Windows 10 Registry

AGENDA

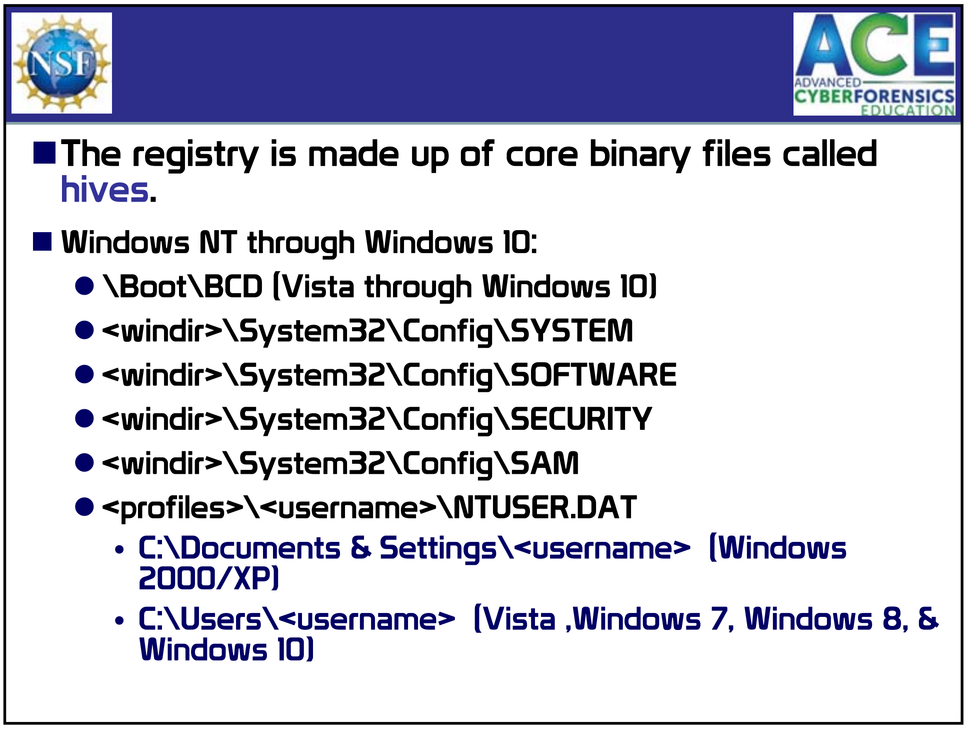
- About Dan Purcell…

AGENDA

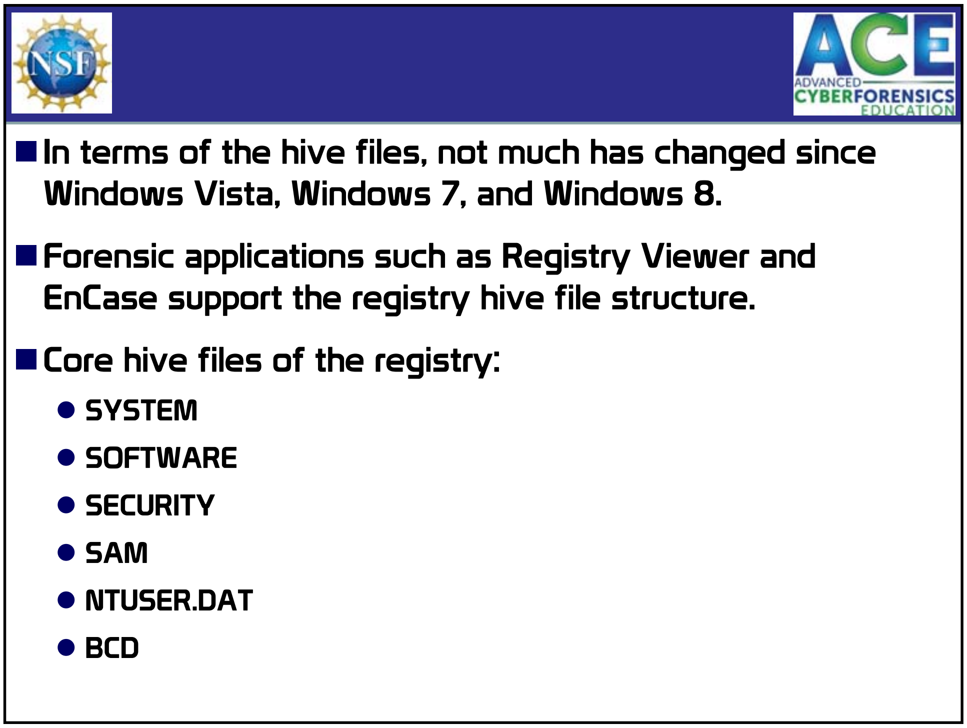
- Basic Registry Terminology & Structure
- Physical v. Logical
- Date & Time Formats Found in the Registry
- Windows 10 Registry Artifacts
- Physical Hive File Basics

- A large database that stores information such as:
  - Program/application settings
  - User settings/activity
  - Login/passwords
  - Historical information
  - Hardware settings
  - Services/processes
  - And so on…

- At first look, the Registry may seem like Matrix code, but 90% of the data in the registry has no forensic value. As examiners, we'll focus on the 10% that matters.



- The registry is made up of core binary files called hives.
- Windows NT through Windows 10:
  - \Boot\BCD (Vista through Windows 10)
  - <windir>\System32\Config\SYSTEM
  - <windir>\System32\Config\SOFTWARE
  - <windir>\System32\Config\SECURITY
  - <windir>\System32\Config\SAM
  - <profiles>\<username>\NTUSER.DAT
    - C:\Documents & Settings\<username> (Windows 2000/XP)
    - C:\Users\<username> (Vista ,Windows 7, Windows 8, & Windows 10)



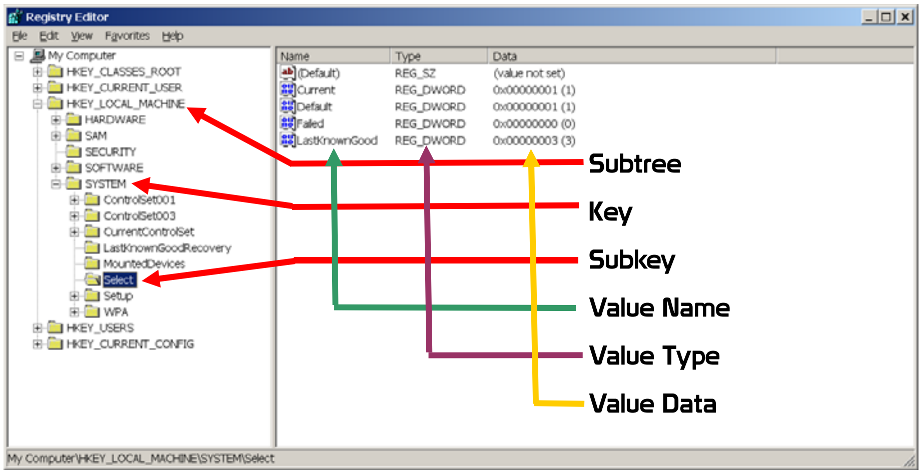
- In terms of the hive files, not much has changed since Windows Vista, Windows 7, and Windows 8.
- Forensic applications such as Registry Viewer and EnCase support the registry hive file structure.
- Core hive files of the registry:
  - SYSTEM
  - SOFTWARE
  - SECURITY
  - SAM
  - NTUSER.DAT
  - BCD

- SYSTEM, SOFTWARE, SECURITY, SAM are located in \Windows\System32\Config directory
- NTUSER.DAT is located in the \Users\<username> directory
- A registry file that was introduced in Windows Vista is “BCD”, which is located in the \Boot directory.
- BCD stands for Boot Configuration Data.
- According to Microsoft, this file replaced boot.ini in XP
- Boot.ini doesn’t support new architectures such as Extensible Firmware Interface (EFI) firmware.
- BCD is compatible with EFI and standard PC/AT arch.
- BCD holds information about the operating system(s) that can be loaded on the PC just like boot.ini.

- When Windows starts, the core files become active for Windows to modify, edit, read, etc.
- Active or Live Registry: normally viewed with Regedit in the Windows environment. (limited view)
- Static Registry: viewed with an offline registry viewer such as EnCase, Access Data Registry Viewer, etc..
- When viewing the active registry through Windows, you are limited in what you can view.
- In addition, the active registry contains some keys/subkeys that are normally not saved in the core registry files/hives (Hardware Key).

- The logical registry is viewed through a forensic or non-forensic application that is capable of reading and displaying the hives, keys, subkeys, and values in a manner that normally shows the parent/child relationship of objects within the hive.
- The physical registry is the binary content of the logical hive files. In order to understand the physical structure, one must understand the signatures of keys and values along with other specific attributes of the registry hive.
- By understanding some of the basics of the physical registry, examiners may identify registry fragments in unallocated clusters, pagefile.sys, slack space, etc.

- Remember, the registry is a hierarchical database, and as such, examiners must be familiar with common registry terminology.



Name	Type	Data
(Default)	REG_SZ	(value not set)
Current	REG_DWORD	0x00000001 (1)
Default	REG_DWORD	0x00000001 (1)
Failed	REG_DWORD	0x00000000 (0)
LastKnownGood	REG_DWORD	0x00000003 (3)

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\Select

Subtree

Key

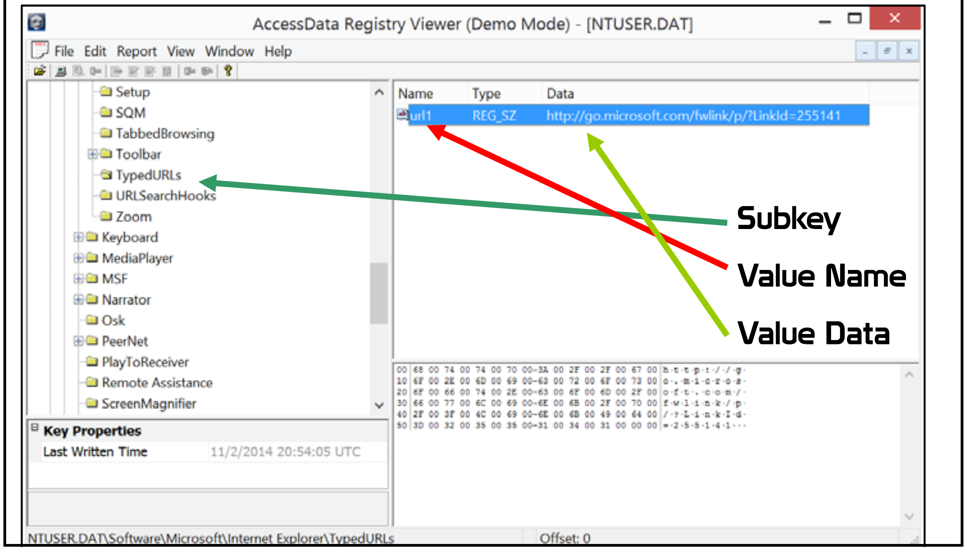
Subkey

Value Name

Value Type

Value Data

Same terms: Access Data Registry Viewer.



Name	Type	Data
url1	REG_SZ	http://go.microsoft.com/fwlink/p/?LinkId=255141

Key Properties

Last Written Time	11/2/2014 20:54:05 UTC

```
00 68 00 74 00 74 00 70 00-3A 00 2F 00 2F 00 67 00 h·t·t·p·:·/·/·g·
10 6F 00 2E 00 6D 00 69 00-63 00 72 00 6F 00 73 00 o·.·m·i·c·r·o·s·
20 6F 00 66 00 74 00 2E 00-63 00 6F 00 6D 00 2F 00 o·f·t·.·c·o·m·/·
30 66 00 77 00 6C 00 69 00-6E 00 6B 00 2F 00 70 00 f·w·l·i·n·k·/·p·
40 2F 00 3F 00 4C 00 69 00-6E 00 6B 00 49 00 64 00 /·?·L·i·n·k·I·d·
50 3D 00 32 00 35 00 35 00-31 00 34 00 31 00 00 00 =·2·5·5·1·4·1···
```

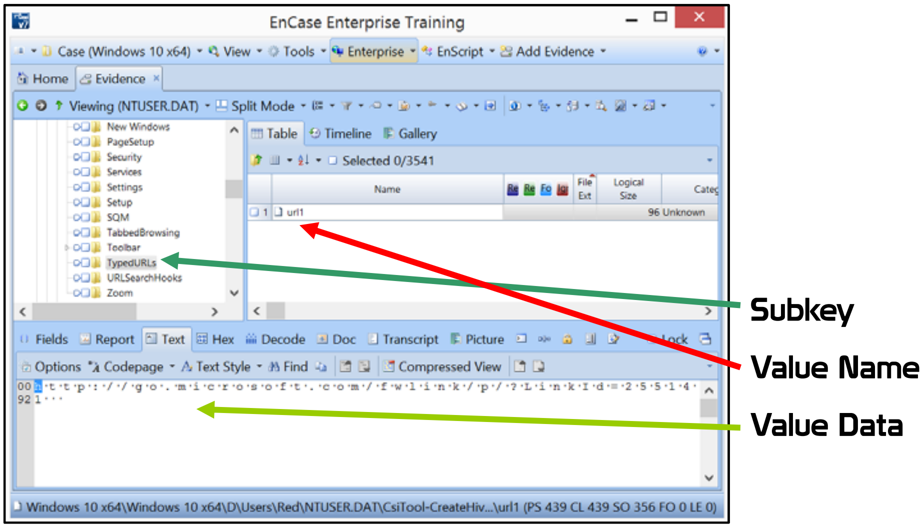
NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURLs   Offset: 0

Subkey

Value Name

Value Data

Same terms (minus subtree), but as viewed within EnCase 7.



	Name	File Ext	Logical Size	Categ
1	url1		96	Unknown

```
00 h·t·t·p·:·/·/·g·o·.·m·i·c·r·o·s·o·f·t·.·c·o·m·/·f·w·l·i·n·k·/·p·/·?·L·i·n·k·I·d·=·2·5·5·1·4·
92 1···
```

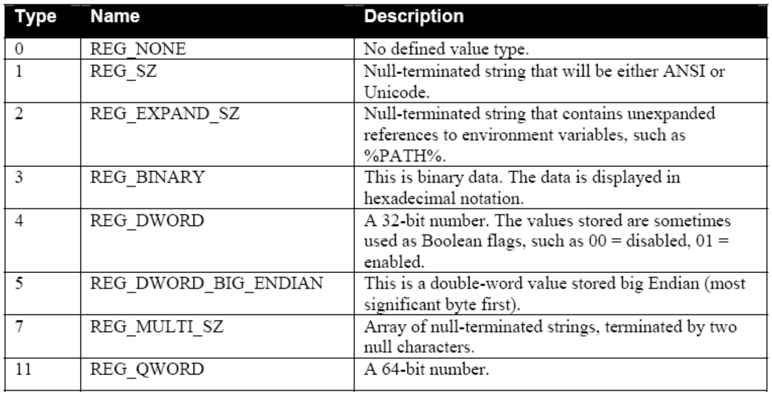
Windows 10 x64\Windows 10 x64\D\Users\Red\NTUSER.DAT\CsiTool-CreateHiv...\url1 (PS 439 CL 439 SO 356 FO 0 LE 0)

Subkey

Value Name

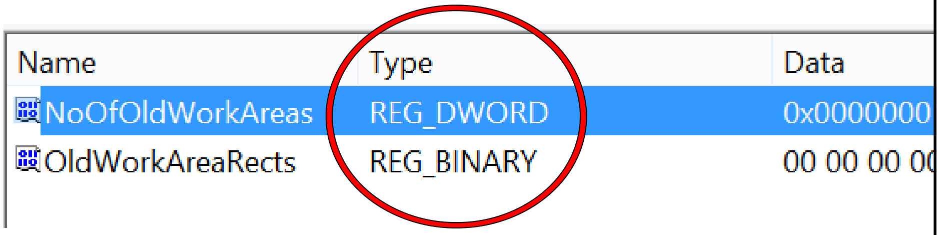
Value Data

- The registry's value types vary depending on the type of data required.
- A common list of value types is provided for reference



Type	Name	Description
0	REG_NONE	No defined value type.
1	REG_SZ	Null-terminated string that will be either ANSI or Unicode.
2	REG_EXPAND_SZ	Null-terminated string that contains unexpanded references to environment variables, such as %PATH%.
3	REG_BINARY	This is binary data. The data is displayed in hexadecimal notation.
4	REG_DWORD	A 32-bit number. The values stored are sometimes used as Boolean flags, such as 00 = disabled, 01 = enabled.
5	REG_DWORD_BIG_ENDIAN	This is a double-word value stored big Endian (most significant byte first).
7	REG_MULTI_SZ	Array of null-terminated strings, terminated by two null characters.
11	REG_QWORD	A 64-bit number.

- Example of Registry Value Type through Access Data's Registry Viewer
- DWORD: 32 bit value, 4 bytes
- Binary: Hex values, no specific length



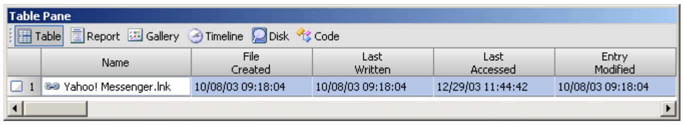
Name	Type	Data
NoOfOldWorkAreas	REG_DWORD	0x0000000
OldWorkAreaRects	REG_BINARY	00 00 00 00

FILETIME FORMAT:

- FILETIME format is used throughout the NTFS file system
- FILETIME format is very common within the Windows Registry and numerous Microsoft software products.
- Important to note that the displayed date/time is subject to the correct offset from GMT/UTC
- To correctly translate, the examiner must determine the regional settings used on the subject's installation of Windows. (we'll cover this in a few minutes)

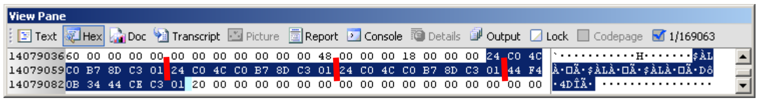
FILETIME FORMAT:

- 8-byte value (always ends to 0x01)
- Number of 100-nanosecond intervals from January 1, 1601 (GMT) to the specified moment.
- Example: Dates and Times for a file on an NTFS volume…



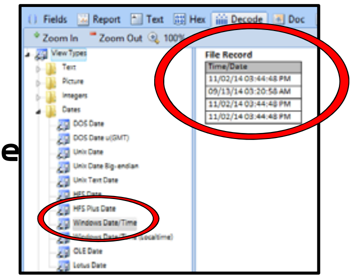
	Name	File Created	Last Written	Last Accessed	Entry Modified
□ 1	Yahoo! Messenger.lnk	10/08/03 09:18:04	10/08/03 09:18:04	12/29/03 11:44:42	10/08/03 09:18:04

- Hex representation within the MFT Entry for the same file:



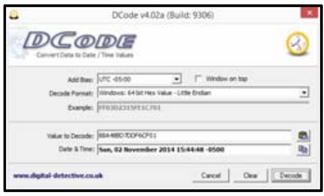
```
1407903660 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 18 00 00 00 24 C0 4C  `···········H·······$ÀL
14079059C0 B7 8D C3 01 24 C0 4C C0 B7 8D C3 01 24 C0 4C C0 B7 8D C3 01 44 F4  À·□Ã·$ÀLÀ·□Ã·$ÀLÀ·□Ã·Dô
140790820B 34 44 CE C3 01 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·4DÎÃ· ················
```

- With the data highlighted, right click in EnCase and select Bookmark Data.
- The Data Type pane allows you to select a number of different Date/Time formats.
- In this case, we've selected Windows Date/Time, which will decode the data in FILETIME format using the default or examiner-selected GMT offset.
- In the bottom portion of the Bookmark Data window, one can see the decoded data.



