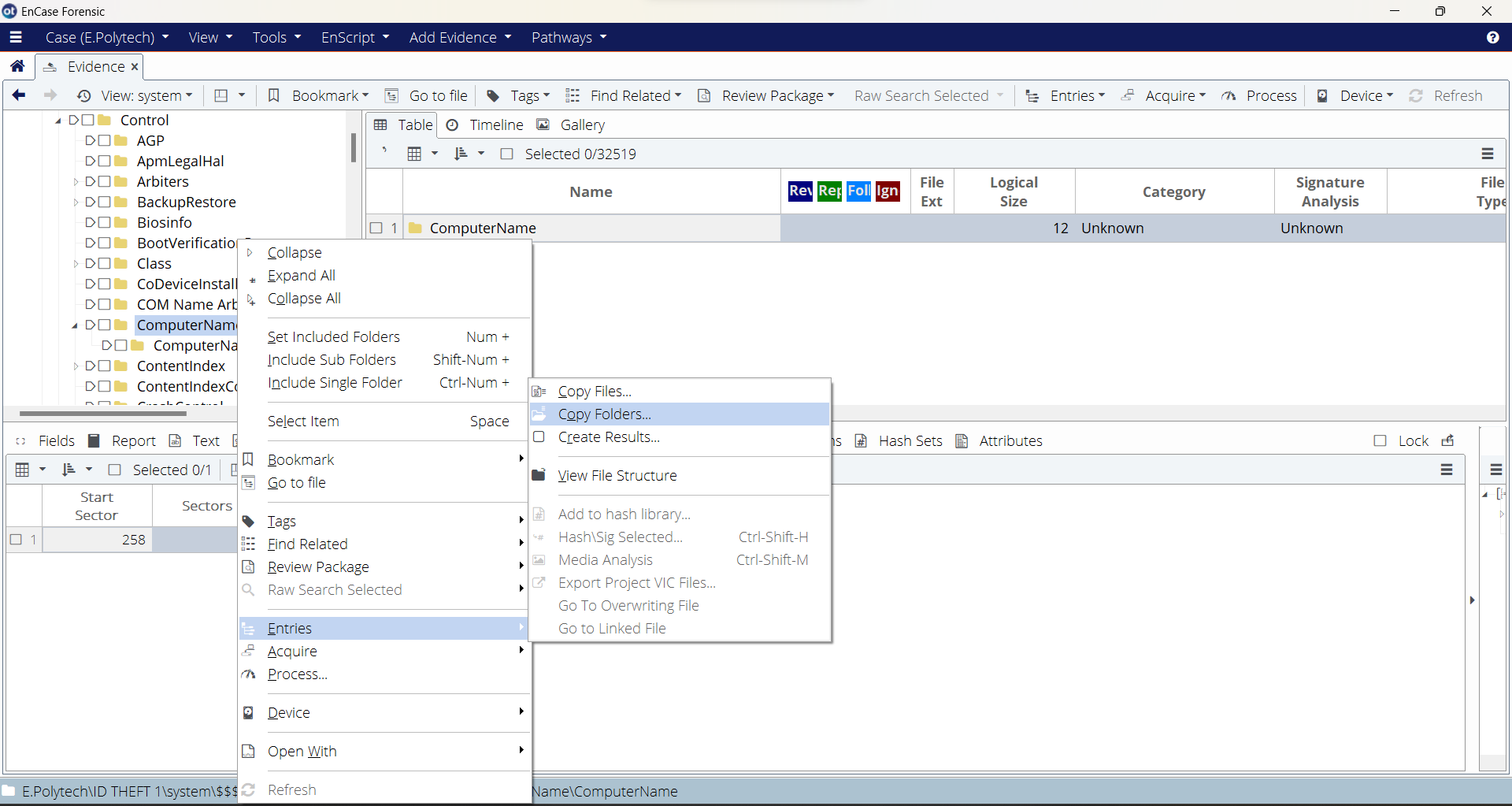


Figure 4.7 Copying the subkey, ComputerName, to inspect.

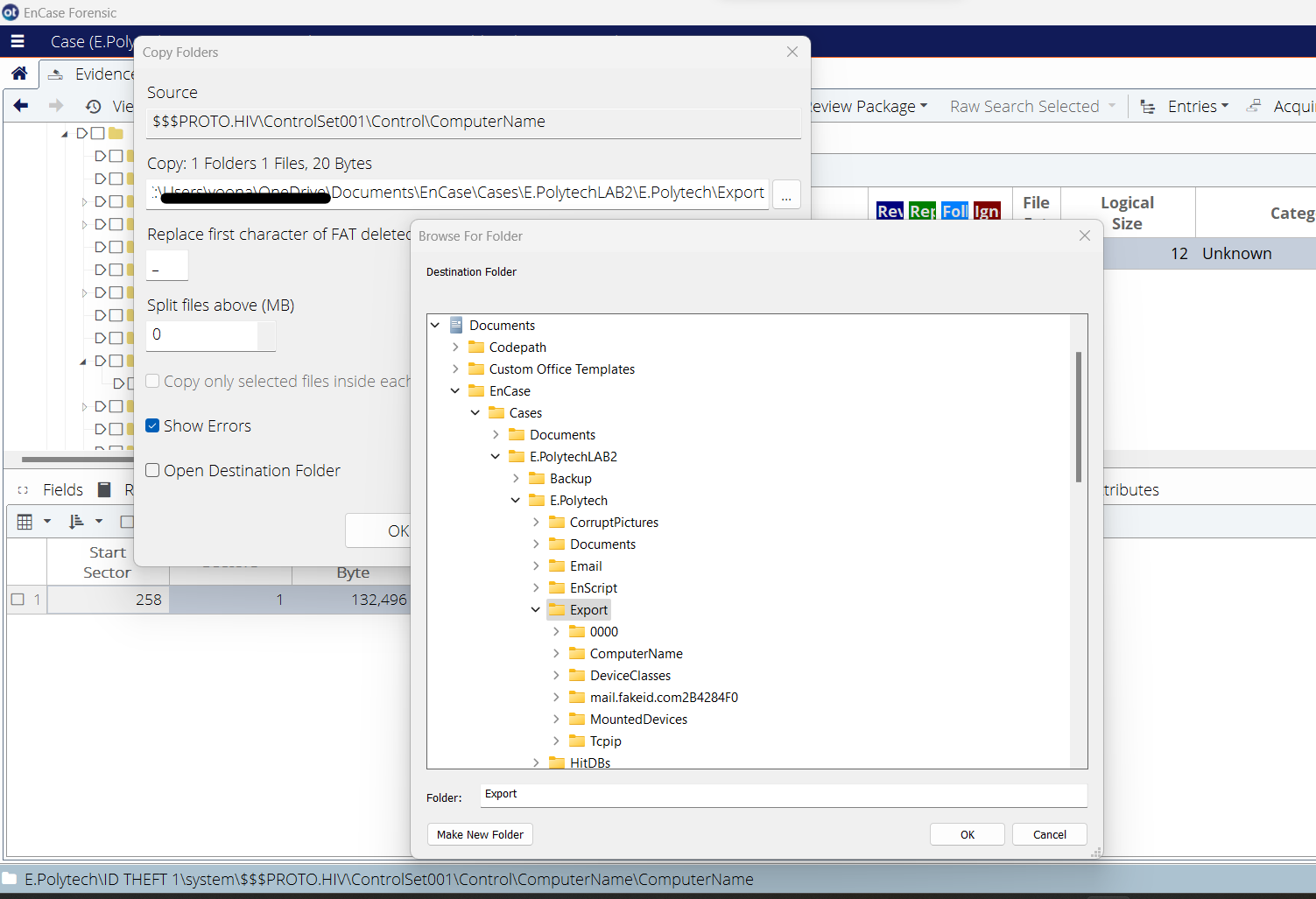


Figure 4.8 Path: \Documents\EnCase\Cases\E.PolytechLAB2\E.Polytech\Export is where the subkey is saved to confirm the name.

On March 31, 2023, at 1:32 PM(PST), Michael Andom confirmed that the ComputerName is KAL by opening the file ComputerName on Notepad.

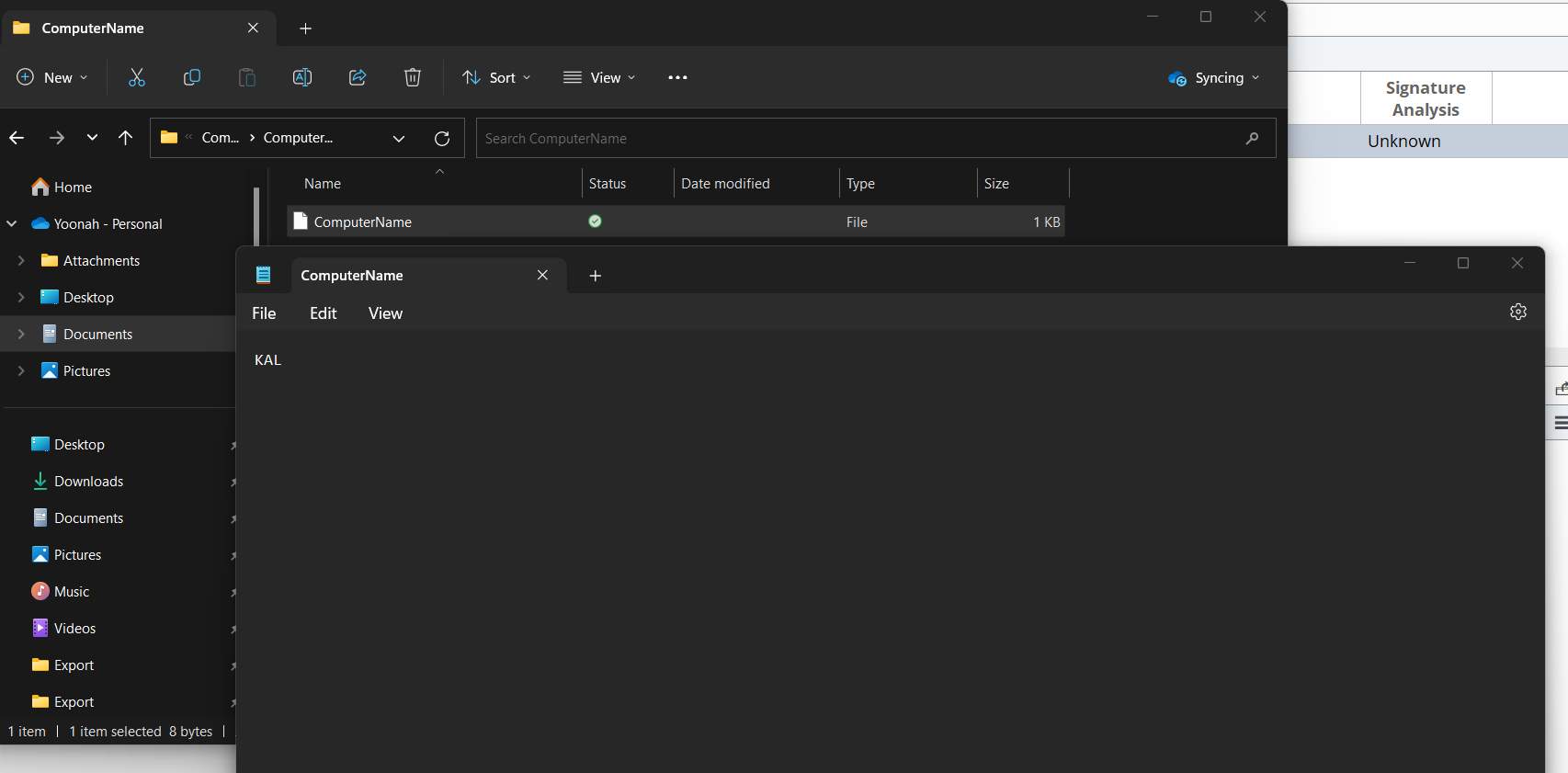


Figure 4.9 ComputerName file opened on Notepad to show the name KAL.

