Lab Report

Name: Inor Wang
Title: Windows Registry Analysis Lab
Case: 25-T101
Date: 09/12/2025

Table of Contents

Document Revision History

Name	Revision Date	Version	Description
Inor Wang	09/12/2025	0.1	Draft

Executive Summary

On September 12, 2025, Inor Wang turned in a report to Professor Jacob D. Stauffer that was requested, to perform an offline examination of Registry files which have been extracted off a copied image of a machine assigned to **Natasha**. The request was prompted to **strengthen Inor Wang's skills and generate an industry-level report that could be replicated by any examiner**. Within this lab, it is requested to **answer 18 questions** with valid explanations, analysis, and screenshots to prove or disprove hypothesis. All hives were analyzed in Eric Zimmerman's Registry Explorer and AccessData Registry Viewer; evidentiary integrity was preserved using MD5, SHA1, and SHA256 hashes.

Key findings from the examination are as follows:

- **System Configuration:** Current Control Set: ControlSet001 – Time zone: Eastern Time (Bias 300 / ActiveTimeBias 240 -> UTC-5 with DST) – Hostname: WIN-S550ED416l9 – Last standard shutdown: 2012-07-17 15:59:47
- **Security Posture:** Windows Defender service present and set to start automatically, not disabled by policy; automatic remediation off. Any actions require administrator approval.
- **Python Information:** Python 2.7 installed in directory, C:\Python27\, with PyWin32-217 – Install window bracketed by last-writes: 2012-06-13 12:58:09–13:11:24 UTC.
- **Accounts & Authentication:** Local accounts: Administrator, Guest, Natasha – Natasha (RID 0x3E8 = 1000): user with Administrator privileges, enabled; 7 logons; last logon 2012-07-17 21:00:58 UTC; password last set 2011-06-06 20:35:00 UTC; no expiration configured – Most recent user: Natasha (most recent F-value logon timestamp).
- **User Application Activity:** Browsers executed: Internet Explorer, Firefox, Chrome. By focus time, Internet Explorer was used most (1:51:15), then Firefox (1:10:19), Chrome (~0:27:01) – Email: Default client Mozilla Thunderbird (used in 2011). Subsequent behavior indicates webmail via Internet Explorer, first typed URL "http://gmail.com/", suggesting Gmail as the active platform at seizure time. – TypedURLs include gmail.com, ucla.edu, roman-empire.net, 172.16.53.138. – RunMRU shows cmd executed via Start => Run.

- **Network Configuration:** Primary NIC: DHCP enabled; last leased IP 172.16.53.141; lease obtained 2012-07-17 21:00:35 UTC (aligned with key last-write).

The registry artifacts conclusively answer the client's questions about configuration, security tooling, user behavior, software installation, and networking. Evidence shows Windows Defender active, Python 2.7 installed mid-June 2012, Natasha as the primary and most recent user, and a DHCP-assigned address (172.16.53.141) at the time of interest. All findings are derived from hashed, verifiable registry paths and reproducible queries.

The methods and results of this investigation should be considered in the context of learning how to navigate the Registry keys to find actionable insights into investigations.

Synopsis

A set of Windows Registry artifacts was provided for offline analysis to **answer defined investigative questions about a seized workstation**. The Registry is a primary source of historical and configuration data (system state, user accounts, software, services, network, and usage traces). The client requested a step-by-step, reproducible workflow with annotated screenshots and explicit Registry paths supporting each finding.

Client Questions:

1. Which ControlSet is the current control set?
2. What is this computer's timezone set to at the time of seizure?
3. What is its assigned computername?
4. When was it last shutdown through standard shutdown procedures?
5. Based on analysis of current services installed on this computer, would you say it's likely or unlikely that this computer was protected with Windows Defender at the time it was seized? Explain.
6. How many Registry keys/sub-keys were last written on the day the computer was last shutdown? Provide an explanation and/or screen print to support your conclusion.
7. What version of Python is likely installed on this computer? Explain.
8. When do you think it was installed?
9. What use accounts are configured on the system?
10. Provide the following information pertaining to the Natasha user account:
    a. Privilege level (i.e. user vs. admin)
    b. How many times logged on
    c. Last logon date/time
    d. When the password was last changed
    e. Is the password set to expire? If so, when?
    f. Is the account enabled or disabled?
11. What user account was the last one to log in? Explain
12. What web browsers did the Natasha user account use? Which was used the most?
13. What email client do you think the Natasha user account used? Explain.
14. What URLs did the Natasha account type in?

15. What did the Natasha account open via the Start => Run line?
16. Does it appear the computer was ever associated with a wi-fi network? Explain.
17. Is this computer configured to obtain an IP address via DHCP? Explain.
18. What was its last IP address?

Scope of Work:

- Acquisition of the forensic image from Professor Stauffer in the UTSA Canvas website.
- Analysis of offline hives using either Registry Explorer or Registry Viewer.
- Verification of evidentiary integrity using MD5, SHA1, and SHA256 cryptographic hashes.

Evidence Analyzed

This section provides details of the digital evidence collected

Evidence ID	**E001**
Name	registry-hive-capture.zip
Type	Zip archive data, at least v2.0 to extract, compression method=deflate
Size	9,543,680 bytes (9.1MB)
MD5	A1E5678C67FBA65AD69D27FC6ABDC0A3
SHA1	88595F161C5D6EF24AC9D00C4D6F29831F6B6330
SHA256	2C0C651A71B7448B9D422399C41E3A88779830725D706836128A1346F3635978

Tools Used

Workstation

Hostname	Operating System	Build	Physical / Virtual	Built
IS-4523-001-WINDOWS	Windows 11	2021	Virtual	09/06/2025

Software

Name	Version	Release	Purpose
Registry Explorer (Eric Zimmerman)	2.0	Apr 2022	Used to parse Windows Registry artifacts
Registry Viewer (AccessData)	2.0.0	Nov 2017	Used to parse Windows Registry artifacts

Analysis Findings

Overview of Examination Procedures

The forensic analysis of the provided Registry hives (SAM, SYSTEM, SOFTWARE, SECURITY, DEFAULT, and NTUSER.DAT under Natasha's users folder) was analyzed within **Registry Viewer** and **Registry Explorer**. The evidence collected was provided by Professor Stauffer in an .zip folder. The evidence was verified via **MD5, SHA1, and SHA256 hashes** to maintain integrity.

Additional targeted analysis was performed using:

- **Registry Explorer (Eric Zimmerman's tool)** → to analyze Windows Registry keys.
- **AccessData Registry Viewer** → to analyze Windows Registry keys.

Throughout the process, all findings were documented, and cryptographic hash values were maintained for validation.

Evidence Reviewed

1. **Registry Hive Capture folder (E001)**: Full hive capture of the computer.

Key Findings

1. Which ControlSet is the current control set?

- **Analysis Performed:**
  - The system hive was analyzed through the AccessData Registry Viewer application.
  - As you can see in Figure 1, the system had two control sets, "ControlSet001" and "ControlSet002". From there, I clicked on the Select key and the value of **Current = "0x00000001 (1)"** which indicates that the **current control set is ControlSet 001**.
  - Path: *system\Select*
- **Answer:**
  The current control set is **ControlSet001**.

- **Supporting Evidence:**

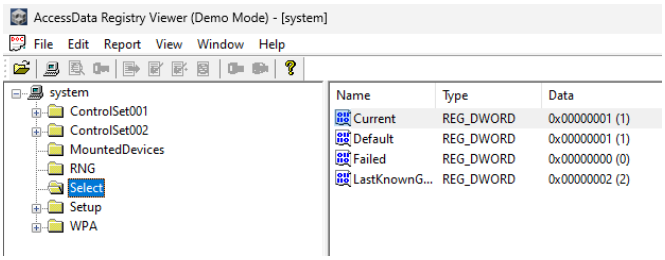

Figure 1. Registry Viewer of the System hive showing the current control set

2. What is this computer's timezone set to at the time of seizure?

- **Analysis Performed:**
  - The system hive was analyzed through the AccessData Registry Viewer application.
  - Within the Select registry key, it contained multiple registry values such as, **TimeZoneKeyName**, which is set to **Eastern Standard Time (UTC).**
  - The registry value, **Bias**, is set to "**0x0000012C (300)**", which corresponds UTC-5. The 300 represents 300 minutes which corresponds to 5 hours hence UTC-5.
  - The registry value, **ActiveTimeBias**, is set to "**0x000000F0 (240)**".
  - Path: *system\ControlSet001\Control\TimeZoneInformation*
- **Answer:**

  Natasha's computer's timezone was set to **UTC-5, with daylight savings enabled.**

- **Supporting Evidence:**

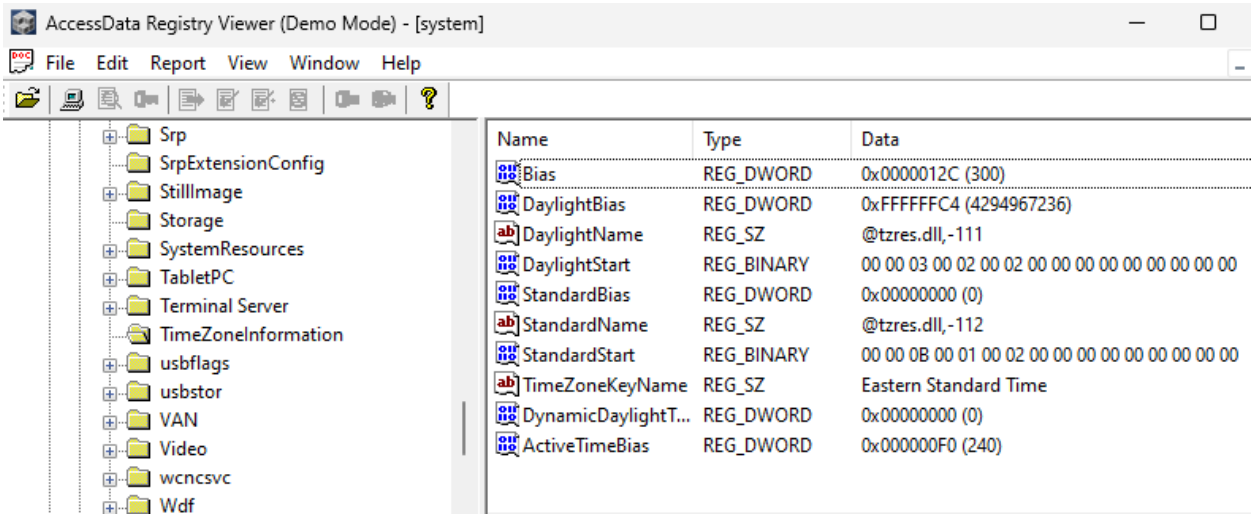

Figure 2. Registry Viewer of the System hive showing the TimeZoneInformation registry key

3. What is the assigned computername?

- **Analysis Performed:**
  - The system hive was analyzed through the AccessData Registry Viewer application.
  - Within the ComputerName registry key, it contained the **ComputerName** registry value of "**WIN-S550ED416I9**", which is the computer name.
  - Path: *system\ControlSet001\Control\ComputerName\ComputerName*
- **Answer:**

  The assigned computer name is "**WIN-S550ED416I9**".