File Record

Time/Date
11/02/14 03:44:48 PM
09/13/14 03:20:58 AM
11/02/14 03:44:48 PM
11/02/14 03:44:48 PM

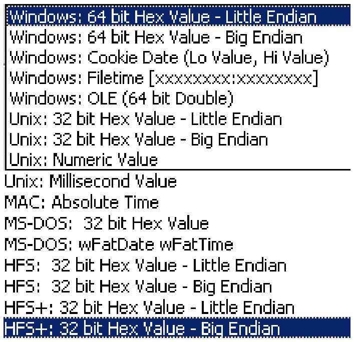

DCode v4.02a (Build: 9306)
DCODE
Convert Data to Date / Time Values
Cancel
Clear
Decode

Add Bias: UTC -05:00
□ Window on top
Decode Format: Windows: 64 bit Hex Value - Little Endian
Example: FF03D2315FE3C701
Value to Decode: 00A48BD7DDF6CF01
Date & Time: Sun, 02 November 2014 15:44:48 -0500

www.digital-detective.co.uk

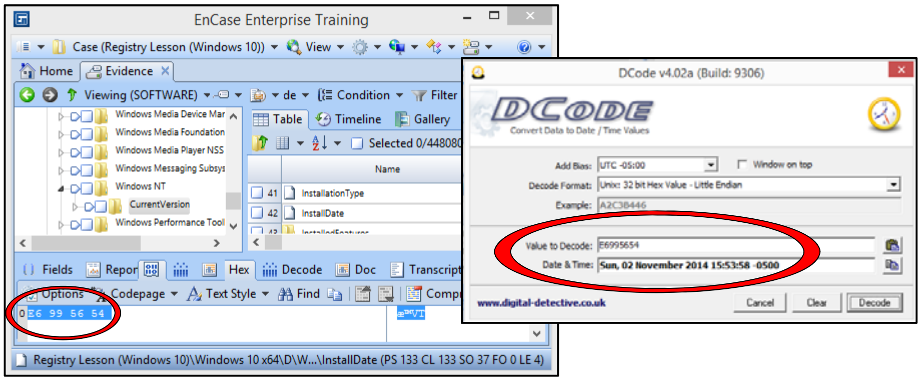
Other Common Date/Time Formats

- DOS Date
- DOS Date (GMT)
- Unix (4 byte – Big Endian also)
- Unix Numeric (10 byte)
- HFS Date
- HFS Plus Date
- Windows (FILETIME – GMT or Local)



Windows: 64 bit Hex Value - Little Endian
Windows: 64 bit Hex Value - Big Endian
Windows: Cookie Date (Lo Value, Hi Value)
Windows: Filetime [xxxxxxxx:xxxxxxxx]
Windows: OLE (64 bit Double)
Unix: 32 bit Hex Value - Little Endian
Unix: 32 bit Hex Value - Big Endian
Unix: Numeric Value
Unix: Millisecond Value
MAC: Absolute Time
MS-DOS: 32 bit Hex Value
MS-DOS: wFatDate wFatTime
HFS: 32 bit Hex Value - Little Endian
HFS: 32 bit Hex Value - Big Endian
HFS+: 32 bit Hex Value - Little Endian
HFS+: 32 bit Hex Value - Big Endian

- Unix 32-bit Date/Time (4 bytes)
- The Software hive in Windows 10 stores the Installation Date/Time under the value name, “InstallDate” with a Unix 32-bit value.
- In your forensic software, select the correct offset from GMT/UTC.



EnCase Enterprise Training

Case (Registry Lesson (Windows 10))

Viewing (SOFTWARE)

	Name
41	InstallationType
42	InstallDate

```
0 E6 99 56 54
```

Registry Lesson (Windows 10)\Windows 10 x64\D\W...\InstallDate (PS 133 CL 133 SO 37 FO 0 LE 4)

DCode v4.02a (Build: 9306)

DCODE Convert Data to Date / Time Values

Add Bias: UTC -05:00 □ Window on top

Decode Format: Unix: 32 bit Hex Value - Little Endian

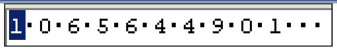
Example: A2C38446

Value to Decode: E6995654

Date & Time: Sun, 02 November 2014 15:53:58 -0500

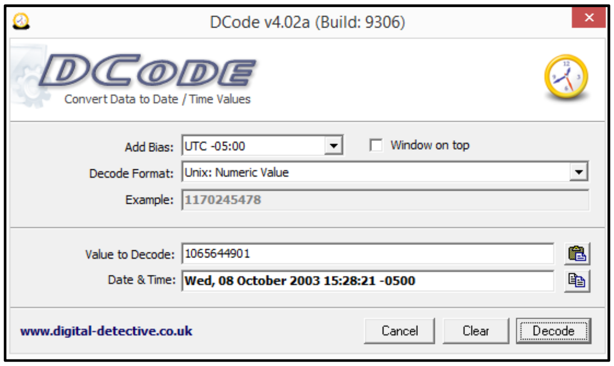
www.digital-detective.co.uk

- Unix Numeric Values are common



1·0·6·5·6·4·4·9·0·1···

- The value data is typically stored in Unicode, so you’ll have to remove the “0x00” 8 bits. In other words, only compute the numbers!
- As previously viewed in this lesson, a good tool to decode dates and times is Craig Wilson’s “DCODE” from www.digital-detective.co.uk.



DCode v4.02a (Build: 9306)

DCODE Convert Data to Date / Time Values

Add Bias: UTC -05:00 □ Window on top

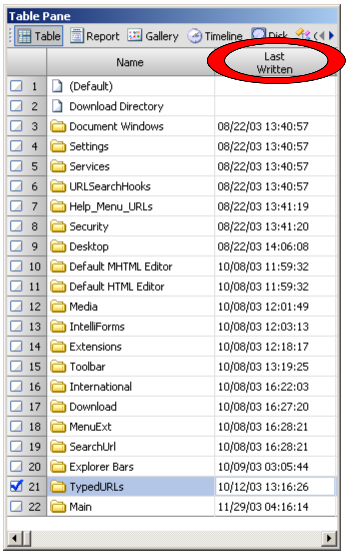
Decode Format: Unix: Numeric Value

Example: 1170245478

Value to Decode: 1065644901

Date & Time: Wed, 08 October 2003 15:28:21 -0500

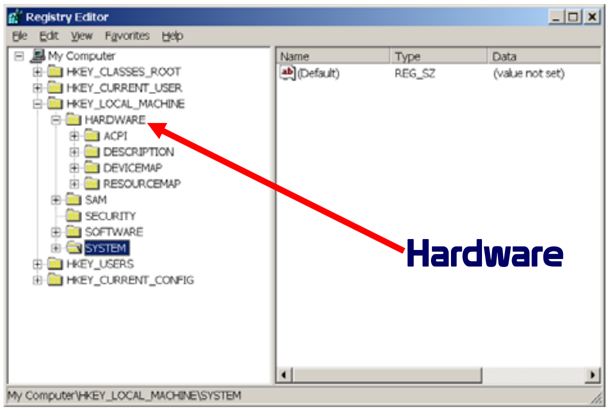
www.digital-detective.co.uk



		Name	Last Written
□	1	(Default)	
□	2	Download Directory	
□	3	Document Windows	08/22/03 13:40:57
□	4	Settings	08/22/03 13:40:57
□	5	Services	08/22/03 13:40:57
□	6	URLSearchHooks	08/22/03 13:40:57
□	7	Help_Menu_URLs	08/22/03 13:41:19
□	8	Security	08/22/03 13:41:20
□	9	Desktop	08/22/03 14:06:08
□	10	Default MHTML Editor	10/08/03 11:59:32
□	11	Default HTML Editor	10/08/03 11:59:32
□	12	Media	10/08/03 12:01:49
□	13	IntelliForms	10/08/03 12:03:13
□	14	Extensions	10/08/03 12:18:17
□	15	Toolbar	10/08/03 13:19:25
□	16	International	10/08/03 16:22:03
□	17	Download	10/08/03 16:27:20
□	18	MenuExt	10/08/03 16:28:21
□	19	SearchUrl	10/08/03 16:28:21
□	20	Explorer Bars	10/09/03 03:05:44
☑	21	TypedURLs	10/12/03 13:16:26
□	22	Main	11/29/03 04:16:14

- The only object that consistently records a modification date/time is the key/subkey. 🗀
- Value Names, Types, and Data do NOT record a last modified date/time.
- If a child object of the subkey is changed (values), the last modified date/time of the subkey will reflect the date and time of the change.

- The "hardware" subtree is not viewable in the static registry.



```
My Computer
  HKEY_CLASSES_ROOT
  HKEY_CURRENT_USER
  HKEY_LOCAL_MACHINE
    HARDWARE
      ACPI
      DESCRIPTION
      DEVICEMAP
      RESOURCEMAP
    SAM
    SECURITY
    SOFTWARE
    SYSTEM
  HKEY_USERS
  HKEY_CURRENT_CONFIG
```

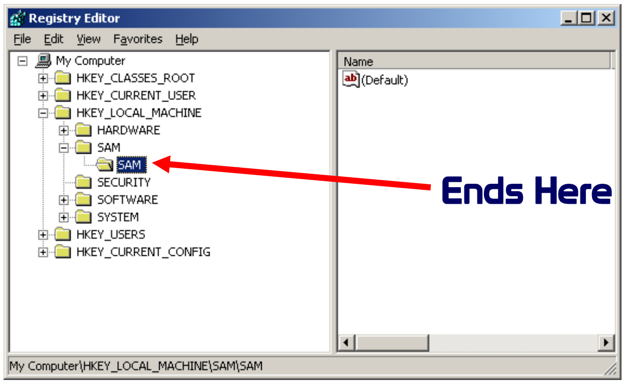
Name	Type	Data
(Default)	REG_SZ	(value not set)

My Computer\HKEY_LOCAL_MACHINE\SYSTEM

Hardware

The hardware subtree is mounted and active when Windows is running. The subtree is dismounted when Windows shuts down.

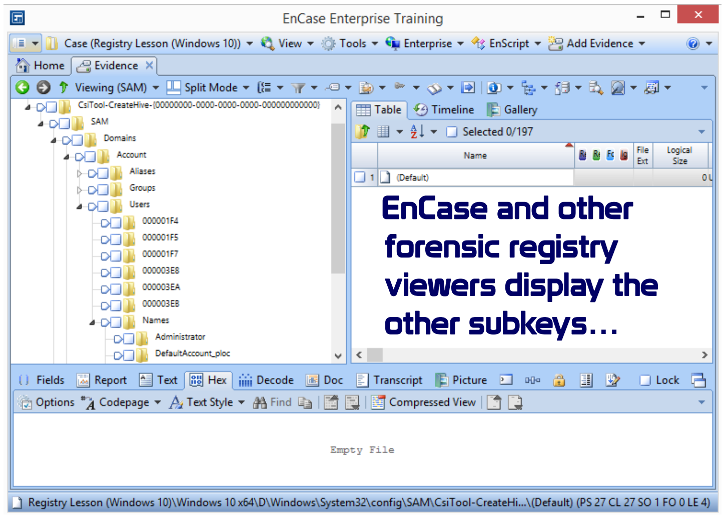
- The live view of the SAM file (Security Accounts Manager) with Regedit is extremely limited (default permissions do not allow viewing).



My Computer\HKEY_LOCAL_MACHINE\SAM\SAM

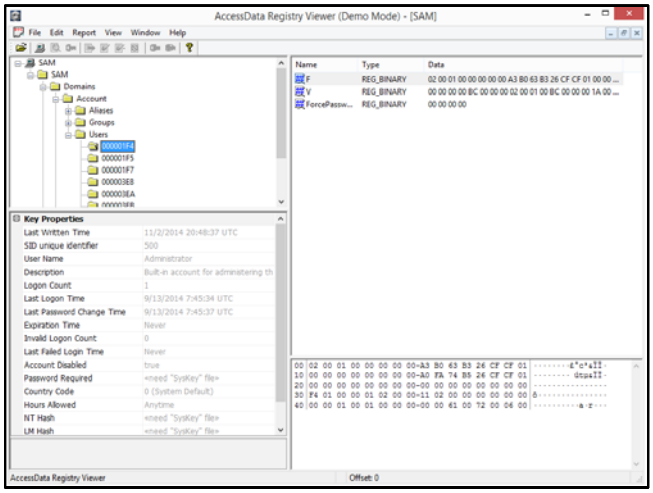
Ends Here

- The static view of the SAM file with EnCase…



Registry Lesson (Windows 10)\Windows 10 x64\D\Windows\System32\config\SAM\CsiTool-CreateHi...\(Default) (PS 27 CL 27 SO 1 FO 0 LE 4)

EnCase and other forensic registry viewers display the other subkeys…



AccessData Registry Viewer (Demo Mode) - [SAM]

Name	Type	Data
F	REG_BINARY	02 00 01 00 00 00 00 00 A3 B0 63 B3 26 CF CF 01 00 00 ...
V	REG_BINARY	00 00 00 00 BC 00 00 00 02 00 01 00 BC 00 00 00 1A 00 ...
ForcePassw...	REG_BINARY	00 00 00 00

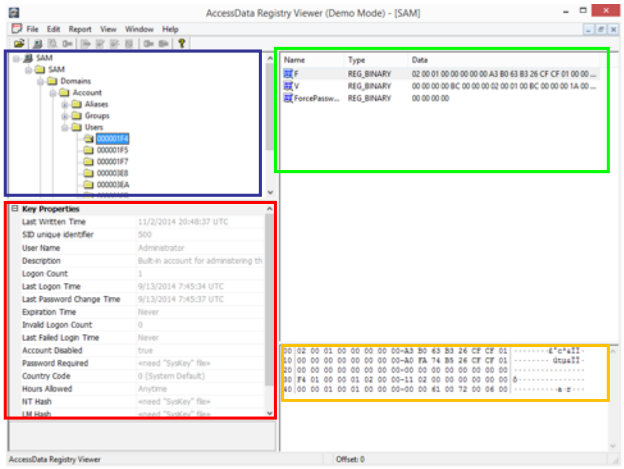
Key Properties

Last Written Time	11/2/2014 20:48:37 UTC
SID unique identifier	500
User Name	Administrator
Description	Built-in account for administering th
Logon Count	1
Last Logon Time	9/13/2014 7:45:34 UTC
Last Password Change Time	9/13/2014 7:45:37 UTC
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	Never
Account Disabled	true
Password Required	«need "SysKey" file»
Country Code	0 (System Default)
Hours Allowed	Anytime
NT Hash	«need "SysKey" file»
LM Hash	«need "SysKey" file»

```
00 02 00 01 00 00 00 00 00-A3 B0 63 B3 26 CF CF 01 ........£"c"&ÏÏ.
10 00 00 00 00 00 00 00 00-A0 FA 74 B5 26 CF CF 01 ........ út µ&ÏÏ.
20 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
30 F4 01 00 00 01 02 00 00-11 02 00 00 00 00 00 00 ô...............
40 00 00 01 00 01 00 00 00-00 00 61 00 72 00 06 00 ..........a.r...
```

AccessData Registry Viewer   Offset: 0

- Registry Viewer 1.8.0.5 is the latest version as of this writing and is compatible with Windows 10 Registry files.
- Layout similar to Regedit
- Reads one registry hive at a time
- Excellent reporting tool!



AccessData Registry Viewer (Demo Mode) - [SAM]

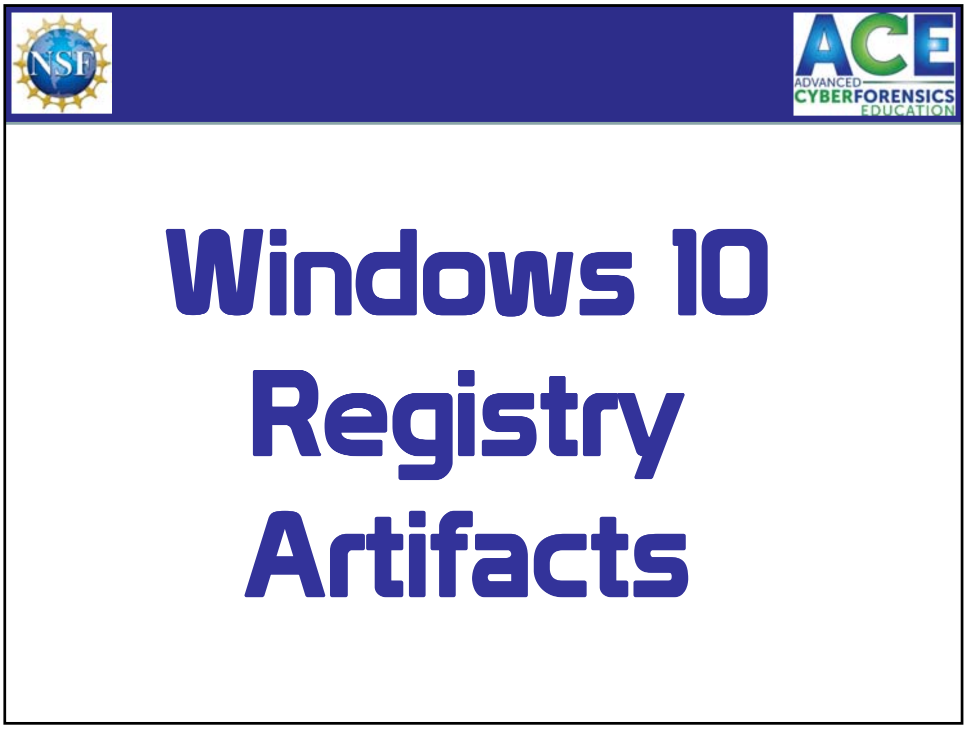
Name	Type	Data
F	REG_BINARY	02 00 01 00 00 00 00 00 A3 B0 63 B3 26 CF CF 01 00 00 ...
V	REG_BINARY	00 00 00 00 BC 00 00 00 02 00 01 00 BC 00 00 00 1A 00 ...
ForcePassw...	REG_BINARY	00 00 00 00

