

## Lab 03 – Windows Registry Analysis

David Murillo Santiago  
Professor Zhang  
IS-4523  
2 March 2025

### INTRODUCTION

---

In this lab, I will conduct a forensic analysis of Windows Registry hives to uncover artifacts related to system configuration and user activity.

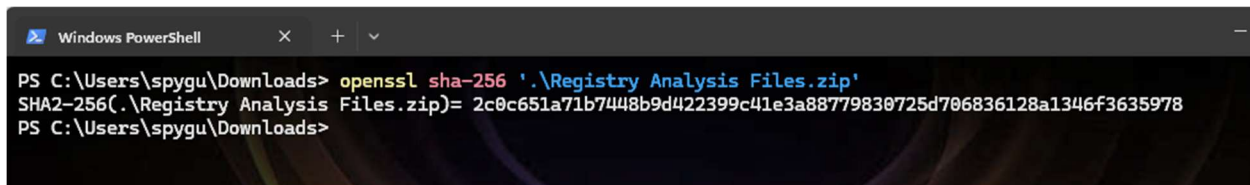
### PROCESS

---

#### Verifying Image Integrity

To begin, I verified the integrity of the hive files that I will analyze by comparing the downloaded ZIP file's SHA-256 hash with the hash provided in the instructions:

`2c0c651a71b7448b9d422399c41e3a88779830725d706836128a1346f3635978`

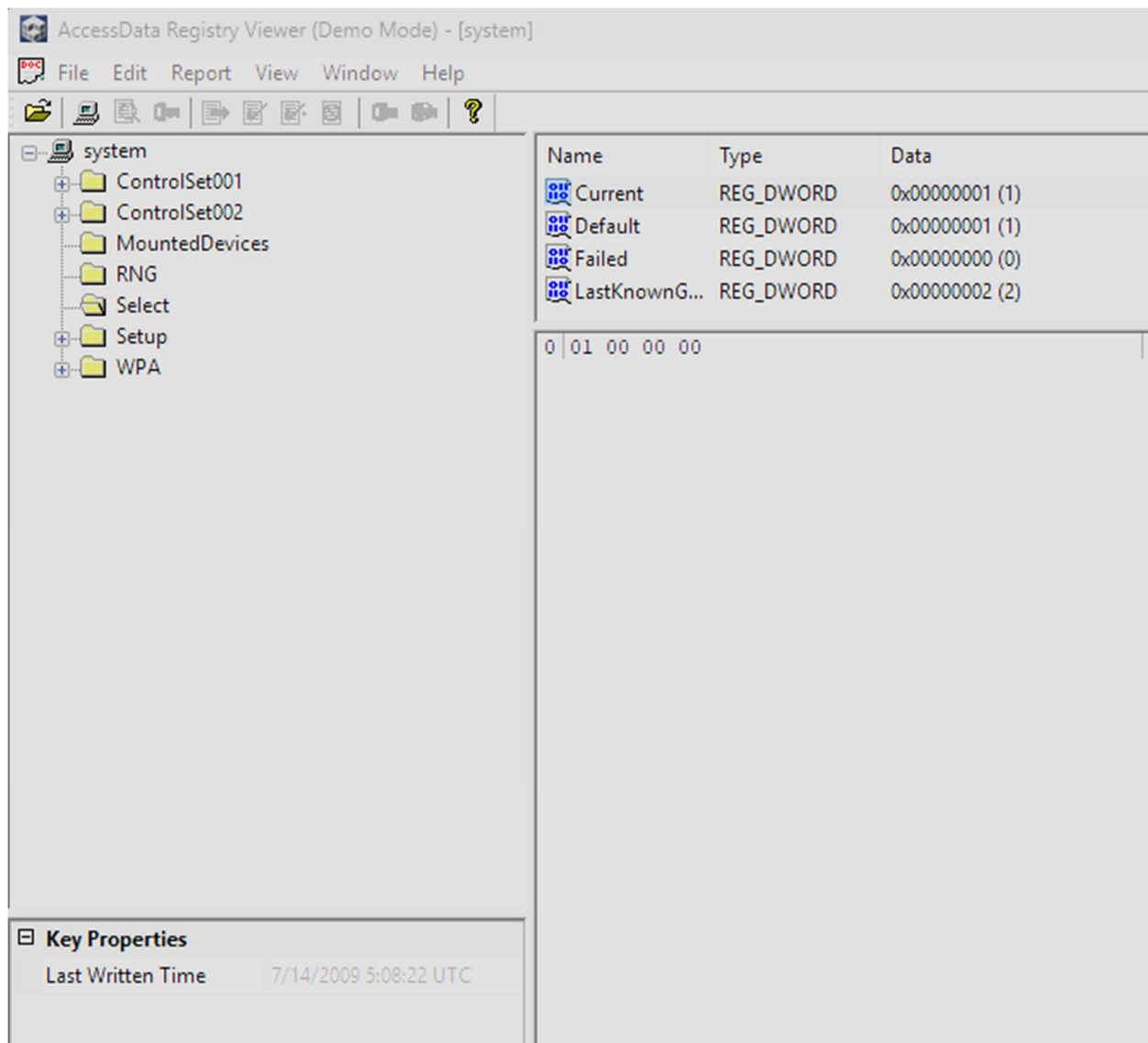


```
Windows PowerShell
PS C:\Users\spygu\Downloads> openssl sha-256 '.\Registry Analysis Files.zip'
SHA2-256(.\'Registry Analysis Files.zip)= 2c0c651a71b7448b9d422399c41e3a88779830725d706836128a1346f3635978
PS C:\Users\spygu\Downloads>
```

*Proven by their matching hashes, the hive file images maintain integrity and can be analyzed.*

#### CurrentControlSet

To find the system's current control set, I analyzed the SYSTEM hive and navigated to the Current key at SYSTEM\Select\Current.



Value for Current Control Set: Current = (1)

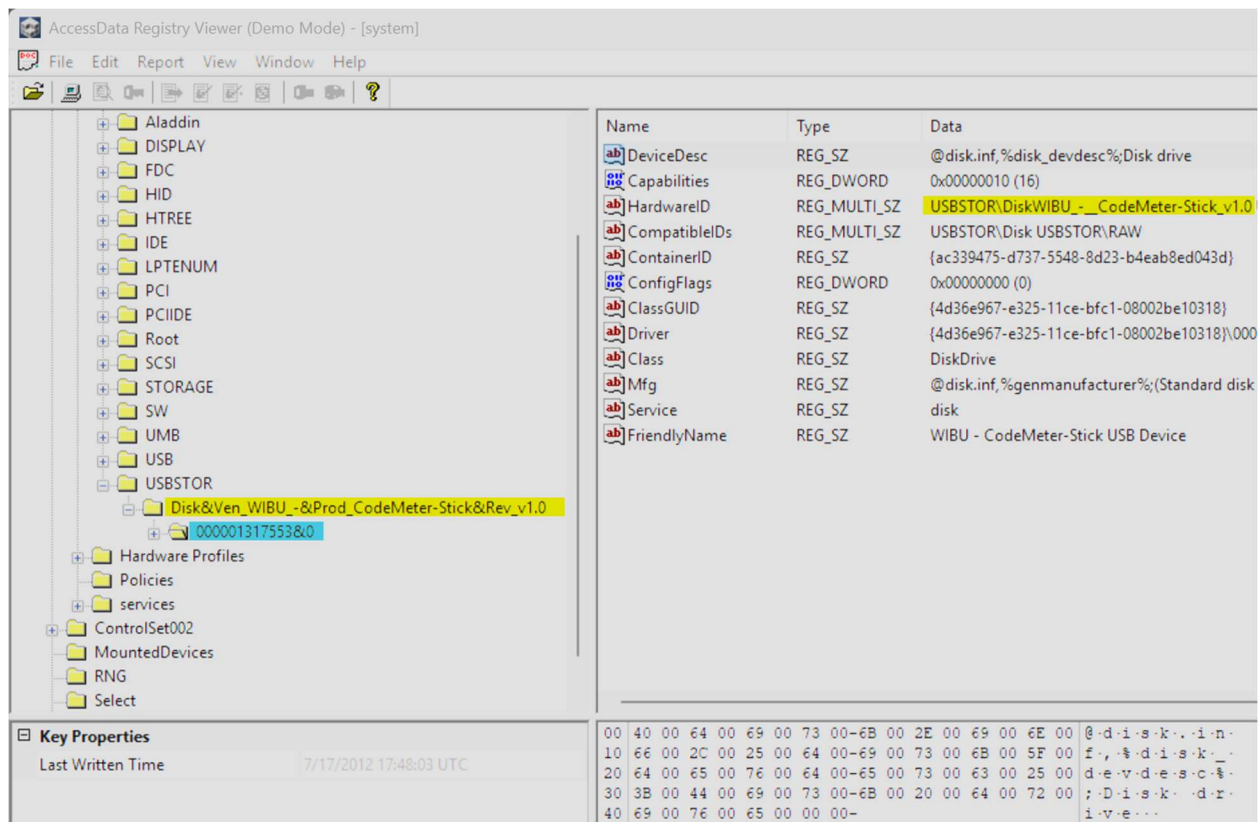
1. Which ControlSet is the current control set?