- **Supporting Evidence:**

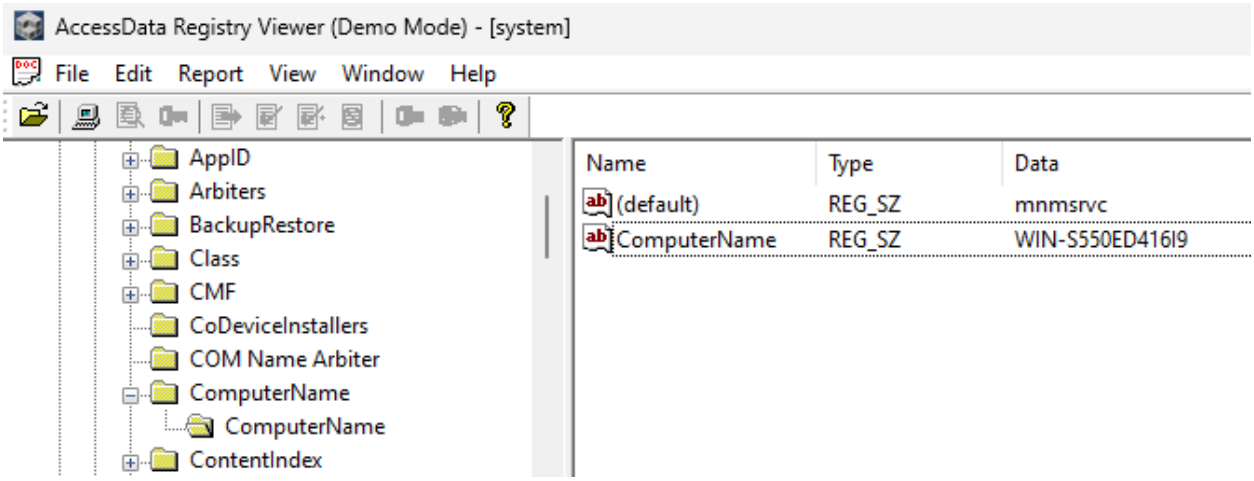

Figure 3. Registry Viewer of the System hive showing ComputerName registry key

4. When was it last shutdown through standard shutdown procedures?

- **Analysis Performed:**

- The system hive was analyzed through the AccessData Registry Viewer application.
- Within the Windows registry key, the **ShutdownTime** registry value shows the last shutdown through standard shutdown procedures which is, "**1A C3 49 19 5F 64 CD 01**". The value is in little-endian hex.
- After using OSINT resources, the examiner discovered a Powershell command to convert the hex (after reversing the bytes since it is in little-endian) to a readable date time format which is shown in Figure 5.
- Path: *system\ControlSet001\Control\Windows*

- **Answer:**

  The last shutdown through standard shutdown procedures was "**07/17/2012 15:59:47**" also known as, "**July 17, 2012 at 3:59:47 pm**".

- **Supporting Evidence:**

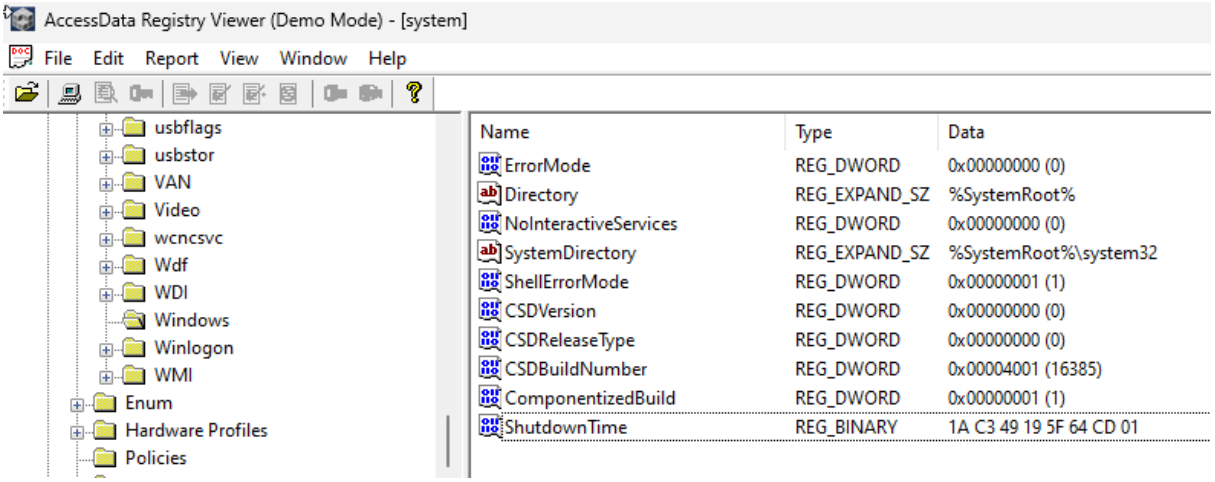

Figure 4. Registry viewer of the system hive showing the Windows registry key

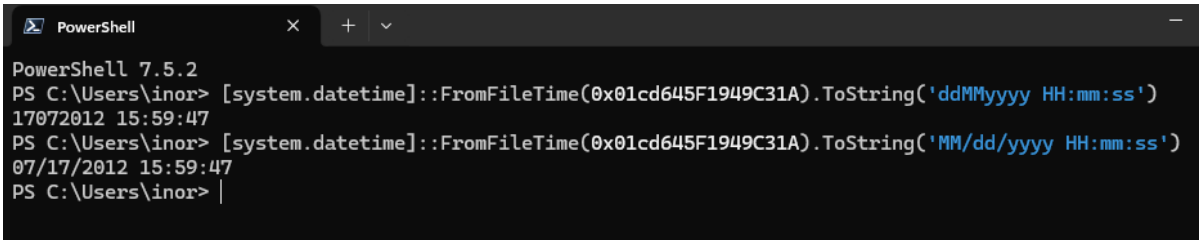

Figure 5. Powershell command to convert FileTime to date time

5. Based on an analysis of current services installed on this computer, would you say it's likely or unlikely that this computer was protected with Windows Defender at the time it was seized? Explain.

- **Analysis Performed:**
  - The system and software hives was analyzed through the AccessData Registry Viewer application.

- In Figure 6, it shows the registry value, "**Start**", which is set to "**0x000000002 (2)**", which means the service is set to start **automatically** at boot.
- In Figure 7, it shows the registry value, "**Windows Defender**", which is set to "**0x00000000 (0)**", which means Windows Defender is **NOT** disabled. Additionally, the registry value, "**DisableRoutinelyTakingAction**", which is set to "**0x00000001 (1)**", which means Windows Defender is set to **NOT automatically** take actions.
- Figure 6's path: system\ControlSet001\services\WinDefend
- Figure 7's path: software\Microsoft\Windows Defender

- **Answer:**

  It is likely that this computer was protected with Windows Defender at the time it was seized and the Start registry value being enabled however, Windows Defender the registry value, DisableRoutinelyTakingAction, is enabled. **Therefore, the computer was protected with Windows Defender and is set to start automatically however, it will only detect and alert, leaving the decision to the computer administrator.**

- **Supporting Evidence:**

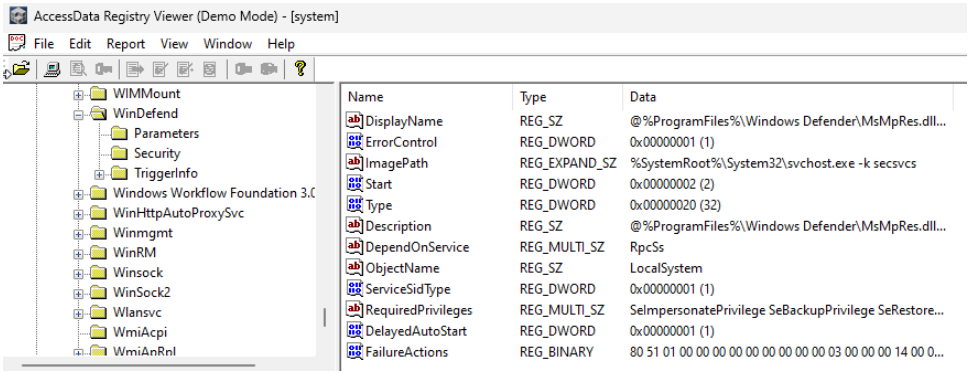

Figure 6. Registry viewer of the system hive showing the WinDefend registry key

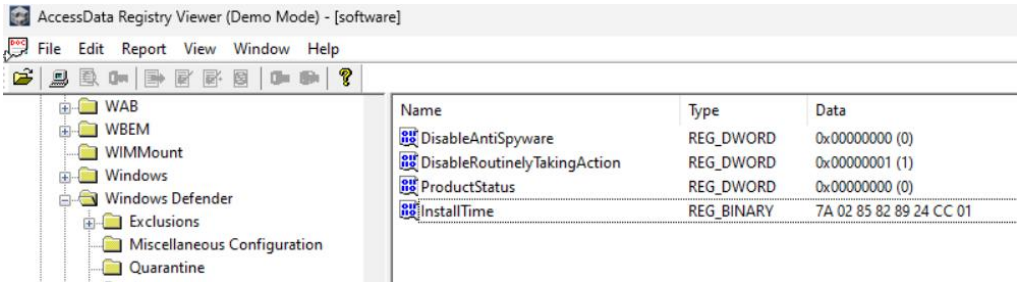

Figure 7. Registry viewer of the software hive showing the Windows Defender registry key

6. How many Registry keys/sub-keys were last written on the day the computer was last shutdown? Provide an explanation and/or screen print to support your conclusion.

- **Analysis Performed:**
  - The default, SAM, SECURITY, software, system, and Natasha's NTUSER.DAT hives was analyzed through the Eric Zimmerman's Registry Explorer application.

- After figuring out what the last shutdown date was in question 4, the examiner loaded all of the hives into Registry Explorer and used the Find feature.
- Within the Find feature, the examiner set the earliest last write timestamp to "**2012-07-17 00:00:00**" and the latest to "**2012-07-17 23:59:59**", in order to find all of the registry keys/sub-keys that were written on that day.
- The bottom of the Find feature showed how many search hits there were which was **5,423**.

- **Answer:**

  There were **5,423 registry keys/sub-keys** last written on the day (2012-07-17) the computer was last shutdown. After loading the default, SAM, SECURITY, software, system, and Natasha's NTUSER.DAT hives, using the Find feature, the examiner determined that there were 5,423 registry keys/sub-keys found as shown in Figure 8.

- **Supporting Evidence:**

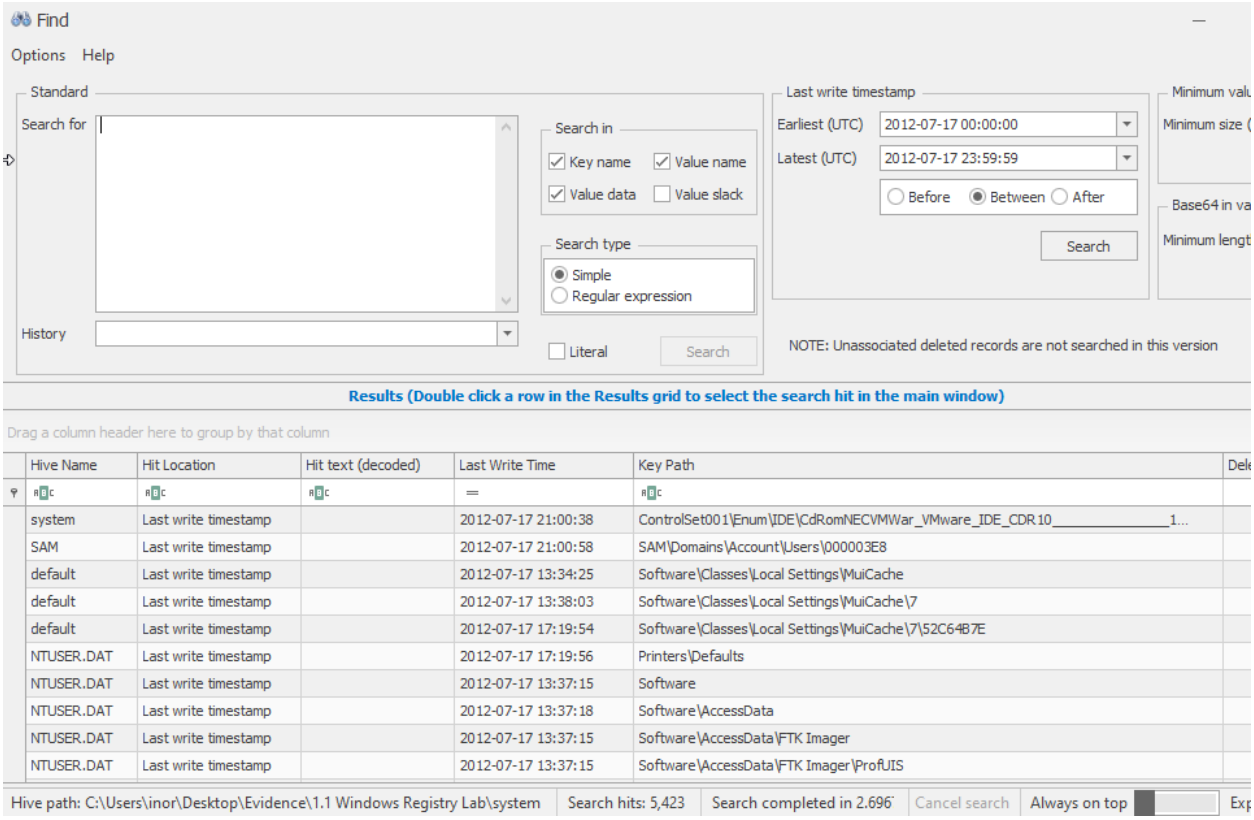

Figure 8. Registry Explorer's Find feature showing the amount of registry keys/sub-keys on 2012-07-17

7. What version of Python is likely installed on this computer? Explain.

- **Analysis Performed:**
  - The software hive was analyzed through the AccessData Registry Viewer application.