Key Properties

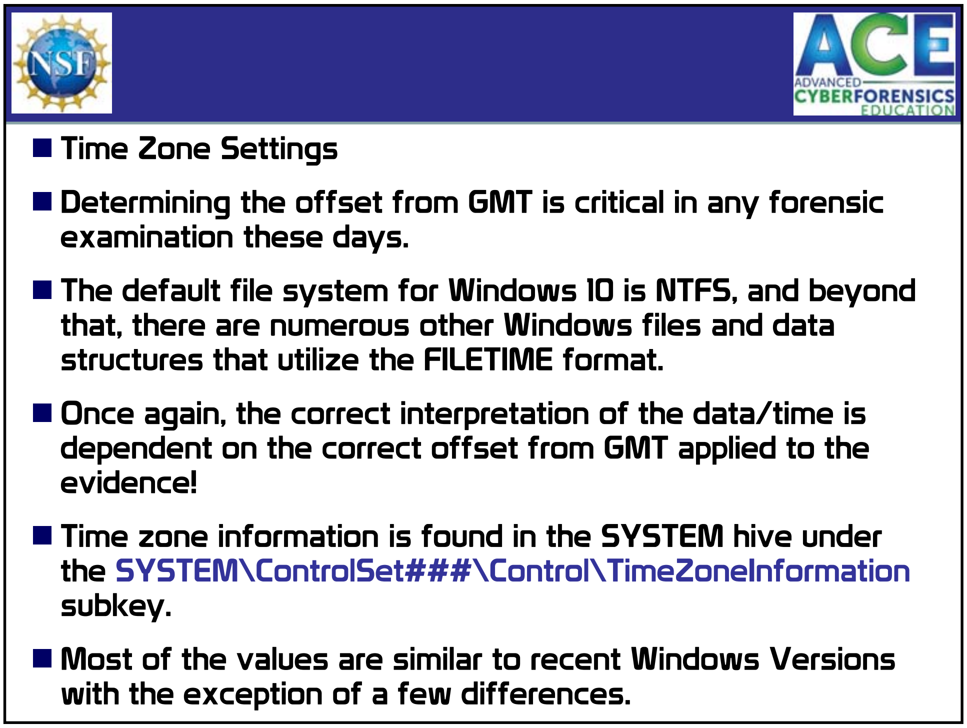
Last Written Time	11/2/2014 20:48:37 UTC
SID unique identifier	500
User Name	Administrator
Description	Built-in account for administering th
Logon Count	1
Last Logon Time	9/13/2014 7:45:34 UTC
Last Password Change Time	9/13/2014 7:45:37 UTC
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	Never
Account Disabled	true
Password Required	«need "SysKey" file»
Country Code	0 (System Default)
Hours Allowed	Anytime
NT Hash	«need "SysKey" file»
LM Hash	«need "SysKey" file»

AccessData Registry Viewer   Offset: 0

- Left pane: keys/subkeys
- Right pane: values
- Bottom left: Key properties mostly, but sometimes value properties, if applicable
- Bottom right: value in hex/text
- Dates/times reported in UTC/GMT (all)

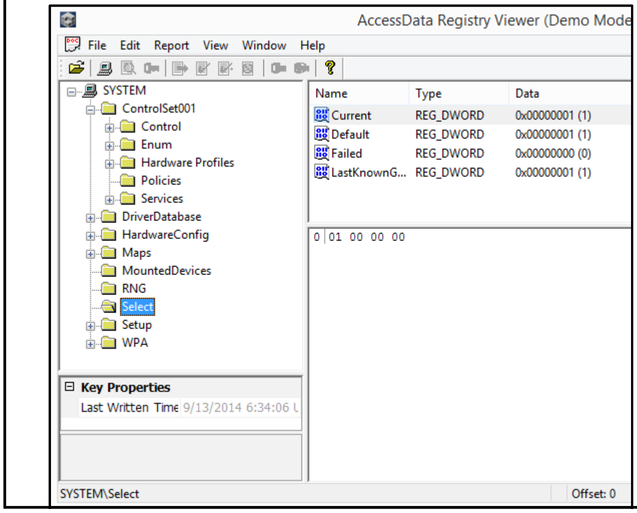


Windows 10 Registry Artifacts



- Time Zone Settings
- Determining the offset from GMT is critical in any forensic examination these days.
- The default file system for Windows 10 is NTFS, and beyond that, there are numerous other Windows files and data structures that utilize the FILETIME format.
- Once again, the correct interpretation of the data/time is dependent on the correct offset from GMT applied to the evidence!
- Time zone information is found in the SYSTEM hive under the SYSTEM\ControlSet###\Control\TimeZoneInformation subkey.
- Most of the values are similar to recent Windows Versions with the exception of a few differences.

- First, determine the current control set.
- Locate the **SYSTEM\Select\Current value**



Name	Type	Data
Current	REG_DWORD	0x00000001 (1)
Default	REG_DWORD	0x00000001 (1)
Failed	REG_DWORD	0x00000000 (0)
LastKnownG...	REG_DWORD	0x00000001 (1)

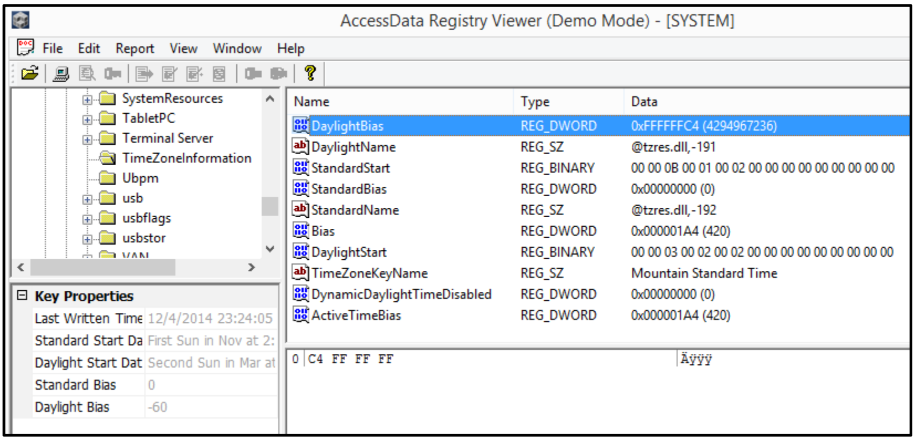
```
0 01 00 00 00
```

Key Properties

Last Written Time 9/13/2014 6:34:06 L

SYSTEM\Select   Offset: 0

- Next, navigate to the **SYSTEM\ControlSet00#\Control\TimeZoneInformation** subkey. *Let's explore the values…*

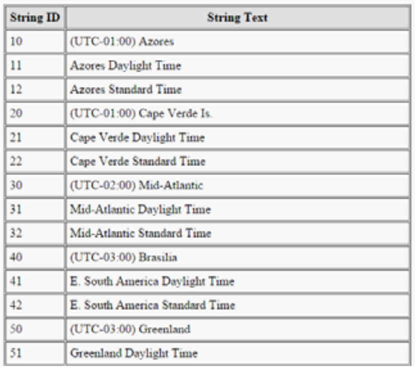

AccessData Registry Viewer (Demo Mode) - [SYSTEM]
File Edit Report View Window Help
SystemResources
TabletPC
Terminal Server
TimeZoneInformation
Ubpm
usb
usbflags
usbstor
VAN

Name	Type	Data
DaylightBias	REG_DWORD	0xFFFFFFC4 (4294967236)
DaylightName	REG_SZ	@tzres.dll,-191
StandardStart	REG_BINARY	00 00 0B 00 01 00 02 00 00 00 00 00 00 00 00 00
StandardBias	REG_DWORD	0x00000000 (0)
StandardName	REG_SZ	@tzres.dll,-192
Bias	REG_DWORD	0x000001A4 (420)
DaylightStart	REG_BINARY	00 00 03 00 02 00 02 00 00 00 00 00 00 00 00 00
TimeZoneKeyName	REG_SZ	Mountain Standard Time
DynamicDaylightTimeDisabled	REG_DWORD	0x00000000 (0)
ActiveTimeBias	REG_DWORD	0x000001A4 (420)

```
0 C4 FF FF FF                                  Äÿÿÿ
```

Key Properties	
Last Written Time	12/4/2014 23:24:05
Standard Start Da	First Sun in Nov at 2:
Daylight Start Dat	Second Sun in Mar at
Standard Bias	0
Daylight Bias	-60

- Daylight Name and Standard Name
- Both refer to TZRES.DLL with a string identifier.
- Within the DLL file, there are string identifiers that refer to specific time zone offsets. See the example below & URL.



String ID	String Text
10	(UTC-01:00) Azores
11	Azores Daylight Time
12	Azores Standard Time
20	(UTC-01:00) Cape Verde Is.
21	Cape Verde Daylight Time
22	Cape Verde Standard Time
30	(UTC-02:00) Mid-Atlantic
31	Mid-Atlantic Daylight Time
32	Mid-Atlantic Standard Time
40	(UTC-03:00) Brasilia
41	E. South America Daylight Time
42	E. South America Standard Time
50	(UTC-03:00) Greenland
51	Greenland Daylight Time

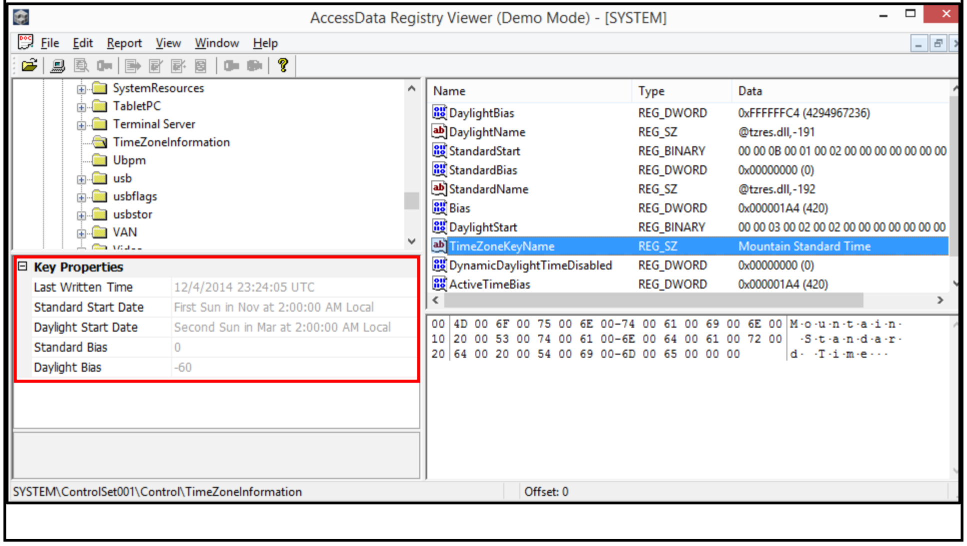
http://www.nirsoft.net/dll_information/windows8/tzres_dll.html

- Daylight Bias: Number of minutes offset from the bias for DST settings
- Standard Bias: Number of minutes offset from the bias for standard (usually zero)
- Daylight Start & Standard Start: (See Next Slide)
- Bias: Number of minutes offset from UTC for the Time Zone Setting
- ActiveTimeBias: Number of minutes offset from UTC for the *current* time setting
- TimeZoneKeyName: Friendly Time Zone Setting Name
- DynamicDaylightTimeDisabled: (See Next Slide)

- Daylight Start & Standard Start
- Sixteen Bytes, 2 bytes per meaning, convert hex to decimal
- Year, Month, Week, Hour, Minutes, Seconds, Milliseconds, Day
  - Year: If the year is zero, it reoccurs every year
  - Month: # indicates the month (1-12)
  - Week: week in the month when the setting will start
  - Hour: # hour of the day in 24-hour format
  - Minutes: # of minutes when the setting will start
  - Seconds: # of seconds when the setting will start
  - Milliseconds: # of seconds when the setting will start
  - Day: Day of the week when the setting will start

- Example of Standard Start value data (hex)
- 00 00 0B 00 01 00 02 00 00 00 00 00 00 00 00 00
  - Year: 00 00 = every year
  - Month: 0B 00 = 11 (November)
  - Week: 01 00 = 1 (first week of the month)
  - Hour: 02 00 = 2 (2nd hour of the day, 0200 hours or 2AM)
  - Minutes: 00 = 0 (no offset)
  - Seconds: 00 = 0 (no offset)
  - Milliseconds: 00 = 0 (no offset)
  - Day: 00 = 0 (no offset)

- Same value as shown in Registry Viewer


AccessData Registry Viewer (Demo Mode) - [SYSTEM]
File Edit Report View Window Help
SystemResources
TabletPC
Terminal Server
TimeZoneInformation
Ubpm
usb
usbflags
usbstor
VAN

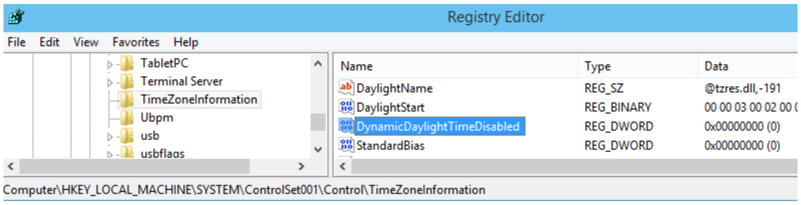
Key Properties	
Last Written Time	12/4/2014 23:24:05 UTC
Standard Start Date	First Sun in Nov at 2:00:00 AM Local
Daylight Start Date	Second Sun in Mar at 2:00:00 AM Local
Standard Bias	0
Daylight Bias	-60

Name	Type	Data
DaylightBias	REG_DWORD	0xFFFFFFC4 (4294967236)
DaylightName	REG_SZ	@tzres.dll,-191
StandardStart	REG_BINARY	00 00 0B 00 01 00 02 00 00 00 00 00 00 00
StandardBias	REG_DWORD	0x00000000 (0)
StandardName	REG_SZ	@tzres.dll,-192
Bias	REG_DWORD	0x000001A4 (420)
DaylightStart	REG_BINARY	00 00 03 00 02 00 02 00 00 00 00 00 00 00
TimeZoneKeyName	REG_SZ	Mountain Standard Time
DynamicDaylightTimeDisabled	REG_DWORD	0x00000000 (0)
ActiveTimeBias	REG_DWORD	0x000001A4 (420)

```
00 4D 00 6F 00 75 00 6E 00-74 00 61 00 69 00 6E 00 M·o·u·n·t·a·i·n·
10 20 00 53 00 74 00 61 00-6E 00 64 00 61 00 72 00  ·S·t·a·n·d·a·r·
20 64 00 20 00 54 00 69 00-6D 00 65 00 00 00       d· ·T·i·m·e···
```

SYSTEM\ControlSet001\Control\TimeZoneInformation Offset: 0

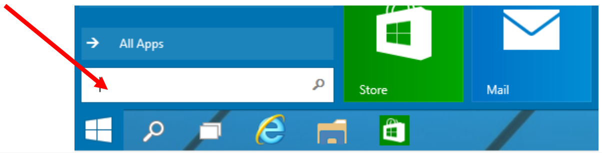
- If a user selects the option to NOT automatically adjust for daylight savings, the value data for the value name "DynamicDaylightTimeDisabled" changes from a 0 to a 1.
- The value data is a 32-bit integer (4 bytes) decoded little endian (hex to decimal). If the value is "1" daylight savings will NOT apply.



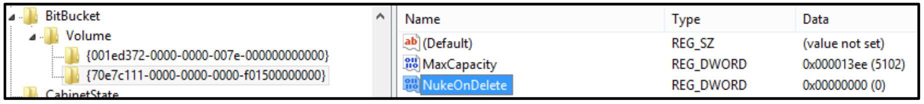
Name	Type	Data
DaylightName	REG_SZ	@tzres.dll,-191
DaylightStart	REG_BINARY	00 00 03 00 02 00 (
DynamicDaylightTimeDisabled	REG_DWORD	0x00000000 (0)
StandardBias	REG_DWORD	0x00000000 (0)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\TimeZoneInformation

- UsrClass.dat is another registry file that was introduced in Windows Vista
- It is located in the \Users\<user name>\AppData \Local\Microsoft\Windows directory.
- From the start menu in Windows 10, the run command no longer exists. It was replaced with a search field directly above the Windows icon.
- Some commands (not all) result in an entry in the \<SID>_Classes\LocalSettings\Software \Microsoft\Windows\Shell\MuiCache subkey



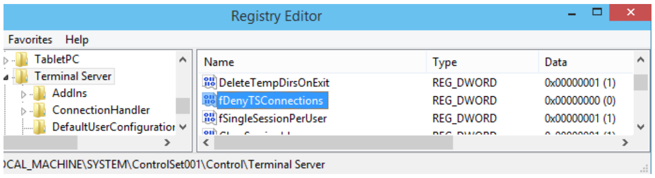
- The properties of the Windows 10 recycle bin have been consistent since Vista.
- In Windows, user's can send (move) files to the Recycle Bin or completely bypass it (similar to Shift + Delete command)
- In Windows 10 (Vista, 7 and 8 as well), the registry path is NTUSER.DAT\Software\Microsoft\ Windows\CurrentVersion\Explorer\BitBucket\Volume\{GUID}\ NukeOnDelete
- 1 = bypass Recycle Bin, 0 = move to Recycle Bin
- This setting is user specific (not the entire system, unless set by a group policy)
- Max capacity of the user's Recycle Bin is also list in the value Max Capacity (hex to decimal = megabytes of maximum files in the bin)



BitBucket
Volume
{001ed372-0000-0000-007e-000000000000}
{70e7c111-0000-0000-0000-f01500000000}
CabinetState

Name	Type	Data
(Default)	REG_SZ	(value not set)
MaxCapacity	REG_DWORD	0x000013ee (5102)
NukeOnDelete	REG_DWORD	0x00000000 (0)

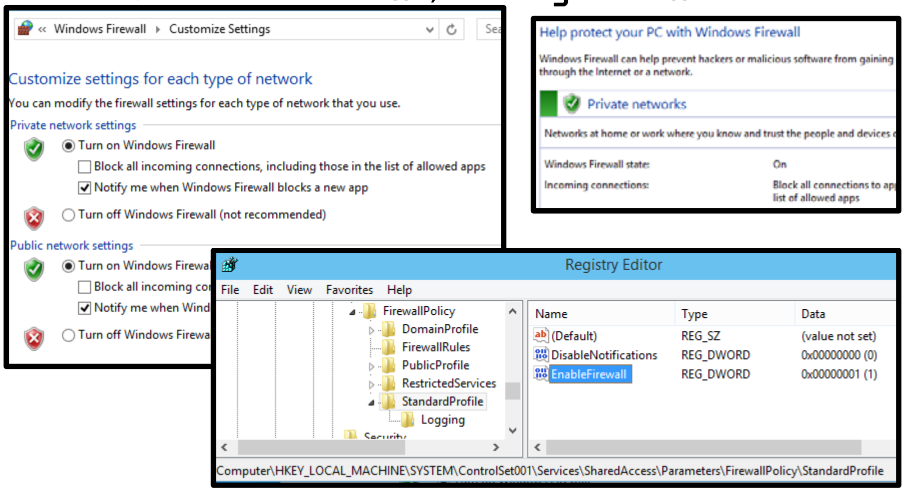
- Remote Desktop (RD) is a feature that allows a user to log in to a computer from a remote location and run the OS, access files, run programs, as it they were sitting in front of the physical device.
- Why should examiners care about this feature?
- “Someone logged into my computer and did this, not me”
- In Windows 10, the registry path to determine if Remote Desktop is turned on or off is SYSTEM\ControlSet###\Control\Terminal Server\fDenyTSConnections
- 1 = RD is turned OFF
- 0 = RD is turned ON



Name	Type	Data
DeleteTempDirsOnExit	REG_DWORD	0x00000001 (1)
fDenyTSConnections	REG_DWORD	0x00000000 (0)
fSingleSessionPerUser	REG_DWORD	0x00000001 (1)

)CAL_MACHINE\SYSTEM\ControlSet001\Control\Terminal Server

- The Windows Firewall is normally turned on by default in both all versions of Windows, including Windows 10.



Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

● Turn on Windows Firewall

☐ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Firewall blocks a new app

○ Turn off Windows Firewall (not recommended)

Public network settings

● Turn on Windows Firewa

☐ Block all incoming co

☑ Notify me when Wind

○ Turn off Windows Firewa

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining through the Internet or a network.

Private networks

Networks at home or work where you know and trust the people and devices

Windows Firewall state: On

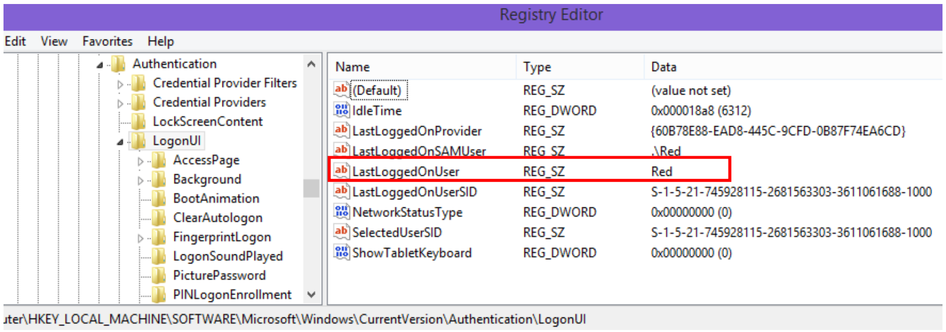
Incoming connections: Block all connections to ap list of allowed apps

Name	Type	Data
(Default)	REG_SZ	(value not set)
DisableNotifications	REG_DWORD	0x00000000 (0)
EnableFirewall	REG_DWORD	0x00000001 (1)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile

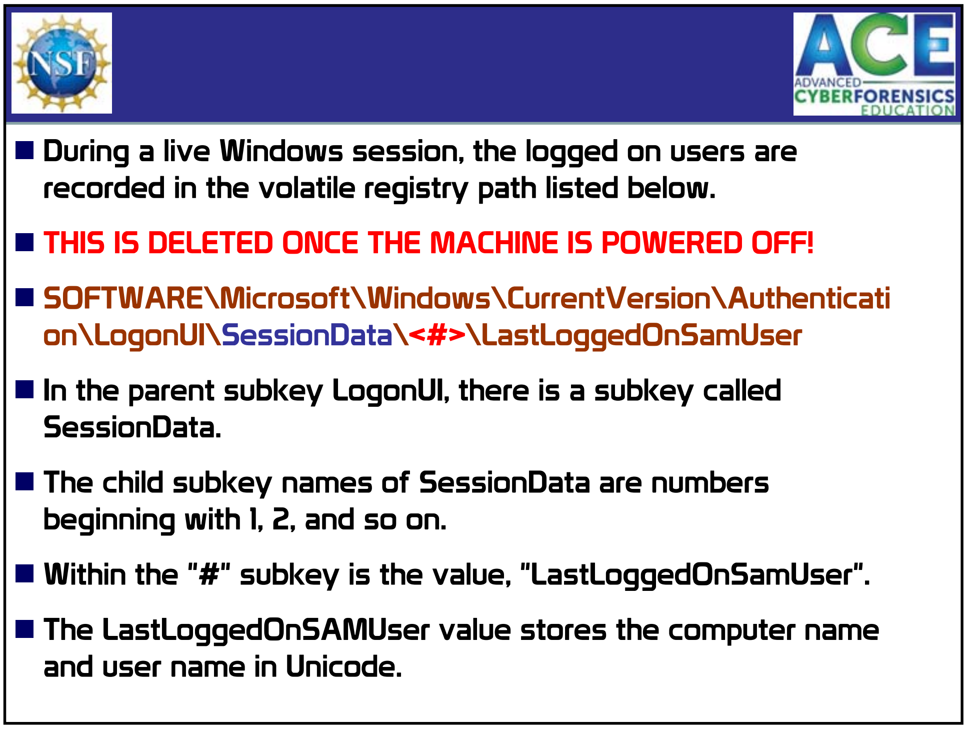
- The following registry values determine the state of the Windows Firewall for private (standard), public, and domain networks.
- SYSTEM\ControlSet###\Services\SharedAccess \Parameters\FirewallPolicy\StandardProfile\EnableFirewall
- SYSTEM\ControlSet###\Services\SharedAccess \Parameters\FirewallPolicy\PublicProfile\EnableFirewall
- SYSTEM\ControlSet###\Services\SharedAccess \Parameters\FirewallPolicy\DomainProfile\EnableFirewall
- 0 = OFF, 1 = ON
- The other surrounding subkeys store service restrictions and firewall rules (standard & user-defined)

- SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\LastLoggedOnUser
- The value data will list the user’s name, which is actually stored in Unicode.

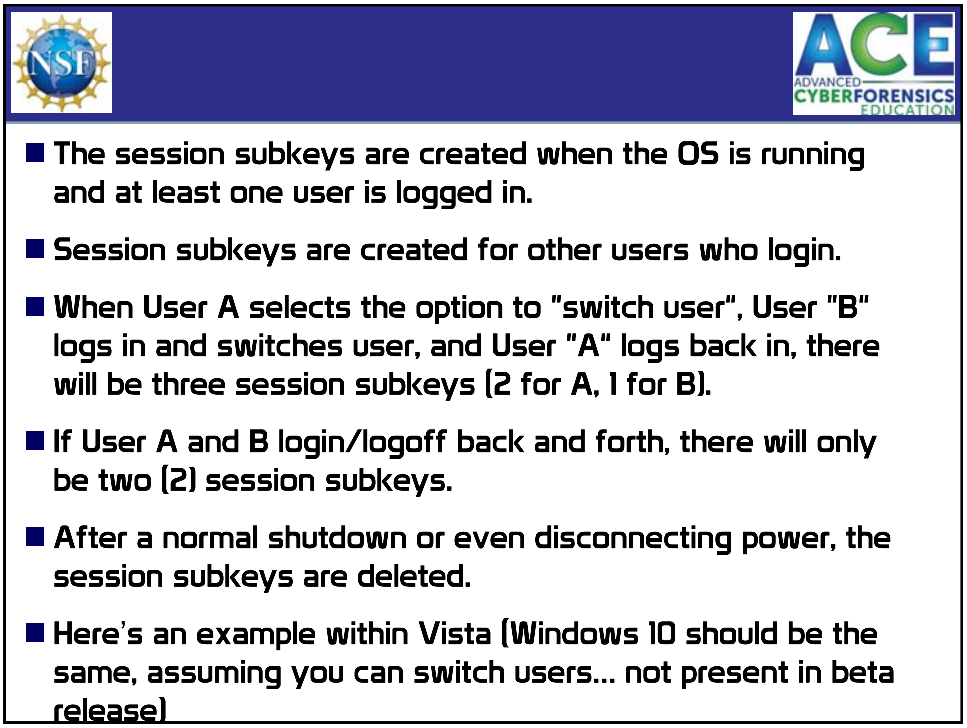


Name	Type	Data
(Default)	REG_SZ	(value not set)
IdleTime	REG_DWORD	0x000018a8 (6312)
LastLoggedOnProvider	REG_SZ	{60B78E88-EAD8-445C-9CFD-0B87F74EA6CD}
LastLoggedOnSAMUser	REG_SZ	.\Red
LastLoggedOnUser	REG_SZ	Red
LastLoggedOnUserSID	REG_SZ	S-1-5-21-745928115-2681563303-3611061688-1000
NetworkStatusType	REG_DWORD	0x00000000 (0)
SelectedUserSID	REG_SZ	S-1-5-21-745928115-2681563303-3611061688-1000
ShowTabletKeyboard	REG_DWORD	0x00000000 (0)

uter\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI

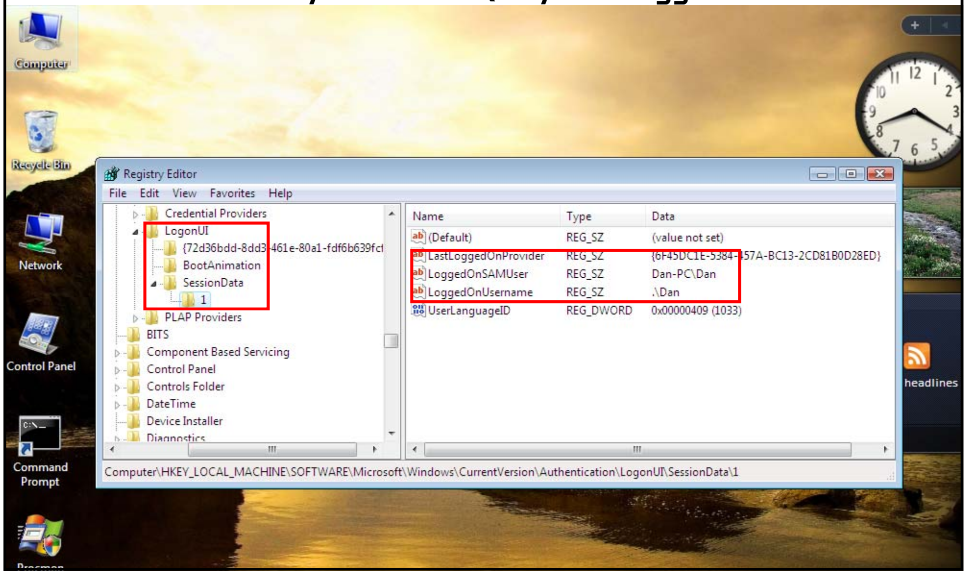


- During a live Windows session, the logged on users are recorded in the volatile registry path listed below.
- THIS IS DELETED ONCE THE MACHINE IS POWERED OFF!
- SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\SessionData\<#>\LastLoggedOnSamUser
- In the parent subkey LogonUI, there is a subkey called SessionData.
- The child subkey names of SessionData are numbers beginning with 1, 2, and so on.
- Within the "#" subkey is the value, "LastLoggedOnSamUser".
- The LastLoggedOnSAMUser value stores the computer name and user name in Unicode.



- The session subkeys are created when the OS is running and at least one user is logged in.
- Session subkeys are created for other users who login.
- When User A selects the option to "switch user", User "B" logs in and switches user, and User "A" logs back in, there will be three session subkeys (2 for A, 1 for B).
- If User A and B login/logoff back and forth, there will only be two (2) session subkeys.
- After a normal shutdown or even disconnecting power, the session subkeys are deleted.
- Here's an example within Vista (Windows 10 should be the same, assuming you can switch users… not present in beta release)

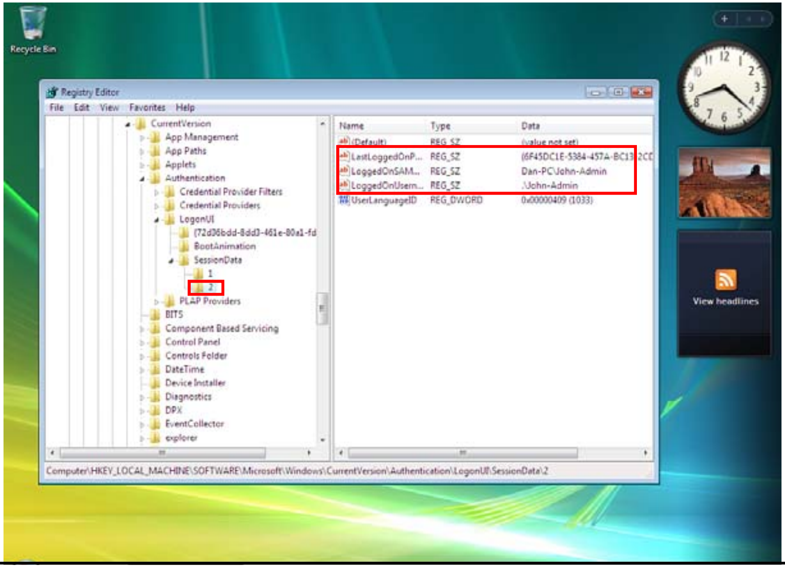
- Note the “1” subkey and values (only user logged in)



Name	Type	Data
(Default)	REG_SZ	(value not set)
LastLoggedOnProvider	REG_SZ	{6F45DC1E-5384-457A-BC13-2CD81B0D28ED}
LoggedOnSAMUser	REG_SZ	Dan-PC\Dan
LoggedOnUsername	REG_SZ	.\Dan
UserLanguageID	REG_DWORD	0x00000409 (1033)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\SessionData\1

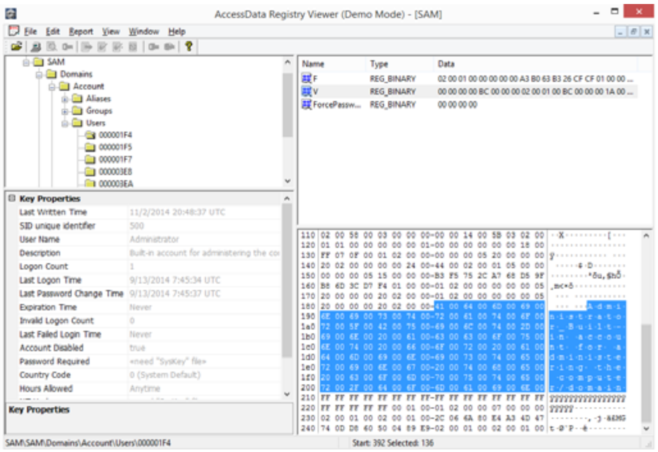
- View of the “2” subkey and values (John is the user)



Name	Type	Data
(Default)	REG_SZ	(value not set)
LastLoggedOnP...	REG_SZ	{6F45DC1E-5384-457A-BC13-2CC
LoggedOnSAM...	REG_SZ	Dan-PC\John-Admin
LoggedOnUsern...	REG_SZ	.\John-Admin
UserLanguageID	REG_DWORD	0x00000409 (1033)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\SessionData\2

- Windows 10 stores local user account information in the SAM hive (name, password, login date/time, hints, etc.)
- Navigate to SAM\Domains\Users



Name	Type	Data
F	REG_BINARY	02 00 01 00 00 00 00 00 A3 B0 63 B3 26 CF CF 01 00 00 ...
V	REG_BINARY	00 00 00 00 BC 00 00 00 02 00 01 00 BC 00 00 00 1A 00 ...
ForcePassw...	REG_BINARY	00 00 00 00

Key Properties

Last Written Time	11/2/2014 20:48:37 UTC
SID unique identifier	500
User Name	Administrator
Description	Built-in account for administering the co
Logon Count	1
Last Logon Time	9/13/2014 7:45:34 UTC
Last Password Change Time	9/13/2014 7:45:37 UTC
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	Never
Account Disabled	true
Password Required	«need "SysKey" file»
Country Code	0 (System Default)
Hours Allowed	Anytime

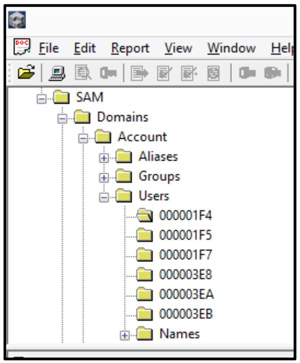
Key Properties

```
110  02 00 58 00 03 00 00 00-00 00 14 00 5B 03 02 00  ··X·········[···
120  01 01 00 00 00 00 00 01-00 00 00 00 00 00 18 00  ················
130  FF 07 0F 00 01 02 00 00-00 00 05 20 00 00 00 00  ÿ···············
140  20 02 00 00 00 00 24 00-44 00 02 00 01 05 00 00   ·····$·D·······
150  00 00 00 05 15 00 00 00-B3 F5 75 2C A7 68 D5 9F  ········³õu,§hÕ
160  B8 6D 3C D7 F4 01 00 00-01 02 00 00 00 00 00 05  ¸m<×ô···········
170  20 00 00 00 20 02 00 00-01 02 00 00 00 00 00 05   ··· ···········
180  20 00 00 00 20 02 00 00-41 00 64 00 6D 00 69 00   ··· ···A·d·m·i·
190  6E 00 69 00 73 00 74 00-72 00 61 00 74 00 6F 00  n·i·s·t·r·a·t·o·
1a0  72 00 5F 00 42 00 75 00-69 00 6C 00 74 00 2D 00  r·_·B·u·i·l·t·-·
1b0  69 00 6E 00 20 00 61 00-63 00 63 00 6F 00 75 00  i·n· ·a·c·c·o·u·
1c0  6E 00 74 00 20 00 66 00-6F 00 72 00 20 00 61 00  n·t· ·f·o·r· ·a·
1d0  64 00 6D 00 69 00 6E 00-69 00 73 00 74 00 65 00  d·m·i·n·i·s·t·e·
1e0  72 00 69 00 6E 00 67 00-20 00 74 00 68 00 65 00  r·i·n·g· ·t·h·e·
1f0  20 00 63 00 6F 00 6D 00-70 00 75 00 74 00 65 00   ·c·o·m·p·u·t·e·
200  72 00 2F 00 64 00 6F 00-6D 00 61 00 69 00 6E 00  r·/·d·o·m·a·i·n·
210  FF FF FF FF FF FF FF FF-FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
220  FF FF FF FF FF 00 01 00-01 02 00 00 07 00 00 00  ÿÿÿÿÿ···········
230  02 00 01 00 02 00 01 00-2C 06 6A 80 E4 A3 4D 47  ········,·j·ä£MG
240  74 0D D8 60 50 04 89 E9-02 00 01 00 02 00 01 00  t·Ø`P··é········
```

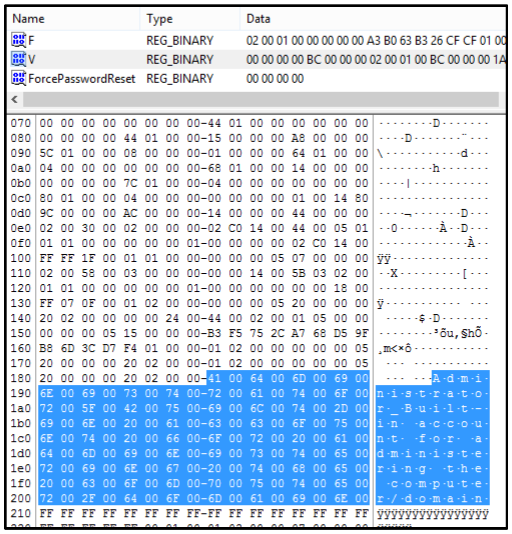
SAM\SAM\Domains\Account\Users\000001F4

Start: 392 Selected: 136

- Under the Users subkey, you will find a series of user folders that written in hex notation.
- As you may recall from previous courses or training, each user is assigned a Security Identifier (SID).
- The last 3+ digits of the SID is referred to as the Relative Identifier or RID.
- Convert the hex value to decimal
- The result is the RID.
- Example: 000001F4 = 500



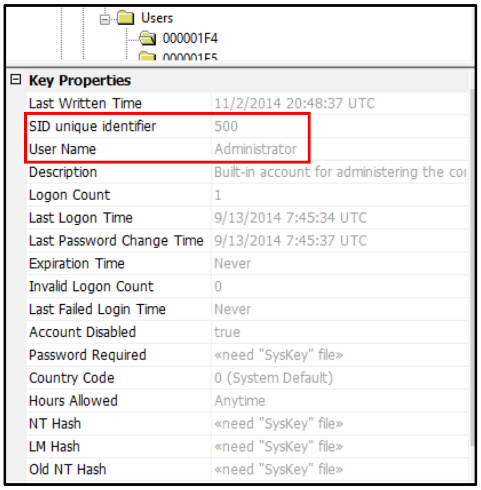
- The V value data shows the name of the user in plain Unicode text
- Administrator is the built-in account on the local machine
- The RID is 500, which is common on installations of Windows from NT to present.