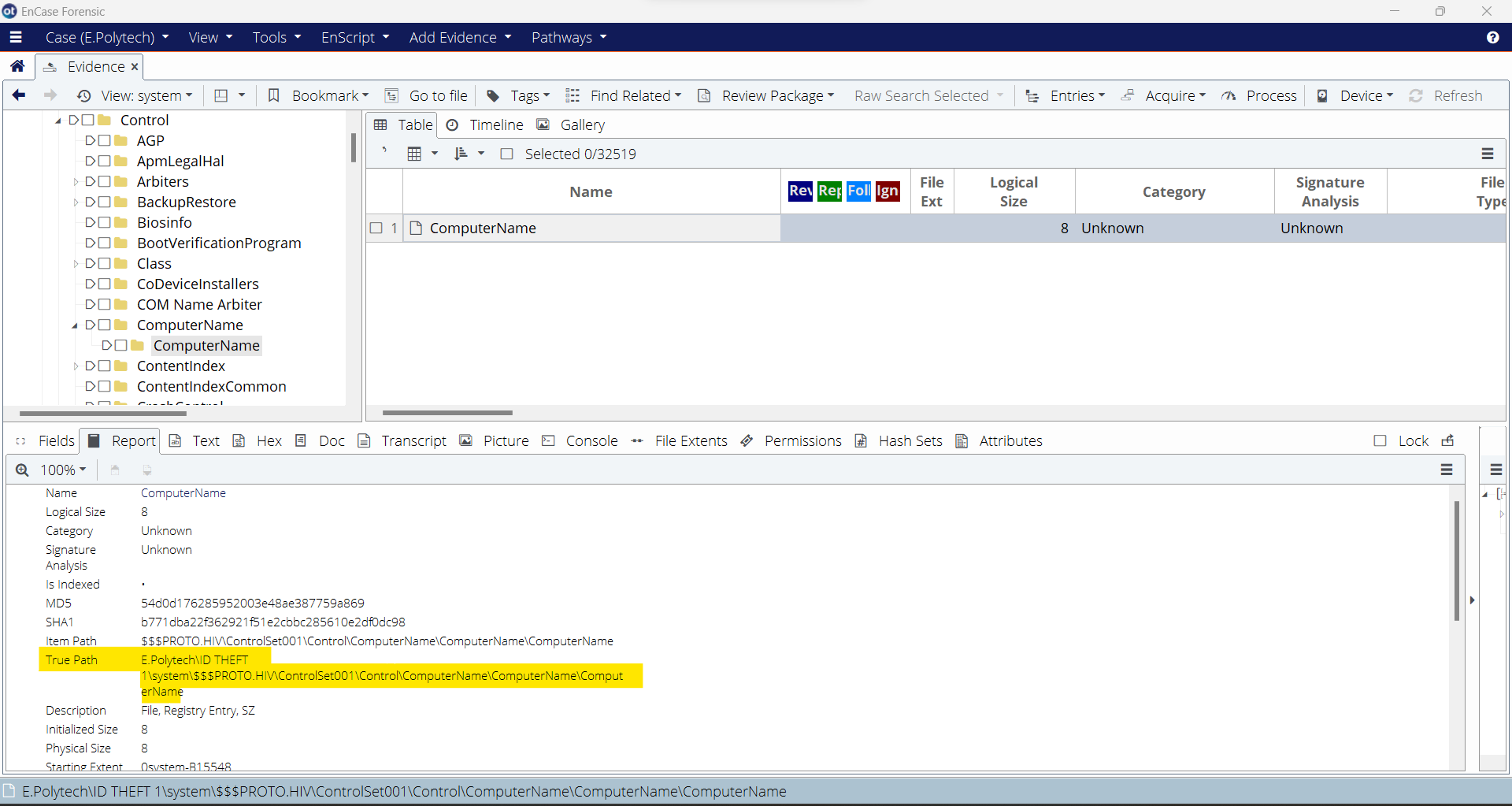


Figure 4.10 True Path: E.Polytech\ID THEFT 1\system\$$$PROTO.HIV\ControlSet001\Control\ComputerName\ComputerName

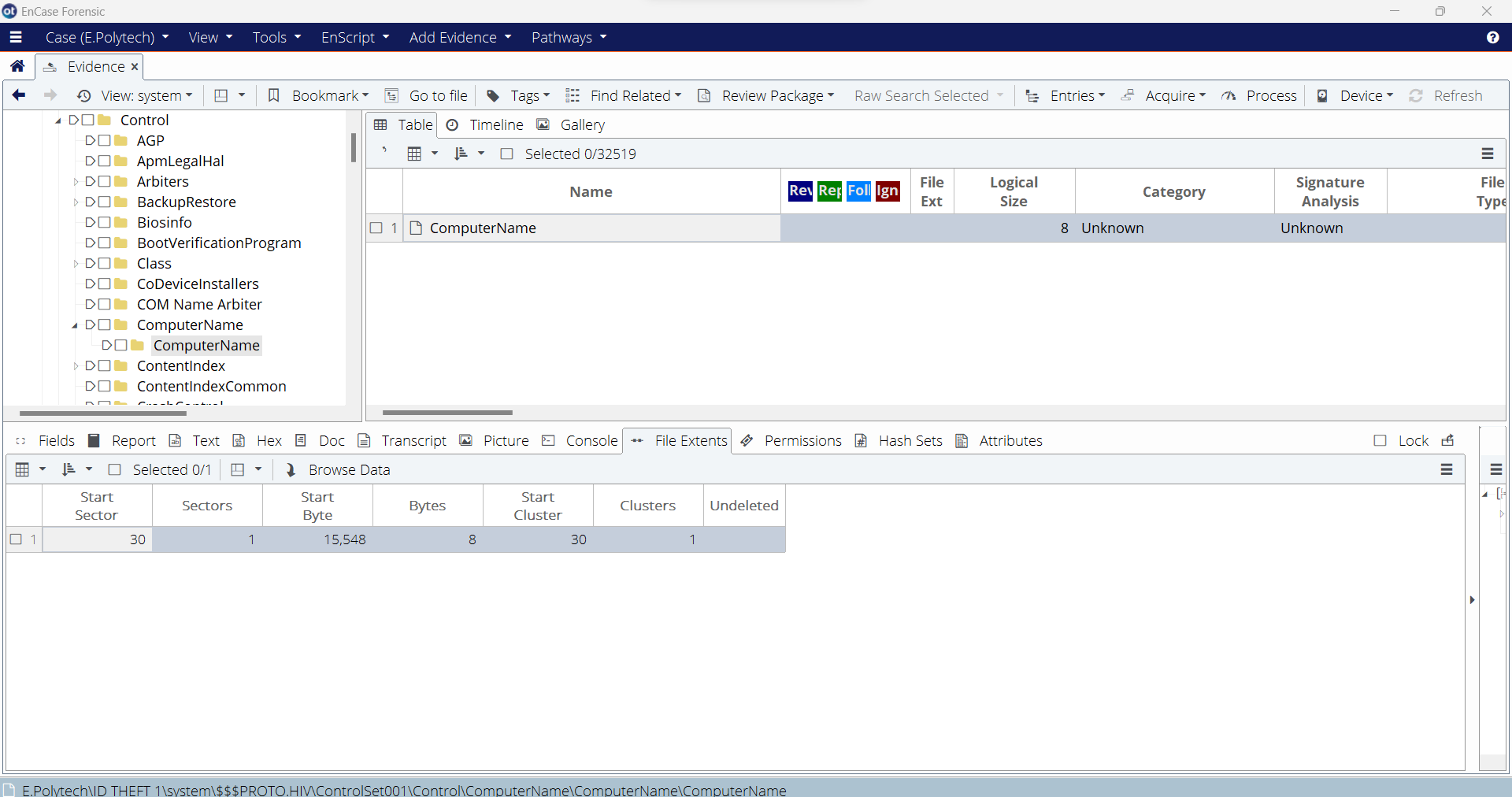


Figure 4.11 Starting Sector 30, Sectors 1, Start Cluster 30, Clusters 1 for ComputerName.

# Part 2 – Registry Analysis – SAM Hive (Michael Andom T.)

Answer the following questions using the SAM hive:

1. Determine all of the user accounts, and provide the user names and SIDs for each user account on this computer.

On March 31, 2023, at 1:09 AM (PST), Michael Andom created a new case for Elvis Polytech in EnCase. At 1:18 am Michael Andom uploaded the evidence file ID THEFT 1.EO1 onto E. Polytech case in EnCase. Michael Andom accessed the contents of ID THEFT 1 at 1:30 AM by clicking on the entry labeled ID THEFT 1 in the navigation pane, which showed a list of data and its category (folders, documents, pictures, unallocated clusters) in the table pane. This is shown in figure 5.1.