The value for Current is 1, meaning that the system's CurrentControlSet is CurrentControlSet\001.

### USB Thumb Drive Forensics

Next, I continued analyzing the SYSTEM hive for information regarding thumb drives plugged into the system. First, I examined the USBStor key to identify the make and model of the drives that had been connected to the system.

The USBStor key is located at: <System Hive>\%CCS%\Enum\USBStor



Product: Wibu CodeMeter Stick. Serial# 000001317553.

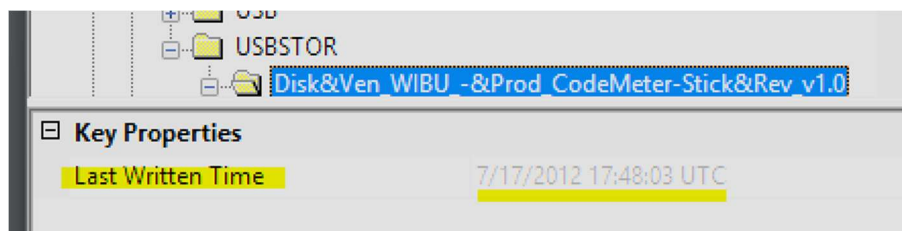
## 2. What is the make & model of the only thumb drive that has inserted into this system?

Within the USBStor key, I found the subkey for the only thumb drive plugged into the system. Analyzing the Device ID from the subkey's name, I discovered that a Wibu CodeMeter Stick was plugged into the system.

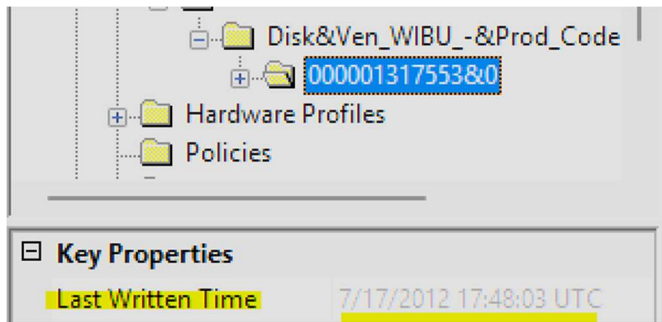
## 3. What is its serial number?

From the Instance ID subkey, I determined that the device's serial number is 000001317553.

Next, I analyzed the 'Last Written' timestamps to determine when the thumb drive was first and last connected since the last reboot. Firstly, I analyzed the timestamp associated with the Device ID subkey.



Device ID Key Last Written on 7/17/2012 at 17:48:03 UTC.



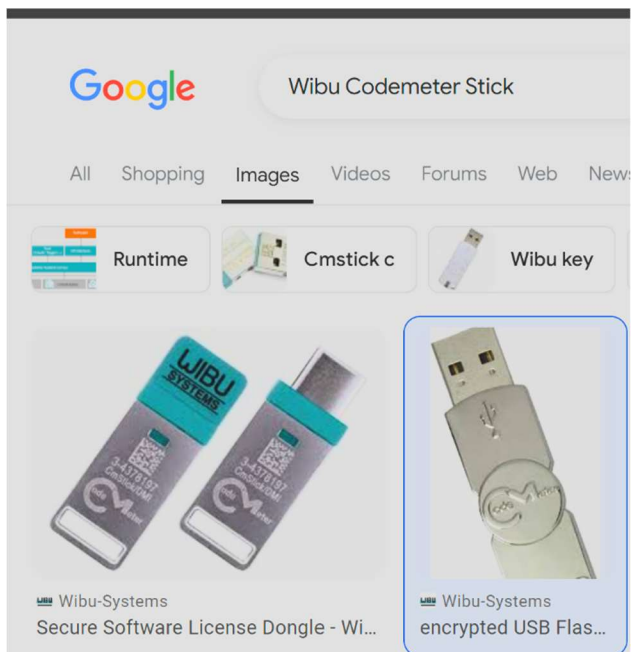
*Instance ID Key Last Written on 7/17/2012 at 17:48:03 UTC.*

#### 4. When was this thumb drive first (since last reboot) and last inserted?

The last write time of the Device ID key 'Disk&Ven\_WIBU\_-&Prod\_CodeMeter-Stick&Rev\_v1.0' reveals that the thumb drive was first inserted on 07/17/2012 at 17:48:03 UTC since the last reboot.

The last write time of the Instance ID key '000001317553&0' reveals that the thumb drive was last inserted on the same date: 07/17/2012 at 17:48:03 UTC.

Next, for more information, I googled the device's make and model.



*Wibu CodeMeter Stick Research*

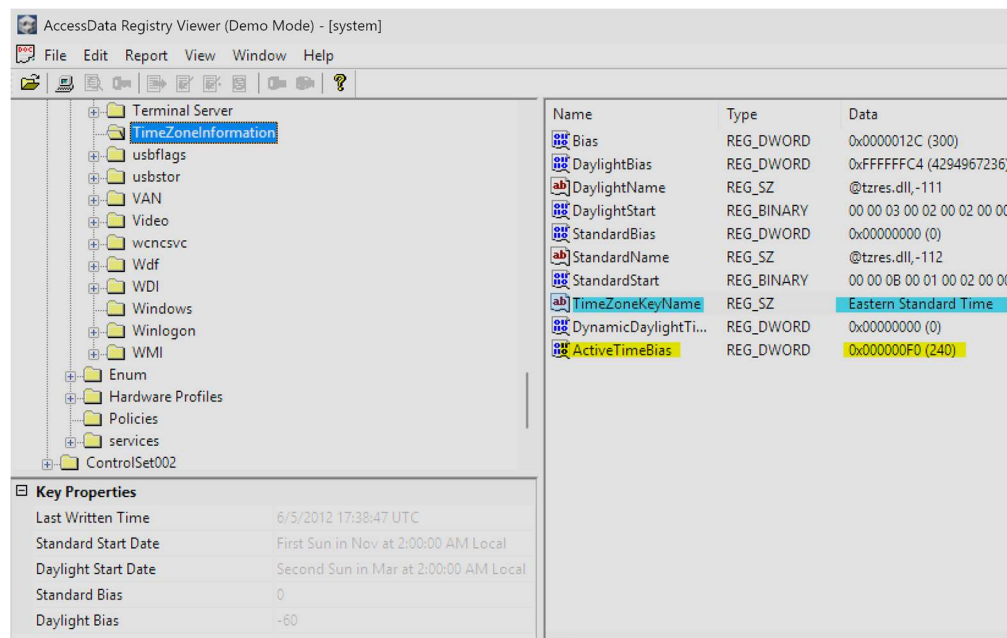
#### 5. "Google" the make & model. What kind of drive is this?