Name	Type	Data
F	REG_BINARY	02 00 01 00 00 00 00 00 A3 B0 63 B3 26 CF CF 01 00
V	REG_BINARY	00 00 00 00 BC 00 00 00 02 00 01 00 BC 00 00 00 1A
ForcePasswordReset	REG_BINARY	00 00 00 00

```
070  00 00 00 00 00 00 00 00-44 01 00 00 00 00 00 00  ········D·······
080  00 00 00 00 44 01 00 00-15 00 00 00 A8 00 00 00  ····D·······¨···
090  5C 01 00 00 08 00 00 00-01 00 00 00 64 01 00 00  \···········d···
0a0  04 00 00 00 00 00 00 00-68 01 00 00 14 00 00 00  ········h·······
0b0  00 00 00 00 7C 01 00 00-04 00 00 00 00 00 00 00  ····|···········
0c0  80 01 00 00 04 00 00 00-00 00 00 00 01 00 14 80  ················
0d0  9C 00 00 00 AC 00 00 00-14 00 00 00 44 00 00 00  ····¬·······D···
0e0  02 00 30 00 02 00 00 00-02 C0 14 00 44 00 05 01  ··0·····À··D···
0f0  01 01 00 00 00 00 00 01-00 00 00 00 02 C0 14 00  ·············À··
100  FF FF 1F 00 01 01 00 00-00 00 00 05 07 00 00 00  ÿÿ··············
110  02 00 58 00 03 00 00 00-00 00 14 00 5B 03 02 00  ··X·········[···
120  01 01 00 00 00 00 00 01-00 00 00 00 00 00 18 00  ················
130  FF 07 0F 00 01 02 00 00-00 00 00 05 20 00 00 00  ÿ···········  ···
140  20 02 00 00 00 00 24 00-44 00 02 00 01 05 00 00   ·····$·D·······
150  00 00 00 05 15 00 00 00-B3 F5 75 2C A7 68 D5 9F  ········³õu,§hÕ·
160  B8 6D 3C D7 F4 01 00 00-01 02 00 00 00 00 00 05  ¸m<×ô···········
170  20 00 00 00 20 02 00 00-01 02 00 00 00 00 00 05   ···  ···········
180  20 00 00 00 20 02 00 00-41 00 64 00 6D 00 69 00   ···  ···A·d·m·i·
190  6E 00 69 00 73 00 74 00-72 00 61 00 74 00 6F 00  n·i·s·t·r·a·t·o·
1a0  72 00 5F 00 42 00 75 00-69 00 6C 00 74 00 2D 00  r·_·B·u·i·l·t·-·
1b0  69 00 6E 00 20 00 61 00-63 00 63 00 6F 00 75 00  i·n· ·a·c·c·o·u·
1c0  6E 00 74 00 20 00 66 00-6F 00 72 00 20 00 61 00  n·t· ·f·o·r· ·a·
1d0  64 00 6D 00 69 00 6E 00-69 00 73 00 74 00 65 00  d·m·i·n·i·s·t·e·
1e0  72 00 69 00 6E 00 67 00-20 00 74 00 68 00 65 00  r·i·n·g· ·t·h·e·
1f0  20 00 63 00 6F 00 6D 00-70 00 75 00 74 00 65 00   ·c·o·m·p·u·t·e·
200  72 00 2F 00 64 00 6F 00-6D 00 61 00 69 00 6E 00  r·/·d·o·m·a·i·n·
210  FF FF FF FF FF FF FF FF-FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
```

- In Registry Viewer, we can view the key properties, which “decodes” the data in the F and V values for us.
- Registry Viewer show the RID as “SID unique identifier”
- In order to access all of the decryption and advanced features of registry viewer, you must have a fully licensed version.

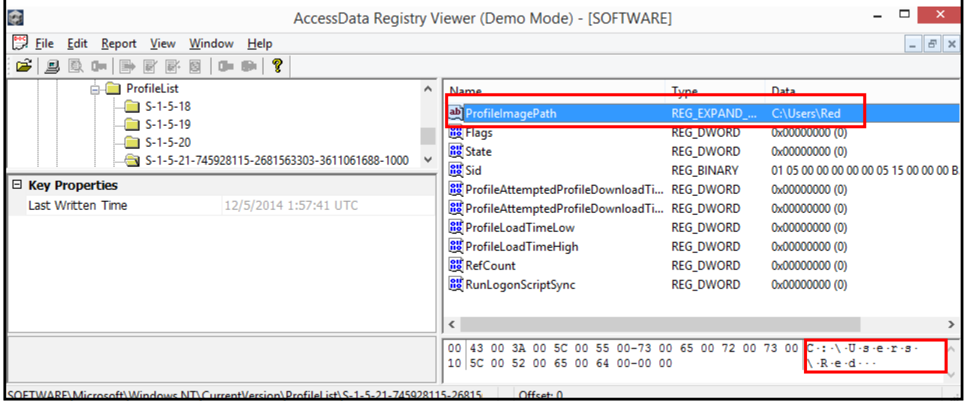


Key Properties

Last Written Time	11/2/2014 20:48:37 UTC
SID unique identifier	500
User Name	Administrator
Description	Built-in account for administering the co
Logon Count	1
Last Logon Time	9/13/2014 7:45:34 UTC
Last Password Change Time	9/13/2014 7:45:37 UTC
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	Never
Account Disabled	true
Password Required	«need "SysKey" file»
Country Code	0 (System Default)
Hours Allowed	Anytime
NT Hash	«need "SysKey" file»
LM Hash	«need "SysKey" file»
Old NT Hash	«need "SysKey" file»

- We have reviewed the data that will be present for local authenticated accounts.
- Domain accounts do not appear under the SAM\Domains\Users subkey.
- Rather, appear under SAM\Domains\Names
- However, there is no way to determine the user's RID (or full SID) from the values.
- Therefore, you must navigate to the SOFTWARE hive as follows
- SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList
- Locate the ProfileImagePath value.

- Review the value data, which shows the logical path to the user's profile folder on the local machine.
- In this example, we see the SID (S-1-5-21-745928115-2681563303-3611061688-1000) for the user, "Red."



ProfileList
- S-1-5-18
- S-1-5-19
- S-1-5-20
- S-1-5-21-745928115-2681563303-3611061688-1000

Key Properties

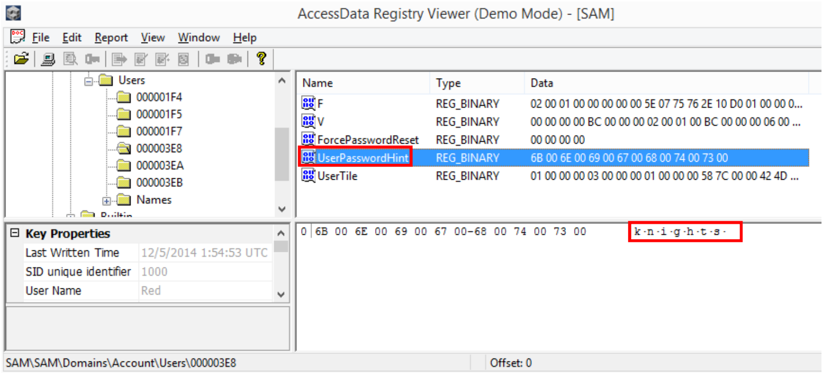
Last Written Time	12/5/2014 1:57:41 UTC

Name	Type	Data
ProfileImagePath	REG_EXPAND_...	C:\Users\Red
Flags	REG_DWORD	0x00000000 (0)
State	REG_DWORD	0x00000000 (0)
Sid	REG_BINARY	01 05 00 00 00 00 00 05 15 00 00 00 B
ProfileAttemptedProfileDownloadTi...	REG_DWORD	0x00000000 (0)
ProfileAttemptedProfileDownloadTi...	REG_DWORD	0x00000000 (0)
ProfileLoadTimeLow	REG_DWORD	0x00000000 (0)
ProfileLoadTimeHigh	REG_DWORD	0x00000000 (0)
RefCount	REG_DWORD	0x00000000 (0)
RunLogonScriptSync	REG_DWORD	0x00000000 (0)

```
00 43 00 3A 00 5C 00 55 00-73 00 65 00 72 00 73 00  C·:·\·U·s·e·r·s·
10 5C 00 52 00 65 00 64 00-00 00                    \·R·e·d···
```

SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-745928115-26815   Offset: 0

- Each user account may have a password hint.
- It is located in the SAM\SAM\Domains\Account\Users\<32-bit hex value>\UserPasswordHint value, the user's hint for their password is stored in Unicode.



AccessData Registry Viewer (Demo Mode) - [SAM]

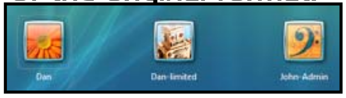
Name	Type	Data
F	REG_BINARY	02 00 01 00 00 00 00 00 5E 07 75 76 2E 10 D0 01 00 00 0...
V	REG_BINARY	00 00 00 00 BC 00 00 00 02 00 01 00 BC 00 00 00 06 00 ...
ForcePasswordReset	REG_BINARY	00 00 00 00
UserPasswordHint	REG_BINARY	6B 00 6E 00 69 00 67 00 68 00 74 00 73 00
UserTile	REG_BINARY	01 00 00 00 03 00 00 00 01 00 00 00 58 7C 00 00 42 4D ...

```
0 | 6B 00 6E 00 69 00 67 00-68 00 74 00 73 00        k·n·i·g·h·t·s·
```

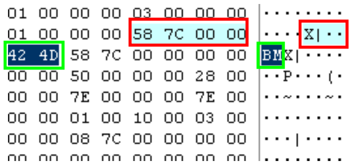
Key Properties	
Last Written Time	12/5/2014 1:54:53 UTC
SID unique identifier	1000
User Name	Red

SAM\SAM\Domains\Account\Users\000003E8   Offset: 0

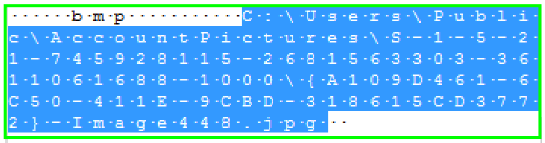
- In the SAM\SAM\Domains\Account\Users\<32-bit hex value>\UserTile value, the user's login tile (graphic) is stored. The graphic is stored within the value data as a bitmap regardless of the original format.



- Offset 12 (4 byte value) = size of graphic
- Offset 16 = beginning of bitmap data "BM"
- At the end of the value, the file type (BMP), volume letter, full path, and file name are stored for the tile.



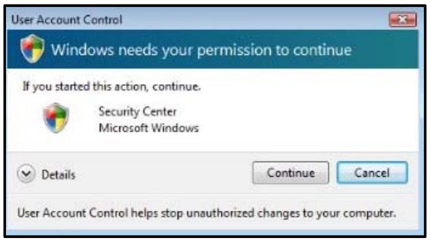
```
01 00 00 00 03 00 00 00  ·········
01 00 00 00 58 7C 00 00  ····X|··
42 4D 58 7C 00 00 00 00  BMX|····
00 00 50 00 00 00 28 00  ··P···(·
00 00 7E 00 00 00 7E 00  ··~···~·
00 00 01 00 10 00 03 00  ········
00 00 08 7C 00 00 00 00  ···|····
00 00 00 00 00 00 00 00  ········
```



```
······b·m·p···········C·:·\·U·s·e·r·s·\·P·u·b·l·i·
c·\·A·c·c·o·u·n·t·P·i·c·t·u·r·e·s·\·S·-·1·-·5·-·2·
1·-·7·4·5·9·2·8·1·1·5·-·2·6·8·1·5·6·3·3·0·3·-·3·6·
1·1·0·6·1·6·8·8·-·1·0·0·0·\·{·A·1·0·9·D·4·6·1·-·6·
C·5·0·-·4·1·1·E·-·9·C·B·D·-·3·1·8·6·1·5·C·D·3·7·7·
2·}·-·I·m·a·g·e·4·4·8·.·j·p·g···
```

- User Account Control (UAC) was introduced in Vista.
- UAC is a security component that enables users to perform common tasks as non-administrators, called standard users, without having to switch to an administrative role or user account.
- A limited user has no administrative rights and cannot install software or perform other administrative functions without the permission of the administrator.
- If a limited user opts to install software, the administrator's password (standard user or administrator) is required.
- UAC is enabled by default, but users can turn this feature off through the Windows 10 Control Panel.

- SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA
- 0 = UAC disabled
- 1 = UAC enabled (default value)



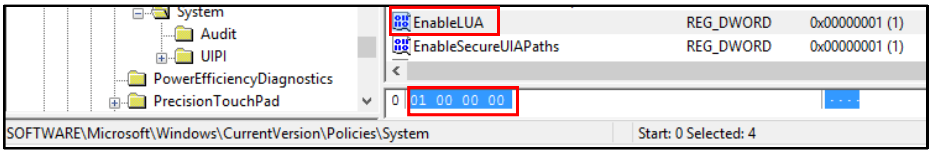
User Account Control

Windows needs your permission to continue

If you started this action, continue.

Security Center
Microsoft Windows

User Account Control helps stop unauthorized changes to your computer.

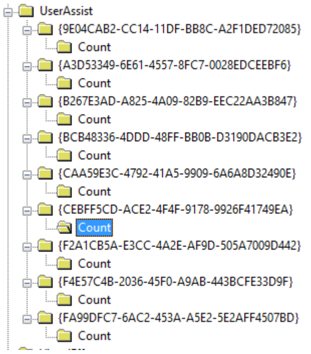


```
EnableLUA              REG_DWORD    0x00000001 (1)
EnableSecureUIAPaths   REG_DWORD    0x00000001 (1)
0  01 00 00 00
```

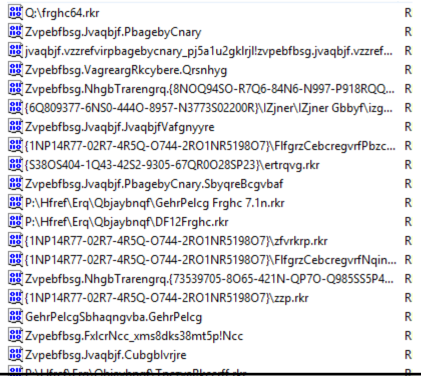
SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System   Start: 0 Selected: 4

- Windows 10 Product Information
- Navigate to SOFTWARE\Microsoft\Windows NT\CurrentVersion\
- Notable Values
  - Installation Date (value = InstallDate, Decode as Unix Date)
  - Product Name (value = ProductName, Unicode)
  - Registered Owner (value = RegisteredOwner, Unicode)
  - Registered Organization (value = RegisteredOrganization, Unicode)
  - System Root (value = SystemRoot, Unicode)
    - Determines assigned volume letter to Windows (usually C)

- UserAssist: Tracks local program and file activity per user
- At least in the Enterprise version of Windows 10, UserAssist keys track user activity much like a running log file.
- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

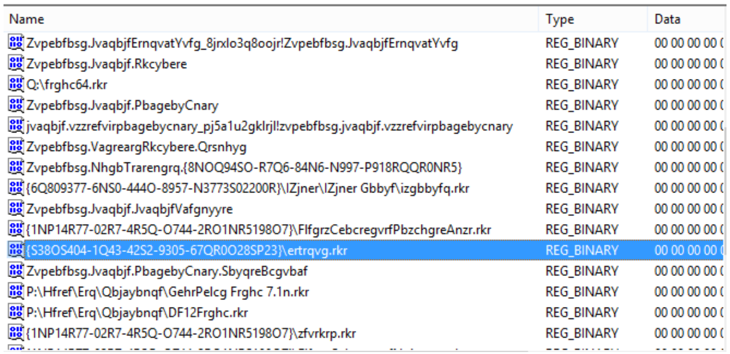


```
UserAssist
    {9E04CAB2-CC14-11DF-BB8C-A2F1DED72085}
        Count
    {A3D53349-6E61-4557-8FC7-0028EDCEEBF6}
        Count
    {B267E3AD-A825-4A09-82B9-EEC22AA3B847}
        Count
    {BCB48336-4DDD-48FF-BB0B-D3190DACB3E2}
        Count
    {CAA59E3C-4792-41A5-9909-6A6A8D32490E}
        Count
    {CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
        Count
    {F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}
        Count
    {F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
        Count
    {FA99DFC7-6AC2-453A-A5E2-5E2AFF4507BD}
        Count
```



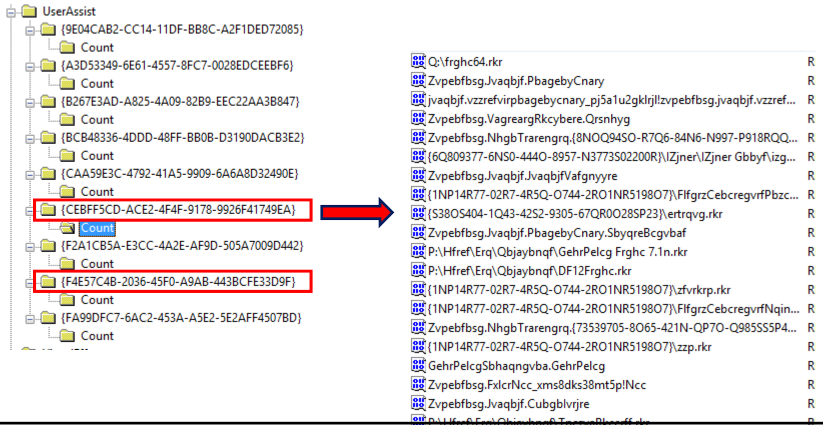
```
Q:\frghc64.rkr                                                              R
Zvpebfbsg.Jvaqbjf.PbagebyCnary                                              R
jvaqbjf.vzzrefvirpbagebycnary_pj5a1u2gklrjl!zvpebfbsg.jvaqbjf.vzzref...    R
Zvpebfbsg.VagreargRkcybere.Qrsnhyg                                          R
Zvpebfbsg.NhgbTrarengrq.{8NOQ94SO-R7Q6-84N6-N997-P918RQQ...                R
{6Q809377-6NS0-444O-8957-N3773S02200R}\IZjner\IZjner Gbbyf\izg...          R
Zvpebfbsg.Jvaqbjf.JvaqbjfVafgnyyre                                          R
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\FlfgrzCebcregvrfPbzc...             R
{S38OS404-1Q43-42S2-9305-67QR0O28SP23}\ertrqvg.rkr                          R
Zvpebfbsg.Jvaqbjf.PbagebyCnary.SbyqreBcgvbaf                                R
P:\Hfref\Erq\Qbjaybnqf\GehrPelcg Frghc 7.1n.rkr                             R
P:\Hfref\Erq\Qbjaybnqf\DF12Frghc.rkr                                        R
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\zfvrkrp.rkr                          R
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\FlfgrzCebcregvrfNqin...             R
Zvpebfbsg.NhgbTrarengrq.{73539705-8O65-421N-QP7O-Q985SS5P4...              R
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\zzp.rkr                              R
GehrPelcgSbhaqngvba.GehrPelcg                                               R
Zvpebfbsg.FxlcrNcc_xms8dks38mt5p!Ncc                                        R
Zvpebfbsg.Jvaqbjf.Cubgblvrjre                                               R
```