- In Figure 9, it shows the InstallPath registry key with a (default) registry value set to "**C:\Python27**\", which is the installation directory of Python.
- In Figure 10, it shows the **pywin32-py2.7** registry key with the Uninstall String registry value set to: ("C:\Python27\Removepywin32.exe" -u "C:\Python27\pywin32-wininst.log").
- Figure 9's path: *system\Python\PythonCore\2.7*
- Figure10's path: *software\Microsoft\Windows\CurrentVersion\Uninstall\pywin32-217*

- **Answer:**

  Due to the presence of the InstallPath registry key, we can confirm that **Python 2.7** was installed. Furthermore, the registry key within the uninstall registry keys, "*software\Microsoft\Windows\CurrentVersion\Uninstall\pywin32-py2.7*", indicates that the **PyWin32-217** extension was also installed. Therefore, **Python 2.7 with PyWin32-217** was installed.

- **Supporting Evidence:**

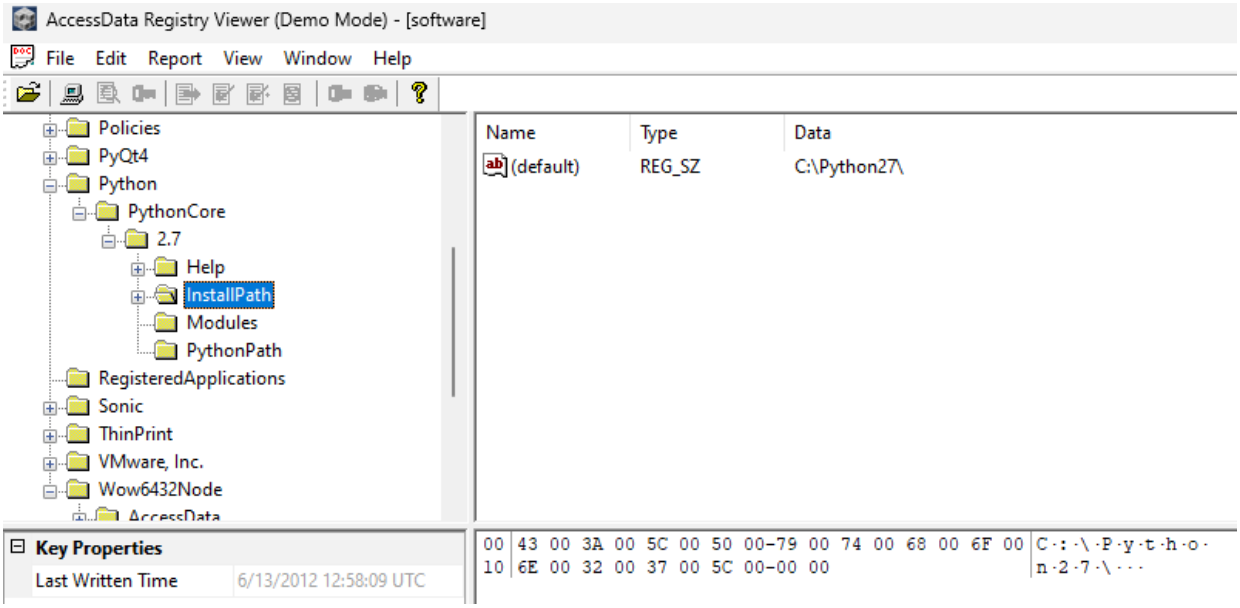

Figure 9. Registry viewer of the software hive showing the InstallPath registry key

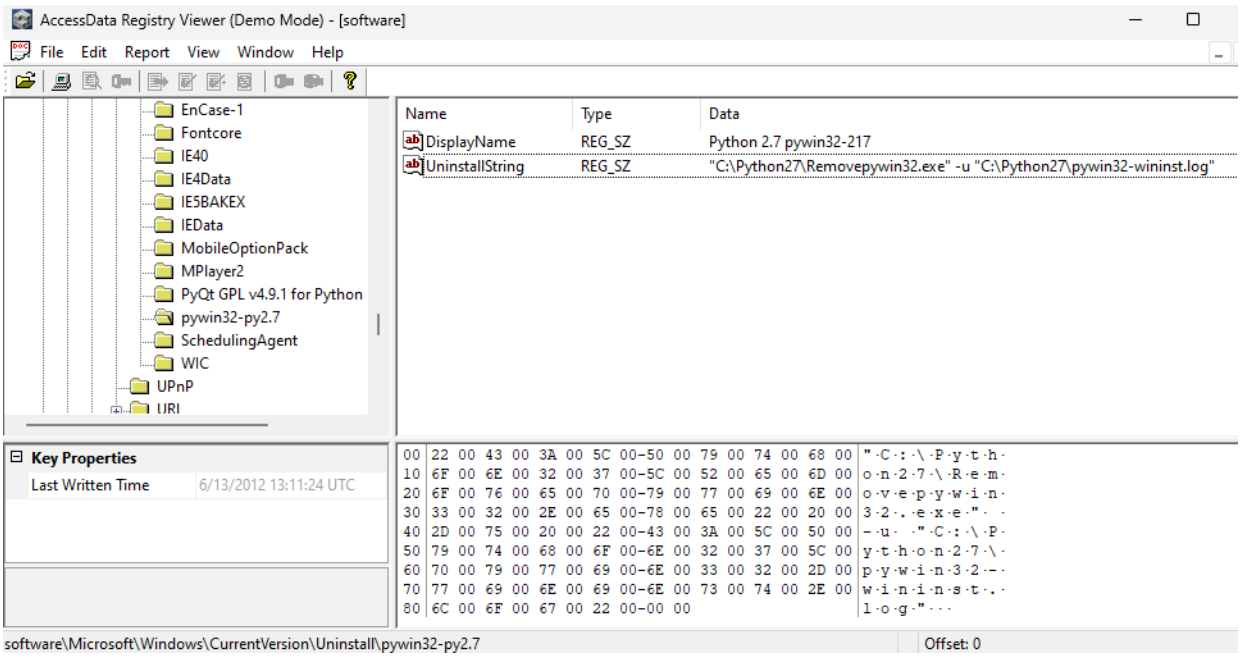

Figure 10. Registry viewer of the software hive showing the pywin32-py2.7 registry key.

8. When do you think it was installed?

- **Analysis Performed:**
  - The software hive was analyzed through the AccessData Registry Viewer application.
  - The last written time of the InstallPath registry key that specifies the Python directory during the beginning of installation is "**6/13/2012 12:58:09 UTC**".
  - The last written time of the Uninstall registry key that specifies the Python uninstaller command during the end of installation is "**6/13/2012 13:11:24 UTC**".
  - Figure 11's path: *system\Python\PythonCore\2.7*
  - Figure12's path: *software\Microsoft\Windows\CurrentVersion\Uninstall\pywin32-217*
- **Answer:**

  Python was installed from **6/13/2012 12:58:09 UTC** to **6/13/2012 13:11:24 UTC** which is shown from the InstallPath and Uninstaller registry key's last write time as shown in Figure's 11 and 12. The InstallPath key is created during the beginning of installation and specifies the Python directory. The uninstall entry is generated by the Windows installer process and provides an uninstaller command, which is only created after Python is fully installed and registered with the system.

- **Supporting Evidence:**

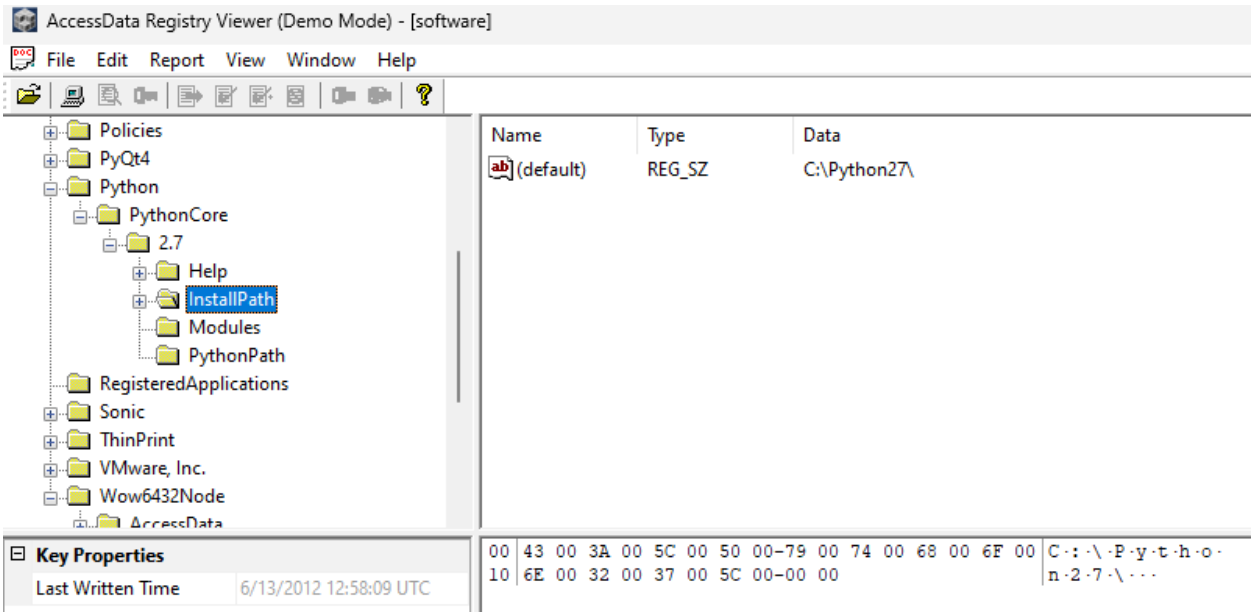

Figure 11. Registry viewer of the software hive showing the InstallPath registry key

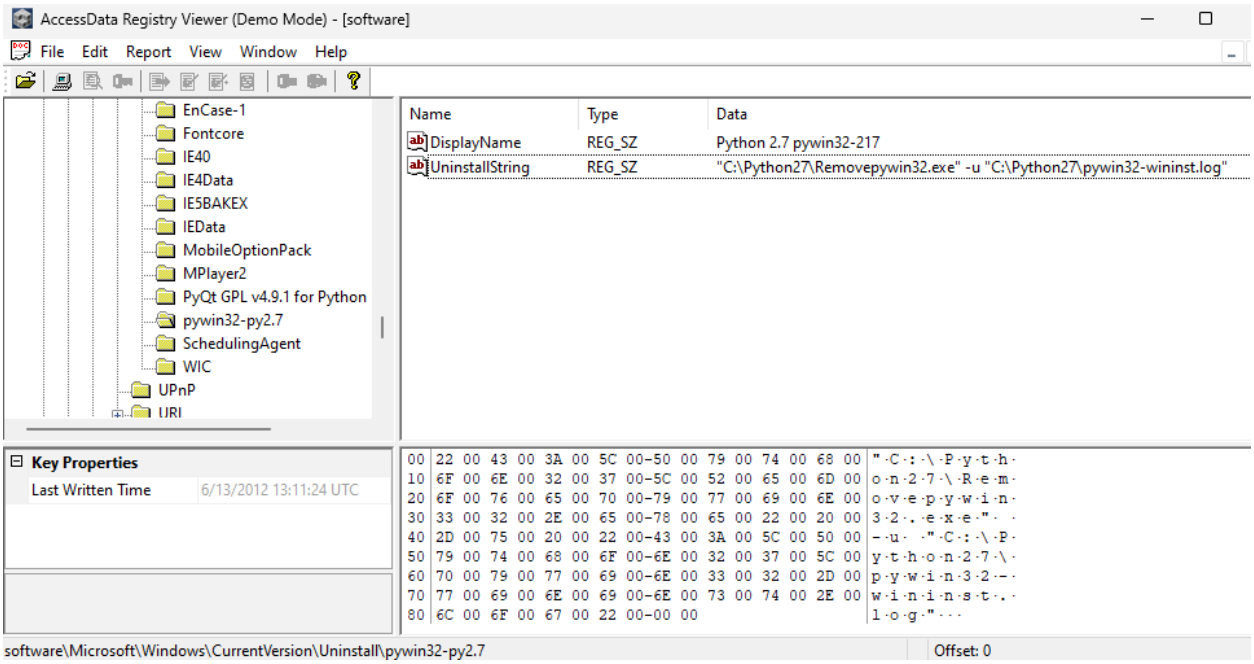

Figure 12. Registry viewer of the software hive showing the pywin32-py2.7 registry key

9. What user accounts are configured on the system?

- **Analysis Performed:**
  - The SAM hive was analyzed through the AccessData Registry Viewer application.
  - Within the Names registry key in the SAM hive, it includes **all the user accounts** that are configured on the system.
  - Path: *SAM\SAM\Domains\Account\Users\Names*
- **Answer:**

  Administrator, Guest, and Natasha are the user accounts that are configured on the system as shown in the Names registry key within the SAM hive shown in Figure 13.