From my research, I found that a "Wibu CodeMeter stick" is a small, portable USB device used to securely store and manage software licenses for various applications.

Next, I continued my analysis of the System hive to determine the computer name, time zone, and when it was last shutdown.

6. What is this computer's time zone set to at the time of seizure?

To find the time zone data, I traversed to the TimeZoneInformation key located at <System Hive>\%CCS%\Control\TimeZoneInformation.



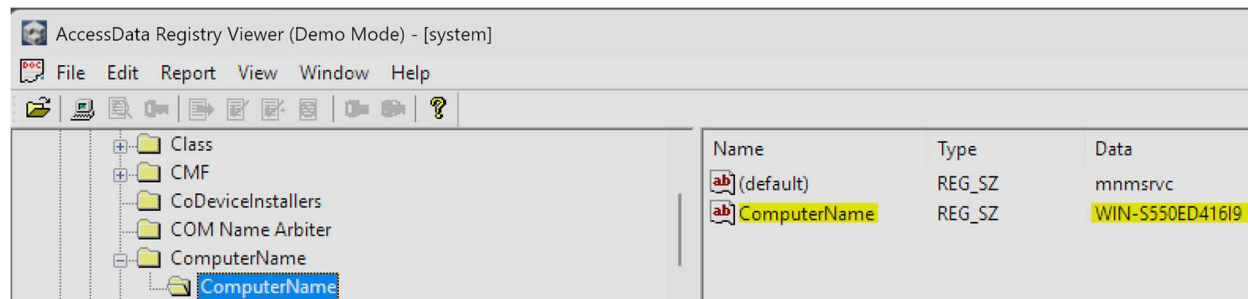
*TimeZoneInformation Key. The system uses Eastern Standard Time.*

From the values within the TimeZoneInformation key, I determined that the system is configured to use Eastern Standard Time. By analyzing the ActiveTimeBias value, I discovered that the device is operating under Daylight Saving Time and is configured to run 240 minutes (4 hours) behind UTC.

Formula: UTC = Local Time + Bias Time

7. What is its assigned computer name?

To find the computer name, I traversed to the ComputerName key located at <System Hive>\%CCS%\Control\ComputerName\ComputerName.

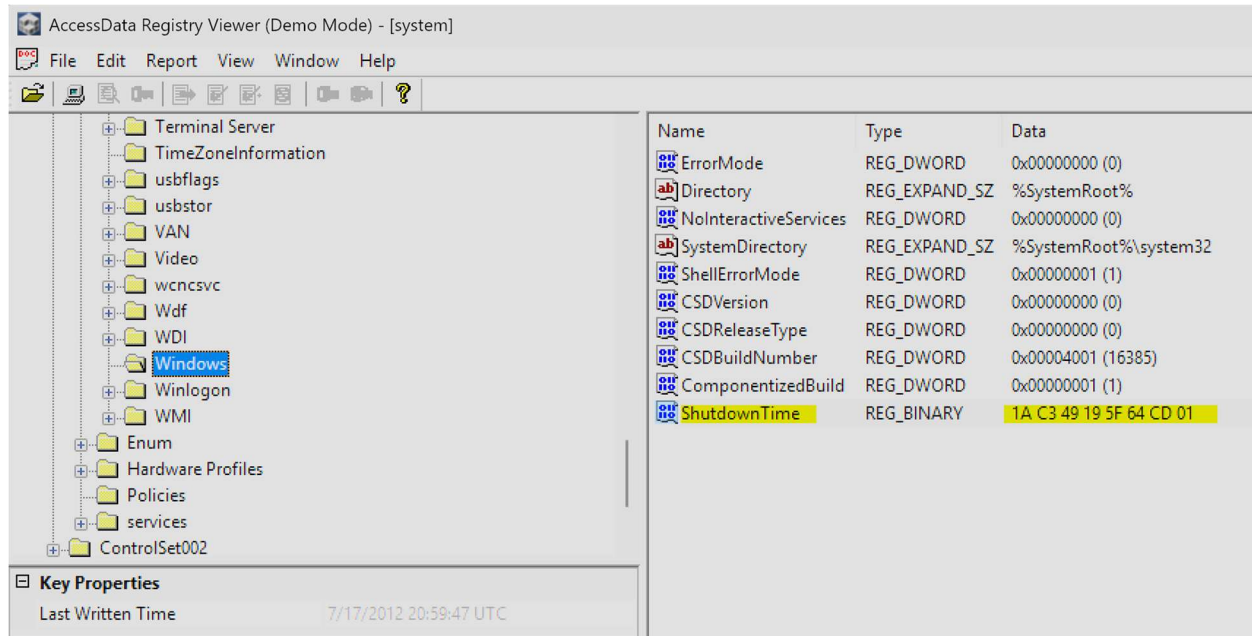


*ComputerName key. The computer's name is WIN-S550ED416I9.*

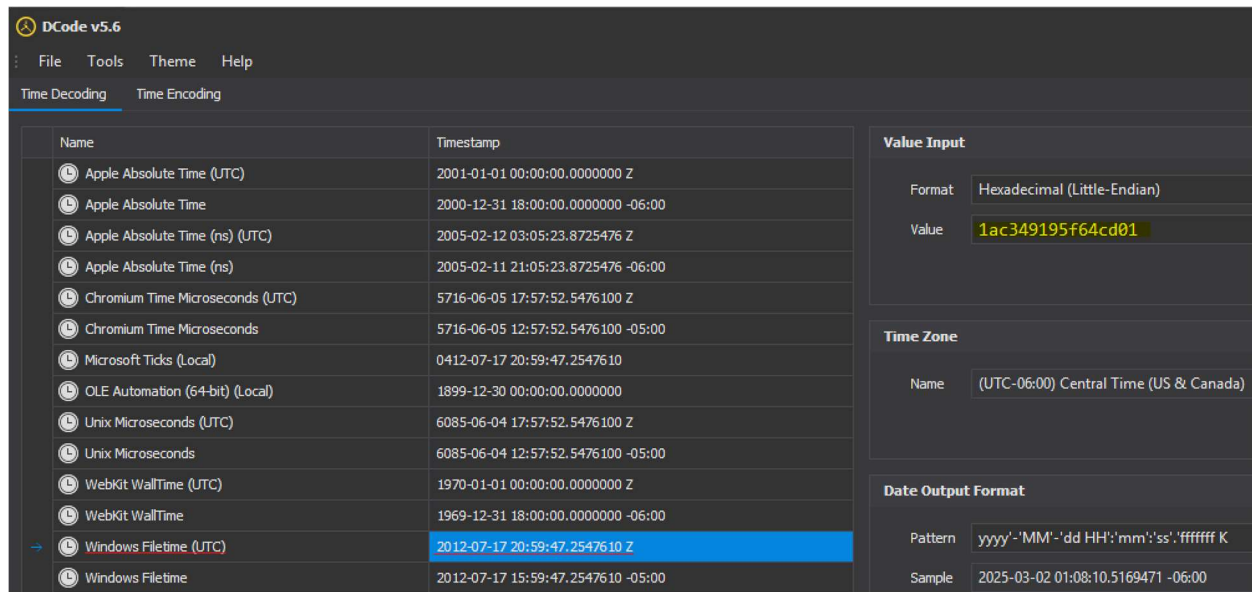
8. When was it last shutdown through standard shutdown procedures?