- User activity is tracked beneath these subkeys in the Count subkeys.
- The value names and value data are encrypted with ROT13 encoding (Caesarian cipher or Rotate by 13 places).
- The letter A would be listed as N while E would be listed as R.
- The raw data looks like this…



Name	Type	Data
Zvpebfbsg.JvaqbjfErnqvatYvfg_8jrxlo3q8oojr!Zvpebfbsg.JvaqbjfErnqvatYvfg	REG_BINARY	00 00 00 00 (
Zvpebfbsg.Jvaqbjf.Rkcybere	REG_BINARY	00 00 00 00 (
Q:\frghc64.rkr	REG_BINARY	00 00 00 00 (
Zvpebfbsg.Jvaqbjf.PbageybCnary	REG_BINARY	00 00 00 00 (
jvaqbjf.vzzrefvirpbagebycnary_pj5a1u2gklrjl!zvpebfbsg.jvaqbjf.vzzrefvirpbagebycnary	REG_BINARY	00 00 00 00 (
Zvpebfbsg.VagreargRkcybere.Qrsnhyg	REG_BINARY	00 00 00 00 (
Zvpebfbsg.NhgbTrarengrq.{8NOQ94SO-R7Q6-84N6-N997-P918RQQR0NR5}	REG_BINARY	00 00 00 00 (
{6Q809377-6NS0-444O-8957-N3773S02200R}\lZjner\lZjner Gbbyf\izgbbyfq.rkr	REG_BINARY	00 00 00 00 (
Zvpebfbsg.Jvaqbjf.JvaqbjfVafgnyyre	REG_BINARY	00 00 00 00 (
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\FlfgrzCebcregvrfPbzchgreAnzr.rkr	REG_BINARY	00 00 00 00 (
{S38OS404-1Q43-42S2-9305-67QR0O28SP23}\ertrqvg.rkr	REG_BINARY	00 00 00 00 (
Zvpebfbsg.Jvaqbjf.PbageybCnary.SbyqreBcgvbaf	REG_BINARY	00 00 00 00 (
P:\Hfref\Erq\Qbjaybnqf\GehrPelcg Frghc 7.1n.rkr	REG_BINARY	00 00 00 00 (
P:\Hfref\Erq\Qbjaybnqf\DF12Frghc.rkr	REG_BINARY	00 00 00 00 (
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\zfvrkrp.rkr	REG_BINARY	00 00 00 00 (

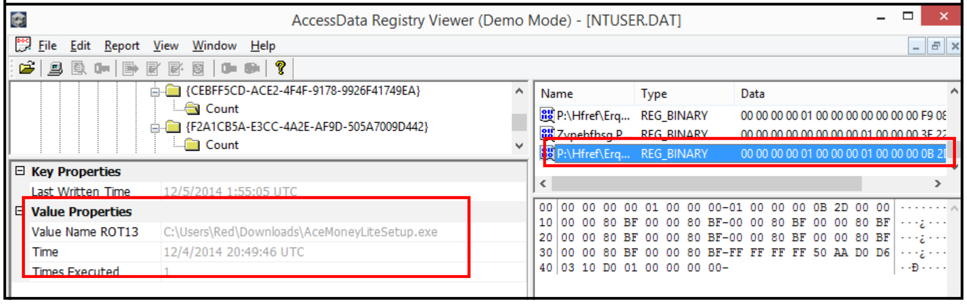
- Subkeys represent Windows Explorer, Internet Explorer, etc.
- {CEBFF5CD-…} = Executable Files
- {F4E57C4B-…} = Shortcut File Execution



```
UserAssist
  {9E04CAB2-CC14-11DF-BB8C-A2F1DED72085}
    Count
  {A3D53349-6E61-4557-8FC7-0028EDCEEBF6}
    Count
  {B267E3AD-A825-4A09-82B9-EEC22AA3B847}
    Count
  {BCB48336-4DDD-48FF-BB0B-D3190DACB3E2}
    Count
  {CAA59E3C-4792-41A5-9909-6A6A8D32490E}
    Count
  {CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
    Count
  {F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}
    Count
  {F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
    Count
  {FA99DFC7-6AC2-453A-A5E2-5E2AFF4507BD}
    Count
```

```
Q:\frghc64.rkr                                                          R
Zvpebfbsg.Jvaqbjf.PbageybCnary                                          R
jvaqbjf.vzzrefvirpbagebycnary_pj5a1u2gklrjl!zvpebfbsg.jvaqbjf.vzzref... R
Zvpebfbsg.VagreargRkcybere.Qrsnhyg                                      R
Zvpebfbsg.NhgbTrarengrq.{8NOQ94SO-R7Q6-84N6-N997-P918RQQ...             R
{6Q809377-6NS0-444O-8957-N3773S02200R}\lZjner\lZjner Gbbyf\izg...       R
Zvpebfbsg.Jvaqbjf.JvaqbjfVafgnyyre                                      R
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\FlfgrzCebcregvrfPbzc...          R
{S38OS404-1Q43-42S2-9305-67QR0O28SP23}\ertrqvg.rkr                      R
Zvpebfbsg.Jvaqbjf.PbageybCnary.SbyqreBcgvbaf                            R
P:\Hfref\Erq\Qbjaybnqf\GehrPelcg Frghc 7.1n.rkr                         R
P:\Hfref\Erq\Qbjaybnqf\DF12Frghc.rkr                                    R
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\zfvrkrp.rkr                      R
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\FlfgrzCebcregvrfNqin...          R
Zvpebfbsg.NhgbTrarengrq.{73539705-8O65-421N-QP7O-Q985SS5P4...           R
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\zzp.rkr                          R
GehrPelcgSbhaqngvba.GehrPelcg                                           R
Zvpebfbsg.FxlcrNcc_xms8dks38mt5p!Ncc                                    R
Zvpebfbsg.Jvaqbjf.Cubgblvrjre                                           R
```

- You will find to Count subkey below each of the GUID subkeys.
- A GUID is a globally unique identifier.
- Registry Viewer decrypts the ROT13 data as shown below.
- ROT13 is basic encryption, which is easily decode with many forensic tools.



AccessData Registry Viewer (Demo Mode) - [NTUSER.DAT]

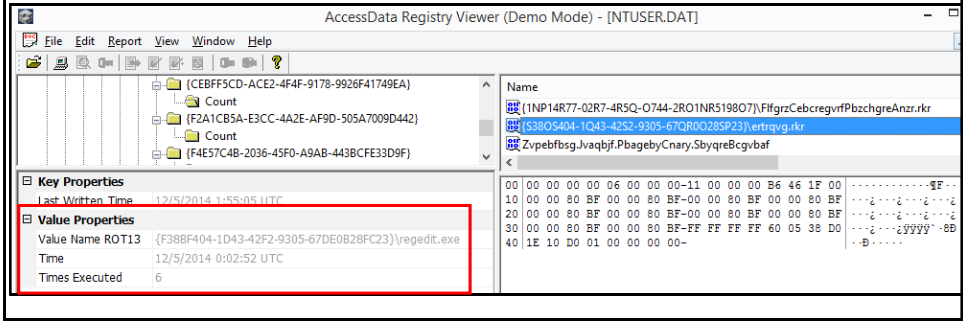
```
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
    Count
{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}
    Count
```

Name	Type	Data
P:\Hfref\Erq...	REG_BINARY	00 00 00 00 01 00 00 00 00 00 00 00 F9 08
Zvpebfbsg.P...	REG_BINARY	00 00 00 00 00 00 00 00 01 00 00 00 3E 22
P:\Hfref\Erq...	REG_BINARY	00 00 00 00 01 00 00 00 01 00 00 00 0B 2D

Key Properties	
Last Written Time	12/5/2014 1:55:05 UTC
Value Properties	
Value Name ROT13	C:\Users\Red\Downloads\AceMoneyLiteSetup.exe
Time	12/4/2014 20:49:46 UTC
Times Executed	1

```
00  00 00 00 00 01 00 00 00-01 00 00 00 0B 2D 00 00  ········
10  00 00 80 BF 00 00 80 BF-00 00 80 BF 00 00 80 BF  ···¿···
20  00 00 80 BF 00 00 80 BF-00 00 80 BF 00 00 80 BF  ···¿···
30  00 00 80 BF 00 00 80 BF-FF FF FF FF 50 AA D0 D6  ···¿···
40  03 10 D0 01 00 00 00 00-                         ··Ð····
```

- In this example, we see that the user executed regedit.exe on 6 occasions.
- The last written time for the subkey is irrelevant.
- The last time this value was updated (stored in the value data) was 12/5/2014 @ 00:02:52 UTC, which is 12/4/2014 @ 07:02:52 Eastern Standard Time. This is accurate.



AccessData Registry Viewer (Demo Mode) - [NTUSER.DAT]

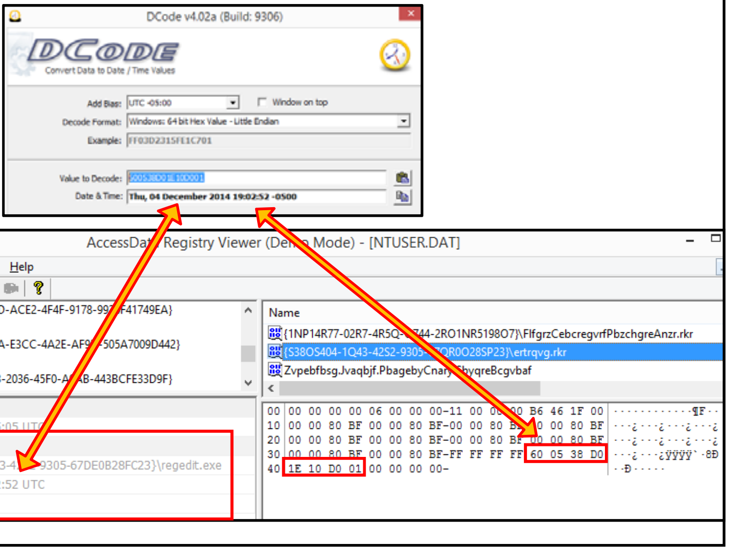
```
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
    Count
{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}
    Count
{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
```

Name
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\FlfgrzCebcregvrfPbzchgreAnzr.rkr
{S38OS404-1Q43-42S2-9305-67QR0O28SP23}\ertrqvg.rkr
Zvpebfbsg.Jvaqbjf.PbagebyCnary.SbyqreBcgvbaf

Key Properties	
Last Written Time	12/5/2014 1:55:05 UTC
Value Properties	
Value Name ROT13	{F38BF404-1D43-42F2-9305-67DE0B28FC23}\regedit.exe
Time	12/5/2014 0:02:52 UTC
Times Executed	6

```
00  00 00 00 00 06 00 00 00-11 00 00 00 B6 46 1F 00  ············¶F··
10  00 00 80 BF 00 00 80 BF-00 00 80 BF 00 00 80 BF  ···¿···¿···¿···¿
20  00 00 80 BF 00 00 80 BF-00 00 80 BF 00 00 80 BF  ···¿···¿···¿···¿
30  00 00 80 BF 00 00 80 BF-FF FF FF FF 60 05 38 D0  ···¿···¿ÿÿÿÿ`·8Ð
40  1E 10 D0 01 00 00 00 00-                         ··Ð·····
```

- The FILETIME value for this 60 05 38 D0 1E 10 D0 01



DCode v4.02a (Build: 9306)

DCode — Convert Data to Date / Time Values

Add Bias: UTC -05:00 □ Window on top

Decode Format: Windows: 64 bit Hex Value - Little Endian

Example: FF03D2315FE1C701

Value to Decode: 600538D01E10D001

Date & Time: Thu, 04 December 2014 19:02:52 -0500

AccessDat Registry Viewer (De   Mode) - [NTUSER.DAT]

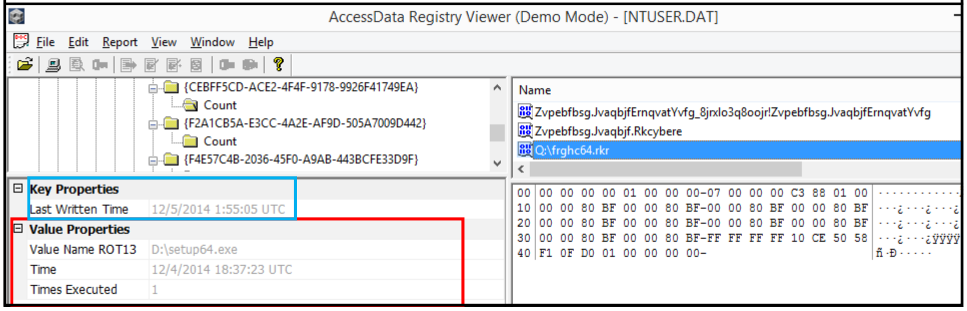
```
{CEBFF5CD-ACE2-4F4F-9178-99  F41749EA}
    Count
{F2A1CB5A-E3CC-4A2E-AF9  505A7009D442}
    Count
{F4E57C4B-2036-45F0-A  AB-443BCFE33D9F}
```

Name
- {1NP14R77-02R7-4R5Q- 744-2RO1NR519807}\FlfgrzCebcregvfPbzchgreAnzr.rkr
- {S38OS404-1Q43-42S2-9305- 7QR0O28SP23}\ertrqvg.rkr
- Zvpebfbsg.Jvaqbjf.PbagebyCnary byqreBcgvbaf

Key Properties	
Last Written Time	12/5/2014 1:55:05 UTC
Value Properties	
Value Name ROT13	{F38BF404-1D43-4 9305-67DE0B28FC23}\regedit.exe
Time	12/5/2014 0:02:52 UTC
Times Executed	6

```
00  00 00 00 00 06 00 00 00-11 00 00 00 B6 46 1F 00   ············¶F··
10  00 00 80 BF 00 00 80 BF-00 00 80 B  0 00 80 BF   ···¿···¿···¿···¿
20  00 00 80 BF 00 00 80 BF-00 00 80 BF 00 00 80 BF   ···¿···¿···¿···¿
30  00 00 80 BF 00 00 80 BF-FF FF FF FF 60 05 38 D0   ···¿···¿ÿÿÿÿ`·8Ð
40  1E 10 D0 01 00 00 00 00-                          ··Ð·····
```

- In this example, we see that the user executed setup64.exe from the D: volume on 1 occasion.
- The last written time for the subkey is greater than the last time the program was executed. Why?
- Recall that the subkey (parent) last modified date/time gets updated ANYTIME the values are updated.



AccessData Registry Viewer (Demo Mode) - [NTUSER.DAT]

```
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
    Count
{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}
    Count
{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
```

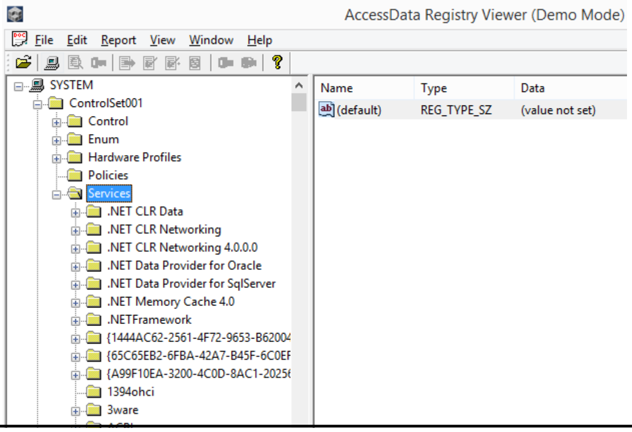
Name
- Zvpebfbsg.JvaqbjfErnqvatYvfg_8jrxlo3q8oojr!Zvpebfbsg.JvaqbjfErnqvatYvfg
- Zvpebfbsg.Jvaqbjf.Rkcybere
- Q:\frghc64.rkr

Key Properties	
Last Written Time	12/5/2014 1:55:05 UTC
Value Properties	
Value Name ROT13	D:\setup64.exe
Time	12/4/2014 18:37:23 UTC
Times Executed	1

```
00  00 00 00 00 01 00 00 00-07 00 00 00 C3 88 01 00   ············
10  00 00 80 BF 00 00 80 BF-00 00 80 BF 00 00 80 BF   ···¿···¿···¿
20  00 00 80 BF 00 00 80 BF-00 00 80 BF 00 00 80 BF   ···¿···¿···¿
30  00 00 80 BF 00 00 80 BF-FF FF FF FF 10 CE 50 58   ···¿···¿ÿÿÿ
40  F1 0F D0 01 00 00 00 00-                          ñ·Ð·····
```

- Windows Computer Name
- Navigate to SYSTEM\ControlSet00#\Control\ComputerName\ComputerName
- This is the friendly name of the computer as it appears on the network (netbios)
- The value is stored in Unicode

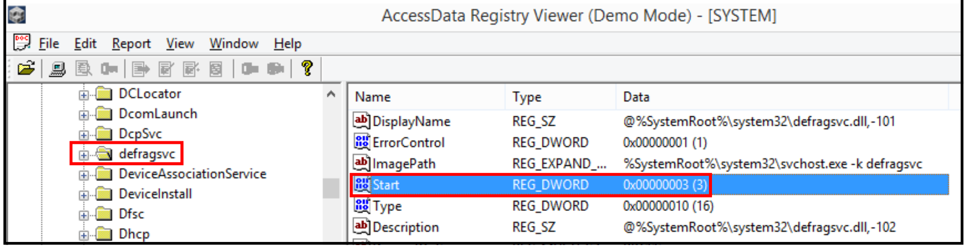
- Windows Services
- Navigate to SYSTEM\ControlSet00#\Service\
- Each subkey name denotes the name of the service



```
SYSTEM
  ControlSet001
    Control
    Enum
    Hardware Profiles
    Policies
    Services
      .NET CLR Data
      .NET CLR Networking
      .NET CLR Networking 4.0.0.0
      .NET Data Provider for Oracle
      .NET Data Provider for SqlServer
      .NET Memory Cache 4.0
      .NETFramework
      {1444AC62-2561-4F72-9653-B62004
      {65C65EB2-6FBA-42A7-B45F-6C0EF
      {A99F10EA-3200-4C0D-8AC1-20256
      1394ohci
      3ware
```

Name	Type	Data
(default)	REG_TYPE_SZ	(value not set)

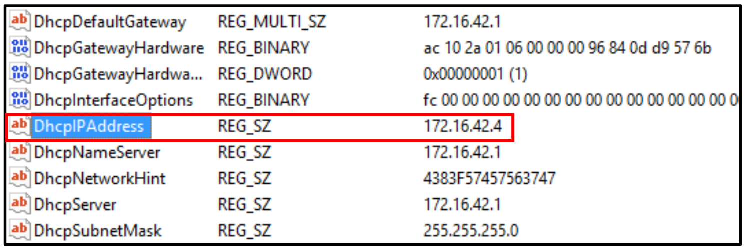
- SYSTEM\ControlSet00#\Service\<name>\Start
- Value that determines how the service will behave
  - 0 = boot
  - 1 = system
  - 2 = automatic
  - 3 = manual *(setting pictured below)*
  - 4 = disabled



