FORENSICS
LAB SERIES

Lab 8: Windows Registry Forensics

Material in this Lab Aligns to the Following Certification Domains/Objectives		
GIAC Certified Forensics Examiner (GCFE) Domains	Certified Cyber Forensics Professional (CCFP) Objectives	Computer Hacking Forensic Investigator (CHFI) Objectives
6: System and Device Profiling and Analysis	4: Digital Forensics	8: Windows Forensics

Document Version: 2016-08-17

Contents

Introduction

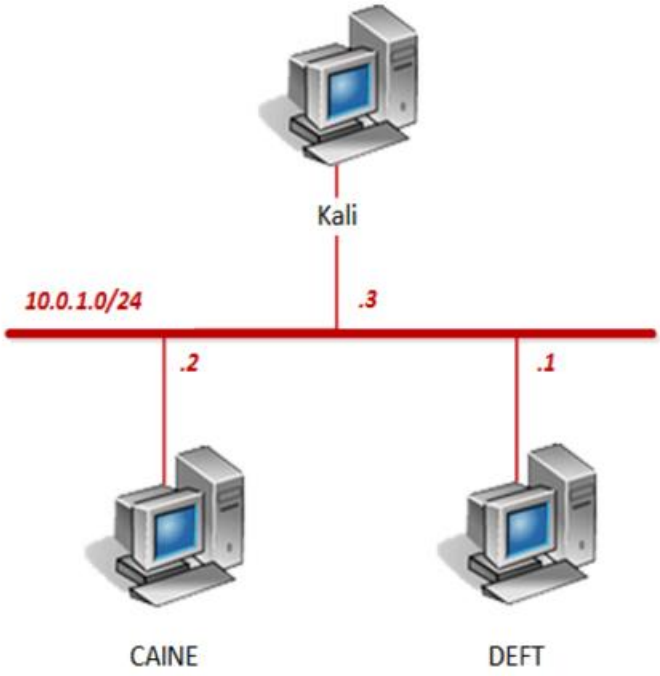
This lab will introduce many places where information is stored in the Windows Registry. By analyzing the registry, a forensic examiner can discover many different pieces of data that are tracked every time the system is used.

Objective

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

1. Using Fred to Open Registry Hives
2. Using Fred to Analyze the Software Hive
3. Using Fred to Analyze the SAM Hive
4. Using Fred to Analyze the System Hive
5. Using Fred to Analyze the NTUSER.DAT File

Pod Topology



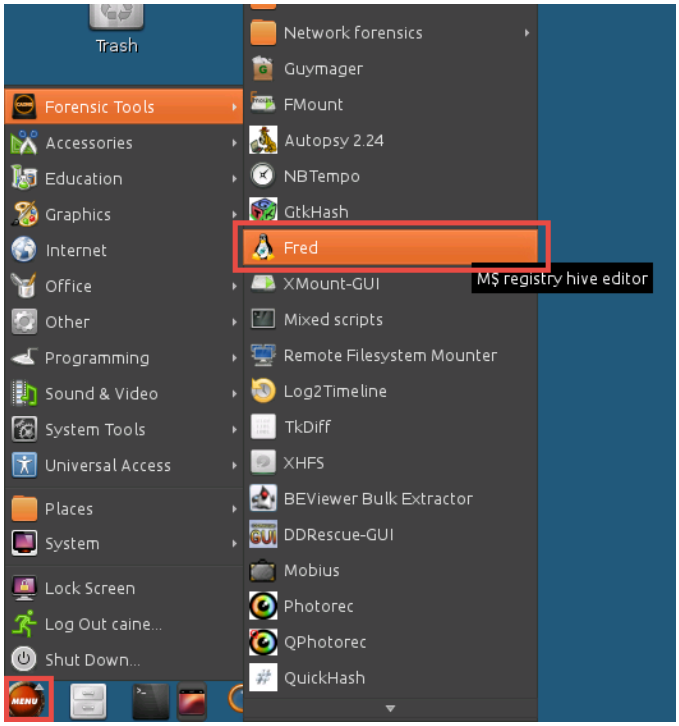
Lab Settings

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.

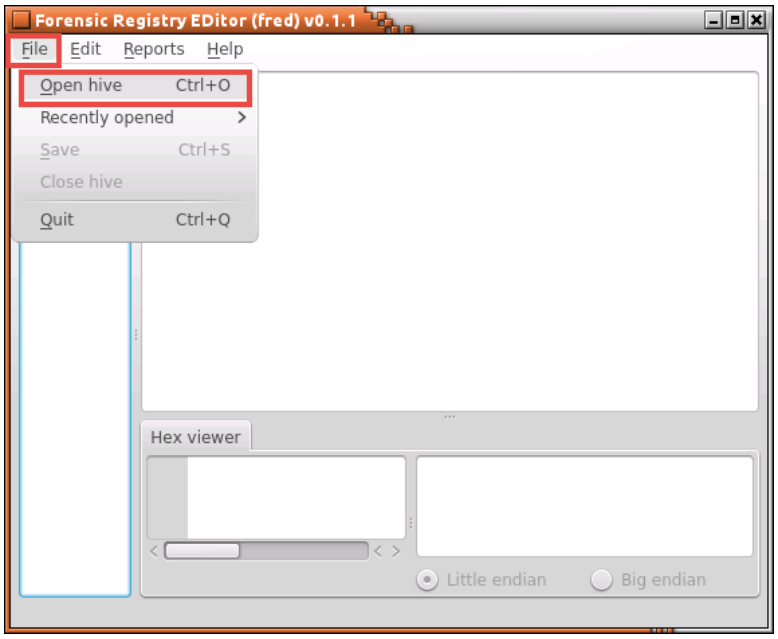
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
DEFT	10.0.1.1	deft	password
CAINE	10.0.1.2	caine	
Kali	10.0.1.3	root	toor

1 Using Fred to Open Registry Hives

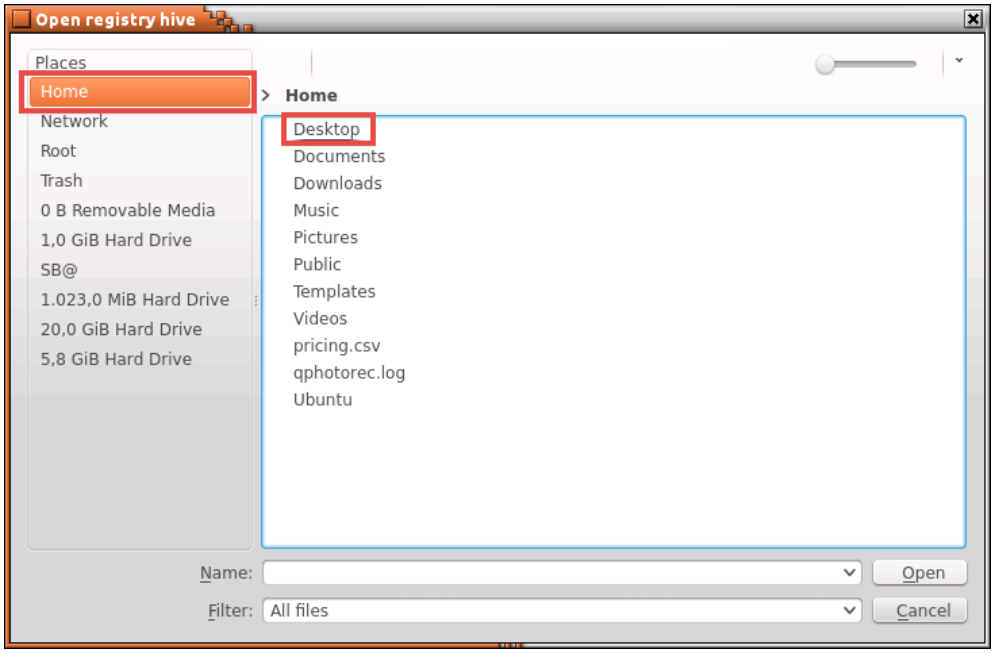
1. Click on the **CAINE** graphic on the *topology page* to open the VM.
2. Navigate to **Menu > Forensic Tools > Fred** to open the registry editor.



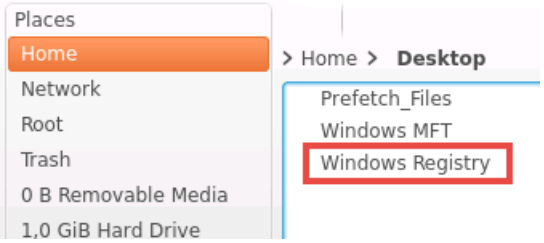
3. The *Fred* application is a forensic registry editor that allows a user to look inside registry hives and view the information. It is not limited like *regedit* in Windows; more values can be shown with *Fred* as opposed to the common *regedit* tool. Using the *Fred* application, go to **File > Open hive**.



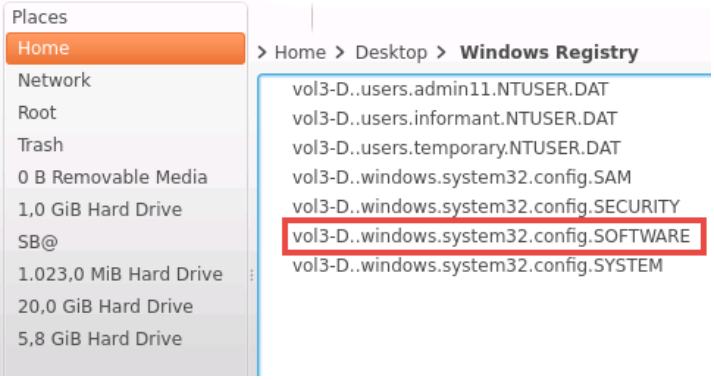
4. In the *Open registry hive* window, navigate to **Home > Desktop**.



5. Click on **Windows Registry**.



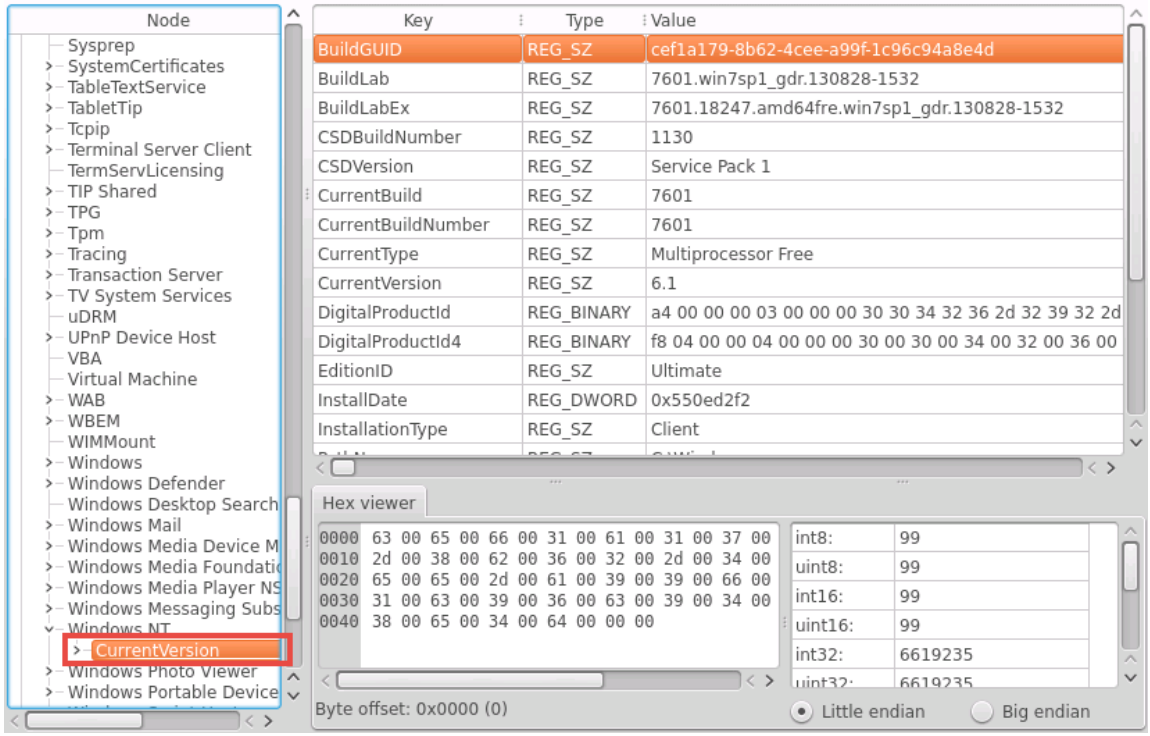
6. Explore the "*software*" hive first by clicking on **vol3-D..windows.system32.config.SOFTWARE**.



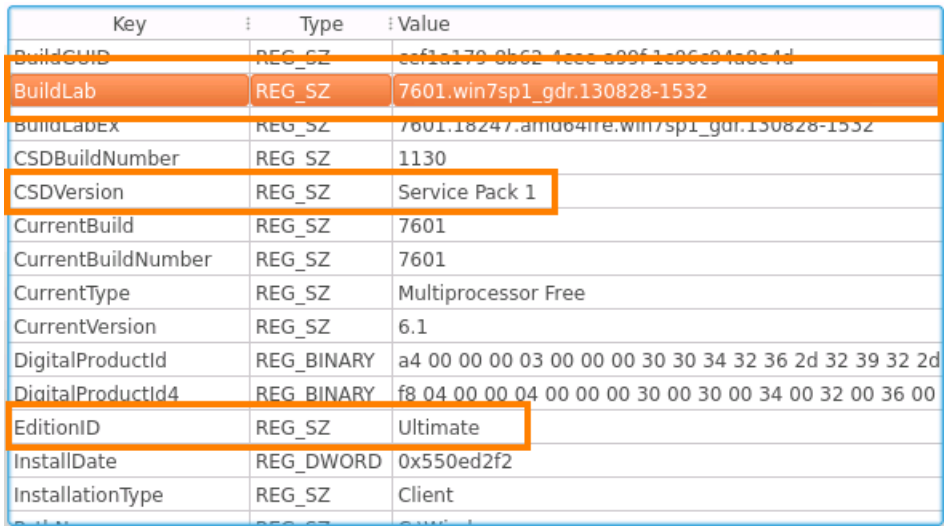
7. Leave the *Fred* application open to continue with the next task.