- **Supporting Evidence:**

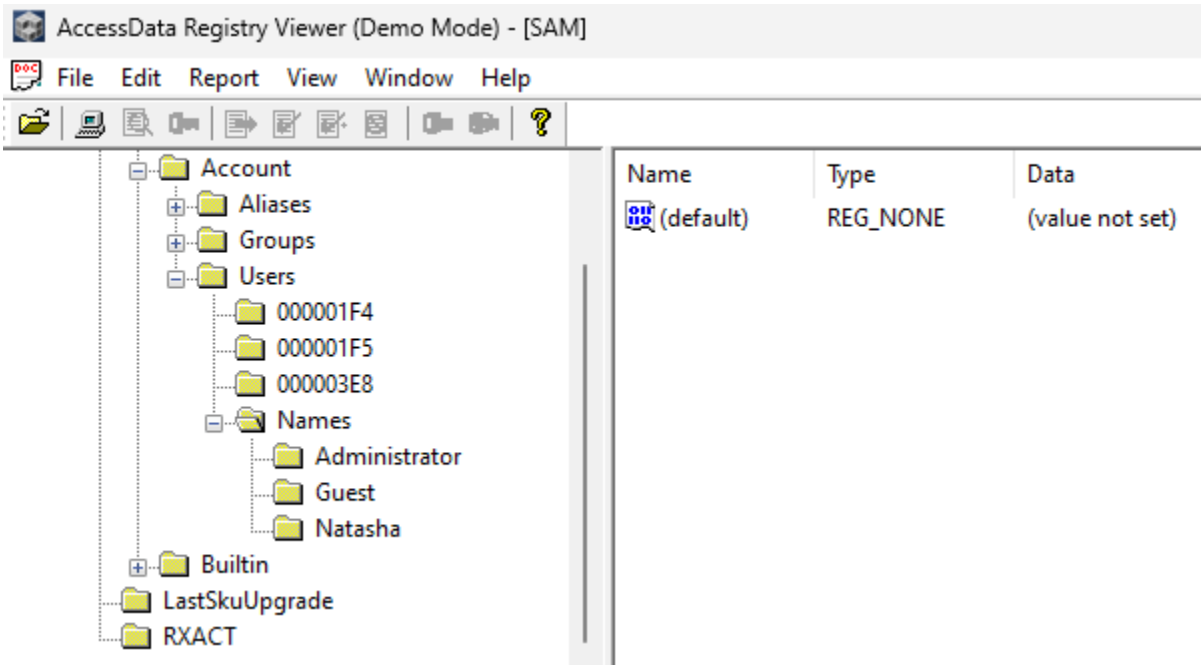

Figure 13. Registry viewer of the SAM hive showing the user accounts configured on the system

10. Provide the following information pertaining to the Natasha user account: a. Privilege level (i.e. user vs. admin) - b. How many times logged on - c. Last logon date/time - d. When the password was last changed - e. Is the password set to expire? If so, when? - f. Is the account enabled or disabled?

- **Analysis Performed:**
  - The SAM hive was analyzed through the AccessData Registry Viewer application.
  - Since Natasha's corresponding RID is 0x3E8, we went to the 000003E8 registry key to find the F and V values.
  - The **F (fixed-length) value** stores critical metadata about the account, including login count, last logon timestamp, password last set timestamp, account expiration, and whether the account is enabled or disabled.
  - The **V (variable-length) value** contains textual and configuration information such as the username, full name, and detailed password policy attributes.
  - Both of these registry values help answer all of these questions which is shown in Figure 14 and 15.
  - Utilized Eric Zimmerman's Registry Explorer's Bookmark to interpret F and V values to understand what Groups was Natasha a part of.
  - Path: *SAM\SAM\Domains\Account\Users\000003E8*
- **Answer:**

  All parts of this question is answered in Figure 14 and 15.

  a. The privilege level of Natasha is **Administrator and Power User**
  b. Natasha logged on **7 times.**
  c. Natasha last logged on at **7/17/2012 21:00:58 UTC**.
  d. Natasha's last password change was on **6/6/2011 20:35:00 UTC.**
  e. Natasha's password is **NOT** set to expire (**Never**).
  f. Natasha's account is **enabled**.

- **Supporting Evidence:**

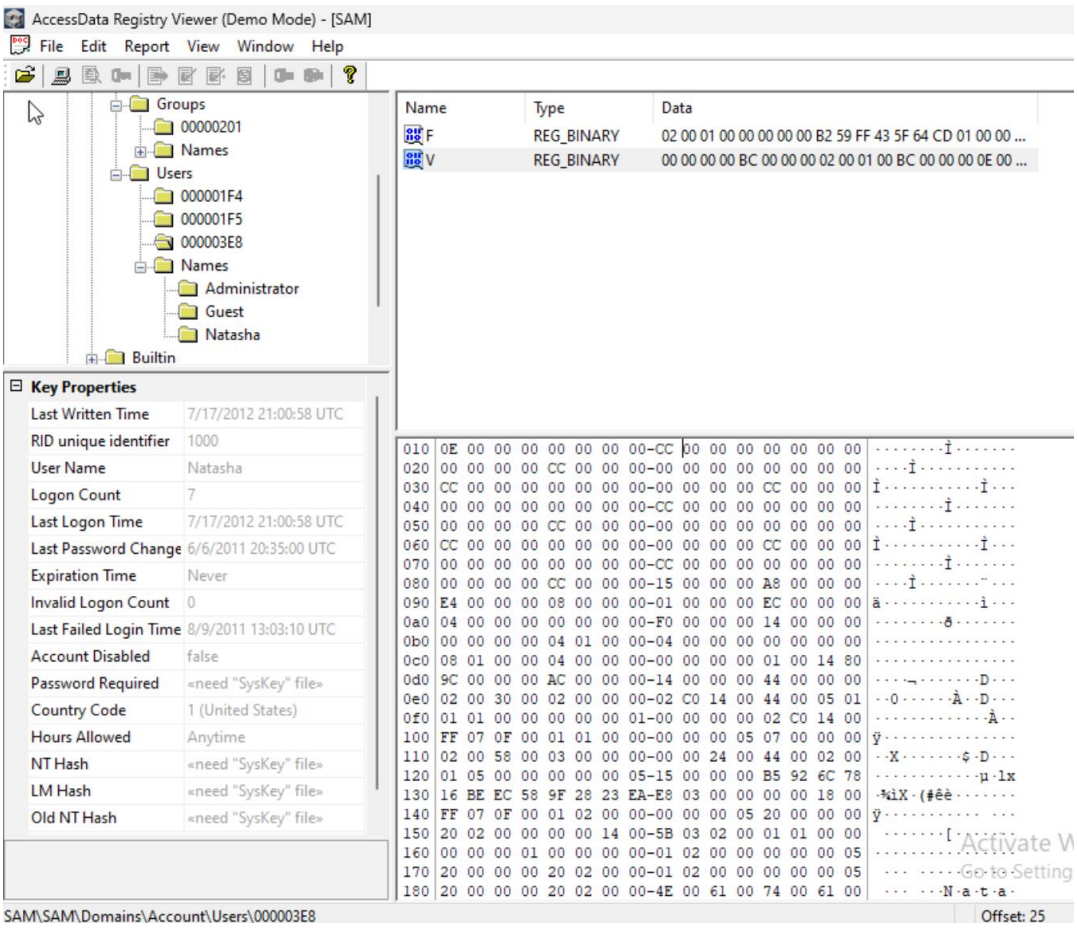

Figure 14. Registry viewer of the SAM hive showing the 000003E8 registry key (Natasha)

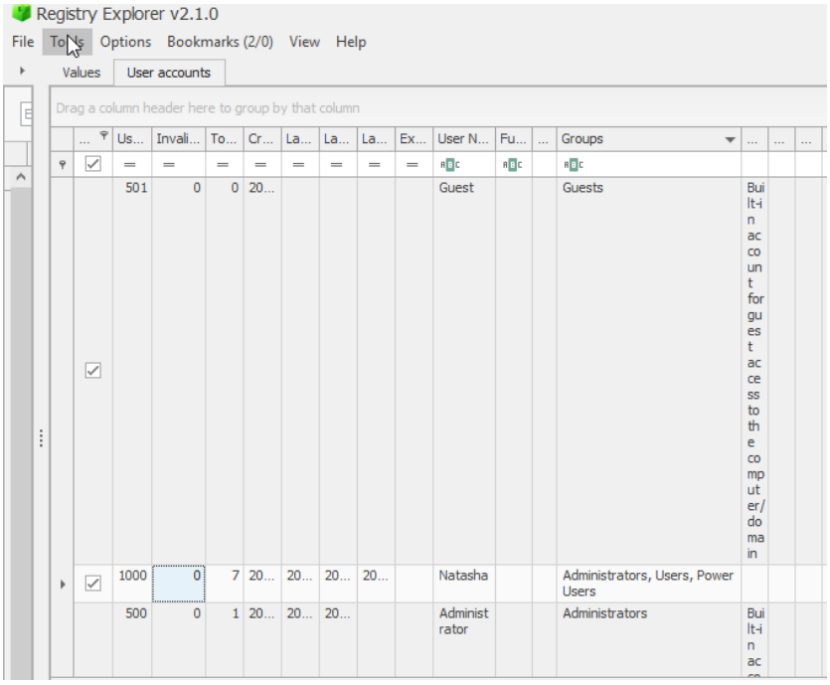

Figure 15. Registry Explorer bookmark for Users of the SAM hive

11. What user account was the last one to log in? Explain.

- **Analysis Performed:**
  - The SAM hive was analyzed through the AccessData Registry Viewer application.
  - The last logon time for the Natasha user account is **7/17/2012 21:00:58 UTC** as shown in Figure 16.
  - The Guest account has **never been logged in** as shown in Figure 17 therefore, the account was not the last one to log in.
  - The last logon time for the Administrator user account is **7/14/2009 5:08:59 UTC** as shown in Figure 18.
  - The LastLoggedOnUser registry value within Authentication and the LogonUI registry sub-key is **Natasha** as shown in Figure 19.
  - Figure 16's Path: *SAM\SAM\Domains\Account|Users\000003E8*
  - Figure 17's Path: *SAM\SAM\Domains\Account|Users\000001F5*
  - Figure 18's Path: *SAM\SAM\Domains\Account|Users\000001F4*
  - Figure 19's Path: *software\Microsoft\Windows\CurrentVersion\Authentication\LogonUI*
- **Answer:**

  The last user account to log in was **Natasha**. This is confirmed by examining the F value in the SAM hive for all user accounts. After examining each F value, the user account with the most recent logon time of all accounts is Natasha (**7/17/2012 21:00:58 UTC**) hence, the last user account to log in was **Natasha**. Additionally, the examiner used Eric Zimmerman's bookmark detailing the LastLoggedOnUser registry value which was **Natasha.**