To find the last shutdown time, I traversed to the ShutDowTime key located at:

<System Hive>\%CCS%\Control\Windows\ShutDownTime



Last Shutdown Time in Hex: 1A C3 49 19 5F 64 CD 01



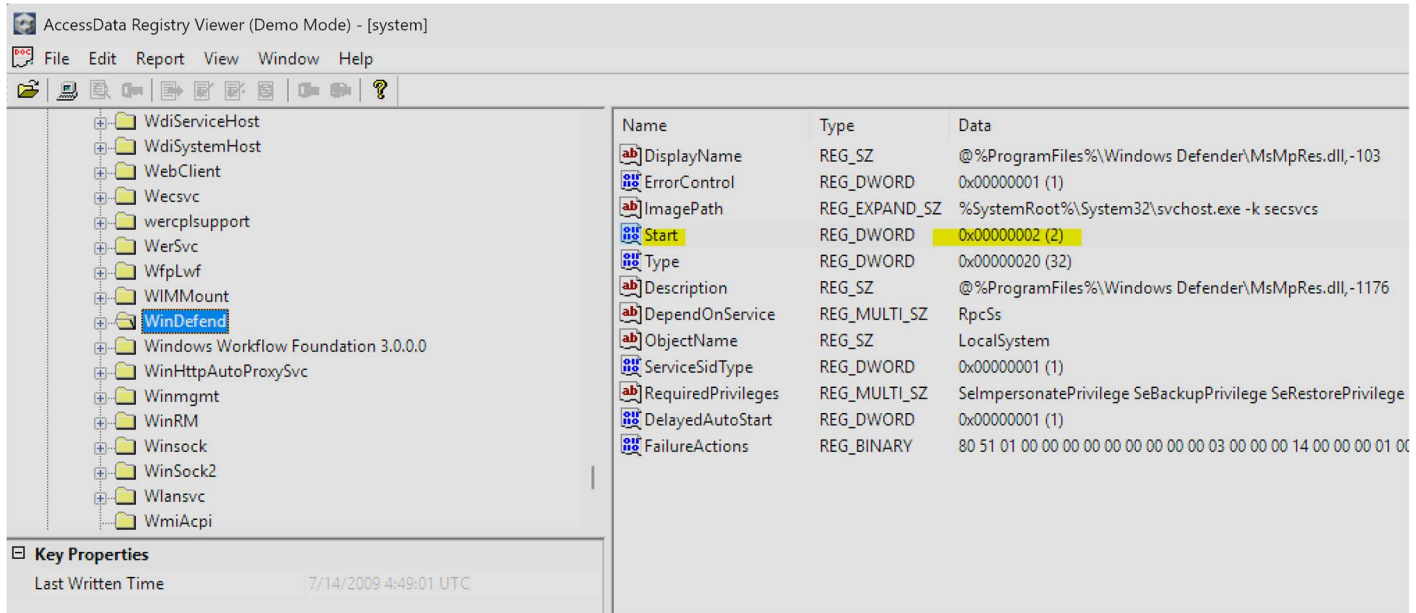
DCode: Translating the Hex shutdown time to Windows Filetime (UTC).

The device last shutdown on 7/17/2012 at 20:59:47 (UTC).



9. 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.

To help determine if the device was protected by Windows Defender, I analyzed the Services key located at: <System Hive>\%CCS%\Services



*Services Key: WinDefend is enabled to Start on boot (2).*

I found an entry for Windows Defender under the Services key. Analyzing WinDefend's values, I determined that the service is configured to start on boot, as indicated by the Start value 0x00000002.

If the Start value had been set to 3, it would indicate that the service is disabled on boot. If it had been set to 4, it would mean that the service can only be manually started by the user. Because the Start value is set to 2, it is likely that the computer was protected by Windows Defender.

10. How many Registry keys/sub-keys were last written on the day the computer was last shutdown?

Next, I applied a 'Search by Date' filter to determine how many keys were last written on the day the computer was last shutdown.

Hive	# of Keys Written on date of Last Shutdown
System	5000
Software	227
Security	0
SAM	1
Default	3
Natasha's NTUSER.dat	184
<b>Total</b>	<b>5415</b>

AccessData Registry Viewer (Demo Mode) - [system]

File Edit Report View Window Help

Search by Last Written Date

Search for keys last written

☒ during a date range 7/17/2012 Search

☐ during and after a given date 7/17/2012 Clear Results

☐ during and before a given date

Search in The Full Registry

Found 5000 keys

Last Written	Key	Values
<input type="checkbox"/> 7/17/2012 21:00:12...	ControlSet001\Control\DeviceClasses\{4afa3d53-74a7-11d0-be5e-00a0...	<one value>
<input type="checkbox"/> 7/17/2012 21:00:12...	ControlSet001\Control\DeviceClasses\{4afa3d53-74a7-11d0-be5e-00a0...	<one value>
<input type="checkbox"/> 7/17/2012 21:00:23...	ControlSet001\Control\DeviceClasses\{4d1e55b2-f16f-11cf-88cb-00111...	<one value>
<input type="checkbox"/> 7/17/2012 21:00:23...	ControlSet001\Control\DeviceClasses\{4d1e55b2-f16f-11cf-88cb-00111...	<one value>
<input type="checkbox"/> 7/17/2012 21:00:23...	ControlSet001\Control\DeviceClasses\{4d1e55b2-f16f-11cf-88cb-00111...	<one value>
<input type="checkbox"/> 7/17/2012 21:00:23...	ControlSet001\Control\DeviceClasses\{4d1e55b2-f16f-11cf-88cb-00111...	<one value>

AccessData Registry Viewer (Demo Mode) - [software]

File Edit Report View Window Help

Search by Last Written Date

Search for keys last written

☒ during a date range 7/17/2012 Search

☐ during and after a given date 7/17/2012 Clear Results

☐ during and before a given date

Search in The Full Registry

Found 227 keys

Last Written	Key	Values
<input type="checkbox"/> 7/17/2012 13:34:25...	Classes\Installer\Features	<no values>
<input type="checkbox"/> 7/17/2012 13:34:25...	Classes\Installer\Features\620EE347986D51245A27AAF893F5E75B	<one value>
<input type="checkbox"/> 7/17/2012 13:33:00...	Classes\Installer\Features\EDB2013007F45D64A9D4CAF4A95D4C0C	<one value>

AccessData Registry Viewer (Demo Mode) - [SECURITY]