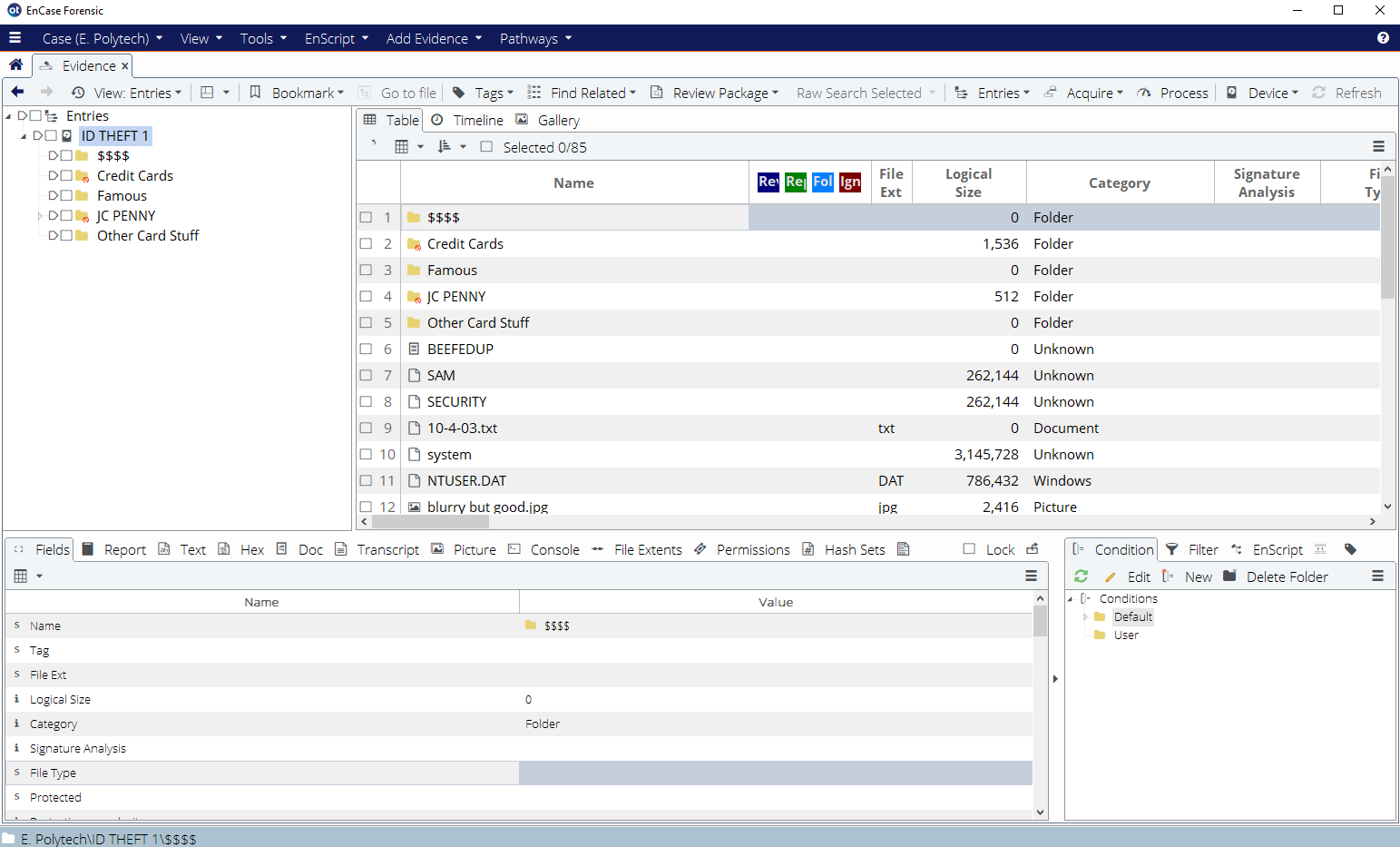


Figure 5.1

Michael Andom selected the SAM hive file in the table pane and copied the file onto the desktop of the workstation at 1:52 am. The SAM file starts at sector # 67,520 and starts at cluster #65,538. Michael Andom then parsed the file using RegRipper, v.3.0 which outputted 2 text files with extensions .log and .txt into the RegRipper3.0-master folder at 1:53 am. The process of parsing the SAM hive file is shown in figure 5.2.

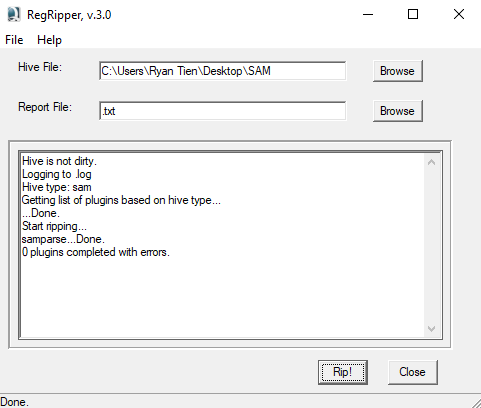


Figure 5.2 Parsing SAM hive file with RegRipper, v.3.0

Michael Andom accessed the text file labeled .txt at 1:56 am, which displayed contents for user and group membership info. The following user accounts, in addition to the user names and SIDs for each user account on the computer is provided below:

Account Type: Default Admin User

Username: Administrator [500]

SID: S-1-5-21-1547161642-813497703-1202660629-500

Account Type: Default Guest Acct

Username: Guest [501]

SID: S-1-5-21-1547161642-813497703-1202660629-501

Account Type: Custom Limited Acct

Username: HelpAssistant [1000]

SID: S-1-5-21-1547161642-813497703-1202660629-1000

Account Type: Custom Limited Acct

Username: SUPPORT\_388945a0 [1002]

SID: S-1-5-21-1547161642-813497703-1202660629-1002

Account Type: Default Admin User

Username: Keith [1003]

SID: S-1-5-21-1547161642-813497703-1202660629-1003

Account Type: Custom Limited Acct:

Username: Jo Ellen [1004]

SID: S-1-5-21-1547161642-813497703-1202660629-1004

Account Type: Default Admin User

Username: HTCIA [1006]

SID: S-1-5-21-1547161642-813497703-1202660629-1006

Account Type: Default Admin User

Username: ID THEFT DUDE [1007]

SID: S-1-5-21-1547161642-813497703-1202660629-1007

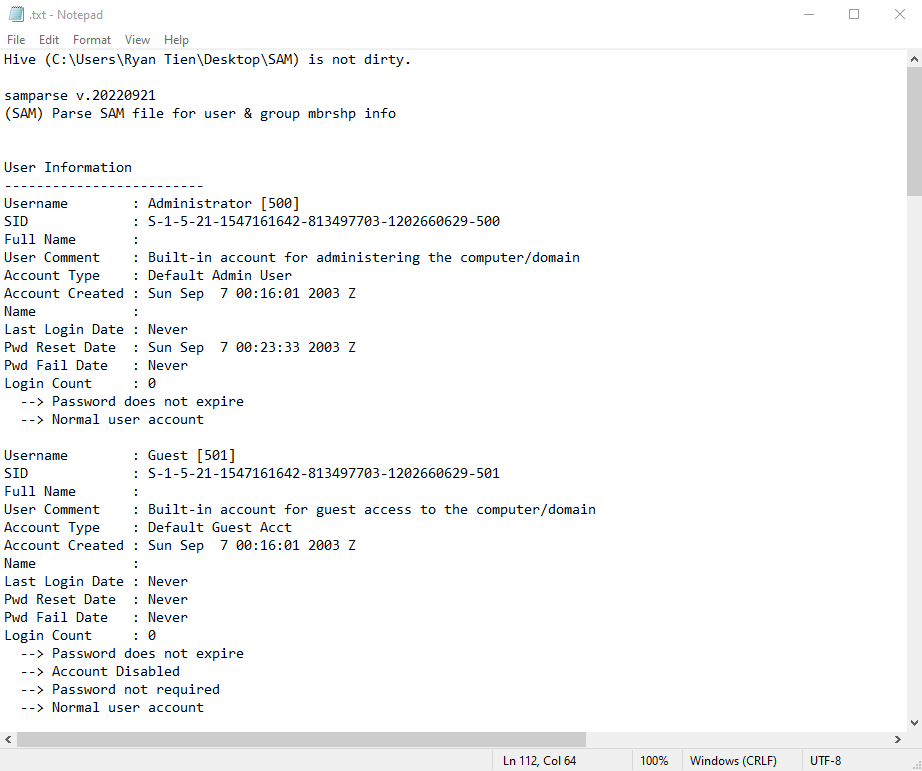


Figure 5.3 Text file “.txt” showing the first two user accounts with the username and SIDs of the user accounts

1. It is thought that Elvis used the user account name of ID THEFT DUDE. Determine when Elvis last logged into this machine using this account. Be sure to convert the time to the correct time zone, and do not simply provide the time in UTC.

According to the text file .txt, which contained contents of user group membership info, Elvis last logged onto the machine using the account name of ID THEFT DUDE on Friday September 26 at 23:07:30 2003 Z. Since the computer’s time zone bias was set to MST, as retrieved in Part 1, the last login date of ID THEFT DUDE was on Friday, September 26, at 05:07:30 PM Mountain Standard Time (MST).

1. Provide information regarding all of the attributes associated with the ID THEFT DUDE user account from the SAM hive. This includes the user name, whether the account is active, the last logged in date/time, whether there is a password, the number of failed login attempts, etc.

Michael Andom retained access on the text file labeled .txt to retrieve all attributes associated with the ID THEFT DUDE user account at 2:31 AM. The information is provided below:

Username: ID THEFT DUDE [1007]

SID: S-1-5-21-1547161642-813497703-1202660629-1007

User Comment: Null

Account Type: Default Admin User

Account Created: Fri Sep 26 19:48:16 UTC - (Fri Sep 26 01:48:16 PM MST)

Last Login Date: Fri Sep 26 23:07:30 UTC - (Fri Sep 26 05:07:30 PM MST)

Password Reset Date: Never

Password Fail Date: Never

Login Count: 8

* Password does not expire
* Normal user account

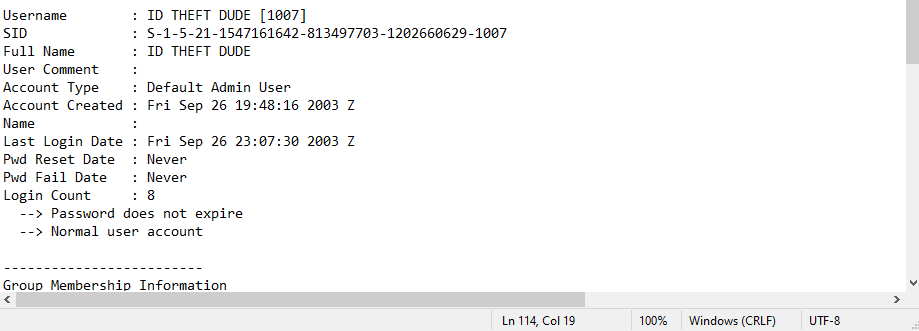


Figure 7.1 User account of ID THEFT DUDE and all attributes associated with the account