- **Supporting Evidence:**

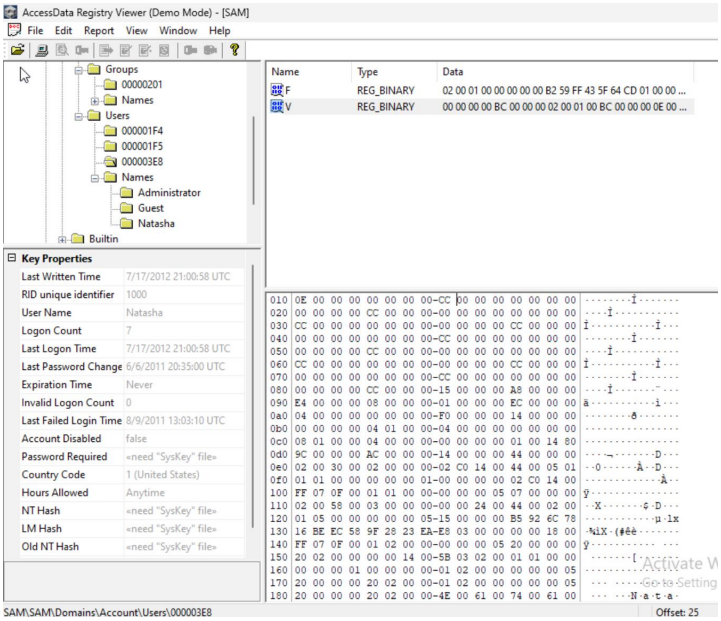

Figure 16. Registry viewer of the SAM host showing the 000003E8 registry key (Natasha)

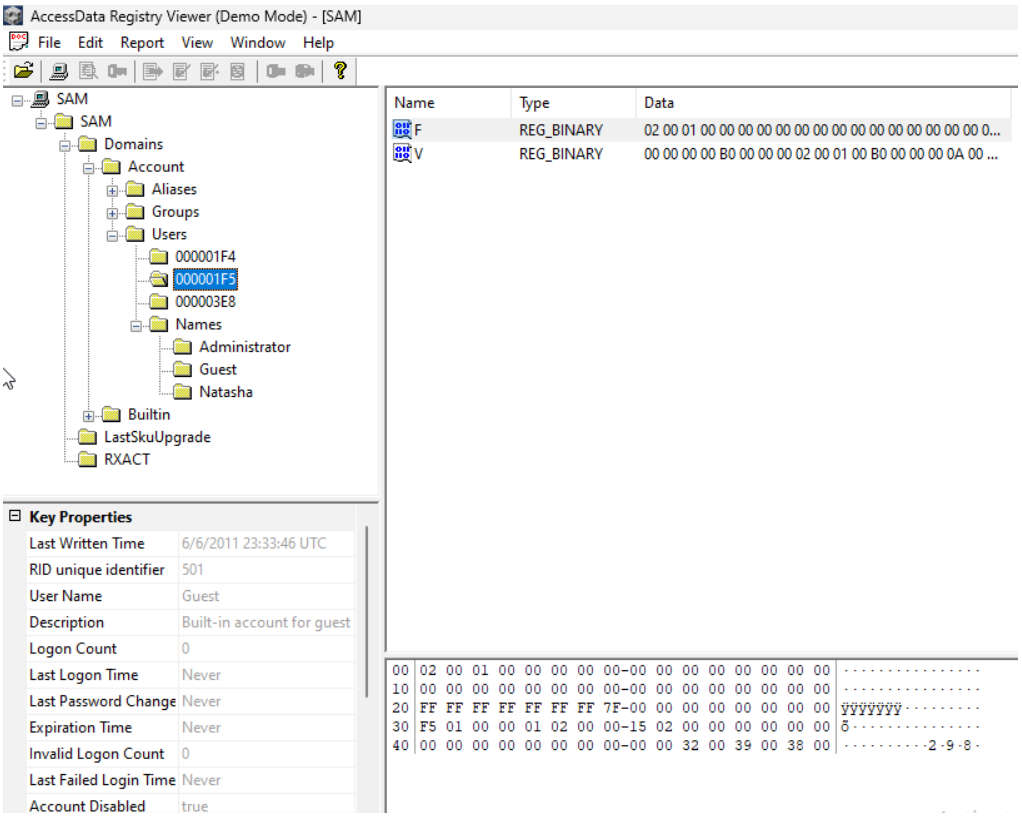

Figure 17. Registry viewer of the SAM host showing the 000001F5 registry key (Guest)

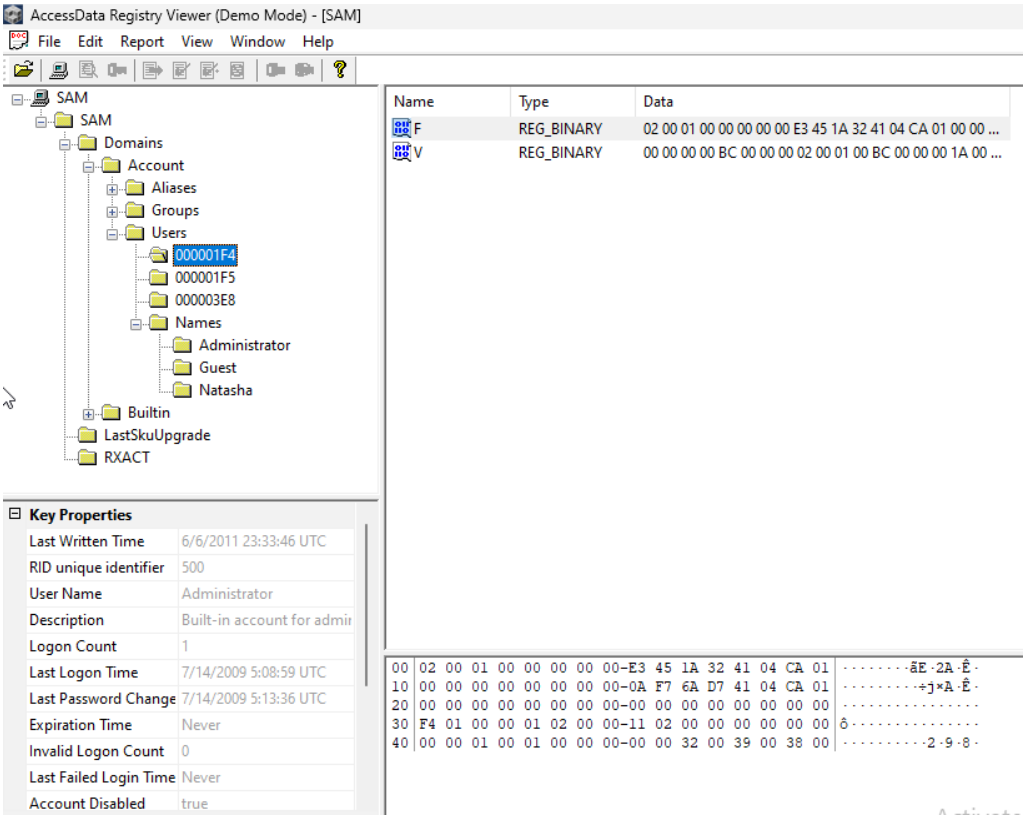

Figure 18. Registry viewer of the SAM hive showing the 000001F4 registry key (Administrator)

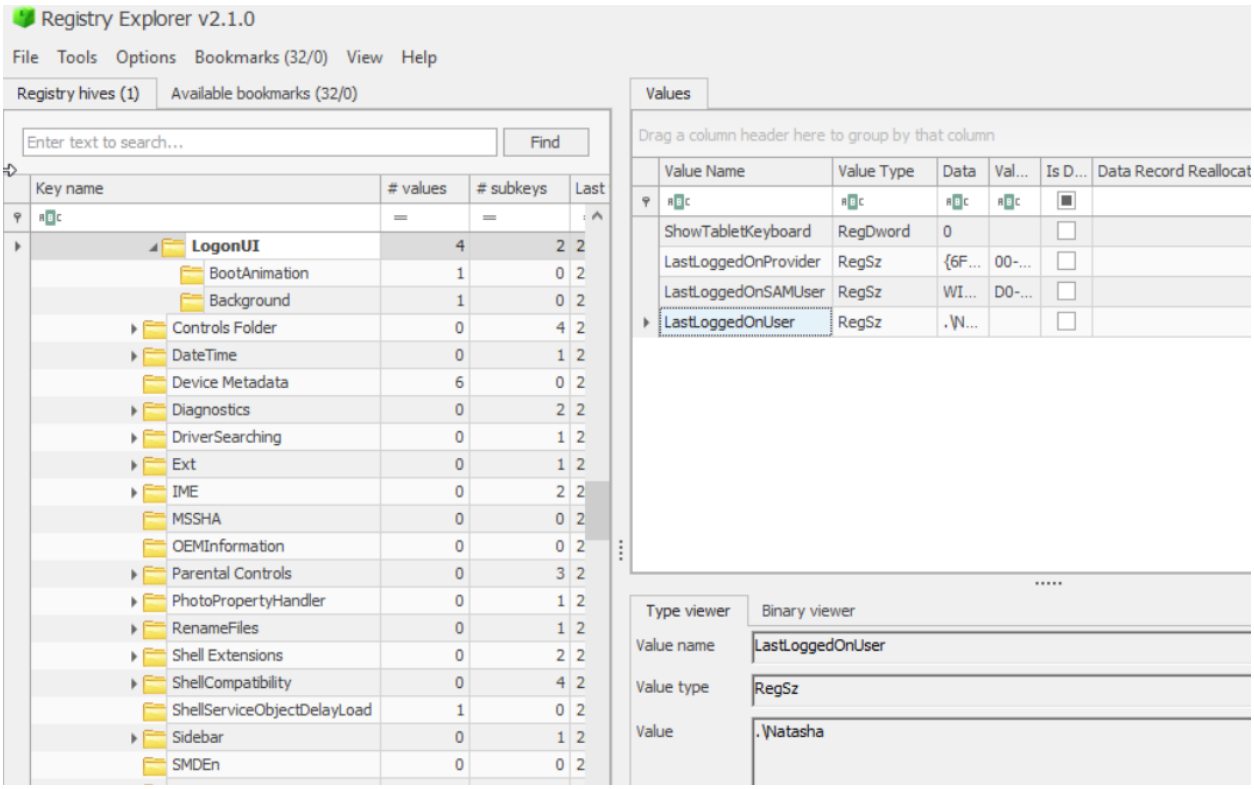

Figure 19. Registry Explorer of the software hive showcasing the LogonUI registry key depicting the LastLoggedOnUser registry value

12. What web browsers did the Natasha user account use? Which was used the most?

- **Analysis Performed:**9
  - Natasha's NTUSER.DAT hive was analyzed through the Eric Zimmerman's Registry Explorer application.
  - When an application is used, it is tracked in UserAssist per user.
  - Within UserAssist, **Internet Explorer, Chrome, and Firefox** was ran.
  - Internet Explorer was ran for **1 hour, 51 minutes, and 15 seconds.**
  - Chrome was ran for **27 minutes and 1 second.**
  - Firefox was ran for **1 hour, 10 minutes, 19 seconds.**
  - Since the Guest user account was never logged on and the Administrator user account was last logged on in 2009, noted in the previous question; **all of the web browsers used was by Natasha.**
  - Path: *software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist*
- **Answer:**

  The Natasha user account used **Internet Explorer, Chrome, and Firefox.** As shown in Figures 20 and 21, the web browser that was used the most was **Internet Explorer** since it's Focus Time was **1 hour, 51 minutes, and 15 seconds**.