2 Using Fred to Analyze the Software Hive

1. Using the *Fred* application, identify what operating system is being examined. Navigate to **Microsoft\Windows NT\CurrentVersion** using the left pane.



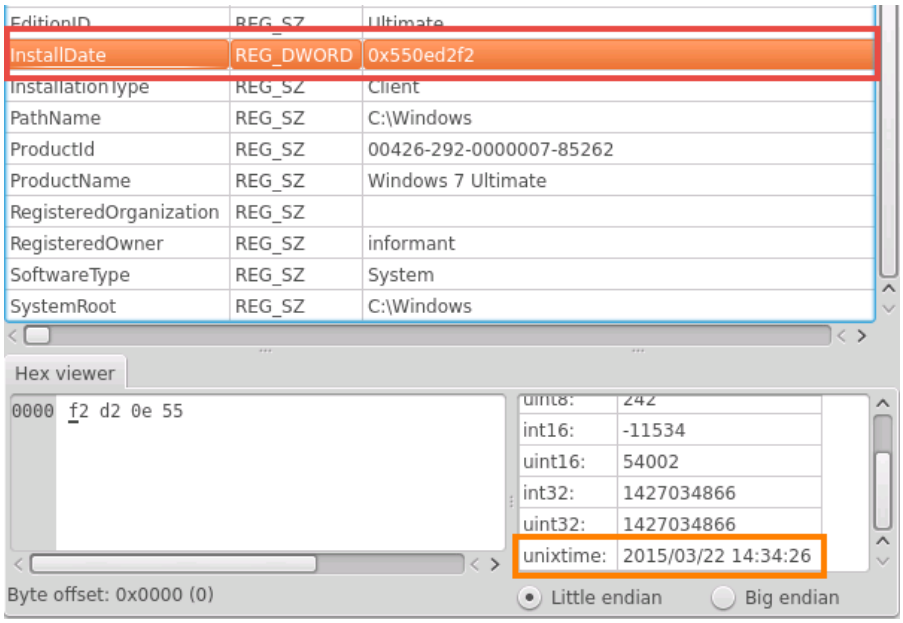
2. Identify the **BuildLab** identifier underneath the *Key* column and notice that the operating system is a *Windows 7 with Service Pack 1 Ultimate Edition*.



3. Scroll the middle pane down and identify the key values for **InstallDate** and **RegisteredOwned**.

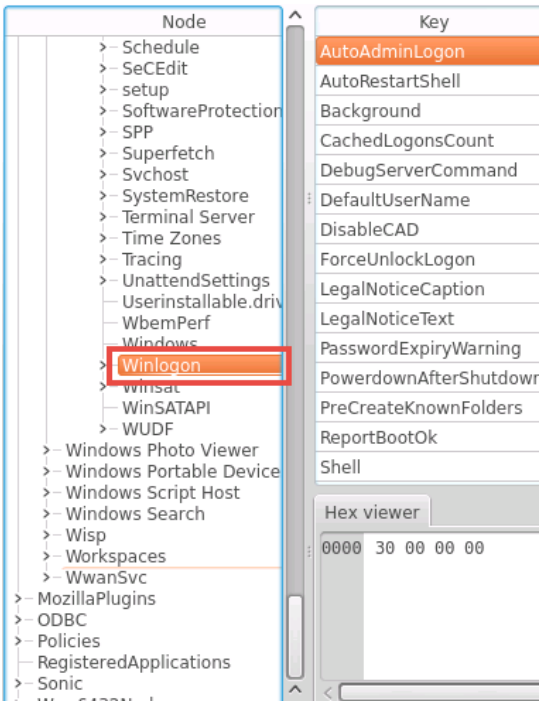
Key	Type	Value
CurrentType	REG_SZ	Multiprocessor Free
CurrentVersion	REG_SZ	6.1
DigitalProductId	REG_BINARY	a4 00 00 00 03 00 00 00 30 30 34 32 36 2d 32 39 32 2d
DigitalProductId4	REG_BINARY	f8 04 00 00 04 00 00 00 30 00 30 00 34 00 32 00 36 00
EditionID	REG_SZ	Ultimate
InstallDate	REG_DWORD	0x550ed2f2
InstallationType	REG_SZ	Client
PathName	REG_SZ	C:\Windows
ProductId	REG_SZ	00426-292-0000007-85262
ProductName	REG_SZ	Windows 7 Ultimate
RegisteredOrganization	REG_SZ	
RegisteredOwner	REG_SZ	informant
SoftwareType	REG_SZ	System
SystemRoot	REG_SZ	C:\Windows

4. To interpret the *InstallDate* value, select the **InstallDate** row and scroll down on the *Hex Viewer* tab located on the bottom pane until *unixtime* is visible.

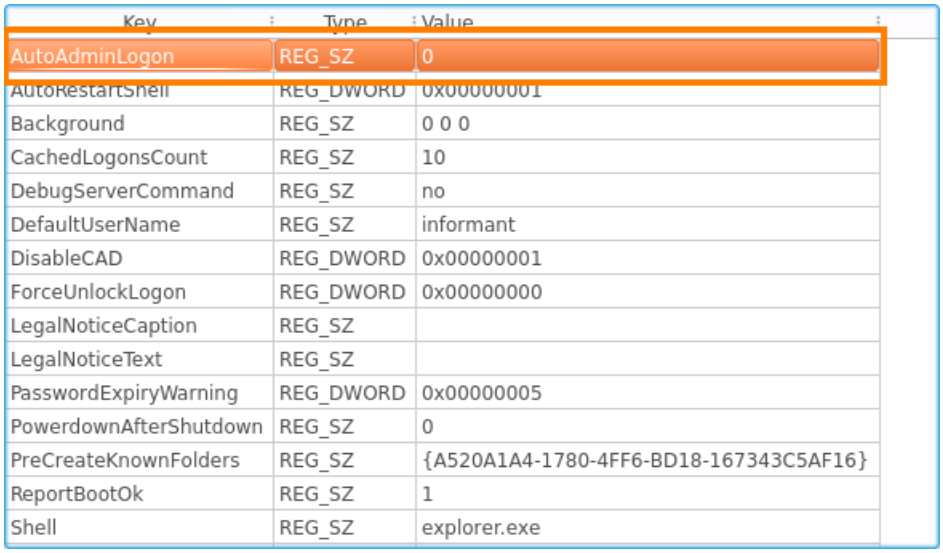


Notice the timestamp is *2015/03/22 14:34:26* which signifies the install date.

5. Identify whether the system is set to auto login. Expand the **CurrentVersion** from the left pane and scroll down to select **Winlogon**. The full path is *Microsoft\Windows NT\CurrentVersion\WinLogon.*

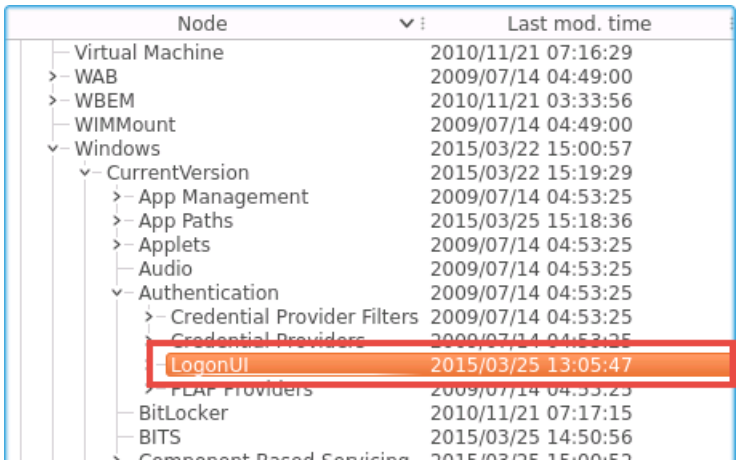


6. Identify the *AutoAdminLogon* underneath the *Key* column in the middle pane and notice that the value is set to "*0*", which translates to the user having to login.

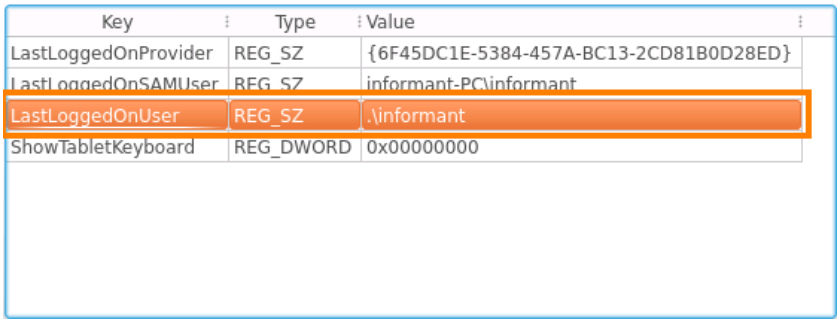


Key	Type	Value
AutoAdminLogon	REG_SZ	0
AutoRestartShell	REG_DWORD	0x00000001
Background	REG_SZ	0 0 0
CachedLogonsCount	REG_SZ	10
DebugServerCommand	REG_SZ	no
DefaultUserName	REG_SZ	informant
DisableCAD	REG_DWORD	0x00000001
ForceUnlockLogon	REG_DWORD	0x00000000
LegalNoticeCaption	REG_SZ	
LegalNoticeText	REG_SZ	
PasswordExpiryWarning	REG_DWORD	0x00000005
PowerdownAfterShutdown	REG_SZ	0
PreCreateKnownFolders	REG_SZ	{A520A1A4-1780-4FF6-BD18-167343C5AF16}
ReportBootOk	REG_SZ	1
Shell	REG_SZ	explorer.exe

7. Identify who last logged into the system. Using the left pane, navigate to **Microsoft\Windows\CurrentVersion\Authentication\LogonUI**.

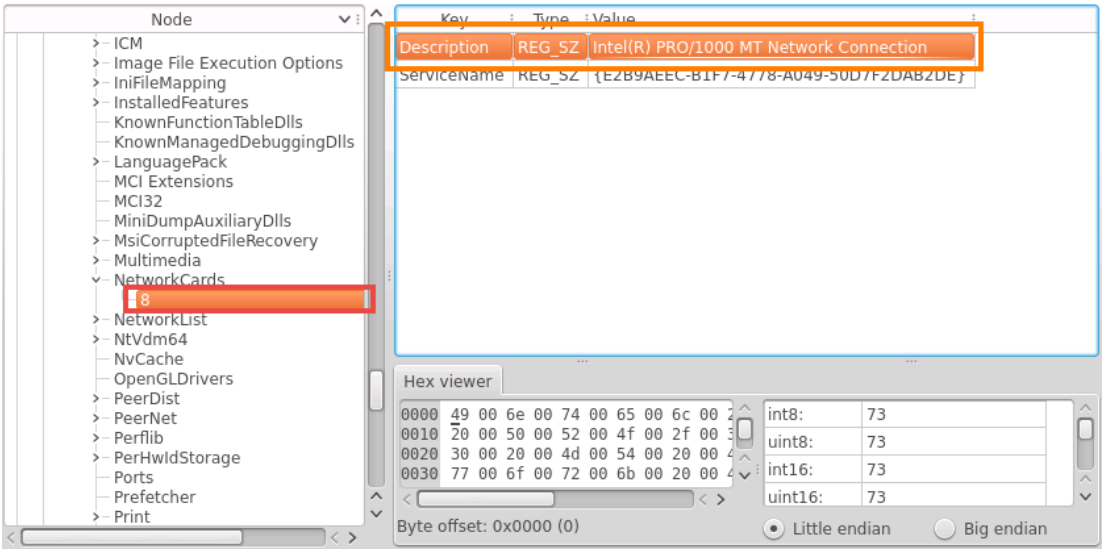


8. Identify the *LastLoggedOnUser* underneath the *Key* column to find its respective value. The last known user to log onto the system is *informant*.