# Part 3 – Registry Analysis – NTUSER.DAT file

Provide answers to the following questions using the NTUSER.DAT file and the information you generated from the report:

1. Police suspect that Elvis was in possession of illegal MP3 files obtained from an RIAA sting operation. How can you determine if Elvis possessed any of the following audio files (by analyzing the NTUSER.DAT file only)?
   1. “La Femme Nikita” Maine Theme (club Version)
   2. Copy of “La Femme Nikita,” “Spies” by Coldplay
   3. “How You Remind Me” (Acoustic) by Nickelback

On March 31, 2023 at 1:15 pm PST, Michael Andom accessed the ID THEFT 1 evidence file and copied the NTUSER.DAT hive file onto the workstation. At 1:26, Michael Andom parsed the NTUSER hive using RegRipper v.3.0, which outputted the report file as a .txt extension as shown in Figure 8.1

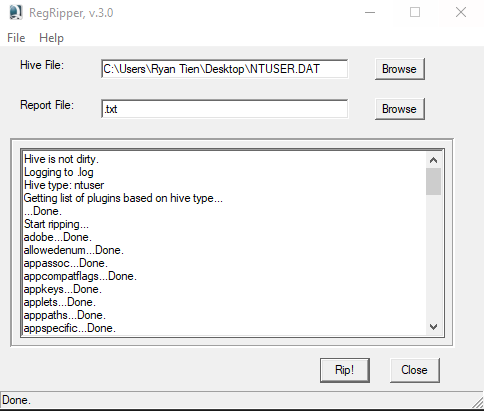


Figure 8.1 Parsing NTUSER.DAT with RegRipper, v.3.0

Michael Andom accessed the report file labeled .txt to access the contents of NTUSER.DAT at 1:27 pm. In the report file, there have been logs indicating access and write dates of the D: volume, and within the D: volume, there were mp3 files present. The full directory path is provided below:

D:\Music from WV\la femme nikita - Main Theme (Club Version).mp3

D:\Music from WV\Copy of La Femme Nikita - Coldplay - Spies (Acoustic).mp3

D:\Music from WV\Nickelback - How you remind me (Acoustic).mp3

The last write time in the OpenSaveMRU/mp3 was 2003-09-26 22:38:59 (2003-09-26 4:38:59 PM MST)

We can determine Elvis possessed these files as last visited directories included the desktop of ID THEFT DUDE and are shown below:

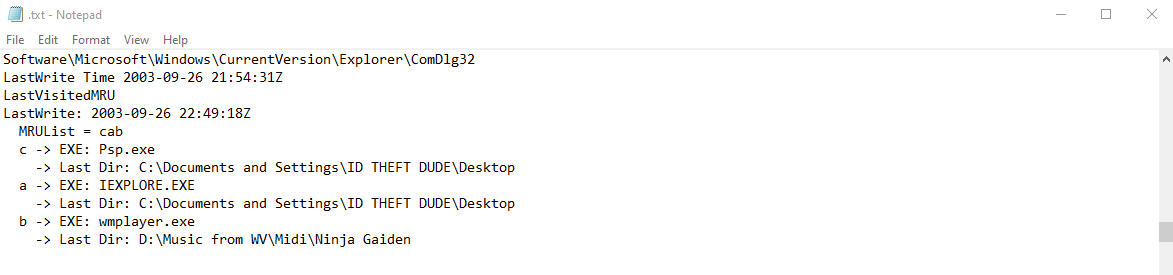


Figure 8.2 Last visited MRU and last directory

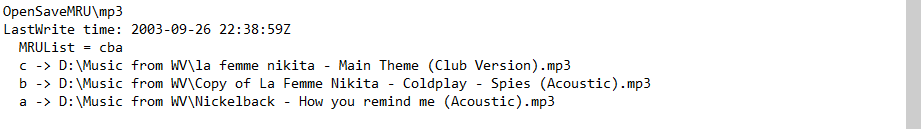


Figure 8.3 Full directory of the mp3 files in the D: volume

The time the directories were last visited as well as the last write time are minutes apart.

**a. Counterfeiting U.S. currency**

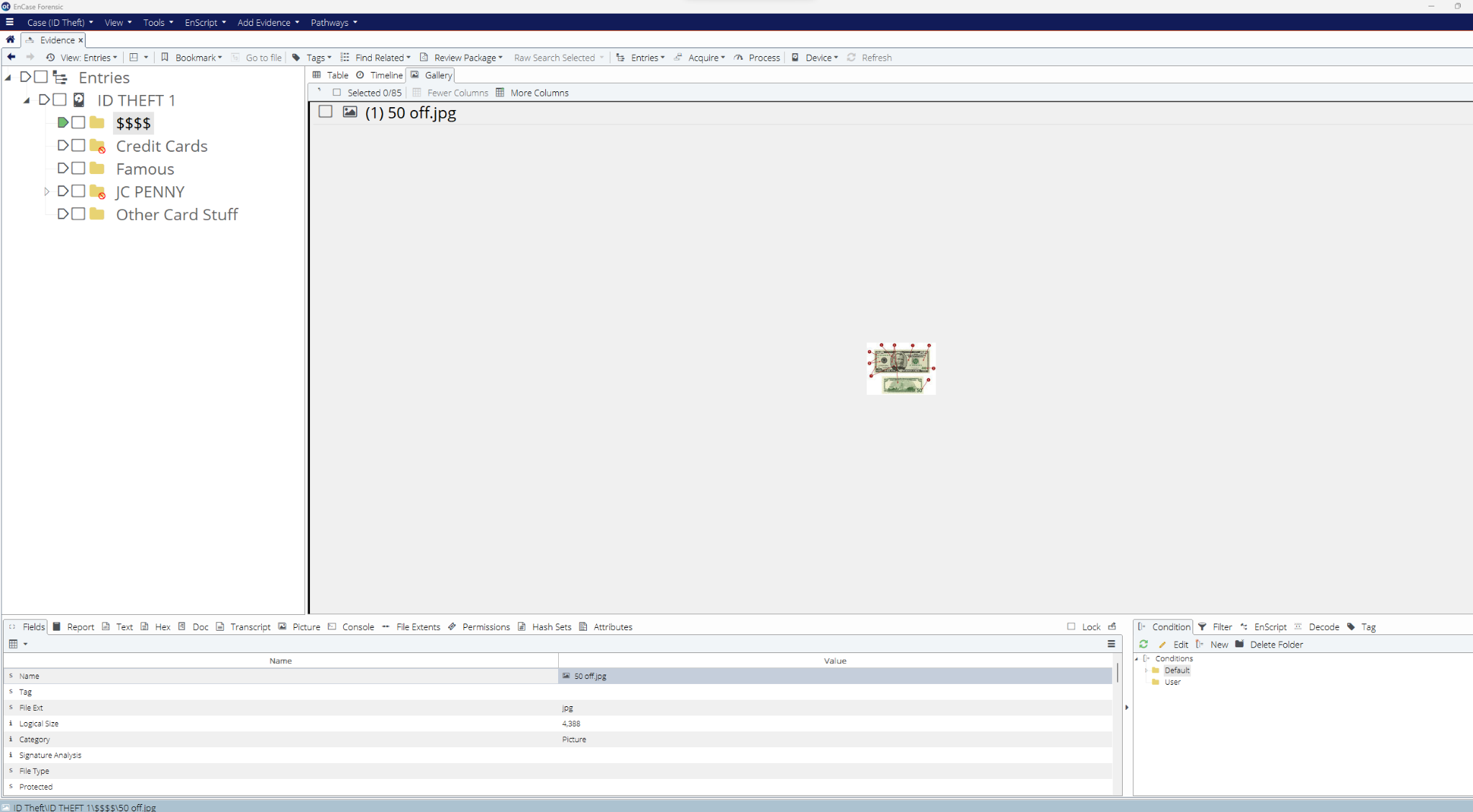
On April 1, 2023, at 2:00 PM(PST) Michael Andom examined a possible counterfeiting operation involving U.S. currency, he initially examined E.Polytech\ID THEFT 1\$$$$\50 off.jpg, which depicted a $50 bill marked with various indicators that highlighted its unique features  


Figure 9.1 True path: E.Polytech\ID THEFT 1\$$$$\50 off.jpg (Start Sector: 3,262, Sectors 9; Start Cluster 1,280, Clusters 9)

On April 1, 2023, at 2:10 PM(PST) Michael Andom examined ID Theft\ID THEFT 1\$$$$\BEWARE !!.jpg. The image displayed an open register of cash alongside a bill scanner designed to detect counterfeit currency.