- **Supporting Evidence:**

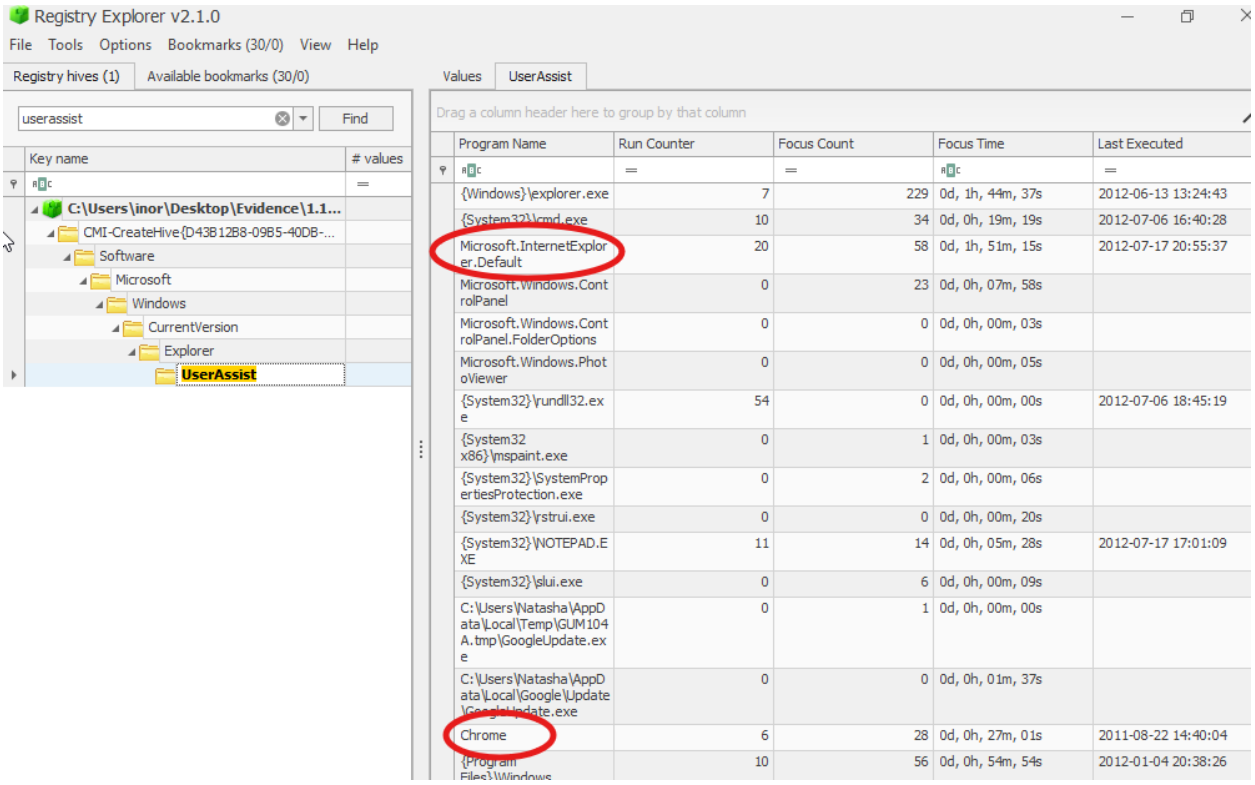

Figure 20. Registry Explorer of the NTUSER.DAT hive showing the UserAssist registry key depicting Internet Explorer and Chrome being used

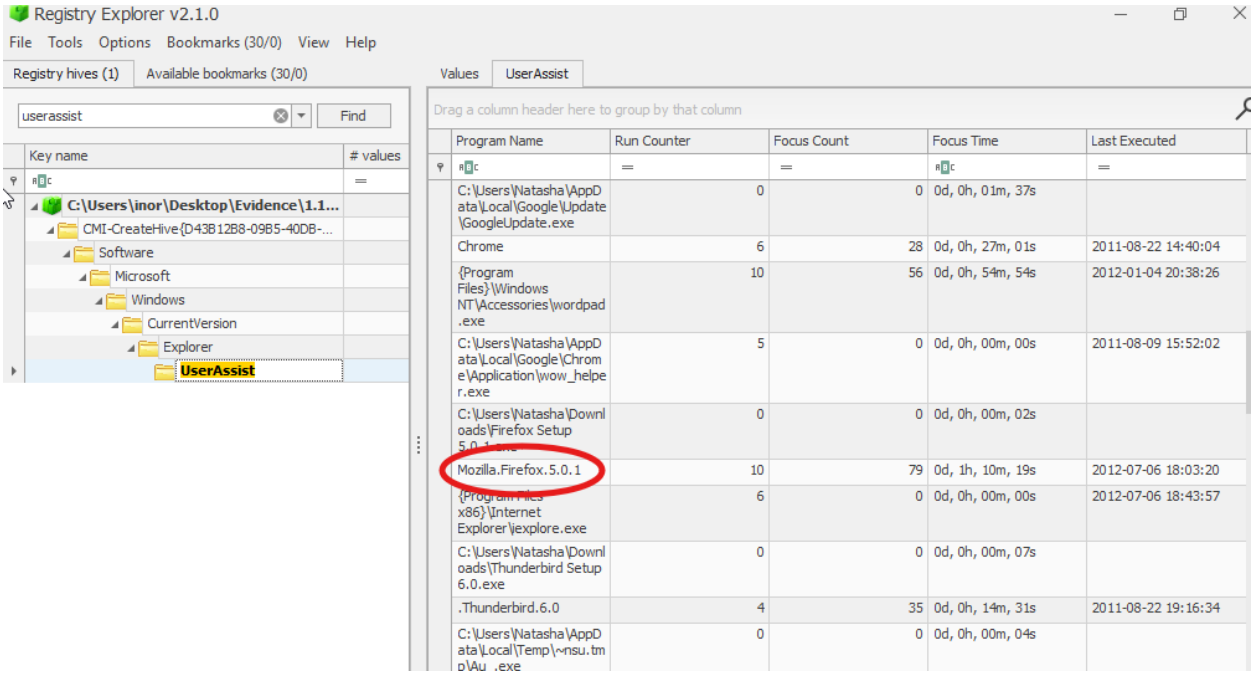

Figure 21. Registry Explorer of the NTUSER.DAT hive showing the UserAssist registry key depicting Firefox being used

13. What email client do you think the Natasha user account used? Explain.

- **Analysis Performed:**
  - Natasha's NTUSER.DAT hive was analyzed both through the AccessData Registry Viewer and Eric Zimmerman's Registry Explorer applications.
  - The default mail client on Natasha's user account is **Mozilla Thunderbird** as shown in Figure 22.
  - Mozilla Thunderbird was used for **14 minutes, and 31 seconds** however, the last execution date was in **2011** as shown in Figure 23.
  - As noted in the previous question, Internet Explorer's last execution date was in **2012**. Therefore, the examiner went to Internet Explorer's TypeURLs registry key to examine if Natasha access a web email client.
  - Natasha's first typed URL in Internet Explorer was **http://www.gmail.com**/.
  - Figure 22's Path: *NTUSER.DAT\Software\Clients\Mail*
  - Figure 23's Path: *NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist*
  - Figure 24's Path: *NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURLs*
- **Answer:**

  The Natasha user account used **Mozilla Thunderbird** as a local email client which is confirmed in the default mail set to Thunderbird as shown in Figure 22. However, the last ran instance of Thunderbird was in 2011 whilst Internet Explorer was in 2012 as shown in Figures 23 and 20. The first typed URL in Internet Explorer was **http://www.gmail.com/** showing that Natasha later relied on Gmail, webmail, via Internet Explorer. **In conclusion, Thunderbird was installed and used earlier, but Gmail through Internet Explorer was likely Natasha's active email platform at the time of seizure.**

- **Supporting Evidence:**

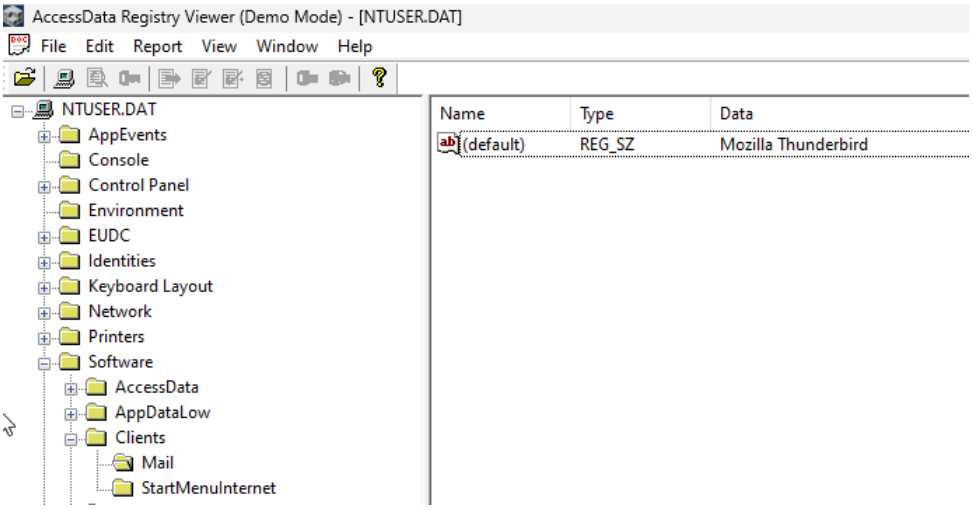

Figure 22. Registry viewer of Natasha's NTUSER.DAT hive showing the Mail registry key

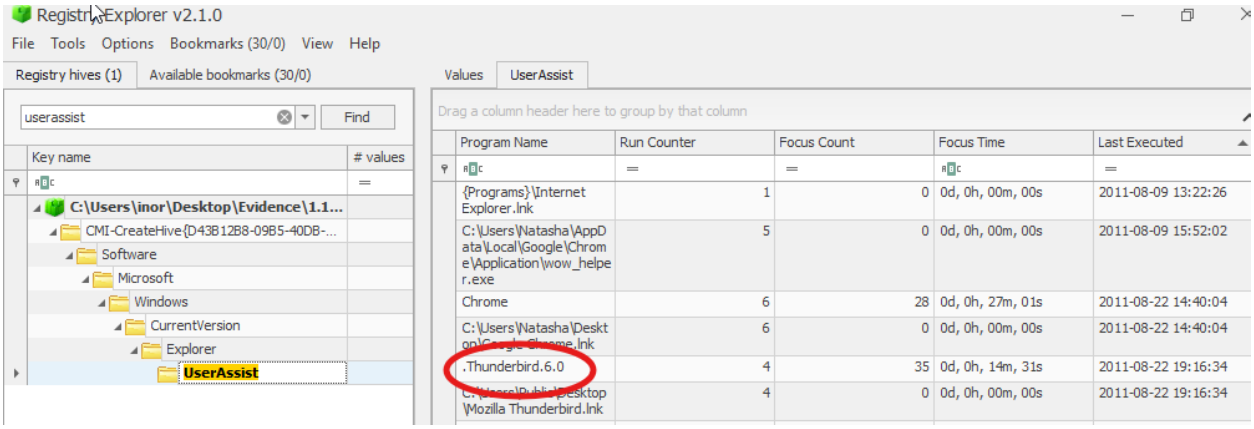

Figure 23. Registry Explorer of Natasha's NTUSER.DAT hive showing the UserAssist registry key depicting Thunderbird

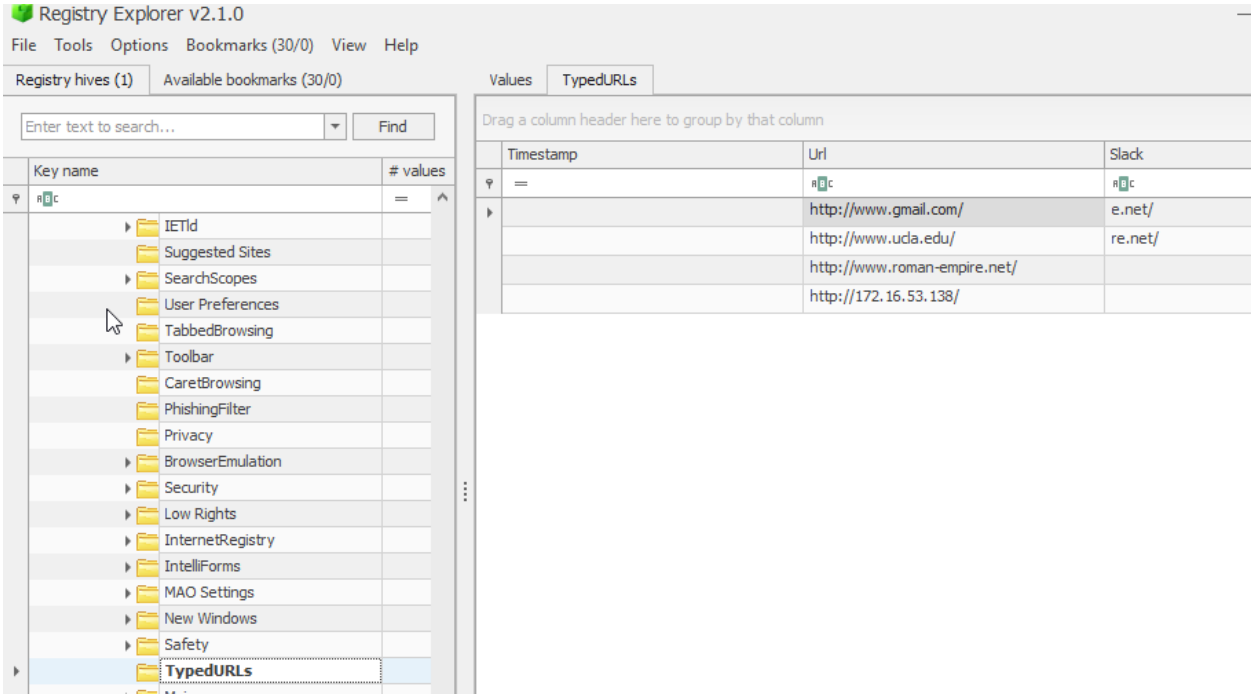

Figure 24. Registry Explorer of Natasha's NTUSER.DAT hive showing the TypedURLs registry key of Internet Explorer

14. What URLs did the Natasha account type in?

- **Analysis Performed:**

- Natasha's NTUSER.DAT hive was analyzed through the Eric Zimmerman's Registry Explorer application.
- Within the **TypedURLs registry key**, it resides all of the URLs that the user typed in, in Internet Explorer.
- Path: *NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURLs*

- **Answer:**

  The Natasha account typed in the following URLs: **"http://www.gmail.com/", "http://www.ucla.edu/", "http://www.roman-empire.net/", and "http://172.16.53.138/"** as shown in Figure 25.