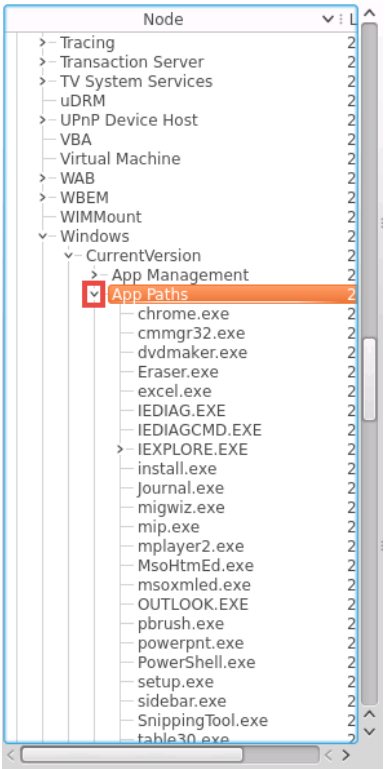
Key	Type	Value
LastLoggedOnProvider	REG_SZ	{6F45DC1E-5384-457A-BC13-2CD81B0D28ED}
LastLoggedOnSAMUser	REG_SZ	informant-PC\informant
LastLoggedOnUser	REG_SZ	.\informant
ShowTabletKeyboard	REG_DWORD	0x00000000

9. Using the left pane, navigate to **Microsoft\Windows NT\CurrentVersion\NetworkCards\8**.

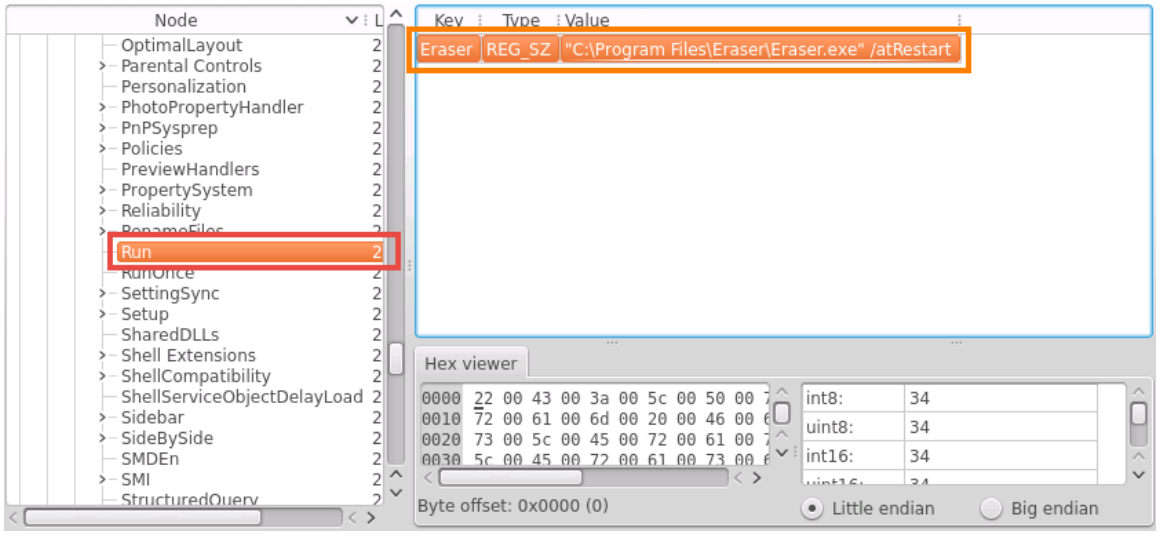


Notice the description of the network card.

10. Using the left pane, navigate to **Microsoft\Windows\CurrentVersion\AppPaths** to identify all the applications that were installed on the machine. Expand the list for *AppPaths* so that the list of installed applications can be visible.

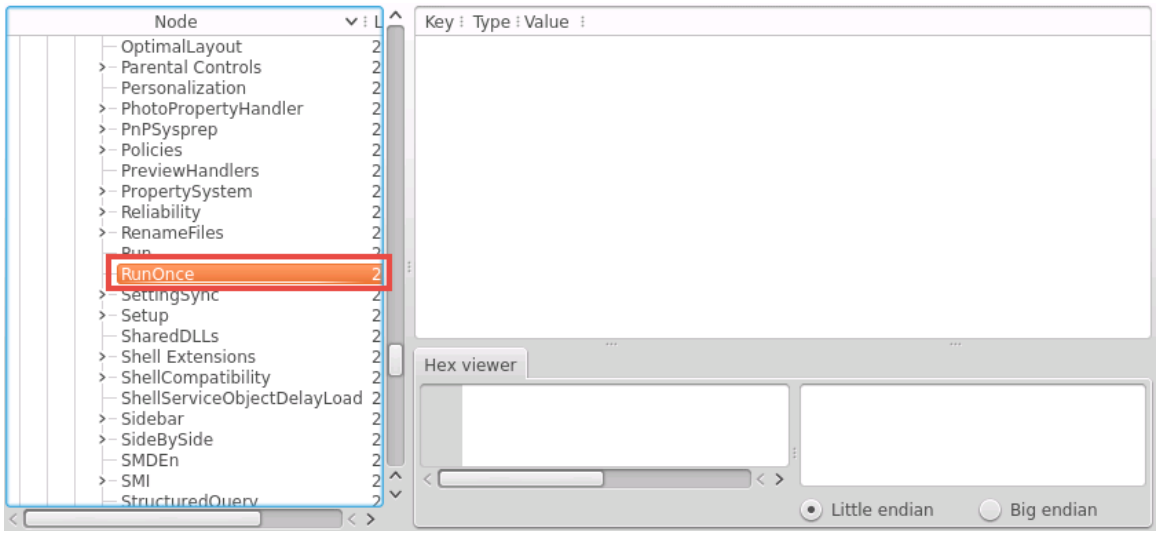


11. Using the left pane, navigate to **Microsoft\Windows\CurrentVersion\Run** to identify which programs where set to run or run once.



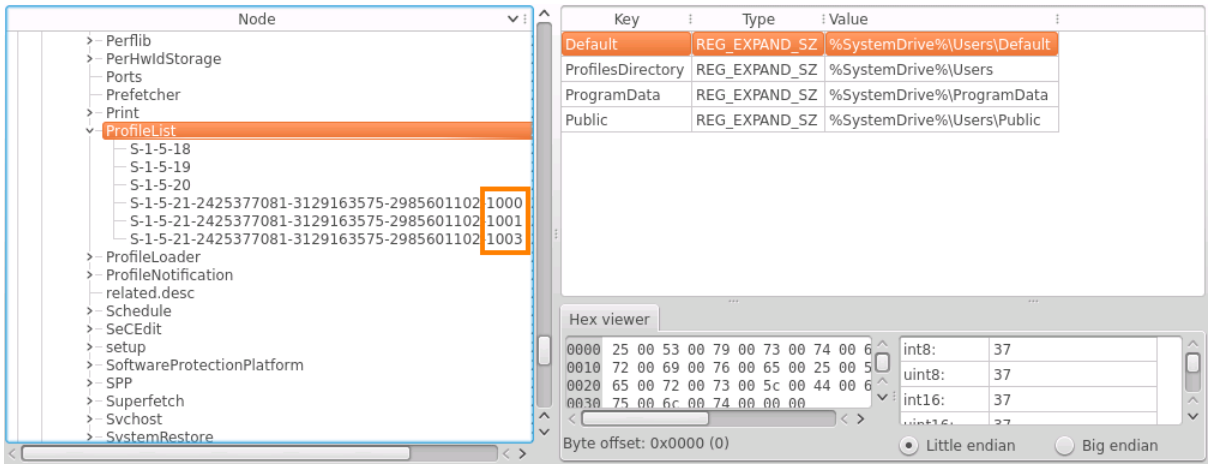
Notice the program "*Eraser.exe*" is set to run at every restart.

12. Using the left pane, click on **RunOnce**, which is directly underneath the *Run* path.



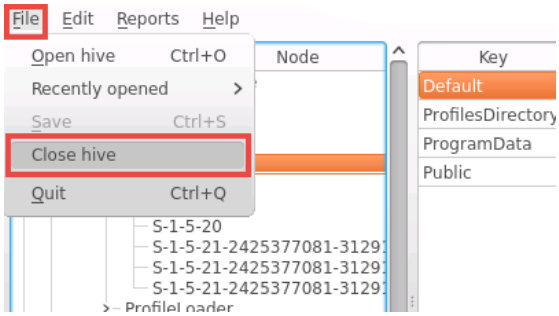
Notice no programs are configured to run once on this system.

13. Using the left pane, navigate to **Microsoft\WindowsNT\CurrentVersion\ProfileList** to check whose accounts are on the system.



There are three profiles in the list. To further analyze the accounts, check them against the *Security Accounts Manager* (*SAM*).

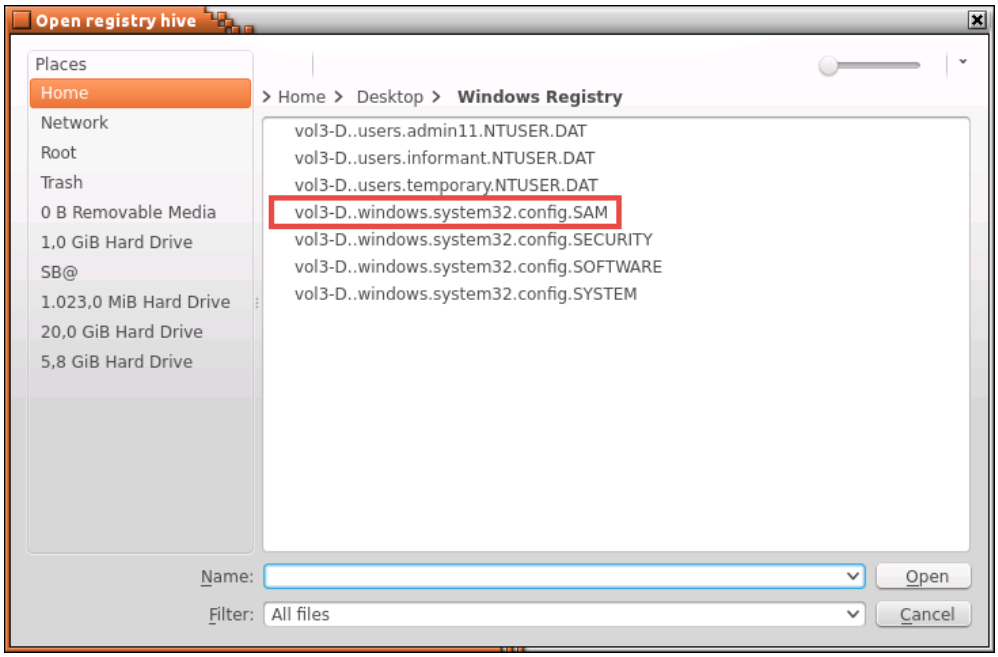
14. Using the *Fred* application, click on **File** at the top-left corner and select **Close hive**.



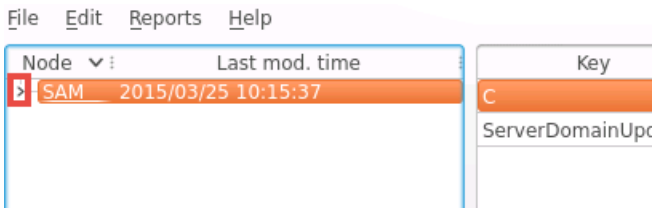
3 Using Fred to Analyze the SAM Hive

1. Using the *Fred* application, click on **File** again, this time selecting **Open hive**.

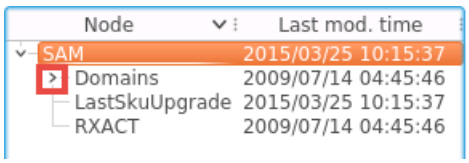
2. In the *Open registry hive* window, make sure to navigate to **Home/Desktop/Windows Registry** and select the "**SAM**" hive.



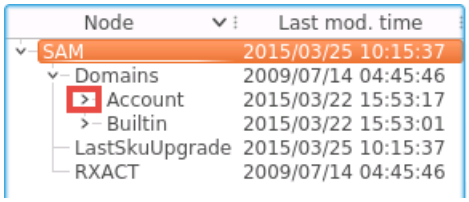
3. In the left pane, expand the **SAM** directory by clicking on its respective **arrow**.



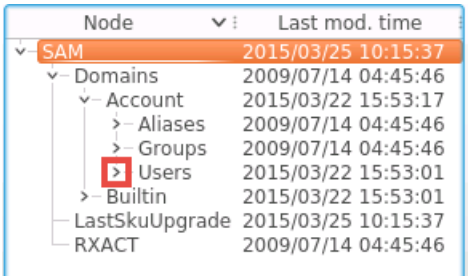
4. Once expanded, expand the **Domains** directory.



5. Expand the **Account** directory.

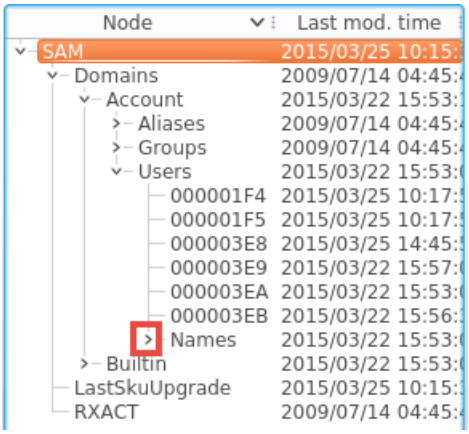


6. Expand the **Users** directory.

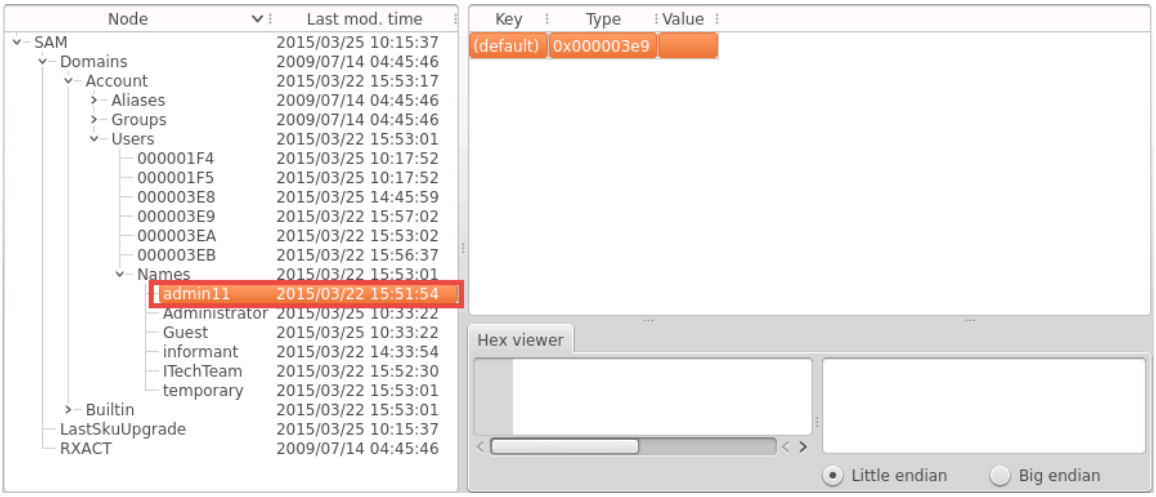


Notice the *Security Identifiers* (*SIDs*) appear for each user account on the system.