DCLocator
DcomLaunch
DcpSvc
defragsvc
DeviceAssociationService
DeviceInstall
Dfsc
Dhcp

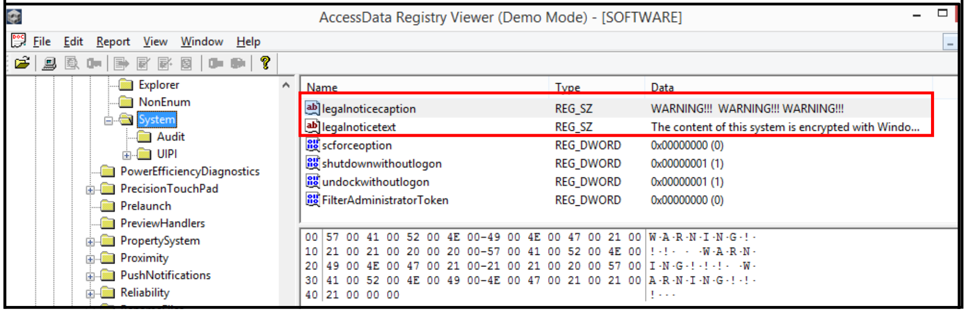
Name	Type	Data
DisplayName	REG_SZ	@%SystemRoot%\system32\defragsvc.dll,-101
ErrorControl	REG_DWORD	0x00000001 (1)
ImagePath	REG_EXPAND_...	%SystemRoot%\system32\svchost.exe -k defragsvc
Start	REG_DWORD	0x00000003 (3)
Type	REG_DWORD	0x00000010 (16)
Description	REG_SZ	@%SystemRoot%\system32\defragsvc.dll,-102

- Windows DHCP IP Address
- Navigate to SYSTEM\ControlSet00#\Services\Tcpip\Parameters\Interfaces\{GUID}\DhcpIPAddress
- This is the IP address given to the computer from the DHCP server / router / service
- The value is stored in Unicode (not pictured below)



DhcpDefaultGateway	REG_MULTI_SZ	172.16.42.1
DhcpGatewayHardware	REG_BINARY	ac 10 2a 01 06 00 00 00 96 84 0d d9 57 6b
DhcpGatewayHardwa...	REG_DWORD	0x00000001 (1)
DhcpInterfaceOptions	REG_BINARY	fc 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
DhcpIPAddress	REG_SZ	172.16.42.4
DhcpNameServer	REG_SZ	172.16.42.1
DhcpNetworkHint	REG_SZ	4383F57457563747
DhcpServer	REG_SZ	172.16.42.1
DhcpSubnetMask	REG_SZ	255.255.255.0

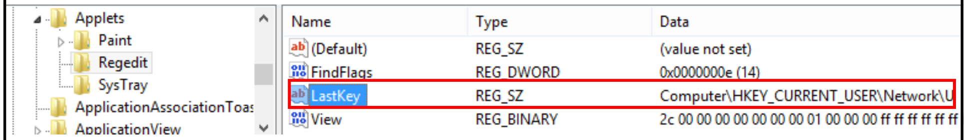
- Legal Notice & Text
- Navigate to SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
- Find the following values: legalnoticetext / legalnoticecaption
- The value is stored in Unicode (not pictured below)



Name	Type	Data
legalnoticecaption	REG_SZ	WARNING!!! WARNING!!! WARNING!!!
legalnoticetext	REG_SZ	The content of this system is encrypted with Windo...
scforceoption	REG_DWORD	0x00000000 (0)
shutdownwithoutlogon	REG_DWORD	0x00000001 (1)
undockwithoutlogon	REG_DWORD	0x00000001 (1)
FilterAdministratorToken	REG_DWORD	0x00000000 (0)

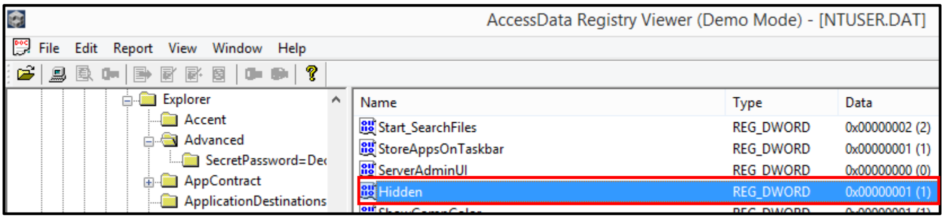
```
00 57 00 41 00 52 00 4E 00-49 00 4E 00 47 00 21 00 W·A·R·N·I·N·G·!·
10 21 00 21 00 20 00 20 00-57 00 41 00 52 00 4E 00 !·!· · ·W·A·R·N·
20 49 00 4E 00 47 00 21 00-21 00 21 00 20 00 57 00 I·N·G·!·!·!· ·W·
30 41 00 52 00 4E 00 49 00-4E 00 47 00 21 00 21 00 A·R·N·I·N·G·!·!·
40 21 00 00 00                                     !···
```

- Last Registry Subkey Viewed
- Navigate to NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit\LastKey
- The last subkey viewed by the user is displayed in the value data.
- It should be noted that this is user specific for each account.



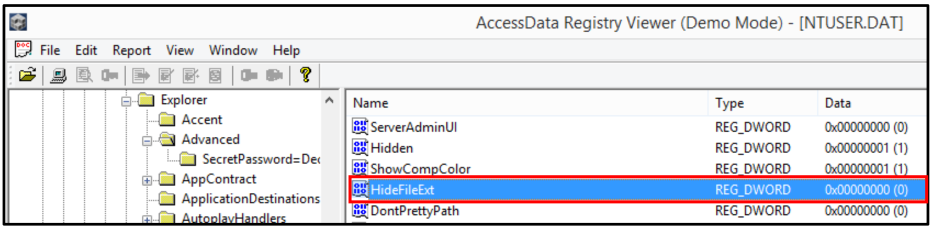
Name	Type	Data
(Default)	REG_SZ	(value not set)
FindFlags	REG_DWORD	0x0000000e (14)
LastKey	REG_SZ	Computer\HKEY_CURRENT_USER\Network\U
View	REG_BINARY	2c 00 00 00 00 00 00 00 01 00 00 00 ff ff ff ff ff ff

- Show / Hide Files (files with hidden attribute)
- Navigate to NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden
  - 0 = DO NOT Show Hidden Files
  - 1 = Show Hidden Files



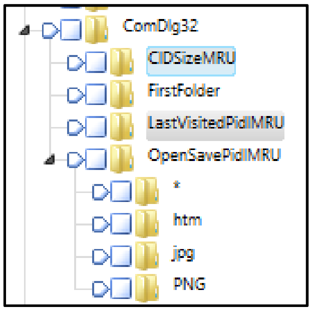
Name	Type	Data
Start_SearchFiles	REG_DWORD	0x00000002 (2)
StoreAppsOnTaskbar	REG_DWORD	0x00000001 (1)
ServerAdminUI	REG_DWORD	0x00000000 (0)
Hidden	REG_DWORD	0x00000001 (1)

- Show / Hide File Extensions
- Navigate to NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt
  - 0 = Show File Extension
  - 1 = Do NOT Show File Extension

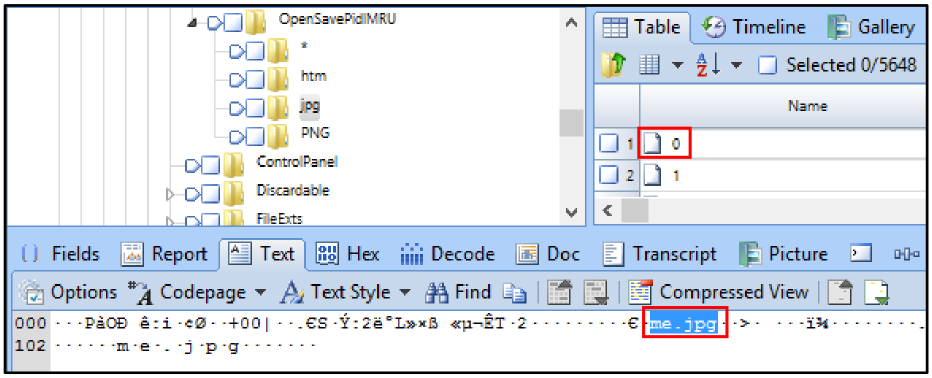


Name	Type	Data
ServerAdminUI	REG_DWORD	0x00000000 (0)
Hidden	REG_DWORD	0x00000001 (1)
ShowCompColor	REG_DWORD	0x00000001 (1)
HideFileExt	REG_DWORD	0x00000000 (0)
DontPrettyPath	REG_DWORD	0x00000000 (0)

- Most Recently Opened: Applications & Files
- Navigate to NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32
- Series of subkeys:
  - LastVisitedPidlMRU: Applications
  - OpenSavePidlMRU: Files
- Applications are generally listed, but this is based on the developer including this registry data
- OpenSavePidlMRU contains files
- 0 value name is most recently opened file, 1 value name is just prior, 2 is just prior, etc.

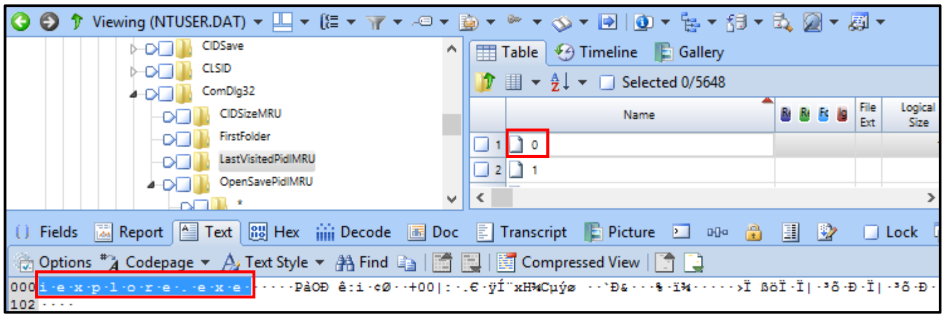


- OpenSavePidlMRU
- A file named “me.jpg” is the most recently opened file by this user.
- As viewed in EnCase v7



```
000 ···PàOÐ ê:i ·¢Ø··+00|···.€S ·Ý:2ë°L»×ß «µ¬ÊT ·2·········€·me.jpg··>·  ···ï¾·········.
102 ······m·e·.·j·p·g·······
```

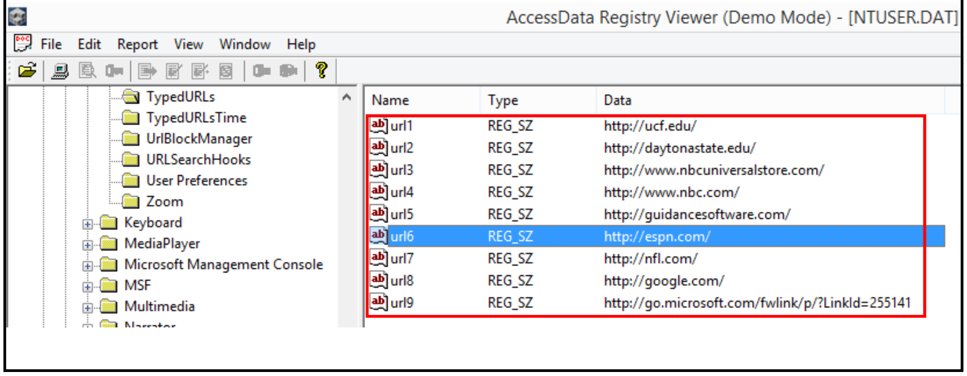
- LastVisitedPidlMRU
- Most recently opened application is iexplore.exe or Internet Explorer
- As viewed in EnCase v7…



	Name
1	0
2	1

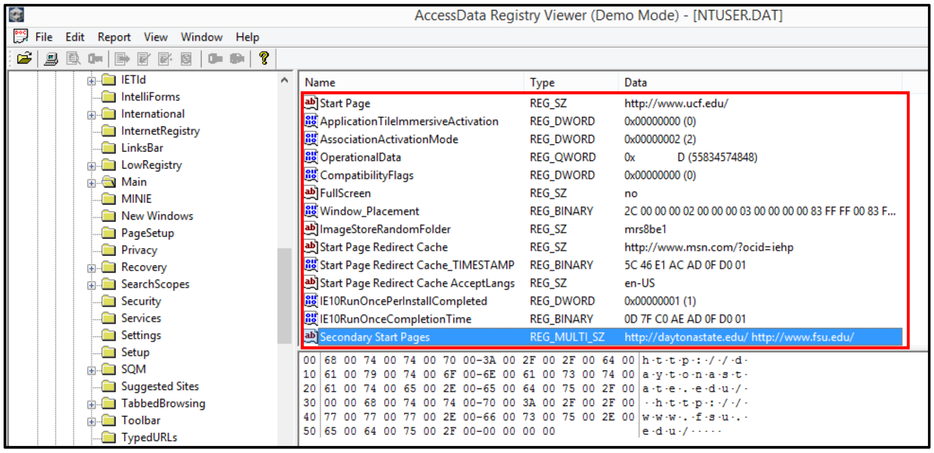
```
000 i·e·x·p·l·o·r·e·.·e·x·e·····PàOÐ ê:i ·¢Ø··+00|:·.€·ÿÍ¨xH¾Cµýø ··`Ð&···⅝·ì¾·····›Ï ßöÏ·Ï|·³õ·Ð·Ï|·³õ·Ð·
102 ····
```

- Internet Explorer Settings
- NTUSER.DAT\Software\Microsoft\Internet Explorer
- Typed URLS subkey holds latest URLS typed in the browser
- 0 is the most recent, 1 is the next previous, and so on…



Name	Type	Data
url1	REG_SZ	http://ucf.edu/
url2	REG_SZ	http://daytonastate.edu/
url3	REG_SZ	http://www.nbcuniversalstore.com/
url4	REG_SZ	http://www.nbc.com/
url5	REG_SZ	http://guidancesoftware.com/
url6	REG_SZ	http://espn.com/
url7	REG_SZ	http://nfl.com/
url8	REG_SZ	http://google.com/
url9	REG_SZ	http://go.microsoft.com/fwlink/p/?LinkId=255141

- NTUSER.DAT\Software\Microsoft\Internet Explorer\Main
- Browser Settings, start pages, tabs, etc…

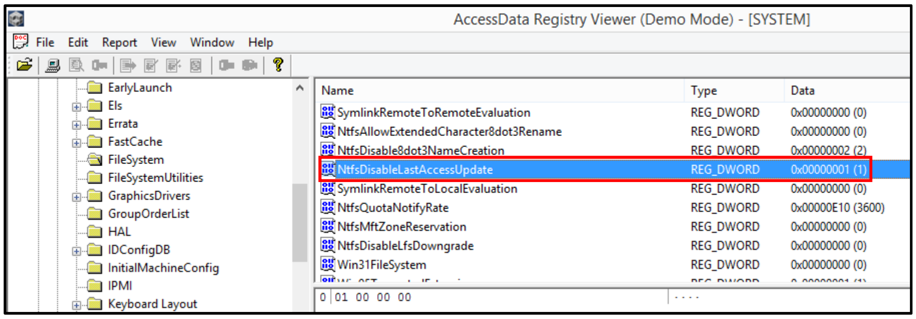


Name	Type	Data
Start Page	REG_SZ	http://www.ucf.edu/
ApplicationTileImmersiveActivation	REG_DWORD	0x00000000 (0)
AssociationActivationMode	REG_DWORD	0x00000002 (2)
OperationalData	REG_QWORD	0x D (55834574848)
CompatibilityFlags	REG_DWORD	0x00000000 (0)
FullScreen	REG_SZ	no
Window_Placement	REG_BINARY	2C 00 00 00 02 00 00 00 03 00 00 00 00 83 FF FF 00 83 F...
ImageStoreRandomFolder	REG_SZ	mrs8be1
Start Page Redirect Cache	REG_SZ	http://www.msn.com/?ocid=iehp
Start Page Redirect Cache_TIMESTAMP	REG_BINARY	5C 46 E1 AC AD 0F D0 01
Start Page Redirect Cache AcceptLangs	REG_SZ	en-US
IE10RunOncePerInstallCompleted	REG_DWORD	0x00000001 (1)
IE10RunOnceCompletionTime	REG_BINARY	0D 7F C0 AE AD 0F D0 01
Secondary Start Pages	REG_MULTI_SZ	http://daytonastate.edu/ http://www.fsu.edu/

```
00 | 68 00 74 00 74 00 70 00-3A 00 2F 00 2F 00 64 00 | h·t·t·p·:·/·/·d·
10 | 61 00 79 00 74 00 6F 00-6E 00 61 00 73 00 74 00 | a·y·t·o·n·a·s·t·
20 | 61 00 74 00 65 00 2E 00-65 00 64 00 75 00 2F 00 | a·t·e·.·e·d·u·/·
30 | 00 00 68 00 74 00 74 00-70 00 3A 00 2F 00 2F 00 | ··h·t·t·p·:·/·/·
40 | 77 00 77 00 77 00 2E 00-66 00 73 00 75 00 2E 00 | w·w·w·.·f·s·u·.·
50 | 65 00 64 00 75 00 2F 00-00 00 00 00             | e·d·u·/·····
```

- As you may recall, Vista, Windows 7, Windows 8, and Windows 10 no longer record the last accessed date and time in the standard information attribute of the each MFT record.
- However, this can be turned on or off by the user.
- Navigate to the SYSTEM \ControlSet###\Control\FileSystem subkey.
- Locate the "NtfsDisableLastAccess" value determines if the last accessed date/time is being recorded or not.
- 1 = not updated
- 0 = updated

- Locate the "NtfsDisableLastAccess" value determines if the last accessed date/time is being recorded or not.
- In Windows 10, last access date/time is not recorded when a file is opened!
- This is a system setting, not by user.