- **Supporting Evidence:**

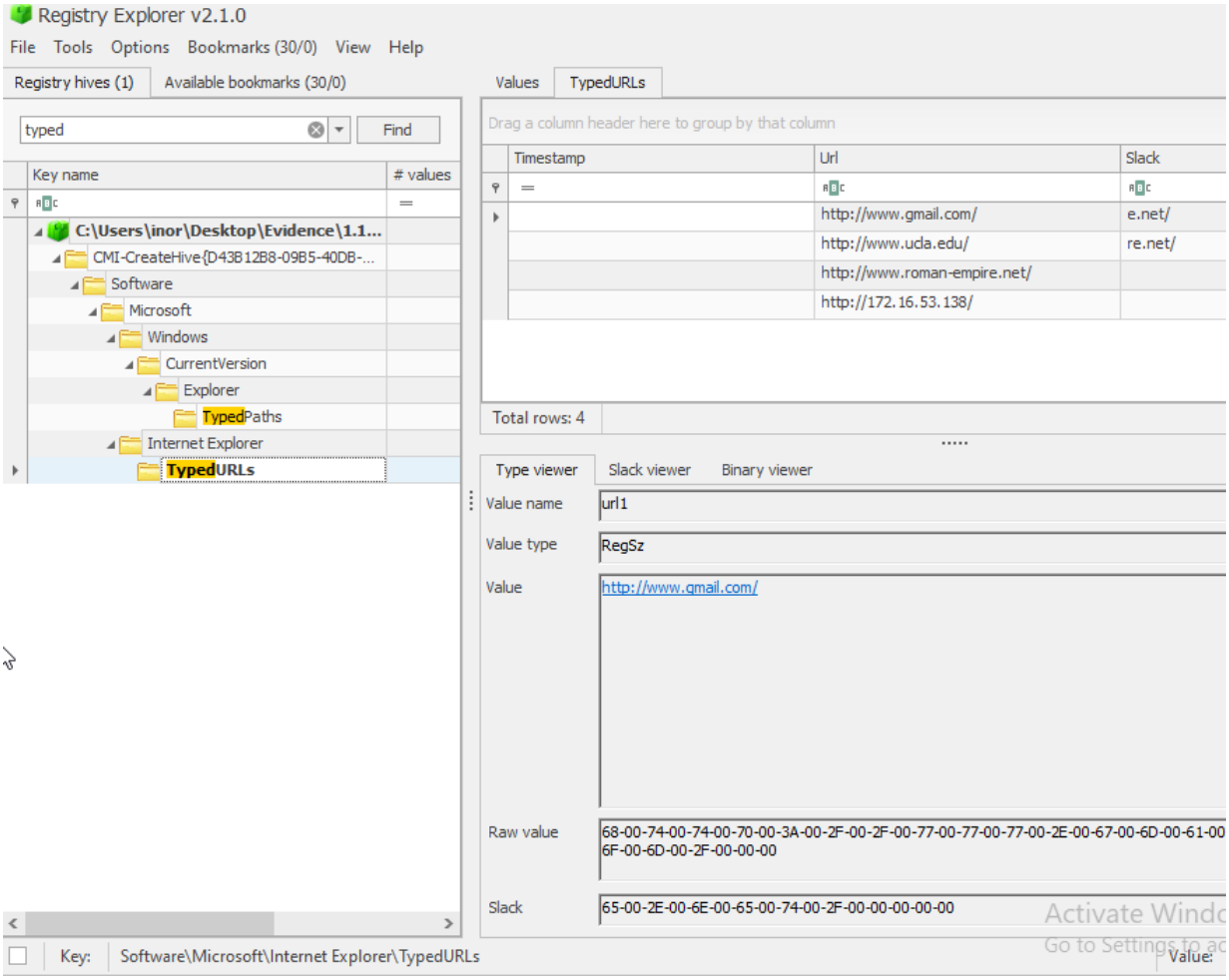

Figure 25. Registry Explorer of Natasha's NTUSER.DAT hive showing the TypedURLs registry key of Internet Explorer

15. What did the Natasha account open via the Start => Run line?

- **Analysis Performed:**

- Natasha's NTUSER.DAT hive was analyzed through the Eric Zimmerman's Registry Explorer application.
- The Start => Run entries are stored in RunMRU. RunMRU keeps a history of commands typed in the Run dialog box.
- As shown in Figure 26, the Natasha user account opened "**cmd**" via Start => Run.
- Path: *NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion*\Explorer\RunMRU

- **Answer:**

  The Natasha user account ran the command prompt (cmd) via the Start => Run line. This was found after locating the RunMRU key which contains the history of commands executed via the Run dialog box.

- **Supporting Evidence:**

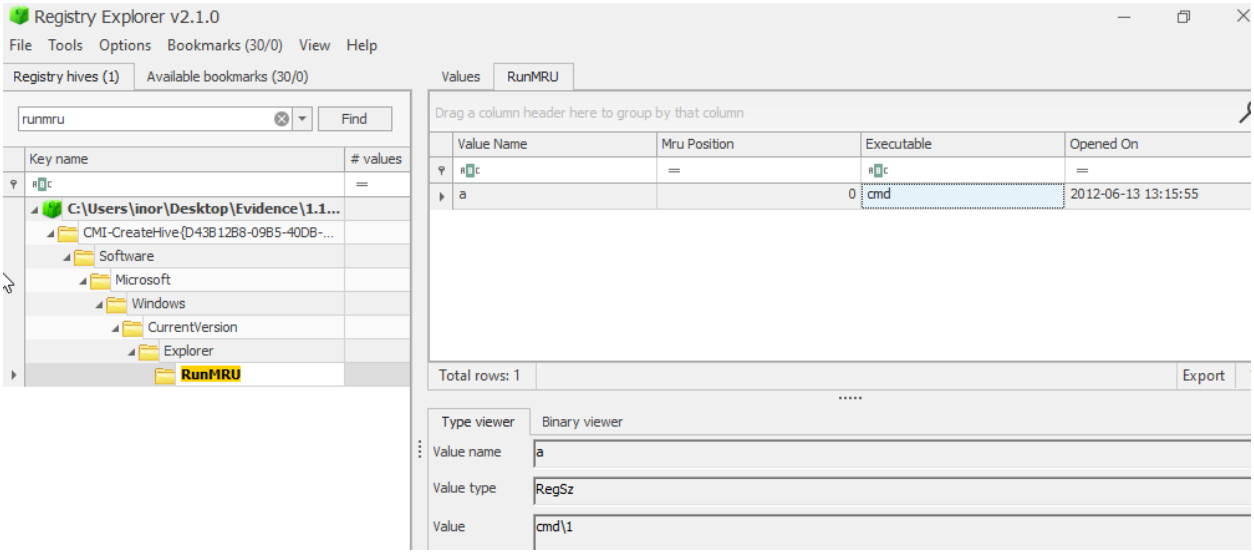

Figure 26. Registry Explorer of Natasha's NTUSER.DAT hive showing the RunMRU registry key

16. Does it appear the computer was ever associated with a wi-fi network? Explain.

- **Analysis Performed:**
  - The software hive was analyzed through the Eric Zimmerman's Registry Explorer application.

- Used Eric Zimmerman's bookmarks to find the NetworkCard registry key and NetworkList registry key
- The NetworkCard registry key contains the network cards that the computer has
- The NetworkList registry key contains every network the computer has connected to
- Figure 27's Path: *software\Microsoft*Windows NT\CurrentVersion\NetworkCards\8
- Figure 28's Path: *software\Microsoft\Windows NT\CurrentVersion\NetworkList*

- **Answer:**

  No, it appears that the computer was never associated with a wi-fi network (wireless). The only network card that the computer has is Intel® PRO/1000 MT Network Connection, which is wired Ethernet NIC, as shown in Figure 27. Additionally, the NetworkList registry key stores every network the computer has connected to and in this case, the computer has only connected through a wired connection (Ethernet), as shown in Figure 28.

- **Supporting Evidence:**

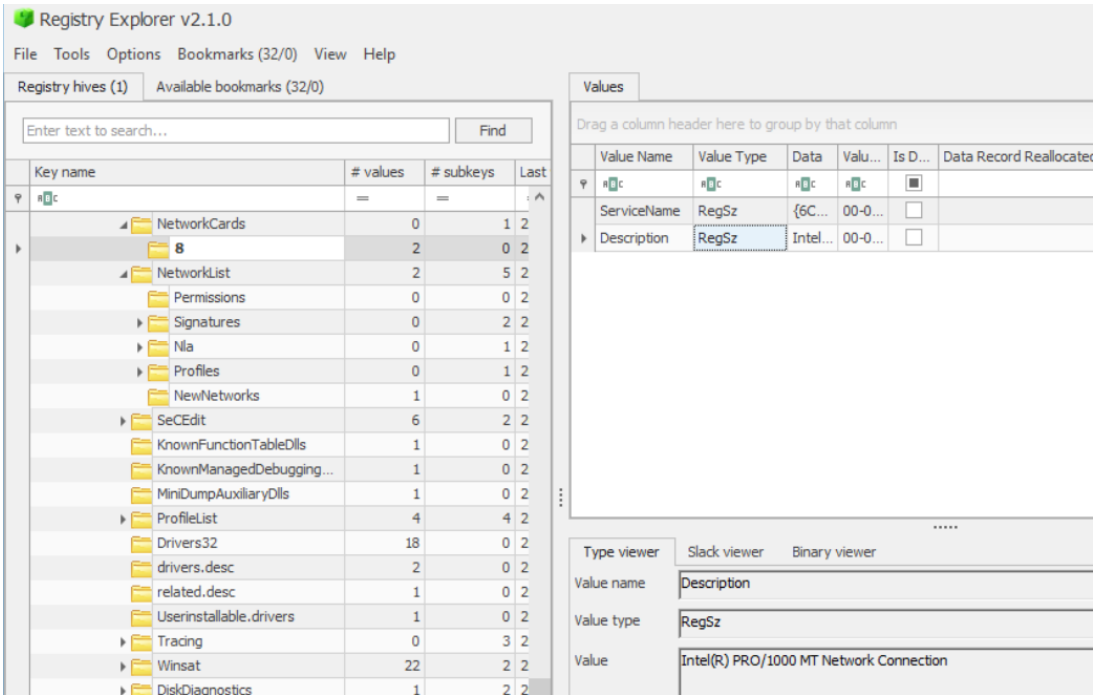

Figure 27. Registry Explorer of the NetworkCards registry key showcasing the only network card