7. To see the actual names of the user accounts, expand the **Names** directory.

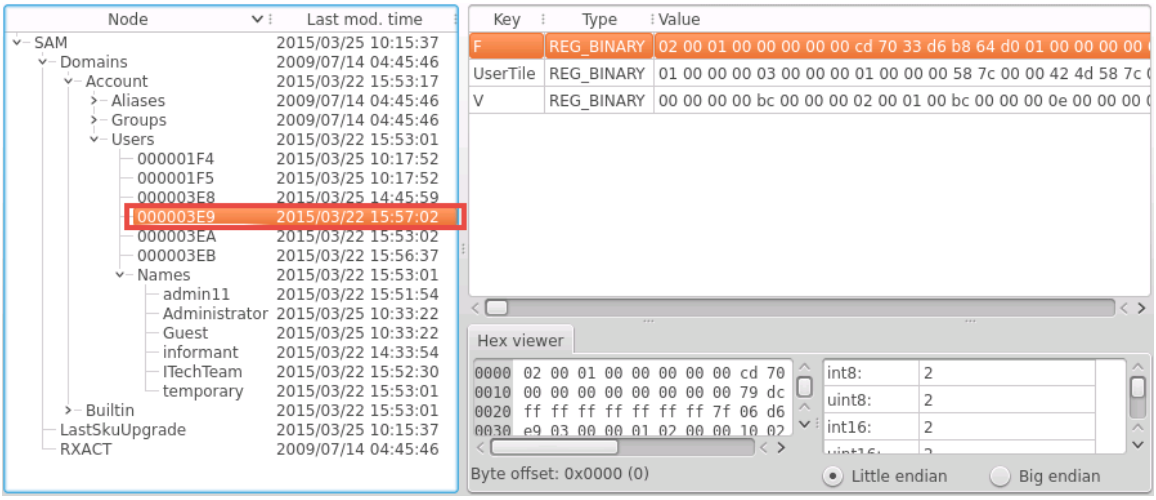


8. In the left pane, click on **admin11** underneath the *Names* directory.



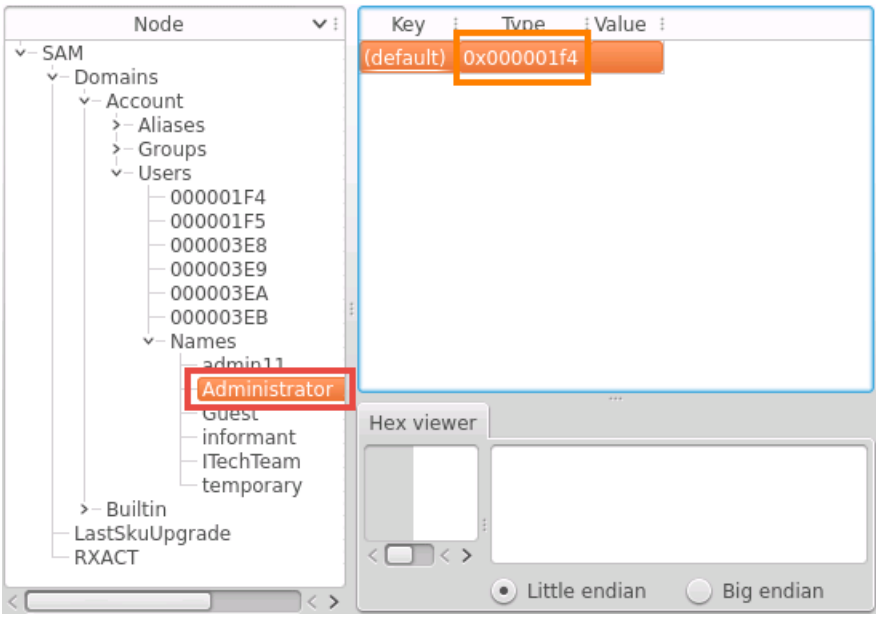
Notice the value of *0x000003e9* underneath the *Type* column in the right pane. This is the respective *SID* value for the user *admin11*.

9. In the left pane, underneath the Users directory, click on **000003E9**.



Notice the information presented.

10. In the left pane, click on Administrator, underneath the Names directory.



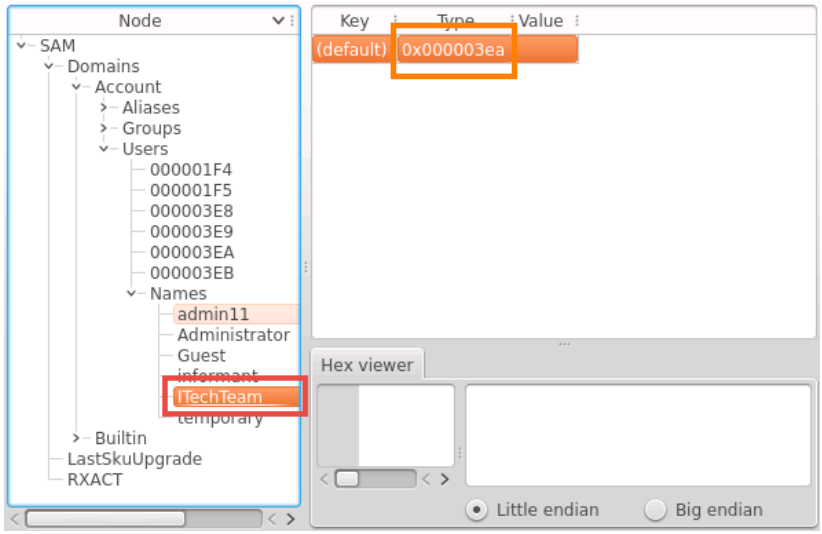
Notice the *SID* for the user *Administrator* is *0x000001f4*.

11. Convert the hex to decimal form.

Hex	Decimal	User
000001F4	500	Default “Administrator” SID value
000001F5	501	Default “Guest” SID value
000003E8	1000	First user created SID value
000003E9	1001	Second user created SID value
000003EA	1002	Third user created SID value
000003EB	1003	Fourth user created SID value

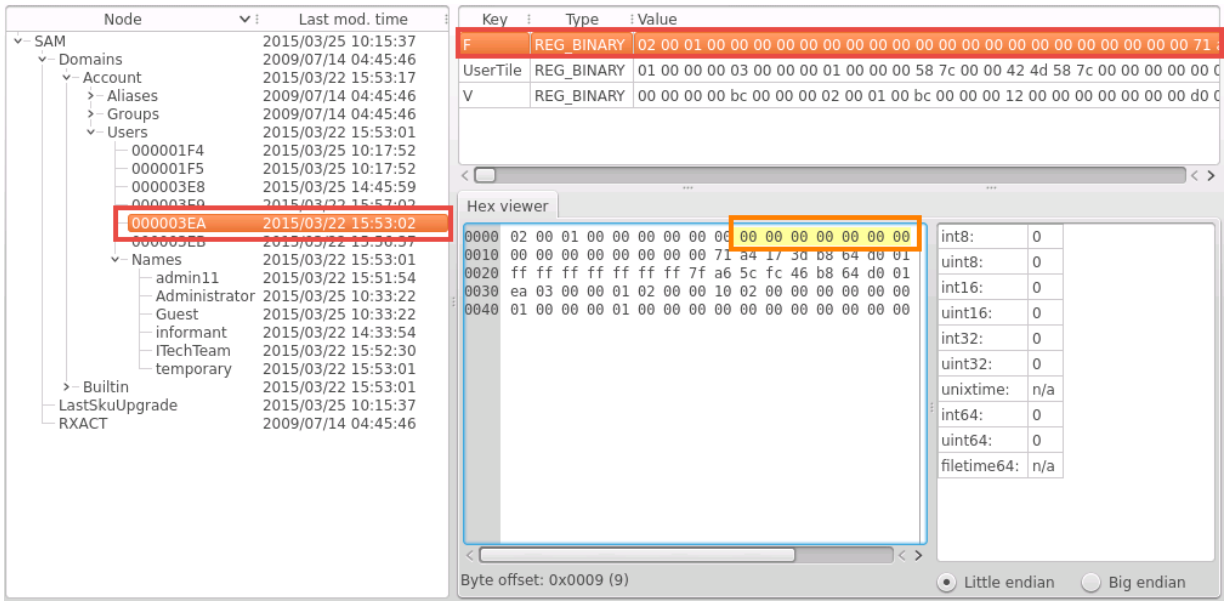
After converting, the *Administrator* account has a decimal value of *500*.

12. Looking back at *Task 2*, *Step 13*, notice that 3 of the accounts have profiles in the "*Software*" hive. The "*1002*" was missing a profile which is the *ITechTeam* account. This means that this particular account never logged into the system. Identify the *SID* value for the *ITechTeam* account by clicking on **ITechTeam** underneath the *Names* directory.



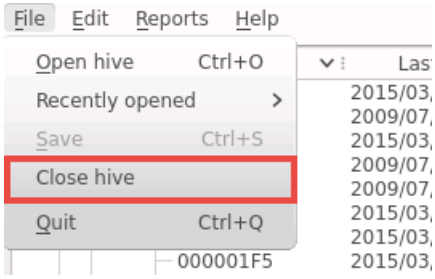
Notice the value for *ITechTeam* is *0x000003ea*.

13. In the left pane, click on **000003EA** underneath the *Users* directory. Using the *Hex viewer* in the bottom right pane, identify bytes 9-16.



Notice that they are all zeros which confirms that the *ITechTeam* has never logged into the system.

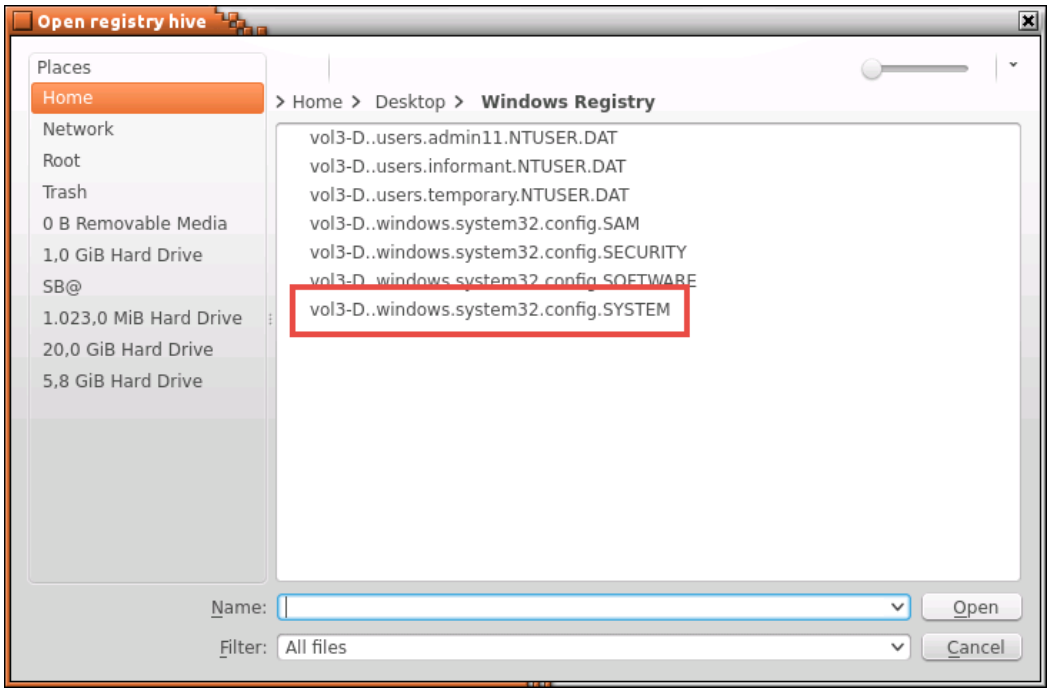
14. Using the *Fred* application, click on **File** at the top left corner and select **Close hive**.



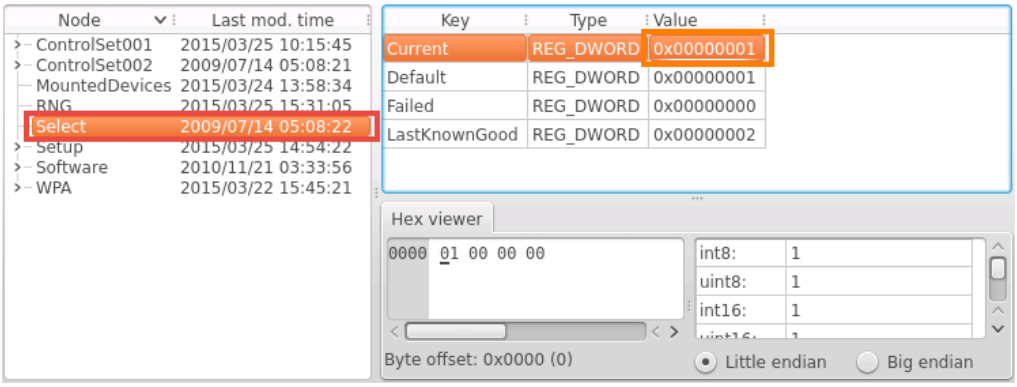
4 Using Fred to Analyze the System Hive

1. Using the *Fred* application, click on **File** and click on **Open hive**.

2. In the *Open registry hive* window, make sure to navigate to **Home/Desktop/Windows Registry** and select the "**SYSTEM**" hive.