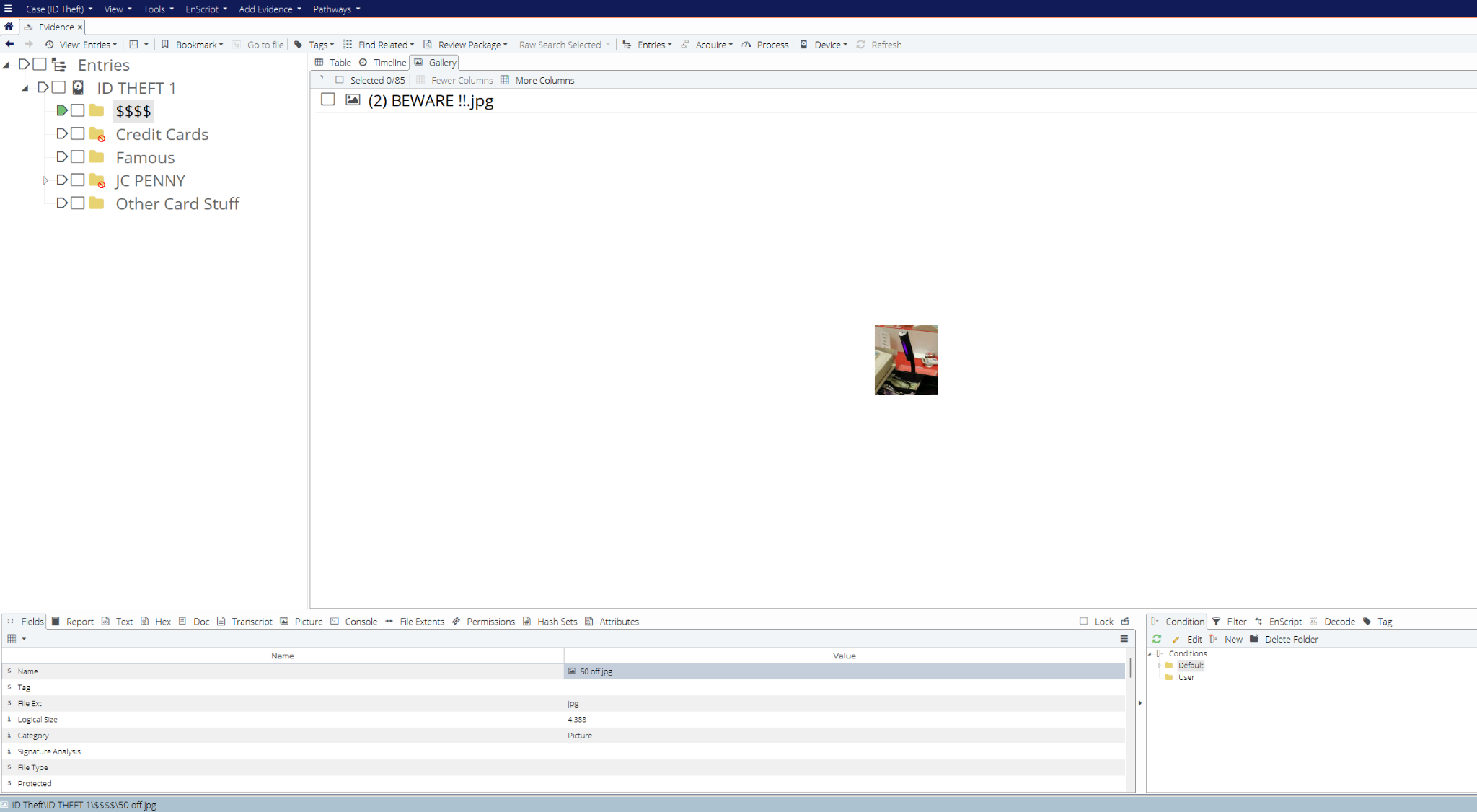


Figure 9.2 True path: E.Polytech\ID THEFT 1\$$$$\BEWARE !!.jpg (Start Sector: 3,271, Sectors 9; Start Cluster 1,289, Clusters 9)

Furthermore, On April 1, 2023, at 2:25 PM(PST), Michael Andom examined E.Polytech\ID THEFT 1\$$$$\High Dollar Purchase.jpg. The picture appeared to be an overlay of three distinct images, one of which contained a graph alongside several currency notes.

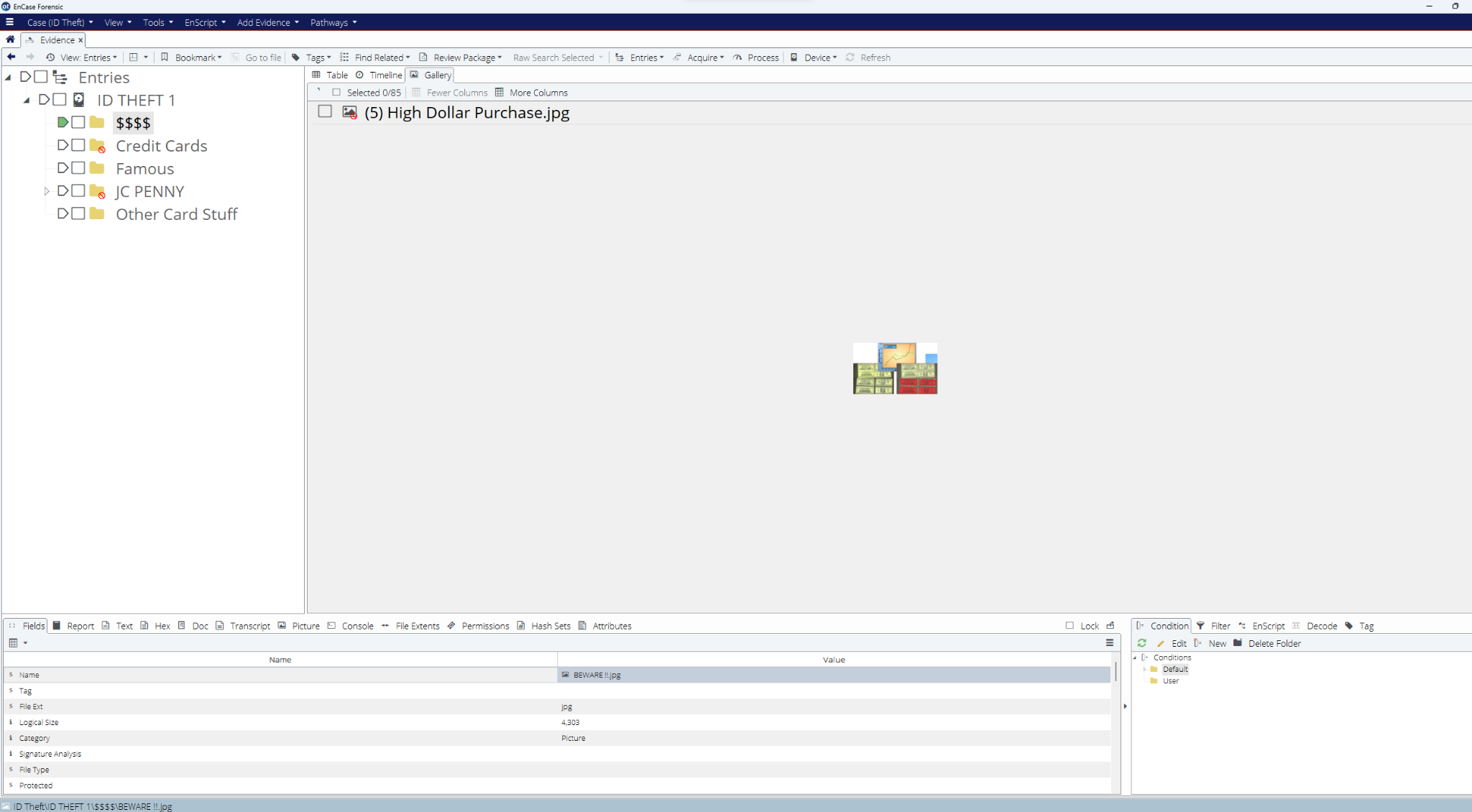


Figure 9.3 True path: E.Polytech\ID THEFT 1\$$$$\High Dollar Purchase.jpg (Start Sector: 3,299, Sectors 9; Start Cluster 1,317, Clusters 9)

On April 1, 2023, at 2:38 PM(PST), Michael Andom examined another piece of evidence in E.Polytech\ID THEFT 1\$$$$\dots off.jpg. The image depicted a marker capable of identifying counterfeit currency by causing discoloration on fake bills.

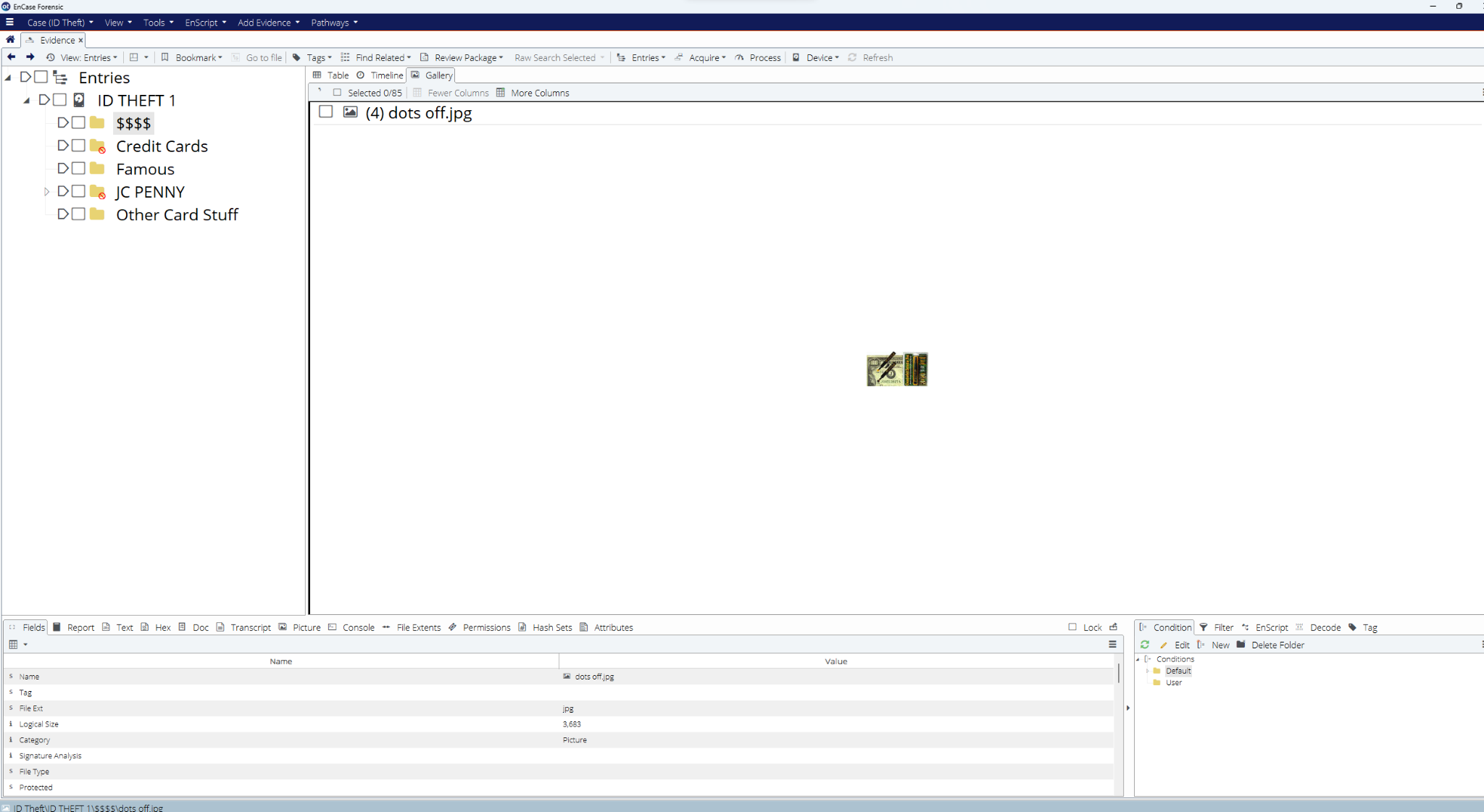


Figure 9.4 True path: E.Polytech\ID THEFT 1\$$$$\dots off.jpg (Start Sector: 3,291, Sectors 9; Start Cluster 1,309, Clusters 8)

1. Locate evidence that can assist in prosecuting the offense of counterfeiting U.S. Passports.

**b. Counterfeiting U.S. passports**

On April 1, 2023, at 2:58 PM(PST) Michael Andom proceeded to examine the folder path E.Polytech\ID THEFT 1\Other Card Stuff\. Here, Michael discovered a .jpg named "passport.jpg" in E.Polytech\ID THEFT 1\Other Card Stuff\passport.jpg. The image shows a passport and a corresponding photograph, suggesting that the user intended to forge a counterfeit U.S. passport.