File Edit Report View Window Help

Search by Last Written Date

Search for keys last written

☒ during a date range 7/17/2012 Search

☐ during and after a given date 7/17/2012 Clear Results

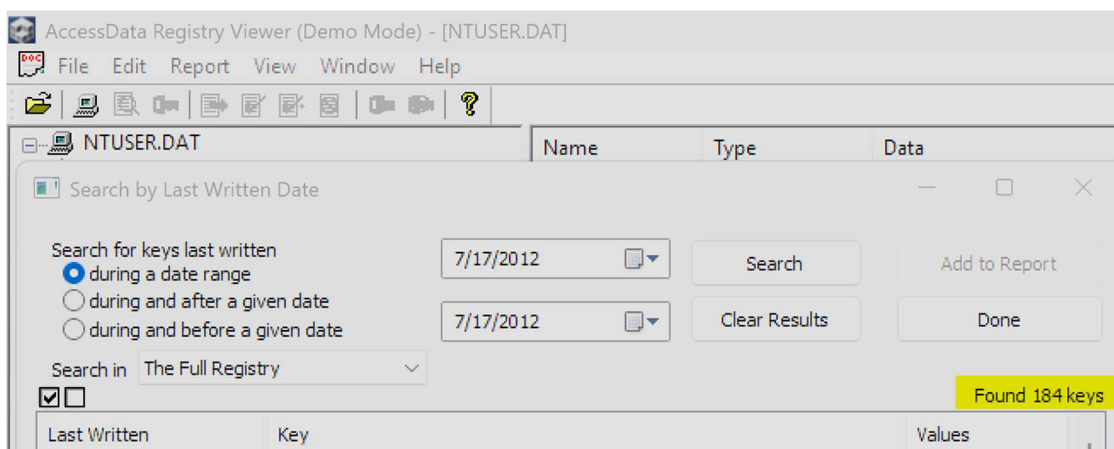
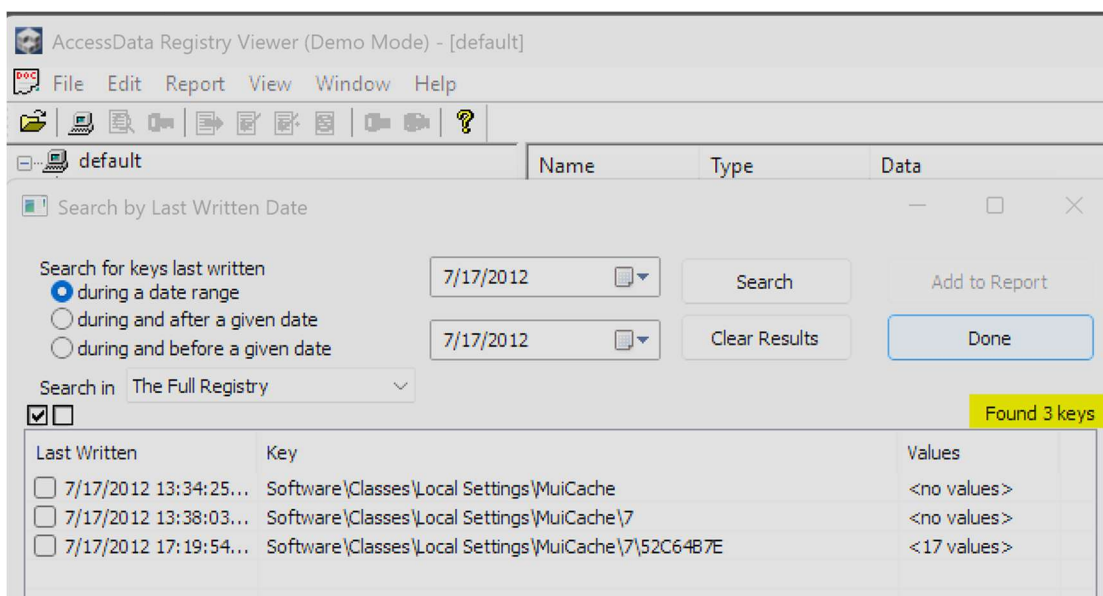
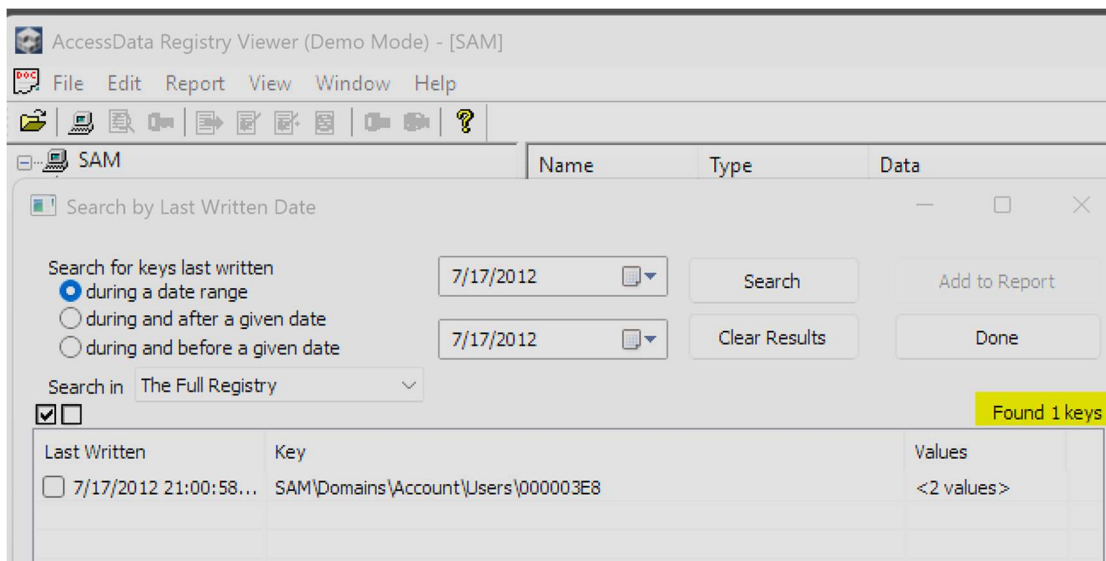
☐ during and before a given date

Search in The Full Registry

Found 0 keys

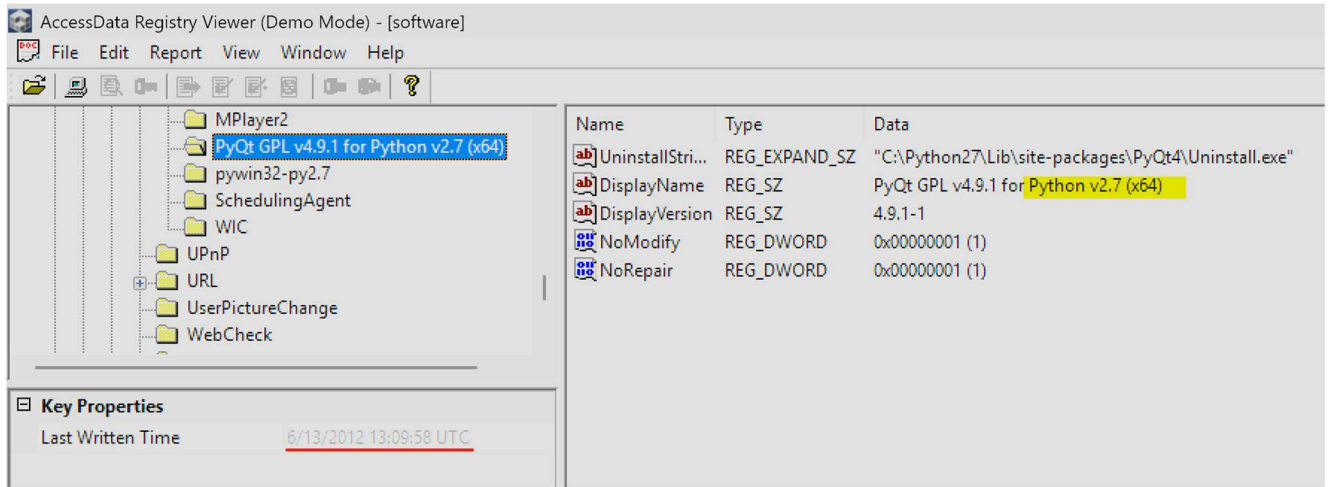
Last Written	Key	Values
--------------	-----	--------