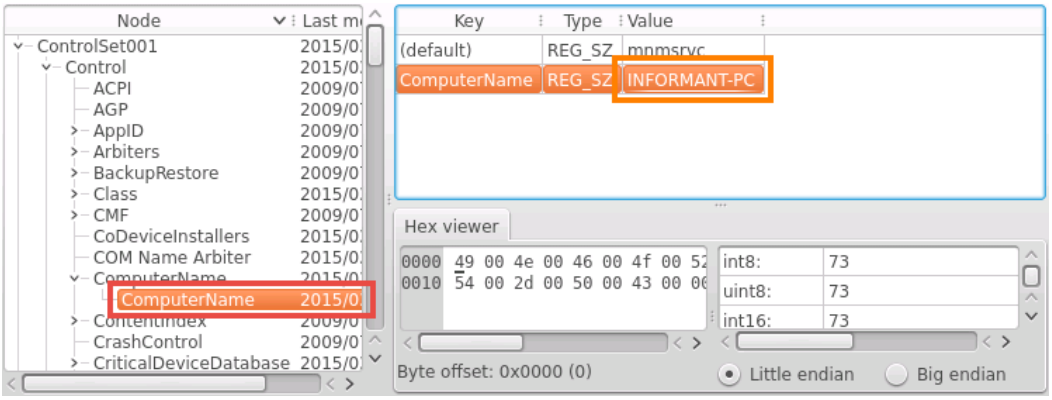


3. Identify which control set the machine was using. In the left pane, click on **Select** and identify the value for *Current*.



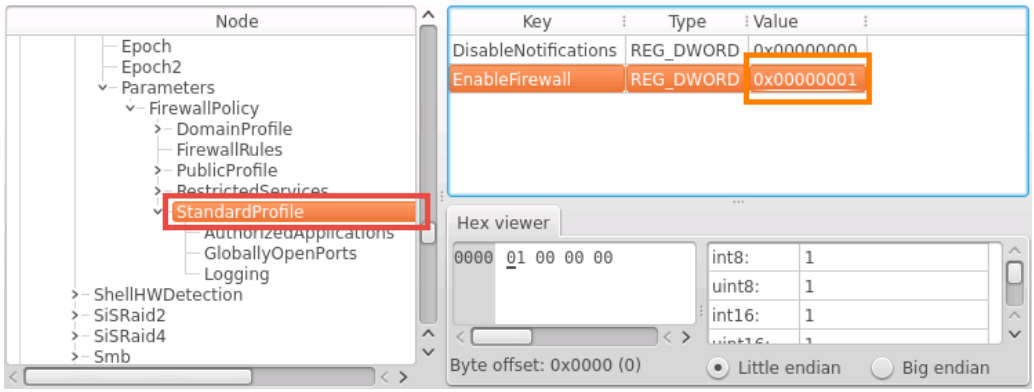
Notice the machine was using the "*ControlSet01*".

4. In the left pane, navigate to **ControlSet001\Control\ComputerName\ComputerName** and notice the value for *ComputerName*.



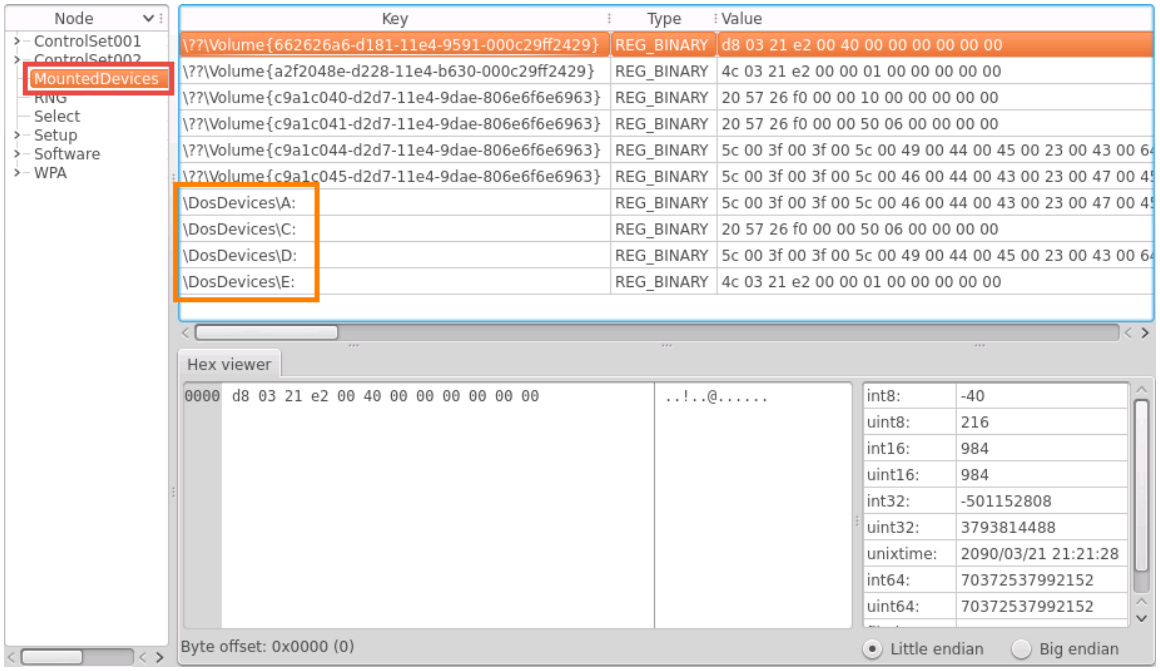
The computer name is *INFORMANT-PC*.

5. In the left pane, navigate to **ControlSet001\services\SharedAccess\Parameters\FirewallPolicy\StandardProfile** and identify the value for *EnableFirewall*.



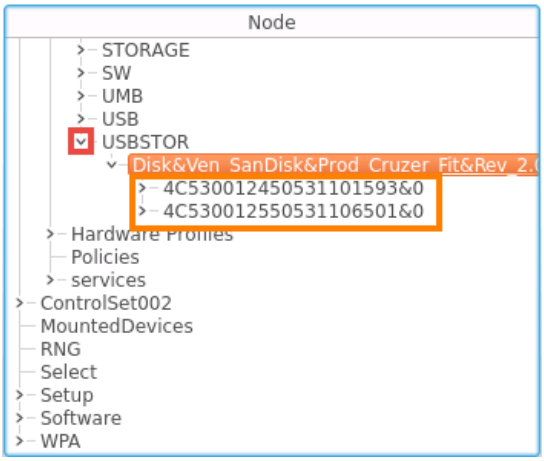
Notice the value is *0x00000001* which signifies that the firewall was active.

6. In the left pane, collapse *ControlSet001* and navigate to **MountedDevices** to identify what was mounted on the system.



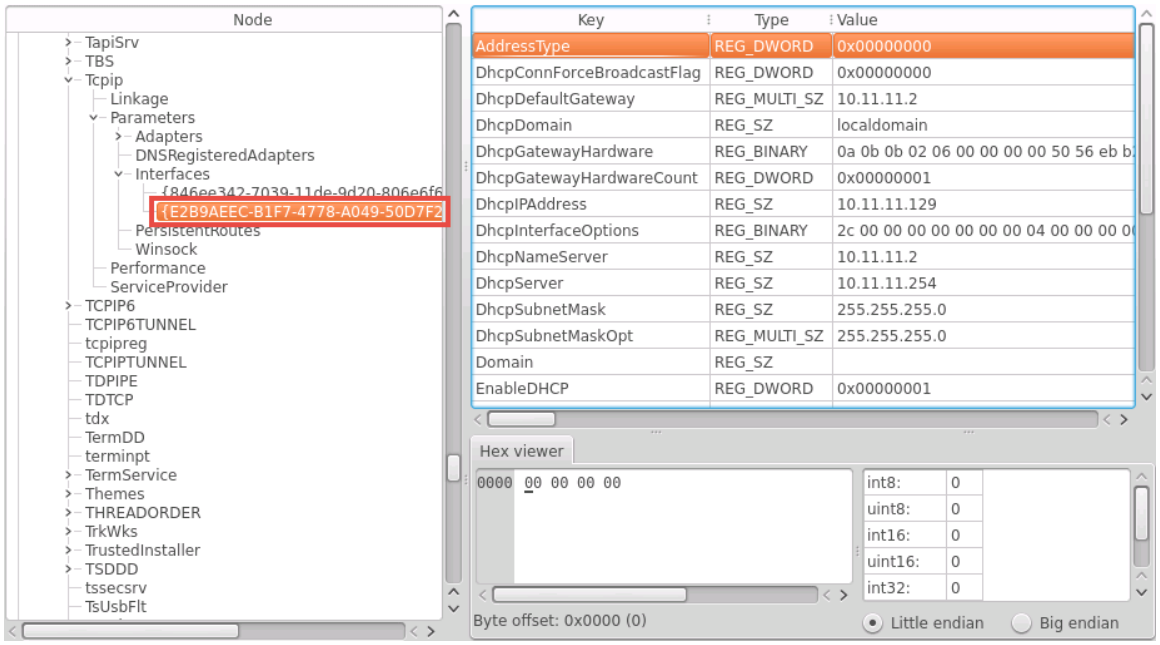
Notice the mounted drive letters visible: *A*, *C*, *D*, and *E*.

7. In the left pane, navigate to **ControlSet001\Enum\USBSTOR** to identify if any removable devices have been plugged into the system.



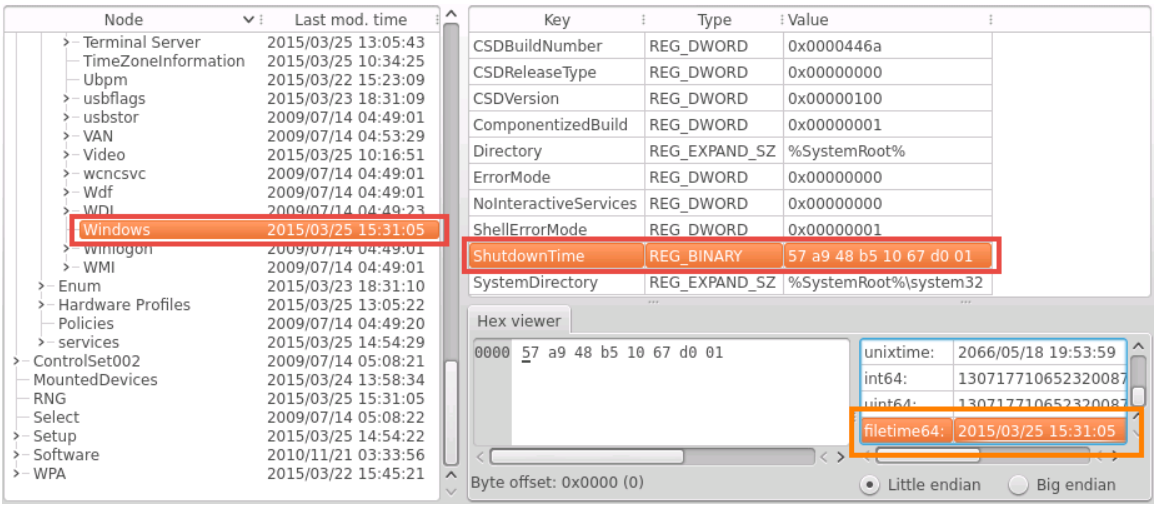
Notice that a *SanDisk* storage device was plugged into the system at some time.

8. In the left pane, navigate to **ControlSet001\services\Tcpip\Parameters\Interfaces** and select the hex number of the adapter discovered from *Task 2*, *Step 9*.



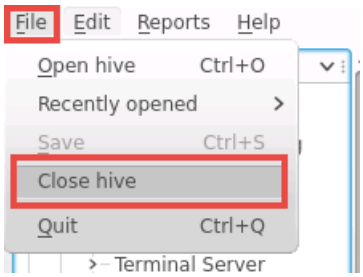
Notice the *IP* settings and how *DHCP* was enabled.

9. In the left pane, navigate to **ControlSet001\Control\Windows** and click on **ShutdownTime** underneath the *Key* column. To identify when the system was last shutdown, look in the bottom-right corner pane for *filetime64*.



Notice the last shutdown of the system occurred on *2015/03/25 15:31:05*.

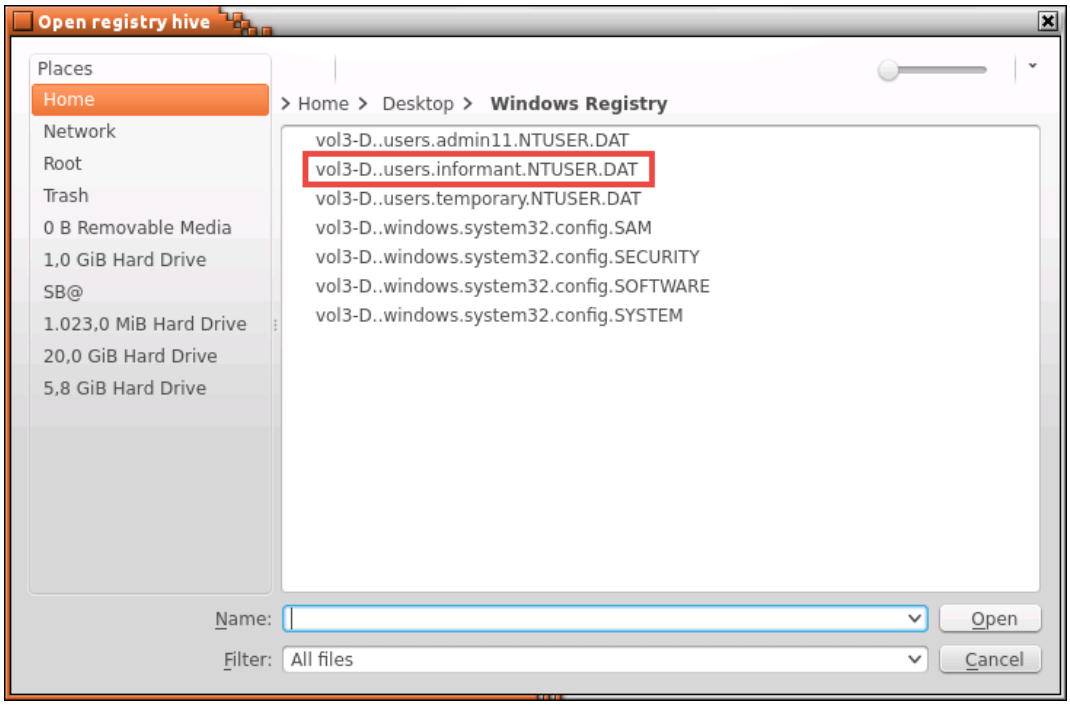
10. Using the *Fred* application, click on **File** at the top left corner and select **Close hive**.