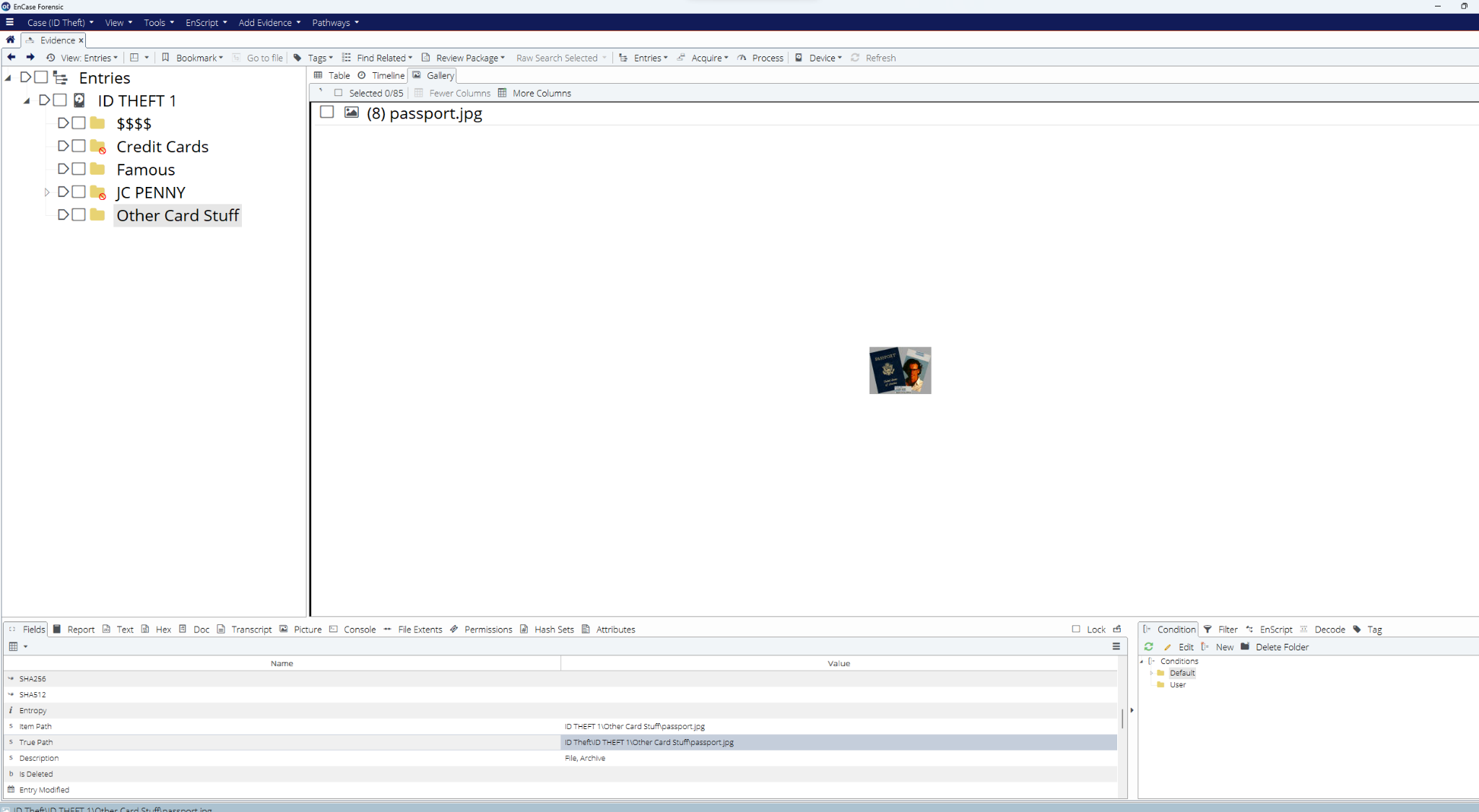


Figure 9.5 True path: E.Polytech\ID THEFT 1\Other Card Stuff\passport.jpg (Start Sector: 2,445, Sectors 7; Start Cluster 463, Clusters 7)

On April 1, 2023, at 3:12 PM(PST) Michael Andom examined a .jpg labeled "this could be handy.jpg," in E.Polytech\ID THEFT 1\Other Card Stuff\this could be handy.jpg. The image depicts a police identification card. The title of the image implies that it could be used to create a counterfeit ID card.

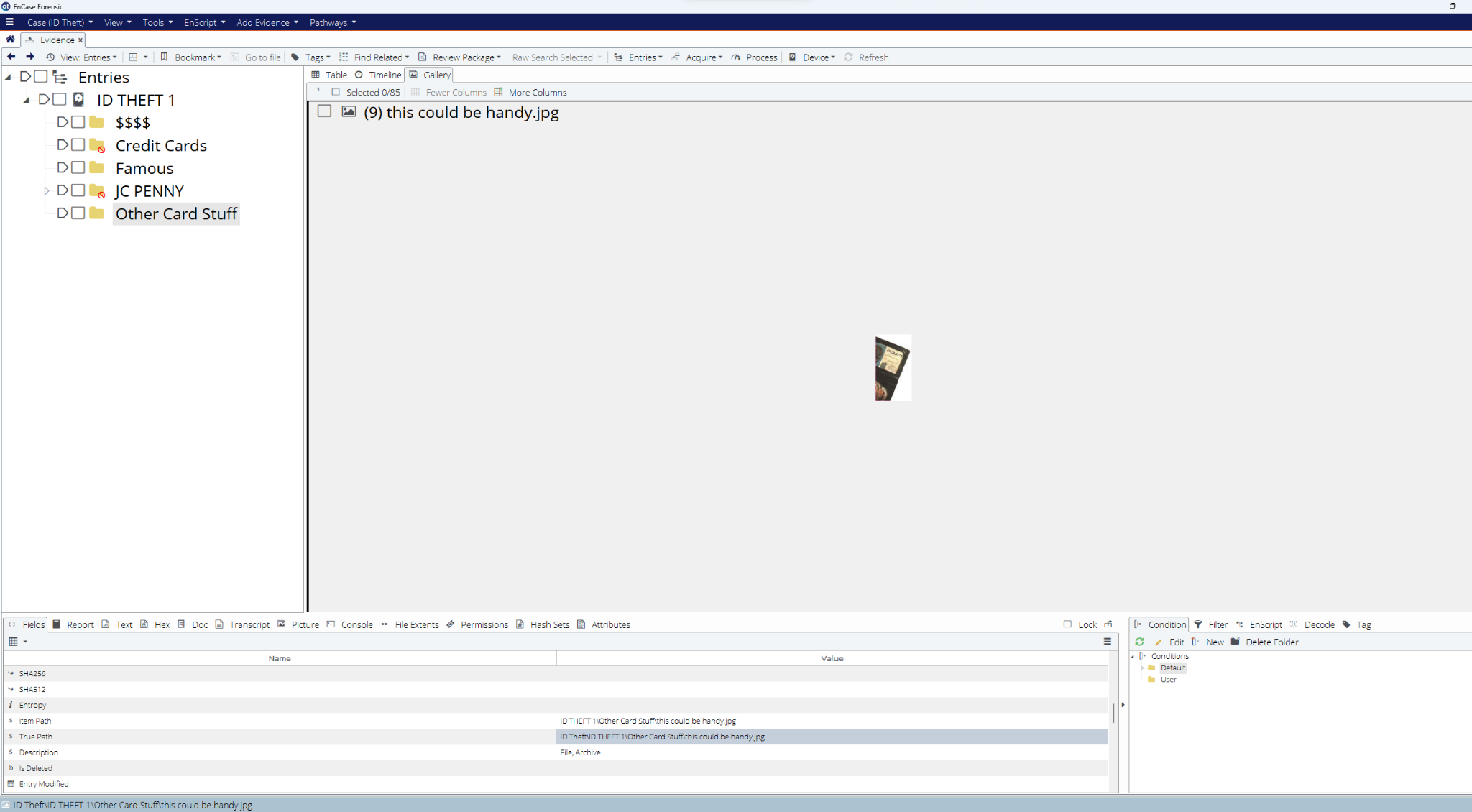


Figure 9.6 True path: E.Polytech\ID THEFT 1\Other Card Stuff\this could be handy.jpg (Start Sector: 2,452, Sectors 5; Start Cluster 470, Clusters 5)

On April 1, 2023, at 3:32 PM(PST), Michael Andom examined a .jpg labeled "fake ids.jpg," in E.Polytech\ID THEFT 1\Other Card Stuff\fake ids.jpg, portraying multiple IDs stacked upon one another, with the two cards on top displaying similar photos but different information. The name of the image implies that these are counterfeit IDs.