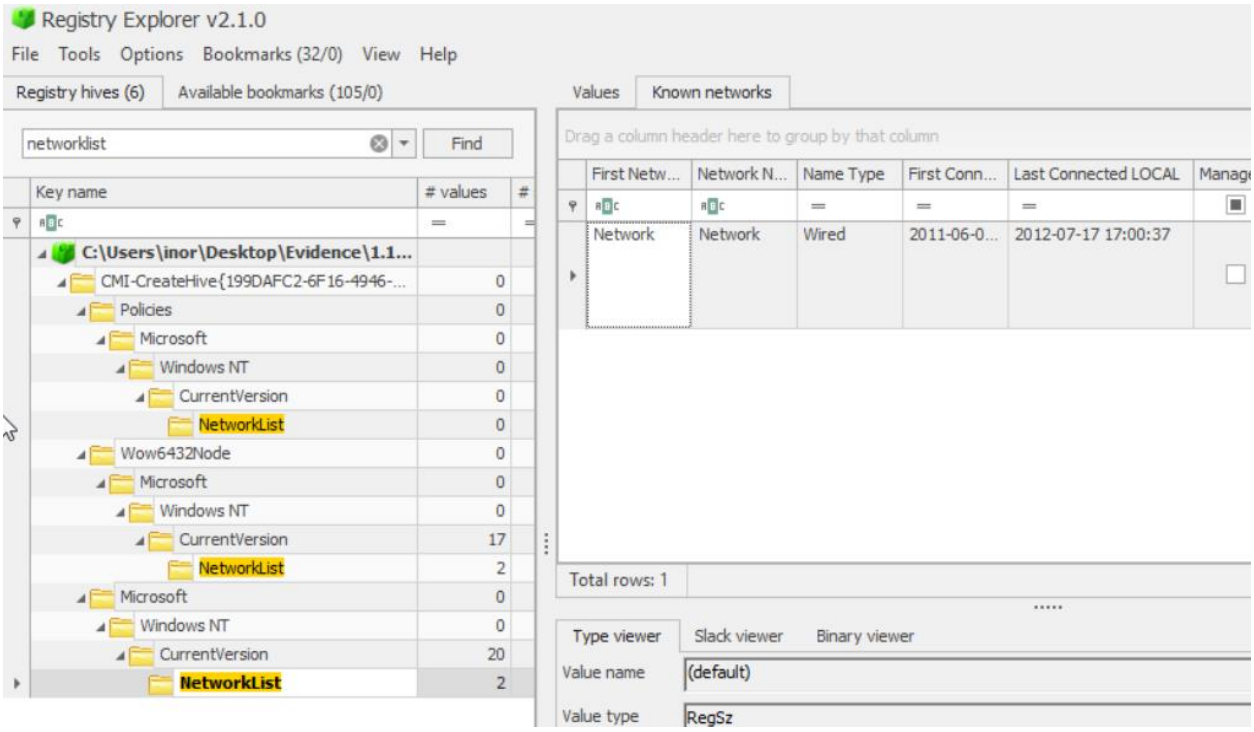

Figure 28. Registry Explorer of the software hive showing the NetworkList registry key

17. Is this computer configured to obtain an IP address via DHCP? Explain.

- **Analysis Performed:**
  - The system hive was analyzed through the AccessData Registry Viewer application.
  - In order to obtain information about the computer's networking configurations, the examiner went to the computer's NIC.
  - Reading the *{6CF7B89F-5508-4094-AF1D-65872D36A357}* registry key, there was a specific registry value, **EnableDHCP**, which was set to **0x00000001 (1)**.
  - Also, there was an IP address obtained via DHCP as shown in the registry value, DhcpIPAddress.
  - Path: *system\ControlSet001\services\Tcpip\Parameters\Interfaces\{6CF7B89F-5508-4094-AF1D-65872D36A357}*
- **Answer:**

  Yes. This computer was configured to obtain an IP address via DHCP. As shown in Figure 29, within the computer's main NIC, the registry value of EnableDHCP is set to **0x000000001 (1)** which means that DHCP is enabled. Additionally, the registry value of DhcpIPAddress is set to **172.16.53.141** which means that an IP address was obtained via DHCP.

- **Supporting Evidence:**

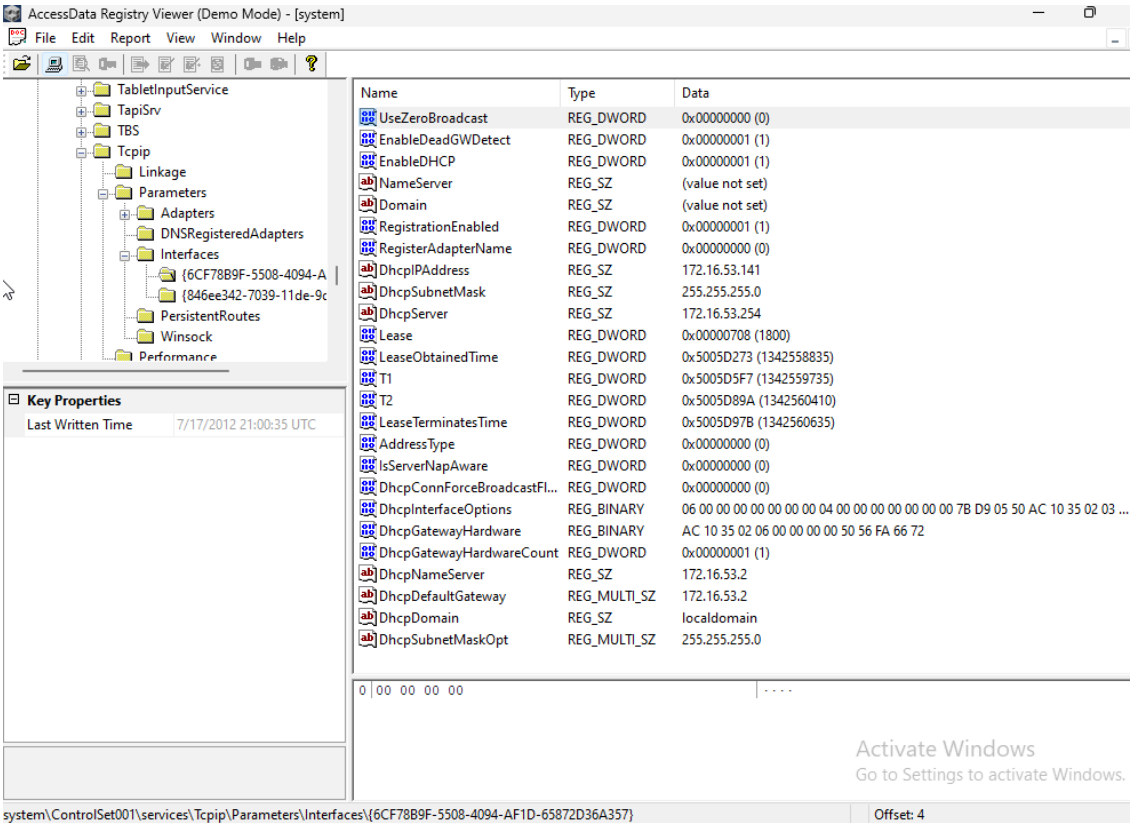

Figure 29. Registry Viewer of the system hive showing the NIC registry key

18. What was its last IP address?

- **Analysis Performed:**
  - The system hive was analyzed through the AccessData Registry Viewer application.
  - The IP address obtained via DHCP is shown in the registry value, DhcpIPAddress, as shown in Figure 30.
  - Due to the nature of DHCP, it leases the IP address and the LeaseObtainedTime is "**0x5005D273 (1342558835)"** which converted to datetime from my MacOS terminal which is "**2012-07-17 21:00:35 UTC**" as shown in Figures 30 and 31. Additionally, the registry key write time was "**7/17/2012 21:00:35 UTC**" which is the exact same as the LeaseObtainedTime.
  - Path: *system\ControlSet001\services\Tcpip\Parameters\Interfaces\{6CF7B89F-5508-4094-AF1D-65872D36A357}*
- **Answer:**

  The last IP address was **172.16.53.141** which was listed under the DhcpIPAddress registry value within the computer's primary NIC's registry key as shown in Figure 27. Additionally, the LeaseObtainedTime of the IP address is "**2012-07-17 21:00:35 UTC**" and the registry key last write time was "**7/17/2012 21:00:35 UTC**" which shows that this was the last IP address before the seizure as shown in Figures 30 and 31.

- **Supporting Evidence:**

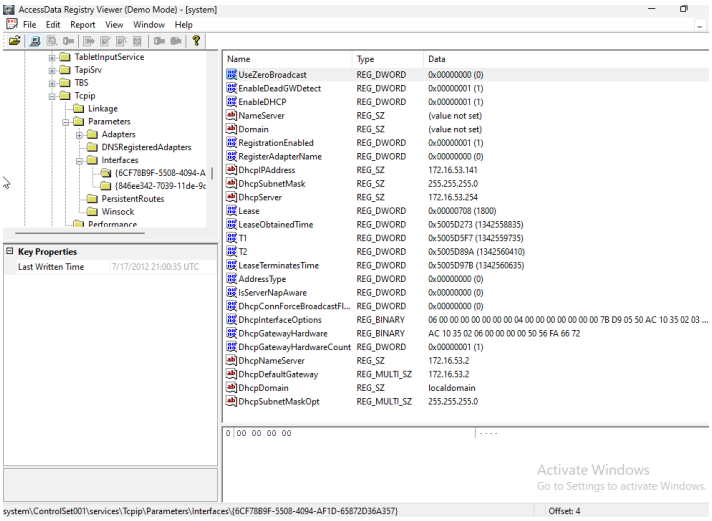

Figure 30. Registry viewer of the system hive showing the primary NIC's registry key

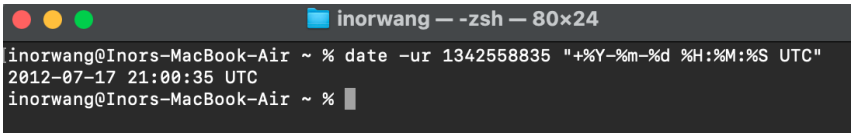

Figure 31. MacOS terminal command to convert decimal to datetime

Conclusion

The examiner, Inor Wang, enjoyed this lab! There is no critique from me. As a note, I really appreciated the report template example, it helped me write this lab without worrying too much about formatting. Thank you.

References

0xStn. (2023, August 17). Windows Forensics 1 [THM]: Introduction to Windows registry forensics. Medium. Retrieved from https://0xstn.medium.com/windows-forensics-1-thm-2fd8ea7ac41d.

Boncaldo's Forensics Blog. (2018, August 1). 4n6 Quick! #01 – Windows users list & login count. Retrieved from https://boncaldoforensics.wordpress.com/2018/08/01/4n6-quick-01-windows-users-list-login-count/.

Boutnaru, S. (2024, August 3). *The Windows Forensic Journey — "NetworkList" (Wireless Network Profiles List)*. *Medium*. https://medium.com/@boutnaru/the-windows-forensic-journey-networklist-wireless-network-profiles-list-17b41a80903f.

Carvey, H. A. (2014). Windows forensic analysis toolkit: Advanced analysis techniques for Windows 8 (Fourth edition). Syngress.

Intel Corporation. (n.d.). *Support for Intel® PRO/1000 MT Desktop Adapter Series: Product information*. Intel. Retrieved September 12, 2025, from https://www.intel.com/content/www/us/en/support/products/63481/ethernet-products/legacy-ethernet-products/intel-pro1000-mt-desktop-adapter-series.html.

Johansen, G., & Safari, an O. M. C. (2020). Digital Forensics and Incident Response—Second Edition.

Ligh, M. H., Case, A., Levy, J., & Walters, A. (2014). The art of memory forensics: Detecting malware and threats in Windows, Linux, and Mac memory. Wiley.

Malware forensics field guide for Windows systems digital forensics field guides. (2012). Syngress.

Oettinger, W., & Safari, an O. M. C. (2020). Learn Computer Forensics.

Reddy, N. (2019). Practical cyber forensics: An incident-based approach to forensic investigations. APress. https://doi.org/10.1007/978-1-4842-4460-9.

Stack Overflow. (2024, June 2). How to convert Windows FILETIME 64-bit hex to date and time? Retrieved from https://stackoverflow.com/questions/78566947/how-to-convert-windows-filetime-64bit-hex-to-date-and-time.

The 4N6 Post. (2023, February). TimeZoneInformation. Retrieved from https://www.4n6post.com/2023/02/timezoneinformation.html.

van Veenendaal, M. (2024, September 29). Windows Registry 101: A guide for forensic investigations. Retrieved from https://www.mennovanveenendaal.com/posts/Windows-Registry-101%2C-A-Guide-for-Forensic-Investigations/.