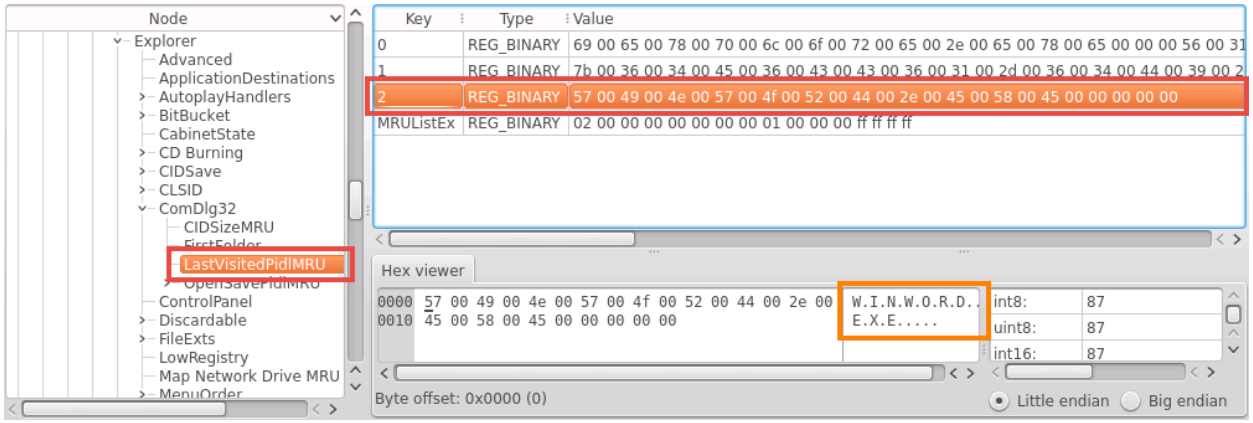
5 Using Fred to Analyze the NTUSER.DAT File

1. Using the *Fred* application, click on **File** and click on **Open hive**.

2. In the *Open registry hive* window, make sure to navigate to **Home/Desktop/Windows Registry** and select the "**informant.NTUSER.DAT**" file.

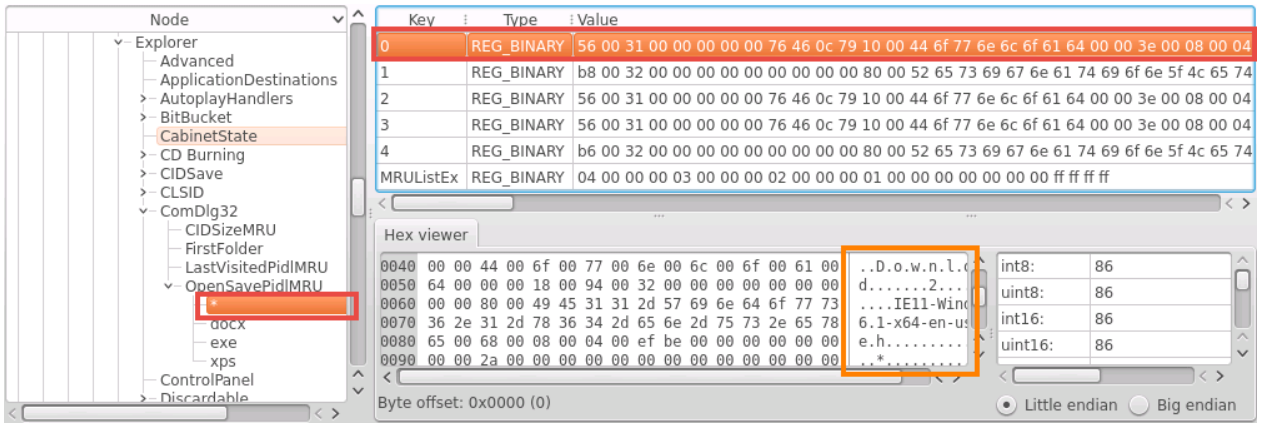


3. In the left pane, navigate to **Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisited PidMRU** to identify the most recently used (*MRU*) items. Click on the **second entry** underneath the *Key* column.



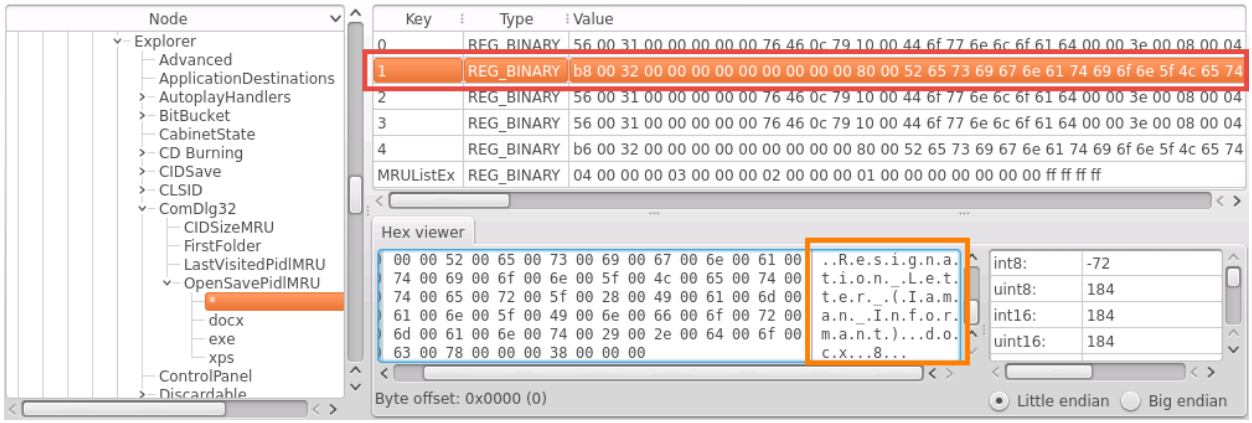
Notice the second entry shows that *WinWord.exe* was opened when looking at the *Hex viewer* details.

4. In the left pane, navigate to **Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSave PidMRU*** to identify the recently saved (*MRU*) items. Click on the **first entry** underneath the *Key* column.



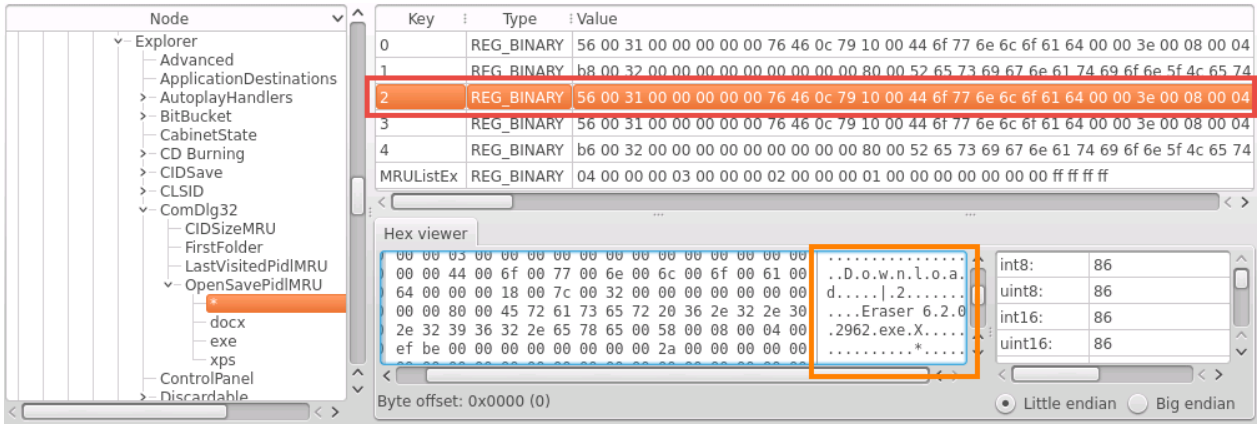
Notice in the *Hex viewer*, entry "*0*" shows that the user, *informant*, downloaded *IE11*.

5. Click on the second entry, "**1**", in the middle pane.



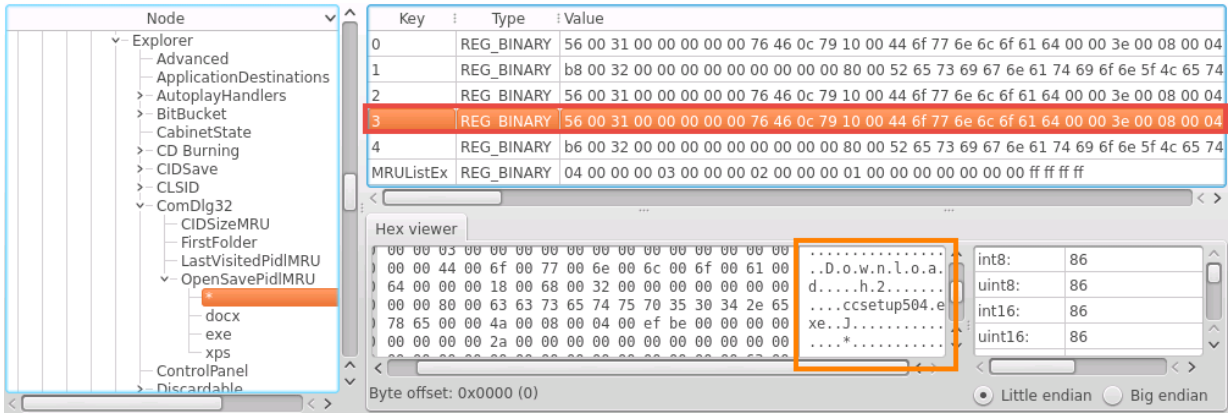
Notice in the *Hex viewer*, entry "*1*" shows that the user, *informant*, either wrote or was reading a resignation letter.

6. Click on the third entry, "**2**", in the middle pane.



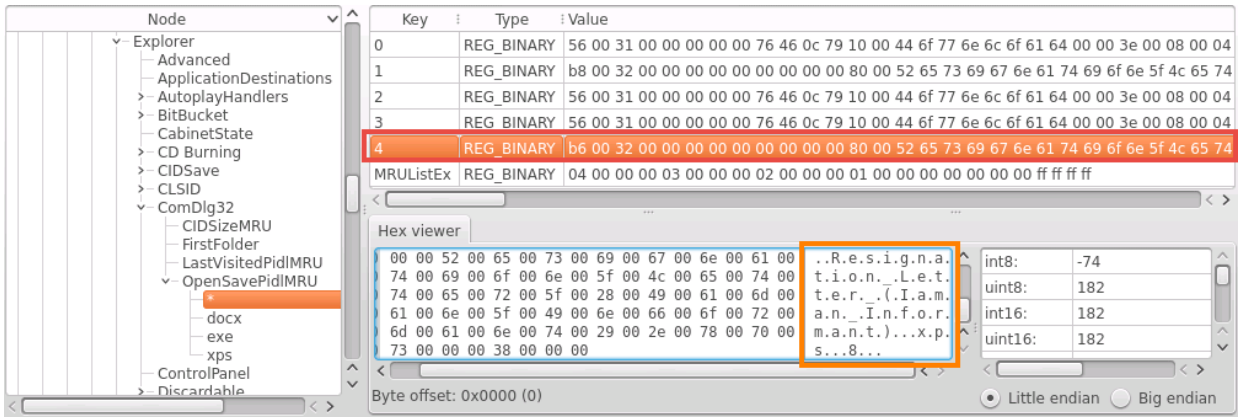
Notice in the *Hex viewer*, entry "*2*" shows that the user, *informant*, downloaded an "*Eraser*" program.

7. Click on the fourth entry, “3”, in the middle pane.



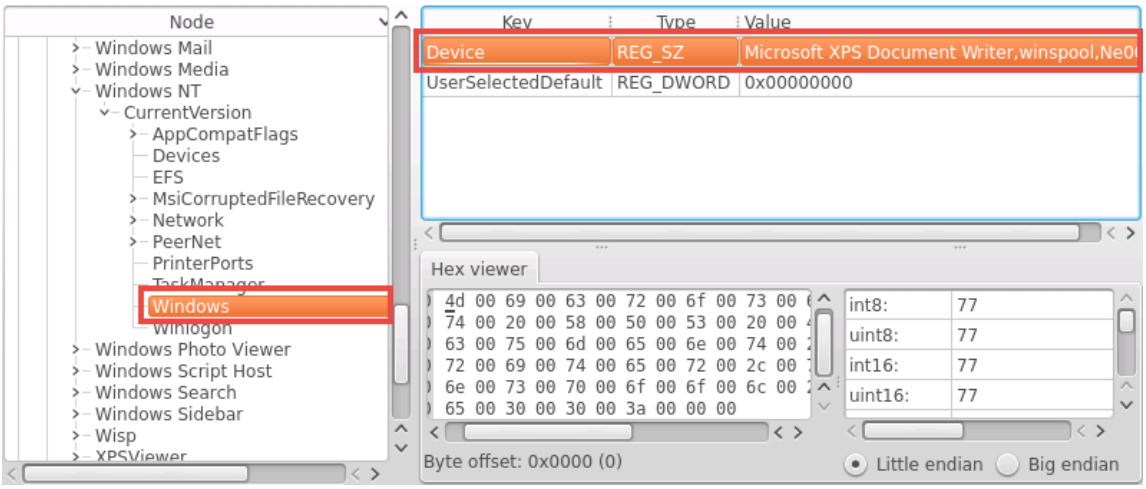
Notice in the *Hex viewer*, entry “*3*” shows that the user, *informant*, downloaded a cleaner program for erasing browser cache.