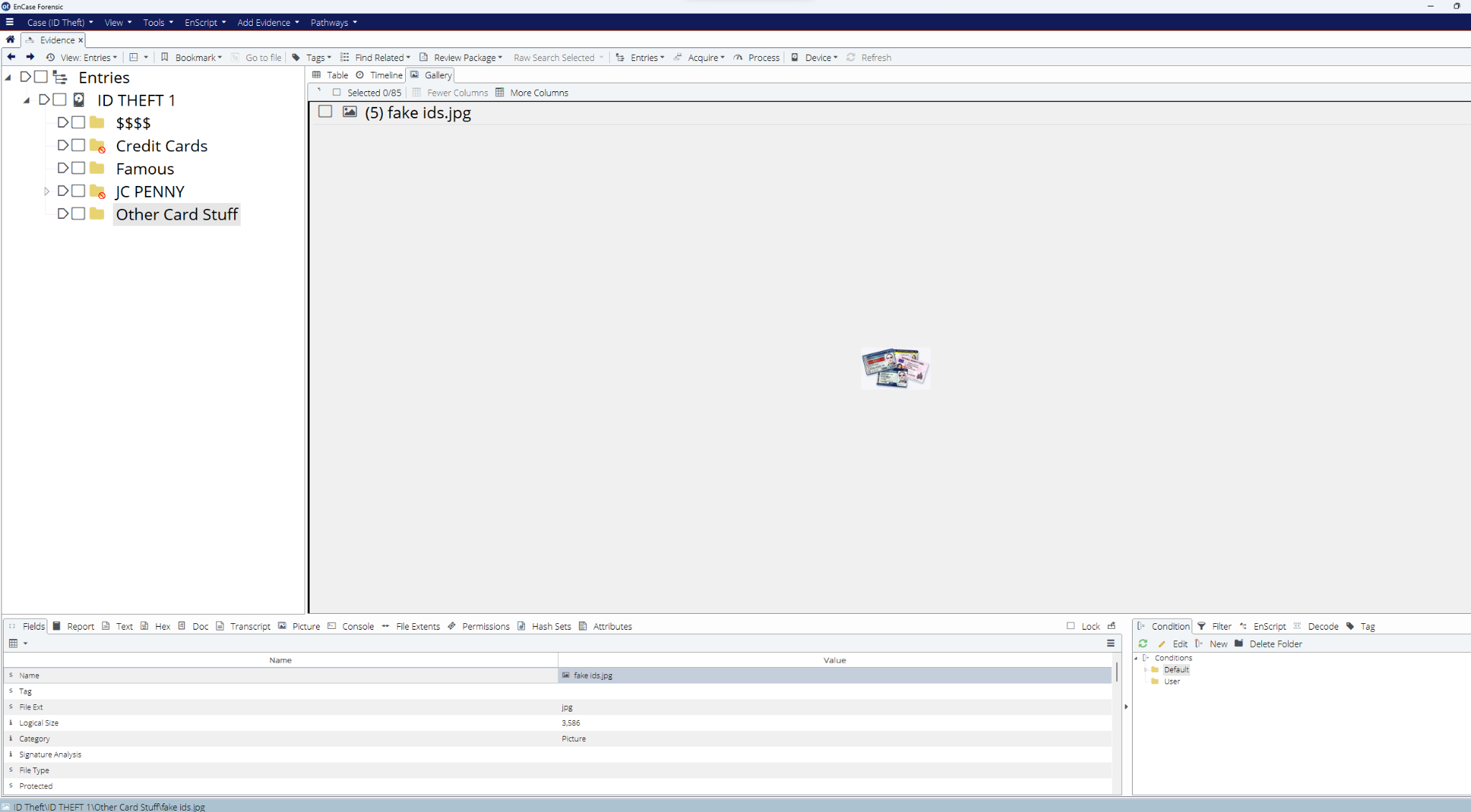


Figure 9.7 True path: E.Polytech\ID THEFT 1\Other Card Stuff\fake ids.jpg (Start Sector: 2,422, Sectors 8; Start Cluster 440, Clusters 8)

On April 1, 2023, at 3:59 PM(PST), Michael Andom examined a .jpg named "top this.jpg" in E.Polytech\ID THEFT 1\Other Card Stuff\top this.jpg. The image displays three individuals holding up what appears to be ID cards. The name suggests that the counterfeit IDs are so precise and genuine in appearance that they surpass any other comparison.

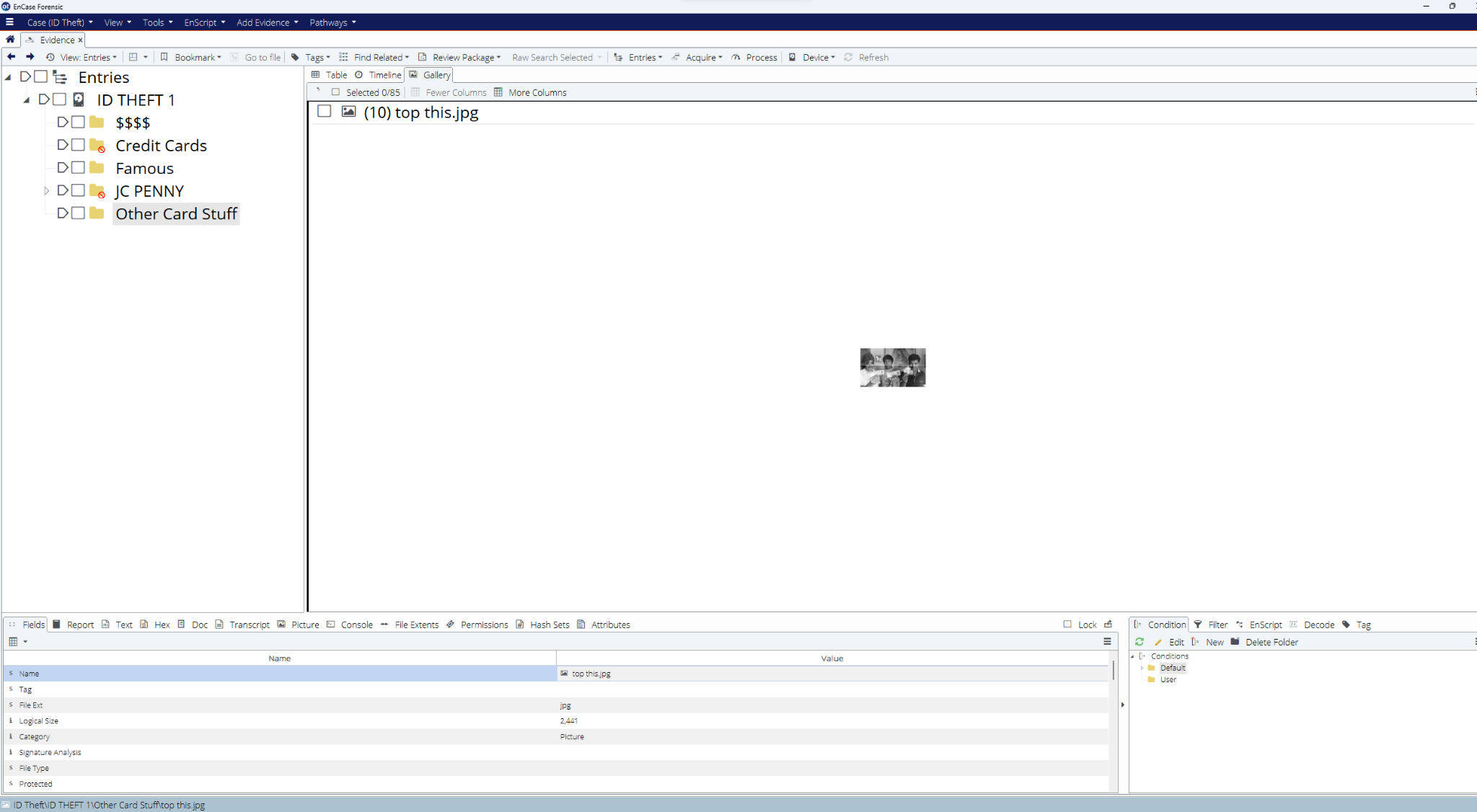


Figure 10.1 True path: E.Polytech\ID THEFT 1\Other Card Stuff\top this.jpg (Start Sector: 2,519, Sectors 5; Start Cluster 440, Clusters 5)

On April 1, 2023, at 4:23 PM(PST), Michael Andom examined a .jpg named "uk id 2.jpg," in E.Polytech\ID THEFT 1\Other Card Stuff\uk id 2.jpg. The image displays a regular United Kingdom ID card. Although this may not serve as evidence for counterfeit U.S. passports, the information or photo on this card could have been easily stolen and utilized to create a fake American passport.

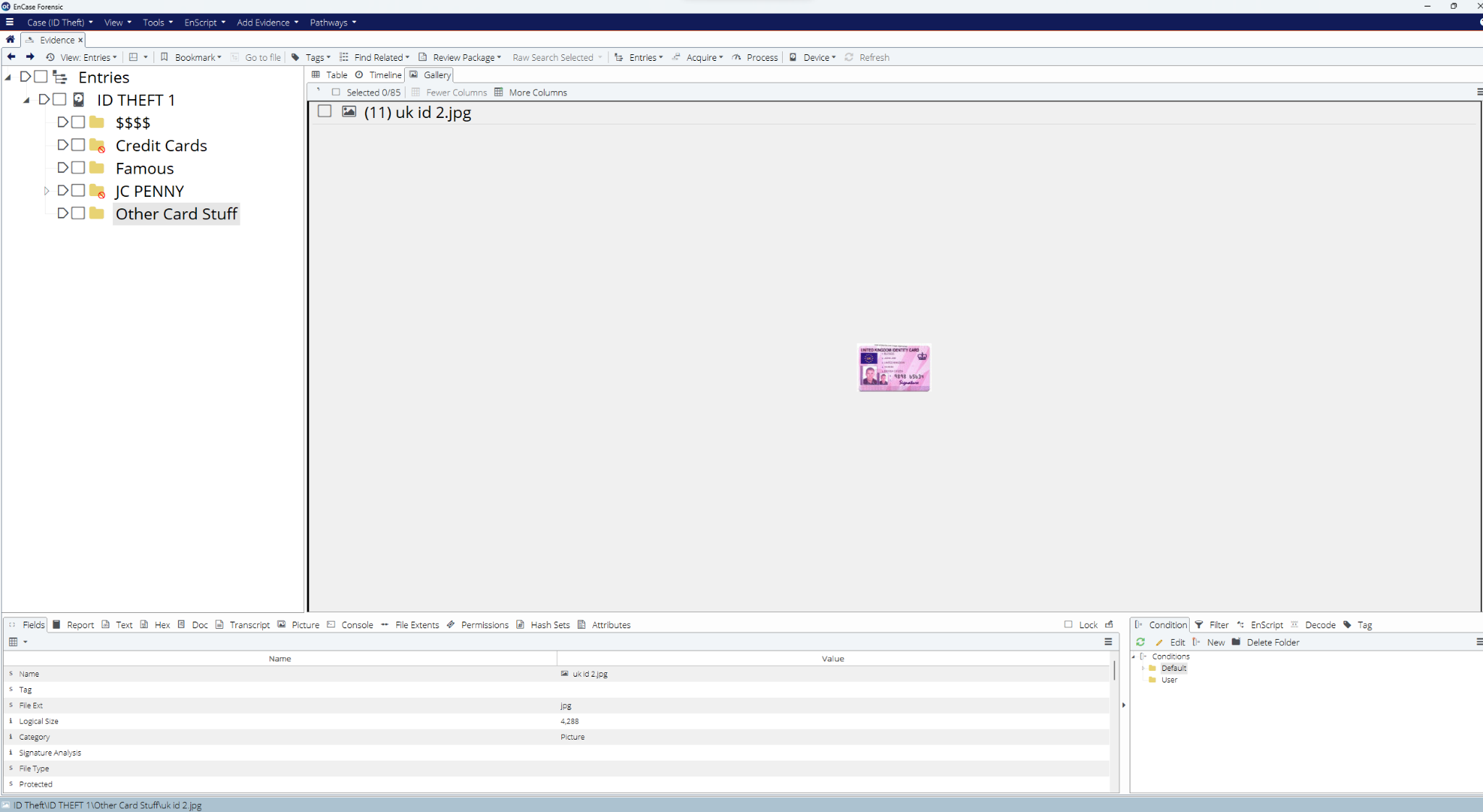


Figure 10.2 True path: E.Polytech\ID THEFT 1\Other Card Stuff\uk id 2.jpg (Start Sector: 2,524, Sectors 9; Start Cluster 542, Clusters 9)

On April 1, 2023, at 4:23 PM(PST), Michael Andom examined a .jpg labeled "uk id.jpg" in E.Polytech\ID THEFT 1\Other Card Stuff\uk id.jpg. The image shows the back side of a United Kingdom ID card, and the serial number information could be copied and transferred to create counterfeit U.S. passports.