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

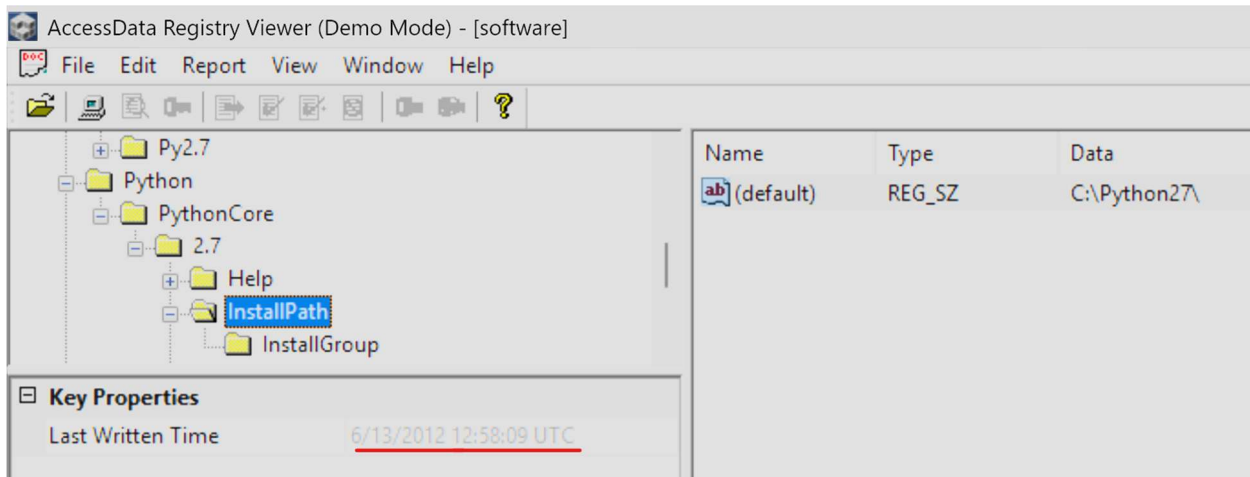
To determine the version of Python installed on the system, I navigated to the SOFTWARE hive and located the Uninstall key at SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall.



*Uninstall Key: Python v2.7 (x64)*

The Uninstall key showed two entries related to Python: 'PyQt' and 'pywin', both of which indicate the use of Python 2.7.

12. When do you think it was installed?



*PythonCore key. Last Write Time = 06/13/2012 at 12:58:09.*

I found proof that Python 2.7 was on the system as early as 12:58:09 on 06/13/2012. PyQt, which also uses Python 2.7, was logged by the registry at 13:09:58 on 06/13/2012, matching the Uninstall key's timestamp. This proves that PyQt was installed at 13:09:58, as the file is created and remains unedited upon program download. However, because Python 2.7 was logged on the system as early as 12:58:09, it is likely that Python was reinstalled, modified, or updated as a result of the PyQt4 installation.

13. What user accounts are configured on the system?

To find the users on the system I analyzed the SAM hive and traversed to the Users hive.

There are 3 users on the system: Administrator, Guest, and Natasha.

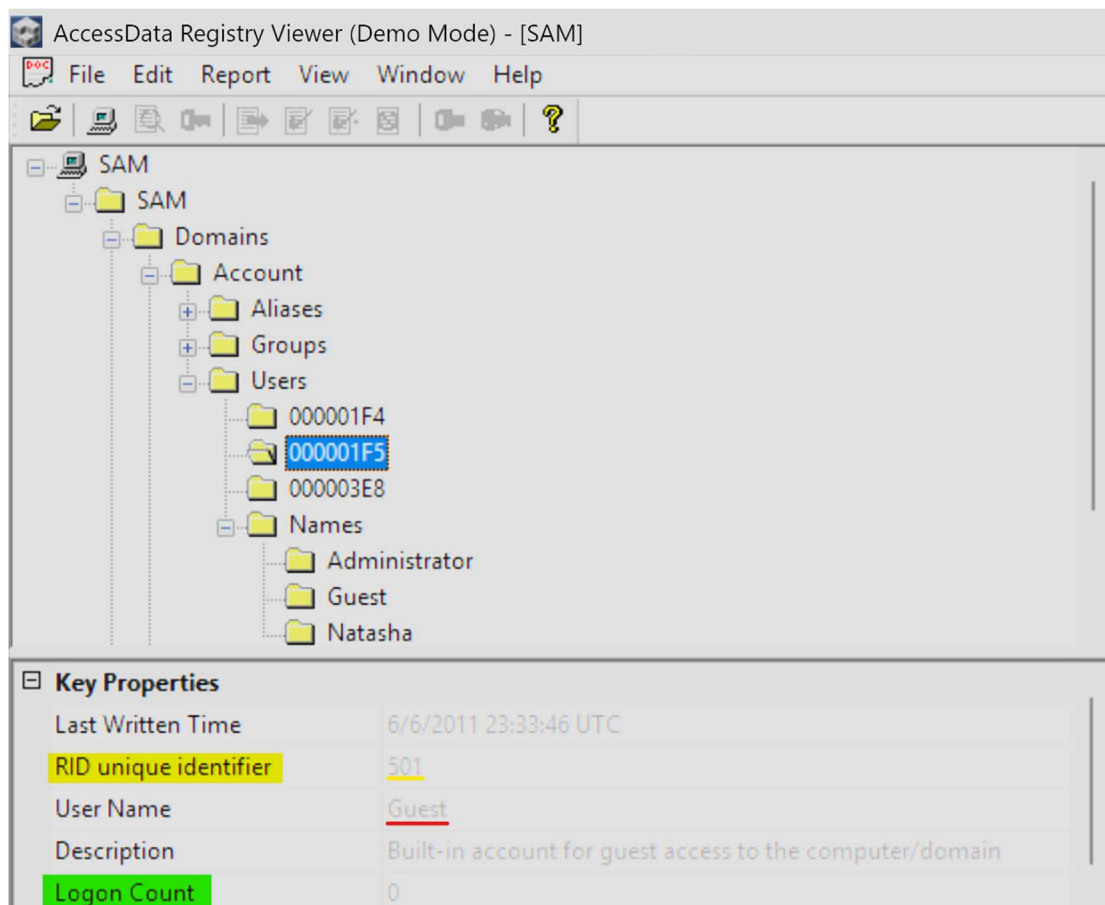
The screenshot shows the AccessData Registry Viewer (Demo Mode) - [SAM] interface. The left pane displays the SAM hive structure, with the 'Users' folder selected. The right pane shows the 'Key Properties' for the selected user, 'Administrator'.

**Key Properties:**

Last Written Time	6/6/2011 23:33:46 UTC
<b>RID unique identifier</b>	<u>500</u>
User Name	<u>Administrator</u>
Description	Built-in account for administering the computer/domain
<b>Logon Count</b>	1
Last Logon Time	7/14/2009 5:08:59 UTC
Last Password Change Time	7/14/2009 5:13:36 UTC

*Admin User Information*

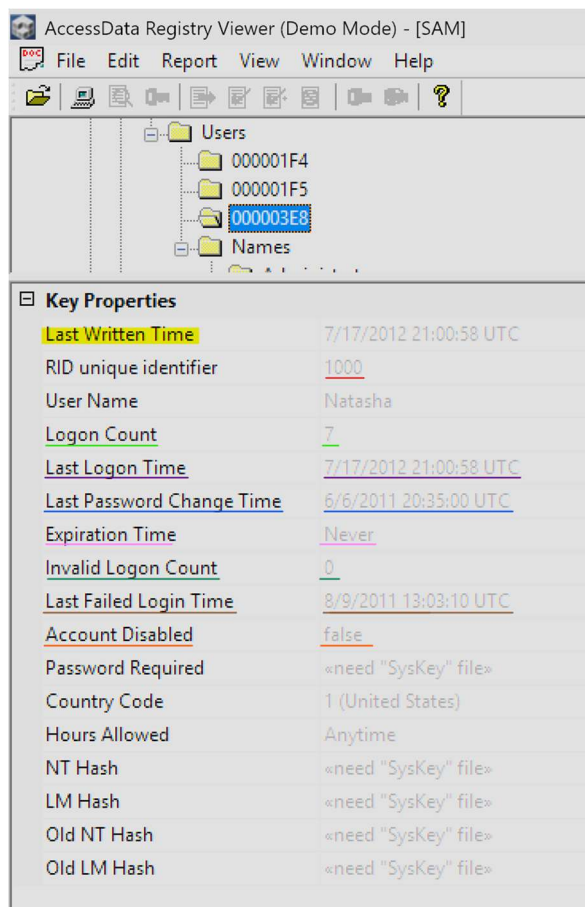
From the RID unique identifier value (500), I found that user 'Administrator' is the admin user for the system. This user has a logon count of 1 and last logged on 7/14/2009.