8. Click on the fifth entry, “**4**”, in the middle pane.



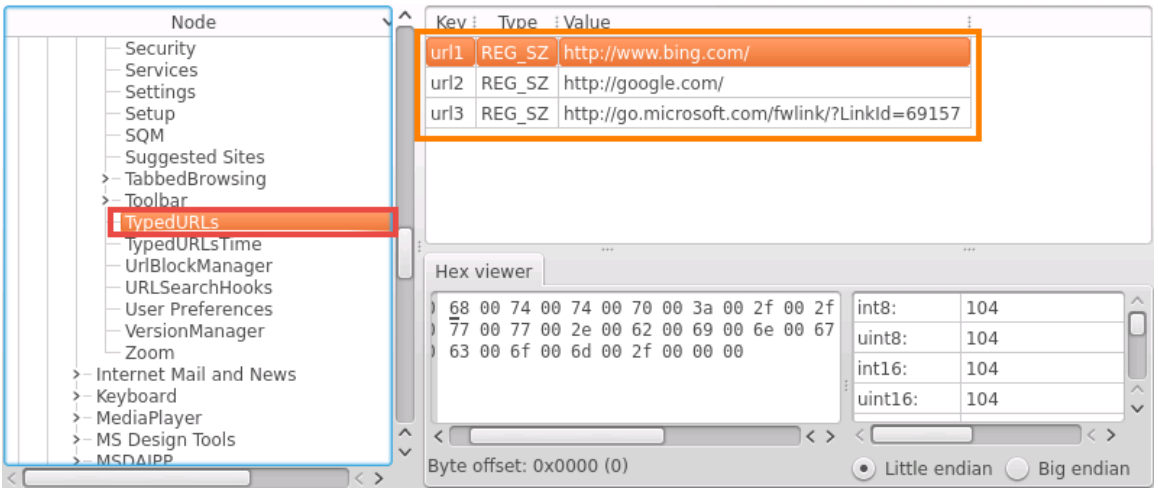
Notice in the *Hex viewer*, entry “*4*” shows that the user, *informant*, saved a resignation letter in *.XPS* format.

9. In the left pane, navigate to **Software\Microsoft\WindowsNT\CurrentVersion\Windows** to identify the default printer. Select the **Device** entry underneath the *Key* column.



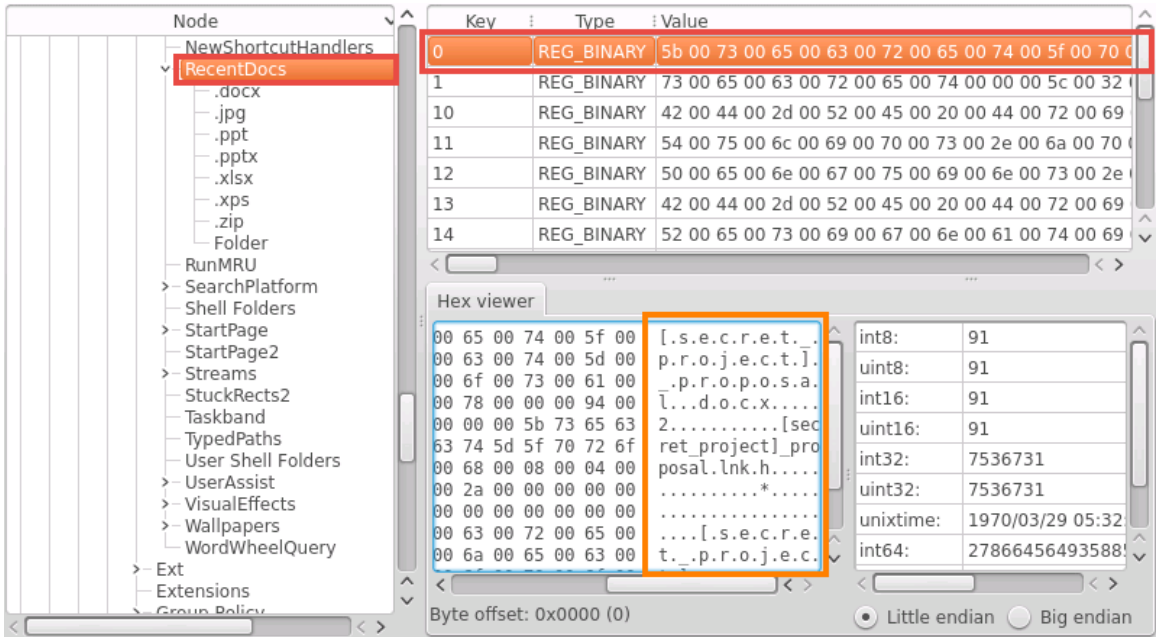
Notice the *Microsoft XPS Document Writer* is the default printer.

10. In the left pane, navigate to **Software\Microsoft\Internet Explorer\TypedURLS** to identify the typed URLs in *IE*, if any.



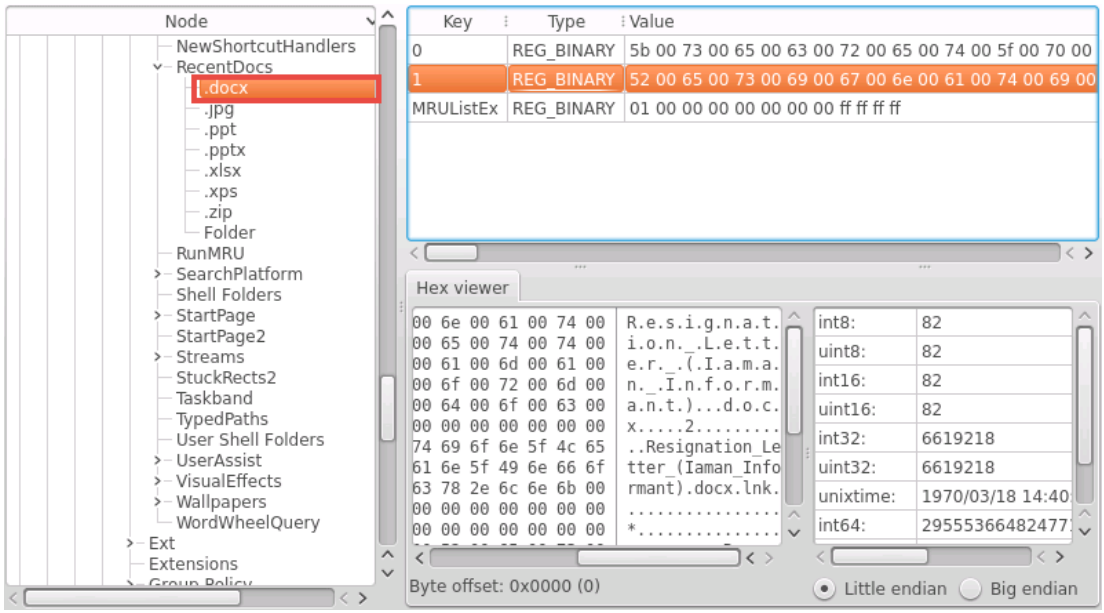
Notice that just two search engine requests appear. This could be due to the eraser software and ccleaner.

11. In the left pane, navigate to **Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs** to identify the documents that may be most recently used. Select the first entry, "**0**", from the middle pane.



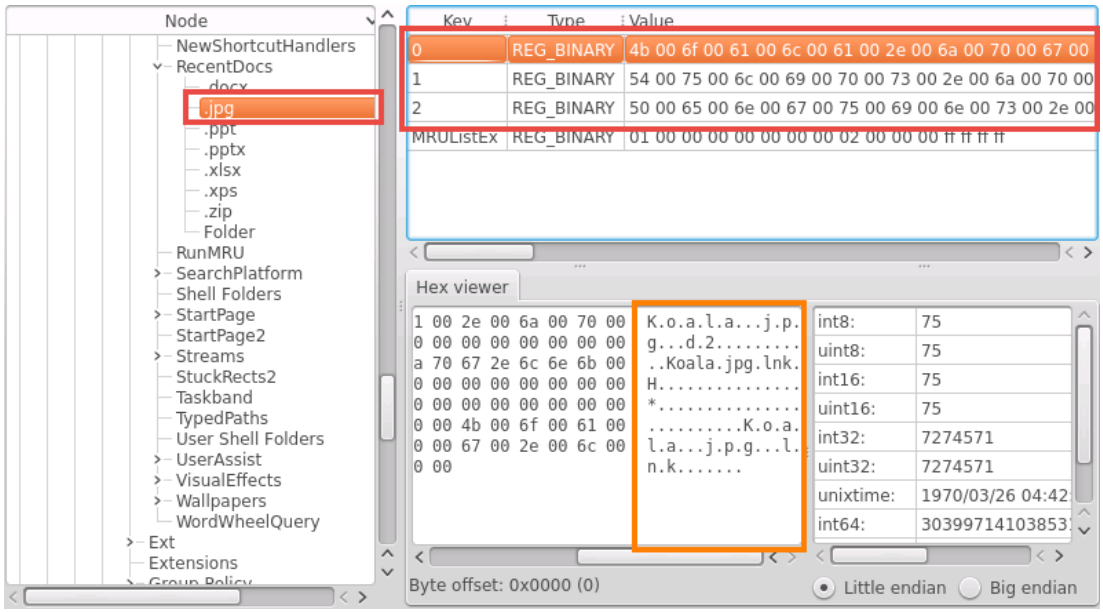
Notice in the *Hex viewer*, entry "*0*" shows a "*secret project proposal.docx*".

12. Organize by different file types, choose **.docx** from the left pane. This helps to only display the *.docx* files types from the *RecentDocs* directory.



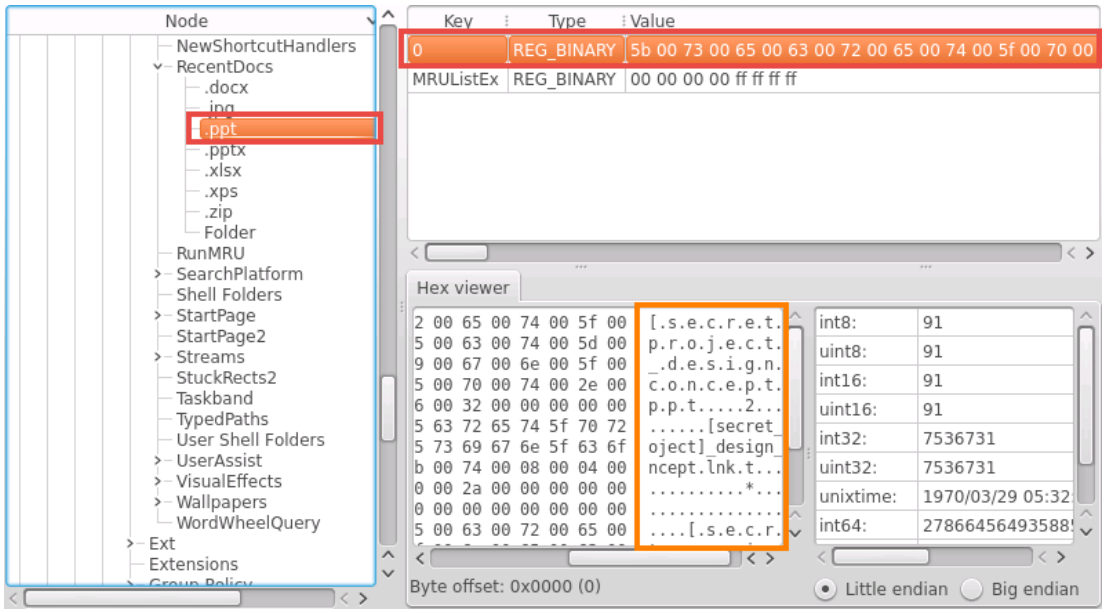
Notice that both the secret project and resignation letter are present.

13. Select **.jpg** from the left pane and analyze the three entries in the middle pane with the *Hex viewer*.



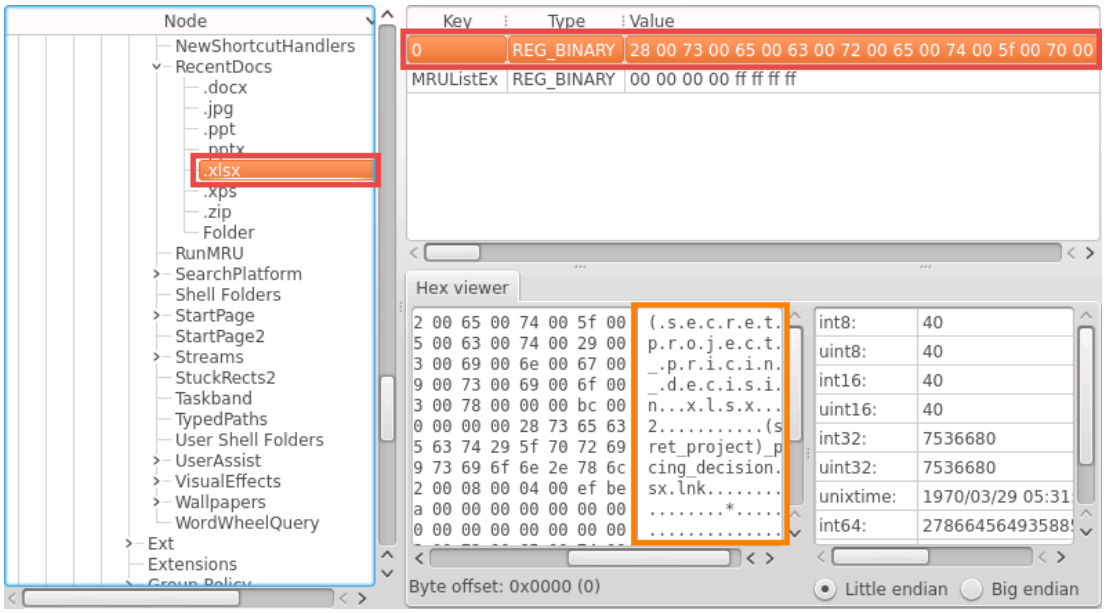
Notice there are three different files present: "*Koala.jpg*", "*Tulips.jpg*", and "*Penguins.jpg*".