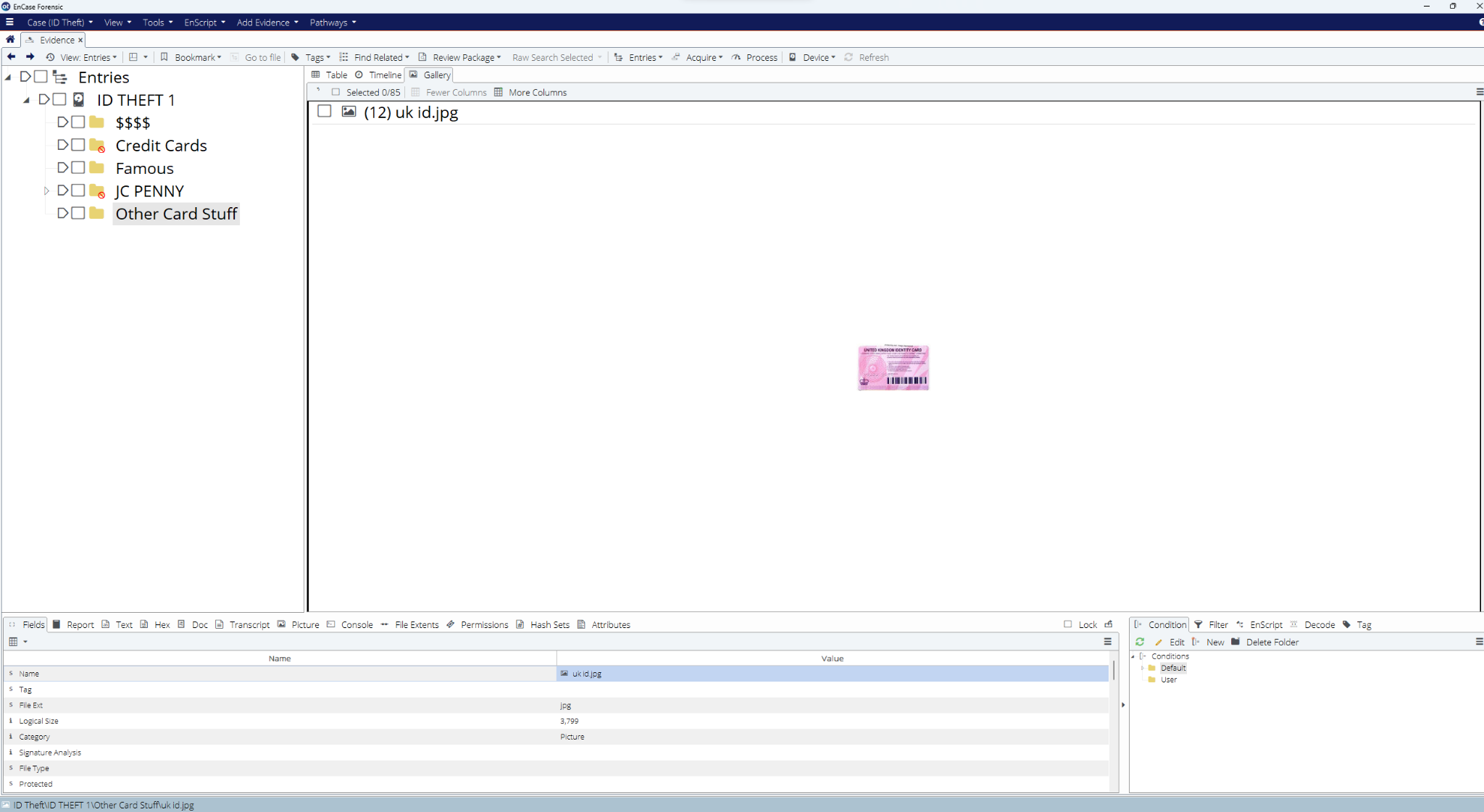
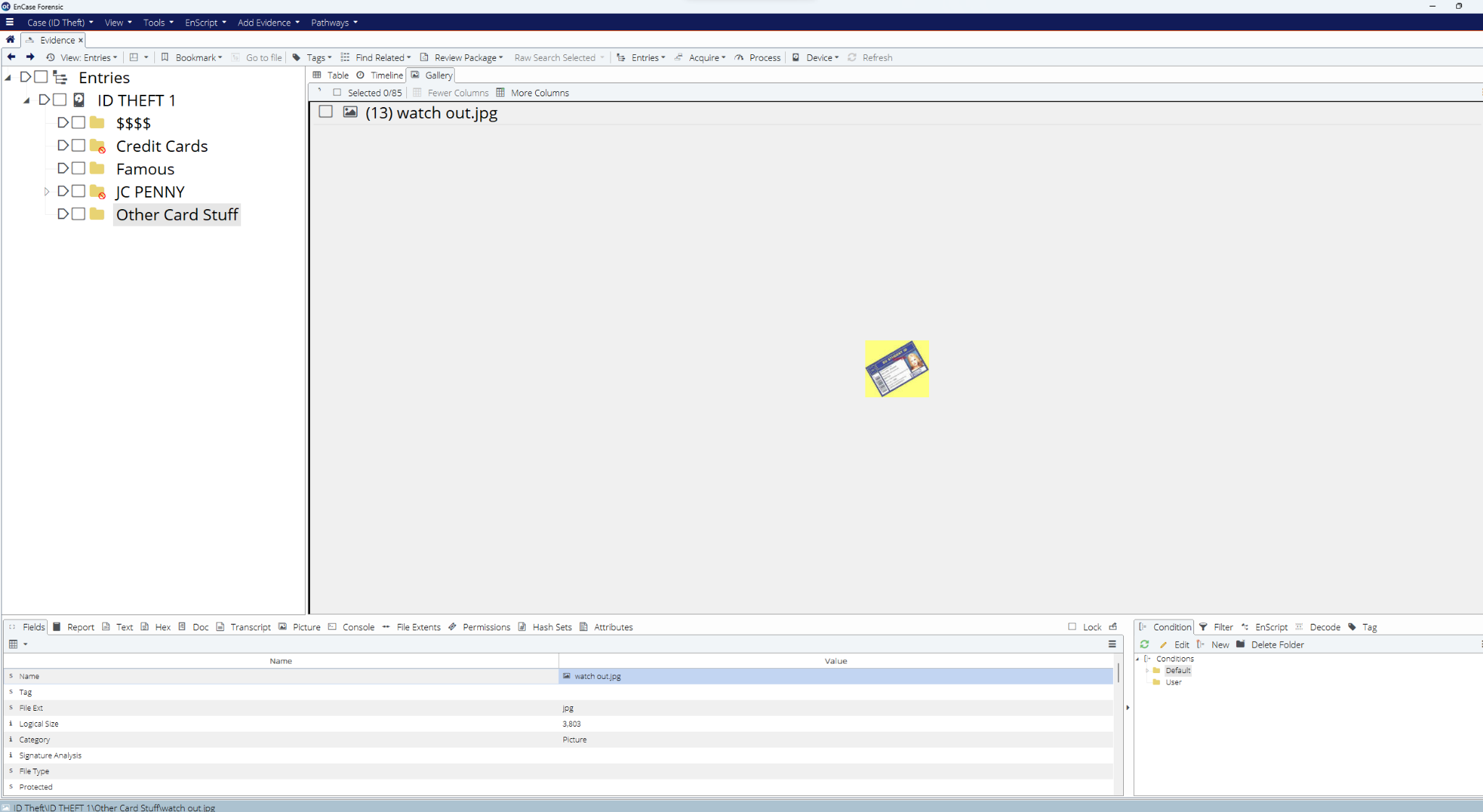


Figure 10.1 True path: E.Polytech\ID THEFT 1\Other Card Stuff\uk id.jpg (Start Sector: 2,533, Sectors 8; Start Cluster 551, Clusters 8)

On April 1, 2023, at 4:43 PM(PST), Michael Andom examined a .jpg labeled "watch out.jpg" in E.Polytech\ID THEFT 1\Other Card Stuff\watch out.jpg. The image displays a European Union Student ID card with a red arrow pointing towards the photo. The title implies that one must exercise caution when using the same photo, photo style, or dimensions for creating counterfeit U.S. passports.



1. Locate evidence that can assist in prosecuting the offense of theft of credit card information.

**c. Theft of credit card information**

Within the Famous folder, there is an image named "This is why JCPENNY!!! .jpg" which displays an email from an individual seeking assistance from JCPenny after their credit card was stolen. This email could provide useful information for individuals involved in credit card theft since it outlines how the stolen credit card has already been reported.

Another image in the Famous folder labeled "made the news !! .jpg" shows a news article about two men who used handheld devices to steal credit card information from restaurant customers. The name of the picture implies that these two suspects were involved in various other cases of counterfeiting.

In the Other Card Stuff folder, there is a GIF labeled "CCG1.GIF" which displays the logo of a company that may be responsible for credit card generation. The credits underneath the logo name two individuals who may have also been involved in the creation of the handheld devices used for credit card theft.

A second GIF in the Other Card Stuff folder labeled "CCG2" provides insight into the suspected credit card generator. This GIF displays how the credit card generation process is done, from entering the card number to selecting the card type and generating multiple cards.

Finally, the last GIF labeled "CCG3.GIF" in the Other Card Stuff folder displays a window, possibly from the same credit card generation program as CCG2. In the window, there is a list of several credit card numbers that may have been stolen.

Overall, the information discovered in these search results is concerning and suggests potential ongoing credit card theft and counterfeiting activity. Further examination and appropriate action may be necessary to prevent future incidents of credit card fraud.

***Tip:*** To find evidence of credit card theft, you can create a regular expression to find American Express Card numbers (e.g., 1234 123456 12345). You can also create another regular expression to find JC Penney Card numbers (e.g., 123 456 789 0 1).