#### *Guest User Information*

From the RID unique identifier value (501), I found that user 'Guest' is the guest user for the system. This user has a logon count of 0 and thus has never logged on.

14. Provide the following information pertaining to the Natasha user account:



*Natasha User Information.*

The Natasha user account has a RID unique identifier of 1000, which typically indicates a standard user account rather than an administrator. The account has logged on 7 times, with the last logon occurring on July 17, 2012, at 21:00:58 UTC. The password was last changed on June 6, 2011, at 20:35:00 UTC. The password is not set to expire, as indicated by the "Expiration Time" field showing Never. The account is enabled, as the "Account Disabled" field is set to false.

15. Which user account was the last one to log in?

Key Properties	
Last Written Time	6/6/2011 23:33:46 UTC
RID unique identifier	500
User Name	Administrator
Description	Built-in account for administering the computer/domain
Logon Count	1
Last Logon Time	7/14/2009 5:08:59 UTC
Last Password Change Time	7/14/2009 5:13:36 UTC

Key Properties	
Last Written Time	7/17/2012 21:00:58 UTC
RID unique identifier	1000
User Name	<u>Natasha</u>
Logon Count	7
Last Logon Time	7/17/2012 21:00:58 UTC
Last Password Change Time	6/6/2011 20:35:00 UTC

Given that the admin user last logged in in 2009, Natasha was the last user to sign in, logging in on 07/17/2012.

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

To find information specific to Natasha's activity, I opened their NTUSER.DAT file and navigated to the UserAssist key.

Key Properties	
Last Written Time	7/17/2012 20:59:25 UTC
Value Properties	
Value Name ROT13	Microsoft.InternetExplorer.Default
Time	7/17/2012 20:55:37 UTC
Times Executed	<u>20</u>

Natasha ran Internet Explorer 20 times.

Key Properties	
Last Written Time	7/17/2012 20:59:25 UTC
Value Properties	
Value Name ROT13	Chrome
Time	8/22/2011 14:40:04 UTC
Times Executed	<u>6</u>

Natasha ran Chrome 6 times.



[-] <b>Key Properties</b>	
Last Written Time	7/17/2012 20:59:25 UTC
[-] <b>Value Properties</b>	
Value Name ROT13	Mozilla.Firefox.5.0.1
Time	7/6/2012 18:03:20 UTC
Times Executed	<u>10</u>

Natasha ran FireFox 10 times.

In the same UserAssist key, I found the executable for the Thunderbird email client along with its setup .exe file.

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

In the same UserAssist key, I found the executable for Thunderbird email client and its set up exe.

[-] <b>Key Properties</b>	
Last Written Time	7/17/2012 20:59:25 UTC
[-] <b>Value Properties</b>	
Value Name ROT13	C:\Users\Natasha\Downloads\Thunderbird Setup 6.0.exe

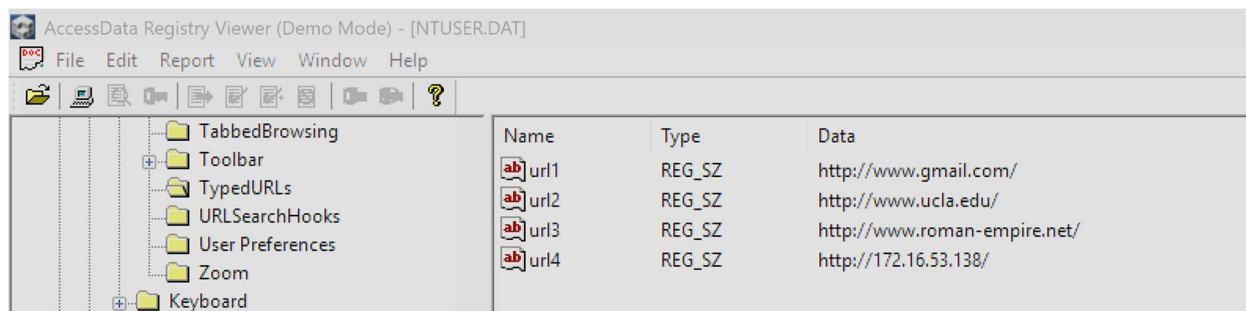
Thunderbird Setup File.

[-] <b>Key Properties</b>	
Last Written Time	7/17/2012 20:59:25 UTC
[-] <b>Value Properties</b>	
Value Name ROT13	Thunderbird.6.0
Time	8/22/2011 19:16:34 UTC
Times Executed	<u>4</u>

Thunderbird Email client File.

Given that Natasha downloaded and ran Thunderbird several times (4), it is likely that they use Thunderbird as their email client.

18. What URLs did the Natasha account type in?



<NTUSR Hive>\software\Microsoft\Internet Explorer\Toolbar\TypedURLs

Because Natasha preferred to use Internet Explorer, I navigated to Internet Explorer's TypedURLs key to determine what URLs the user entered.

The user entered the following URLs: <http://www.gmail.com/>, <http://www.ucla.edu/>, <http://www.roman-empire.net/>, and <http://172.16.53.138/>.

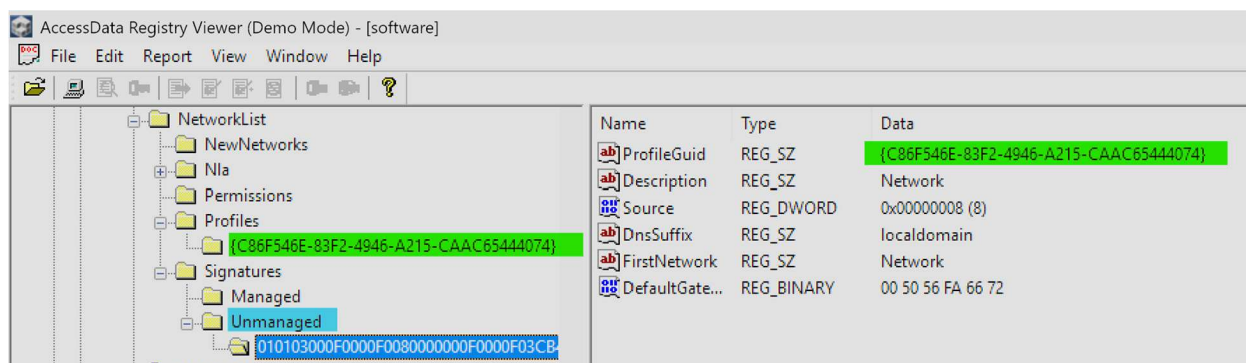
19. What did the Natasha account open via the Start→Run line?