14. Select **.ppt** from the left pane and analyze the first entry in the middle pane with the *Hex viewer*.



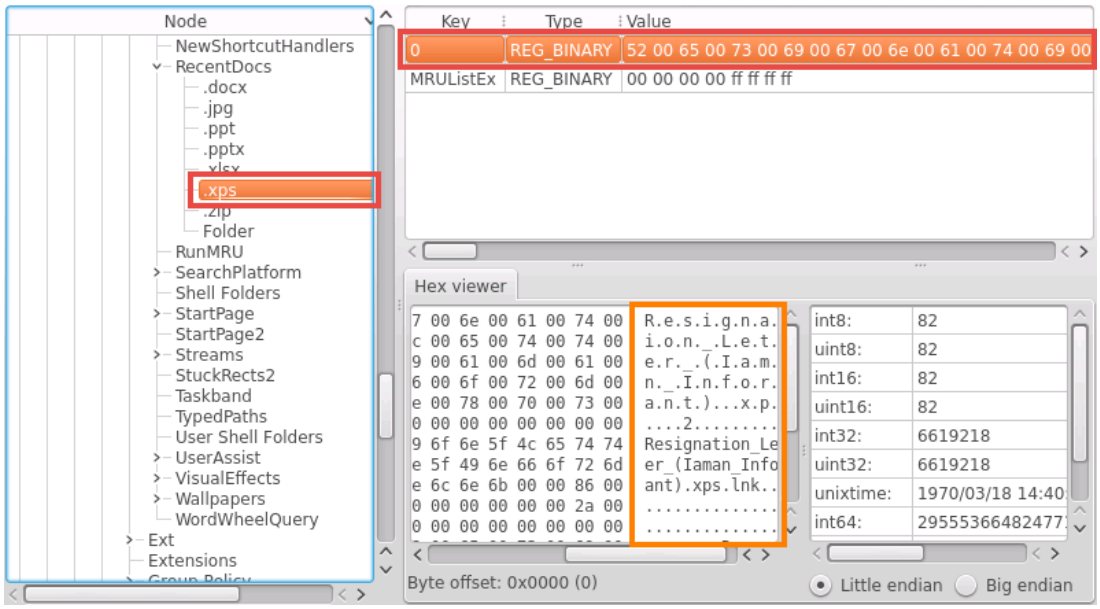
Notice a *PowerPoint* file for a secret project design is present.

15. Select **.xlsx** from the left pane and analyze the first entry in the middle pane with the *Hex viewer*.



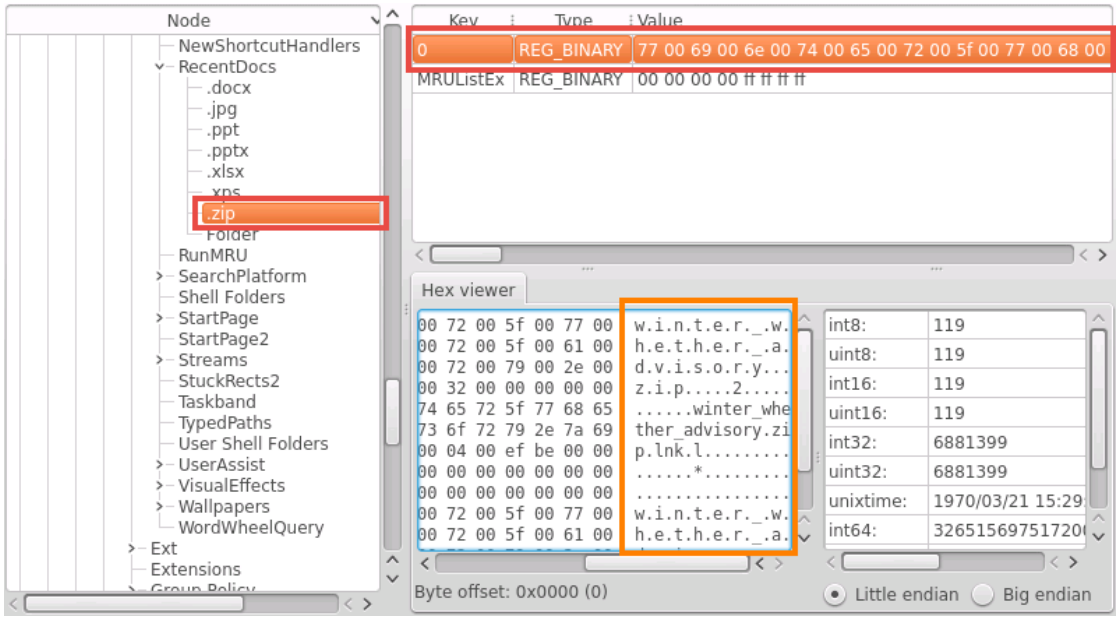
Notice a spreadsheet file for secret project pricing is present.

16. Select **.xps** from the left pane and analyze the first entry in the middle pane with the *Hex viewer*.



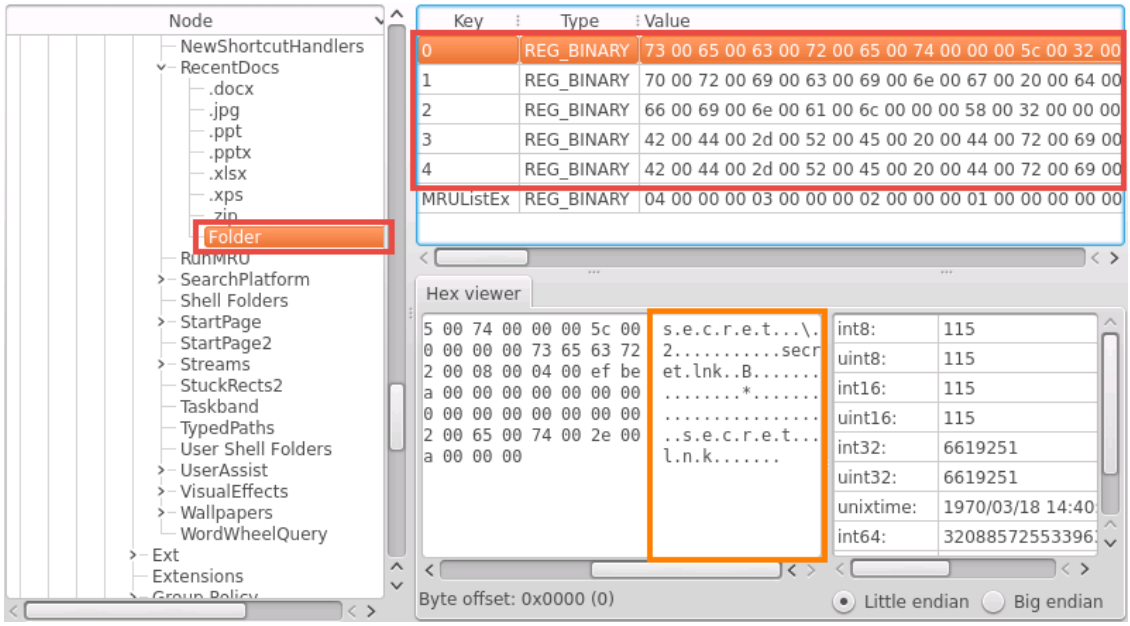
Notice the resignation letter appears.

17. Select **.zip** from the left pane and analyze the first entry in the middle pane with the hex viewer.

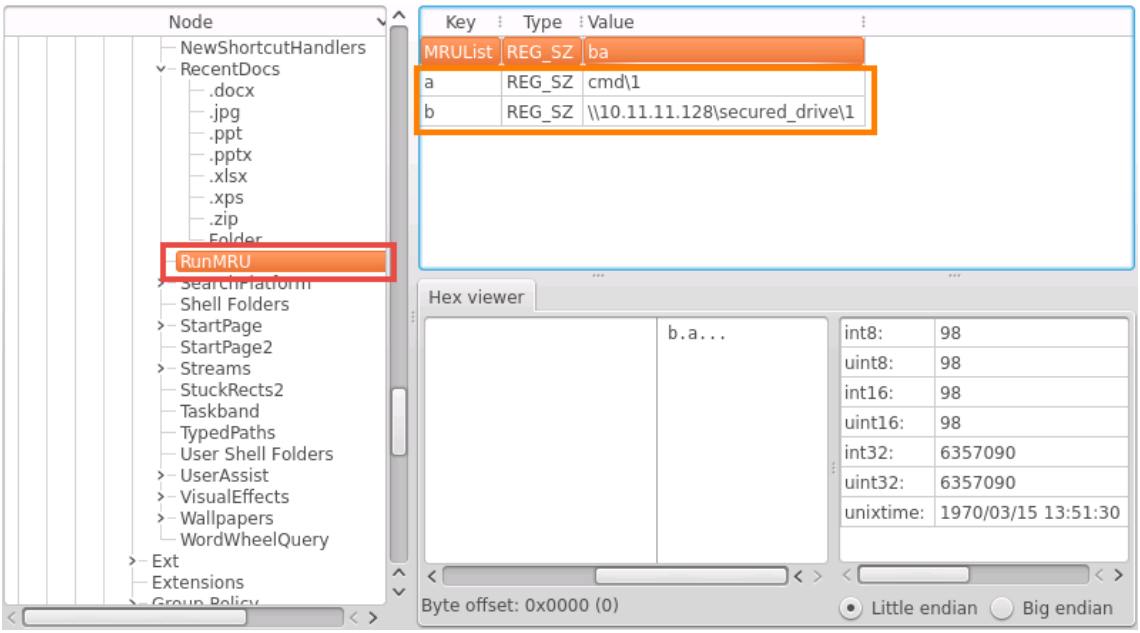


Notice a zip file called "*winter whether advisory*" is present.

18. Select **Folder** from the left pane and analyze the first 5 entries in the middle pane. When going through the entries, notice that there are shortcuts "*lnk*" files to various files found earlier in this lab.

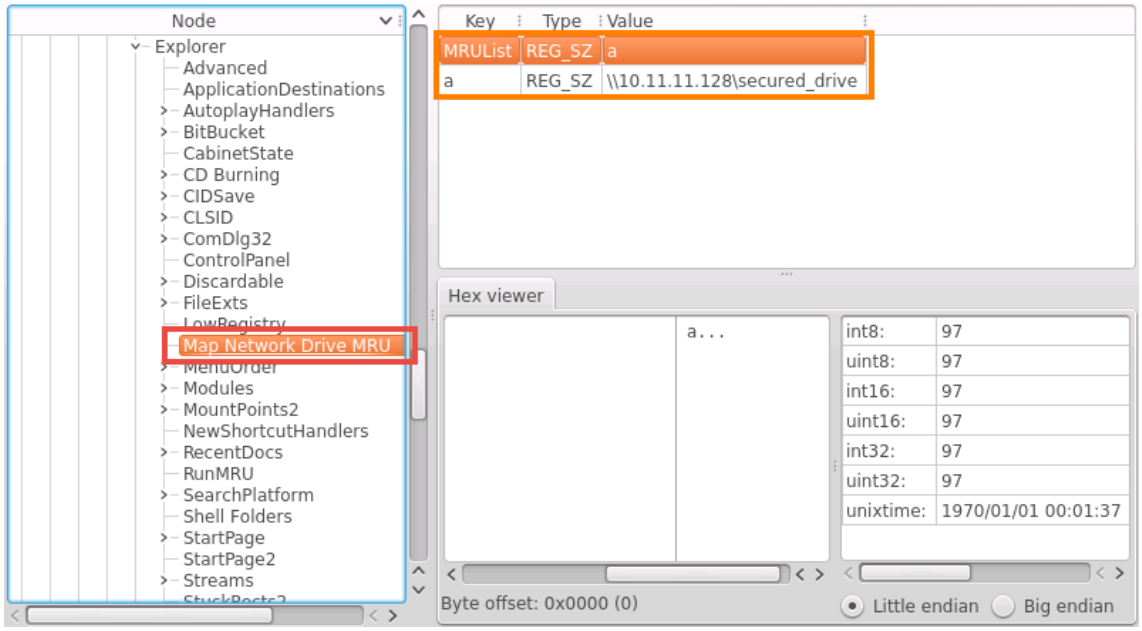


19. In the left pane, navigate to **Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU** to identify whether any commands were run on the system.



Notice that from the command prompt window, it appears that the user mapped a network drive to *10.11.11.128* and named it "*secured_drive*".

20. In the left pane, navigate to **Software\Microsoft\Windows\Explorer\Map Network Drive MRU** to confirm if a network drive was indeed attached.



Notice the registry stores information in several places. There is a lot of data and there are still more keys to explore within the registry itself. Despite the possible use of "*Eraser*" and "*CCleaner*", a number of information can still be retrieved.

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