I tried opening the RunMRU key located at <NTUSER.dat

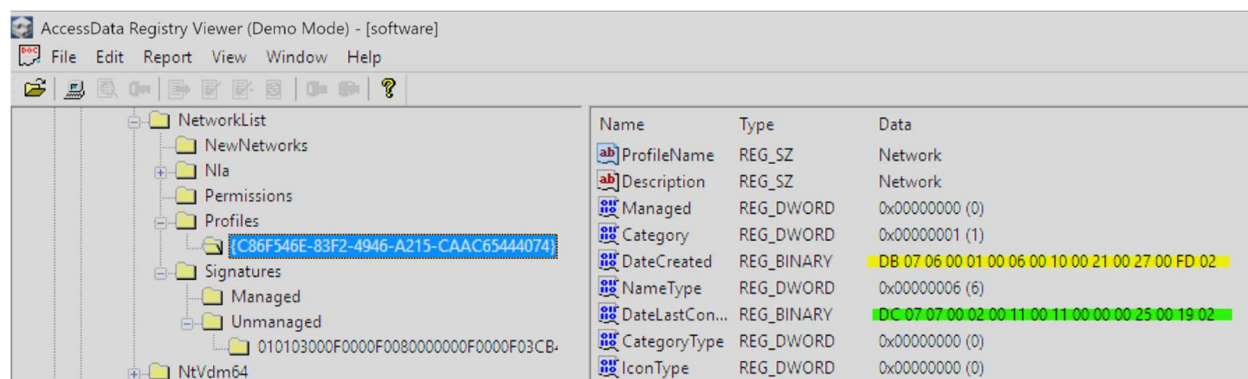
Hive>\Microsoft\Windows\CurrentVersion\Explorer\RunMRU to find what files Natasha opened from the Run dialog but the program kept crashing.

20. Does it appear the computer was ever associated with a home Wi-Fi network?

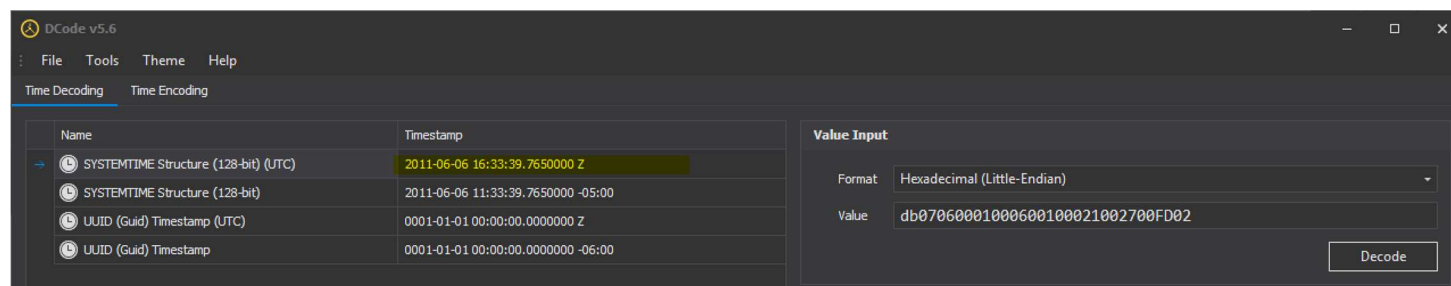
Yes the computer was connected to a local network using a wireless connection.



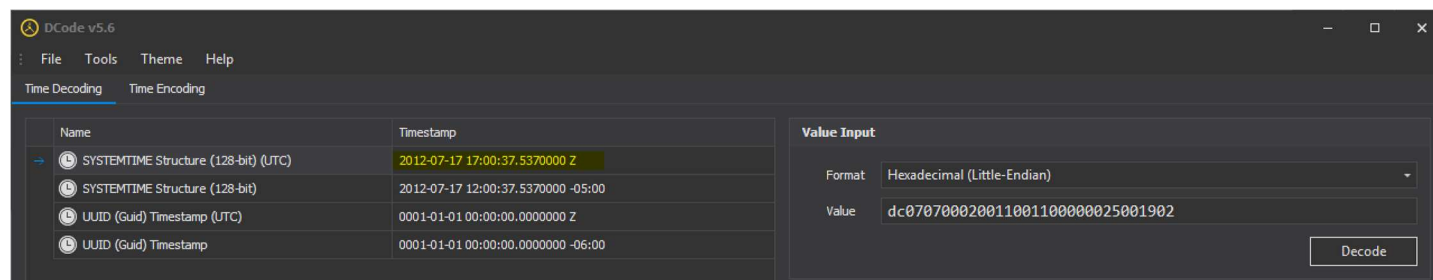
The computer was connected to a wireless (Unmanaged) Wi-Fi network.



Timestamp of first and last connection.



First Connection.



Last connection.

Last Connected Timestamp:

2012-07-17 17:00:37.5370000 UTC

Local Time: 2012-07-17 12:00:37.5370000 (-05:00)

First Connected Timestamp:

2011-06-06 16:33:39.7650000 UTC

Local Time: 2011-06-06 11:33:39.7650000 (-05:00)

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

22. What was its last IP address?

AccessData Registry Viewer (Demo Mode) - [system]			
File Edit Report View Window Help			
		Name	Data
<ul style="list-style-type: none"> <li>stisvc</li> <li>storflt</li> <li>storvsc</li> <li>swenum</li> <li>swprv</li> <li>SysMain</li> <li>TabletInputService</li> <li>TapiSrv</li> <li>TBS</li> <li>Tcpip <ul style="list-style-type: none"> <li>Linkage</li> <li>Parameters</li> <li>Adapters</li> <li>DNSRegisteredAdapters</li> <li>Interfaces <ul style="list-style-type: none"> <li>{6CF78B9F-5508-4094-AF1D-65872D36A357}</li> <li>{846ee342-7039-11de-9d20-806eef6e6963}</li> </ul> </li> <li>PersistentRoutes</li> <li>Winsock</li> <li>Performance</li> <li>ServiceProvider</li> </ul> </li> <li>TCPIP6</li> <li>TCPIP6TUNNEL</li> <li>tcpipreg</li> </ul>		UseZeroBroadcast	REG_DWORD 0x00000000 (0)
		EnableDeadGWDetect	REG_DWORD 0x00000001 (1)
		EnableDHCP	REG_DWORD 0x00000001 (1)
		NameServer	REG_SZ (value not set)
		Domain	REG_SZ (value not set)
		RegistrationEnabled	REG_DWORD 0x00000001 (1)
		RegisterAdapterName	REG_DWORD 0x00000000 (0)
		DhcpIPAddress	REG_SZ 172.16.53.141
		DhcpSubnetMask	REG_SZ 255.255.255.0
		DhcpServer	REG_SZ 172.16.53.254
		Lease	REG_DWORD 0x00000708 (1800)
		LeaseObtainedTime	REG_DWORD 0x5005D273 (1342558835)
		T1	REG_DWORD 0x5005D5F7 (1342559735)
		T2	REG_DWORD 0x5005D89A (1342560410)
		LeaseTerminatesTime	REG_DWORD 0x5005D97B (1342560635)
		AddressType	REG_DWORD 0x00000000 (0)
		IsServerNapAware	REG_DWORD 0x00000000 (0)
		DhcpConnForceBroadcastFlag	REG_DWORD 0x00000000 (0)
Key Properties		DhcpInterfaceOptions	REG_BINARY 06 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 7B D9 0...
Last Written Time		DhcpGatewayHardware	REG_BINARY AC 10 35 02 06 00 00 00 50 56 FA 66 72
		DhcpGatewayHardwareCount	REG_DWORD 0x00000001 (1)
		DhcpNameServer	REG_SZ 172.16.53.2

#### DHCP Information.

DHCP was enabled, as indicated by the 1 in the EnableDHCP value, with the last assigned IP address being 172.16.53.141. According to the LastWriteTime, the device was assigned this IP address on 07/17/2012 at 21:00:35 UTC.