AccessData Registry Viewer (Demo Mode) - [SYSTEM]

EarlyLaunch
Els
Errata
FastCache
FileSystem
FileSystemUtilities
GraphicsDrivers
GroupOrderList
HAL
IDConfigDB
InitialMachineConfig
IPMI
Keyboard Layout

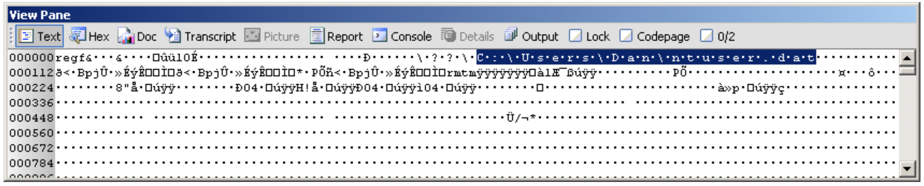
Name	Type	Data
SymlinkRemoteToRemoteEvaluation	REG_DWORD	0x00000000 (0)
NtfsAllowExtendedCharacter8dot3Rename	REG_DWORD	0x00000000 (0)
NtfsDisable8dot3NameCreation	REG_DWORD	0x00000002 (2)
NtfsDisableLastAccessUpdate	REG_DWORD	0x00000001 (1)
SymlinkRemoteToLocalEvaluation	REG_DWORD	0x00000000 (0)
NtfsQuotaNotifyRate	REG_DWORD	0x00000E10 (3600)
NtfsMftZoneReservation	REG_DWORD	0x00000000 (0)
NtfsDisableLfsDowngrade	REG_DWORD	0x00000000 (0)
Win31FileSystem	REG_DWORD	0x00000000 (0)

```
0 01 00 00 00    ....
```

Physical Registry Hive Overview

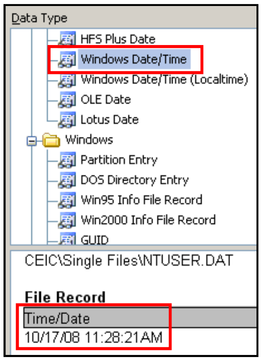
- NOTE: We will review a few aspects of the binary registry
- This lesson is not intended to be comprehensive as the registry is very complex.
- The intent of this lesson is to familiarize you with some of the basic structures of the registry.
- Why?
- How often do you run across search hits in slack, unallocated, or just by other examination techniques?
- Have you missed critical data?
- This will give you a jump start in the right direction…

- Let's explore some of the binary structures of the hive…
- The binary structure of the registry hive is composed of blocks, bins, and cells.
- Blocks are 4096 bytes in length
- The header of a registry hive is "regf" if 0x66676572
- The first block contains information about the registry hive itself.



```
000000regf&···&····□ûül0É·················  ····Ð······\·?·?·\·C·:·\·U·s·e·r·s·\·D·a·n·\·n·t·u·s·e·r·.·d·a·t··········
000112ð<·BpjÛ·»ÉýÊ□□Ì□ð<·BpjÛ·»ÉýÊ□□Ì□*·PÕñ<·BpjÛ·»ÉýÊ□□Ì□rmtmÿÿÿÿÿÿÿÿ□àlÆ¯Đúÿÿ··········PÕ·····················¤···ô···
000224········8"å·□úÿÿ········Ð04·□úÿÿH!å·□úÿÿÐ04·□úÿÿi04·□úÿÿ········□·······················à»p·□úÿÿç··············
000336·································································································
000448············ ························ ·······················Ü/¬*·············································
000560·································································································
000672·································································································
000784·································································································
```

- At file offset 12 from the beginning of the registry hive, the FILETIME date/time value records the last update date/time of the hive file itself
- The FILETIME value (discussed later) is 8 bytes in length, and can be decoded within EnCase, Dcode.exe, etc…



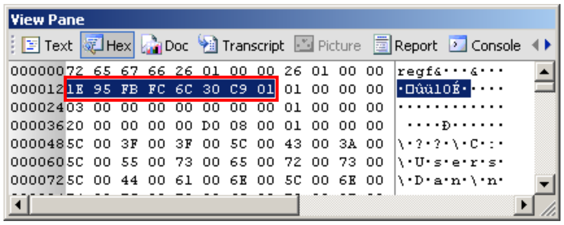
Data Type

- HFS Plus Date
- Windows Date/Time
- Windows Date/Time (Localtime)
- OLE Date
- Lotus Date
- Windows
  - Partition Entry
  - DOS Directory Entry
  - Win95 Info File Record
  - Win2000 Info File Record
  - GUID

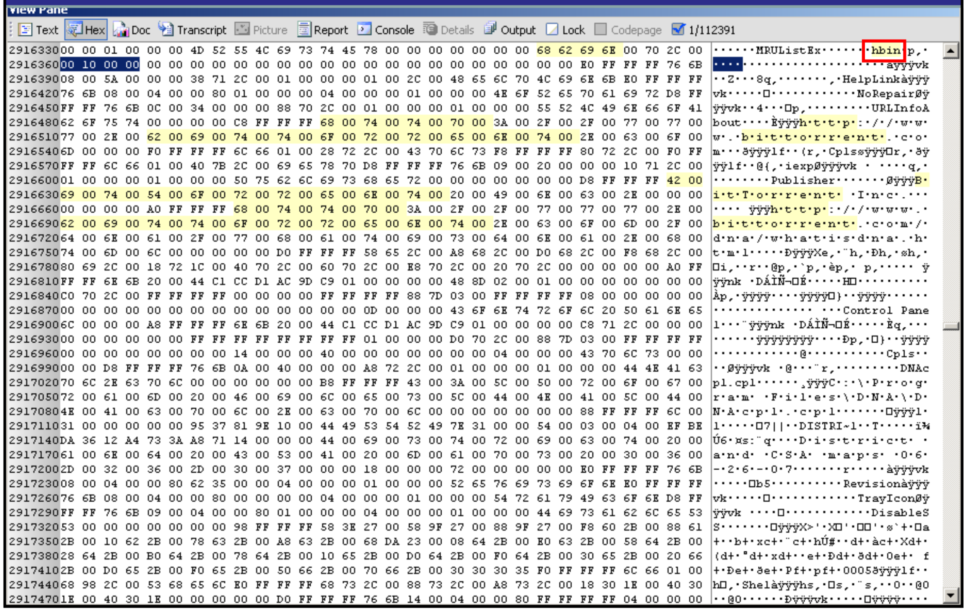
CEIC\Single Files\NTUSER.DAT

File Record

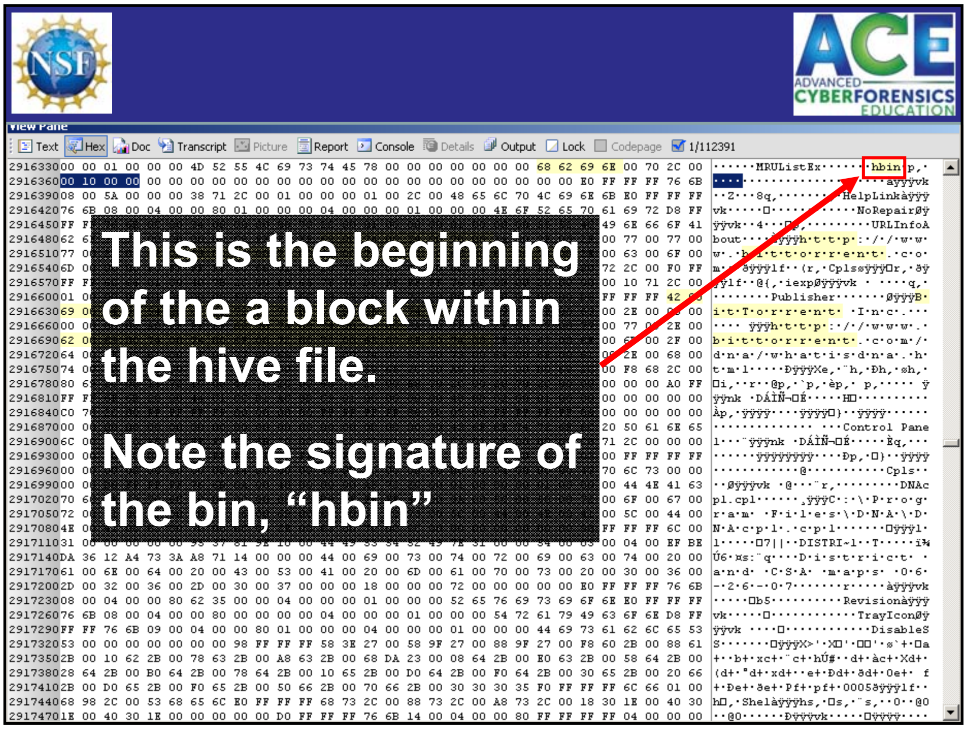
Time/Date
10/17/08 11:28:21AM



```
00000072 65 67 66 26 01 00 00 26 01 00 00  regf&···&···
0000121E 95 FB FC 6C 30 C9 01 01 00 00 00  ·□ûül0É·····
00002403 00 00 00 00 00 00 00 01 00 00 00  ············
00003620 00 00 00 00 D0 08 00 01 00 00 00   ····Ð······
0000485C 00 3F 00 3F 00 5C 00 43 00 3A 00  \·?·?·\·C·:·
0000605C 00 55 00 73 00 65 00 72 00 73 00  \·U·s·e·r·s·
0000725C 00 44 00 61 00 6E 00 5C 00 6E 00  \·D·a·n·\·n·
```

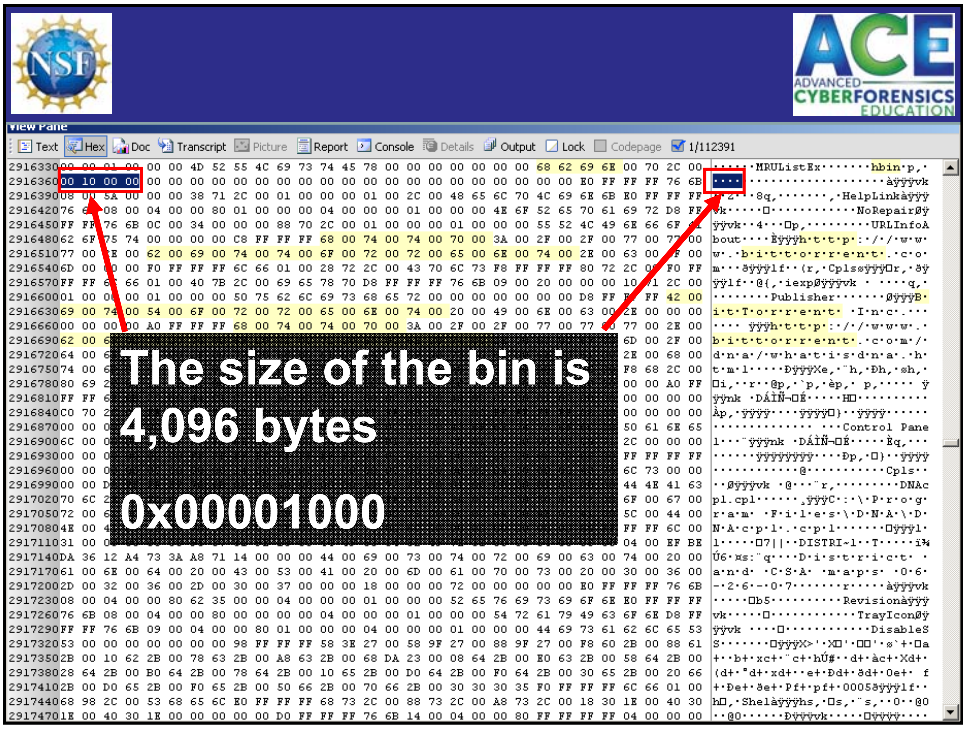


```
291633000 00 01 00 00 00 4D 52 55 4C 69 73 74 45 78 00 00 00 00 00 00 00 68 62 69 6E 00 70 2C 00  ······MRUListEx······hbin·p,·
291636000 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 E0 FF FF FF 76 6B  ·····················àÿÿÿvk
291639008 00 5A 00 00 00 38 71 2C 00 01 00 00 00 01 00 2C 00 48 65 6C 70 4C 69 6E 6B E0 FF FF FF  ··Z···8q,·······,·HelpLinkàÿÿÿ
291642076 6B 08 00 04 00 00 80 01 00 00 00 04 00 00 00 01 00 00 00 4E 6F 52 65 70 61 69 72 D8 FF  vk·····□············NoRepairØÿ
2916450FF FF 76 6B 0C 00 34 00 00 00 88 70 2C 00 01 00 00 00 01 00 00 00 55 52 4C 49 6E 66 6F 41  ÿÿvk··4···□p,·········URLInfoA
291648062 6F 75 74 00 00 00 00 C8 FF FF FF 68 00 74 00 74 00 70 00 3A 00 2F 00 2F 00 77 00 77 00  bout····Èÿÿÿh·t·t·p·:·/·/·w·w·
291651077 00 2E 00 62 00 69 00 74 00 74 00 6F 00 72 00 72 00 65 00 6E 00 74 00 2E 00 63 00 6F 00  w·.·b·i·t·t·o·r·r·e·n·t·.·c·o·
29165406D 00 00 00 F0 FF FF FF 6C 66 01 00 28 72 2C 00 43 70 6C 73 F8 FF FF FF 80 72 2C 00 F0 FF  m···ðÿÿÿlf··(r,·Cplsøÿÿÿ□r,·ðÿ
2916570FF FF 6C 66 01 00 40 7B 2C 00 69 65 78 70 D8 FF FF FF 76 6B 09 00 20 00 00 00 10 71 2C 00  ÿÿlf··@{,·iexpØÿÿÿvk · ····q,·
291660001 00 00 00 01 00 00 00 50 75 62 6C 69 73 68 65 72 00 00 00 00 00 00 00 D8 FF FF FF 42 00  ········Publisher·······ØÿÿÿB·
291663069 00 74 00 54 00 6F 00 72 00 72 00 65 00 6E 00 74 00 20 00 49 00 6E 00 63 00 2E 00 00 00  i·t·T·o·r·r·e·n·t· ·I·n·c·.···
291666000 00 00 00 A0 FF FF FF 68 00 74 00 74 00 70 00 3A 00 2F 00 2F 00 77 00 77 00 77 00 2E 00  ···· ÿÿÿh·t·t·p·:·/·/·w·w·w·.·
291669062 00 69 00 74 00 74 00 6F 00 72 00 72 00 65 00 6E 00 74 00 2E 00 63 00 6F 00 6D 00 2F 00  b·i·t·t·o·r·r·e·n·t·.·c·o·m·/·
291672064 00 6E 00 61 00 2F 00 77 00 68 00 61 00 74 00 69 00 73 00 64 00 6E 00 61 00 2E 00 68 00  d·n·a·/·w·h·a·t·i·s·d·n·a·.·h·
291675074 00 6D 00 6C 00 00 00 00 00 D0 FF FF FF 58 65 2C 00 A8 68 2C 00 D0 68 2C 00 F8 68 2C 00  t·m·l·····ÐÿÿÿXe,·¨h,·Ðh,·øh,·
291678080 69 2C 00 18 72 1C 00 40 70 2C 00 60 70 2C 00 E8 70 2C 00 20 70 2C 00 00 00 00 00 A0 FF  □i,··r··@p,·`p,·èp,· p,····· ÿ
2916810FF FF 6E 6B 20 00 44 C1 CC D1 AC 9D C9 01 00 00 00 00 48 8D 02 00 01 00 00 00 00 00 00 00  ÿÿnk ·DÁÌÑ¬□É·····H□··········
2916840C0 70 2C 00 FF FF FF FF 00 00 00 00 FF FF FF FF 88 7D 03 00 FF FF FF FF 08 00 00 00 00 00  Àp,·ÿÿÿÿ····ÿÿÿÿ□}··ÿÿÿÿ······
291687000 00 00 00 00 00 00 00 00 00 00 00 00 00 0D 00 00 00 43 6F 6E 74 72 6F 6C 20 50 61 6E 65  ··············  ···Control Pane
29169006C 00 00 00 A8 FF FF FF 6E 6B 20 00 44 C1 CC D1 AC 9D C9 01 00 00 00 00 C8 71 2C 00 00 00  l···¨ÿÿÿnk ·DÁÌÑ¬□É·····Èq,···
291693000 00 00 00 00 00 FF FF FF FF FF FF FF FF 01 00 00 00 D0 70 2C 00 88 7D 03 00 FF FF FF FF  ······ÿÿÿÿÿÿÿÿ····Ðp,·□}··ÿÿÿÿ
291696000 00 00 00 00 00 00 00 14 00 00 00 40 00 00 00 00 00 00 00 04 00 00 00 43 70 6C 73 00 00  ············@···········Cpls··
291699000 00 D8 FF FF FF 76 6B 0A 00 40 00 00 00 A8 72 2C 00 01 00 00 00 01 00 00 00 44 4E 41 63  ··Øÿÿÿvk ·@···¨r,·········DNAc
291702070 6C 2E 63 70 6C 00 00 00 00 00 00 B8 FF FF FF 43 00 3A 00 5C 00 50 00 72 00 6F 00 67 00  pl.cpl······¸ÿÿÿC·:·\·P·r·o·g·
291705072 00 61 00 6D 00 20 00 46 00 69 00 6C 00 65 00 73 00 5C 00 44 00 4E 00 41 00 5C 00 44 00  r·a·m· ·F·i·l·e·s·\·D·N·A·\·D·
29170804E 00 41 00 63 00 70 00 6C 00 2E 00 63 00 70 00 6C 00 00 00 00 00 00 00 88 FF FF FF 6C 00  N·A·c·p·l·.·c·p·l·······□ÿÿÿl·
291711031 00 00 00 00 00 95 37 81 9E 10 00 44 49 53 54 52 49 7E 31 00 00 54 00 03 00 04 00 EF BE  1·····□7||··DISTRI~1··T·····ï¾
2917140DA 36 12 A4 73 3A A8 71 14 00 00 00 44 00 69 00 73 00 74 00 72 00 69 00 63 00 74 00 20 00  Ú6·¤s:¨q····D·i·s·t·r·i·c·t· ·
291717061 00 6E 00 64 00 20 00 43 00 53 00 41 00 20 00 6D 00 61 00 70 00 73 00 20 00 30 00 36 00  a·n·d· ·C·S·A· ·m·a·p·s· ·0·6·
29172002D 00 32 00 36 00 2D 00 30 00 37 00 00 00 18 00 00 00 72 00 00 00 00 00 E0 FF FF FF 76 6B  -·2·6·-·0·7·······r·····àÿÿÿvk
291723008 00 04 00 00 80 62 35 00 00 04 00 00 00 01 00 00 00 52 65 76 69 73 69 6F 6E E0 FF FF FF  ·····□b5··········Revisionàÿÿÿ
291726076 6B 08 00 04 00 00 80 00 00 00 00 04 00 00 00 01 00 00 00 54 72 61 79 49 63 6F 6E D8 FF  vk·····□············TrayIconØÿ
2917290FF FF 76 6B 09 00 04 00 00 80 01 00 00 00 04 00 00 00 01 00 00 00 44 69 73 61 62 6C 65 53  ÿÿvk ····□············DisableS
291732053 00 00 00 00 00 00 00 98 FF FF FF 58 3E 27 00 58 9F 27 00 88 9F 27 00 F8 60 2B 00 88 61  S·······□ÿÿÿX>'·X□'·□□'·ø`+·□a
29173502B 00 10 62 2B 00 78 63 2B 00 A8 63 2B 00 68 DA 23 00 08 64 2B 00 E0 63 2B 00 58 64 2B 00  +··b+·xc+·¨c+·hÚ#··d+·àc+·Xd+·
291738028 64 2B 00 B0 64 2B 00 78 64 2B 00 10 65 2B 00 D0 64 2B 00 F0 64 2B 00 30 65 2B 00 20 66  (d+·°d+·xd+··e+·Ðd+·ðd+·0e+· f
29174102B 00 D0 65 2B 00 F0 65 2B 00 50 66 2B 00 70 66 2B 00 30 30 30 35 F0 FF FF FF 6C 66 01 00  +·Ðe+·ðe+·Pf+·pf+·0005ðÿÿÿlf··
291744068 98 2C 00 53 68 65 6C E0 FF FF FF 68 73 2C 00 88 73 2C 00 A8 73 2C 00 18 30 1E 00 40 30  h□,·Shelàÿÿÿhs,·□s,·¨s,··0··@0
29174701E 00 40 30 1E 00 00 00 00 00 D0 FF FF FF 76 6B 14 00 04 00 00 80 FF FF FF FF 04 00 00 00  ··@0······Ðÿÿÿvk·····□ÿÿÿÿ····
```



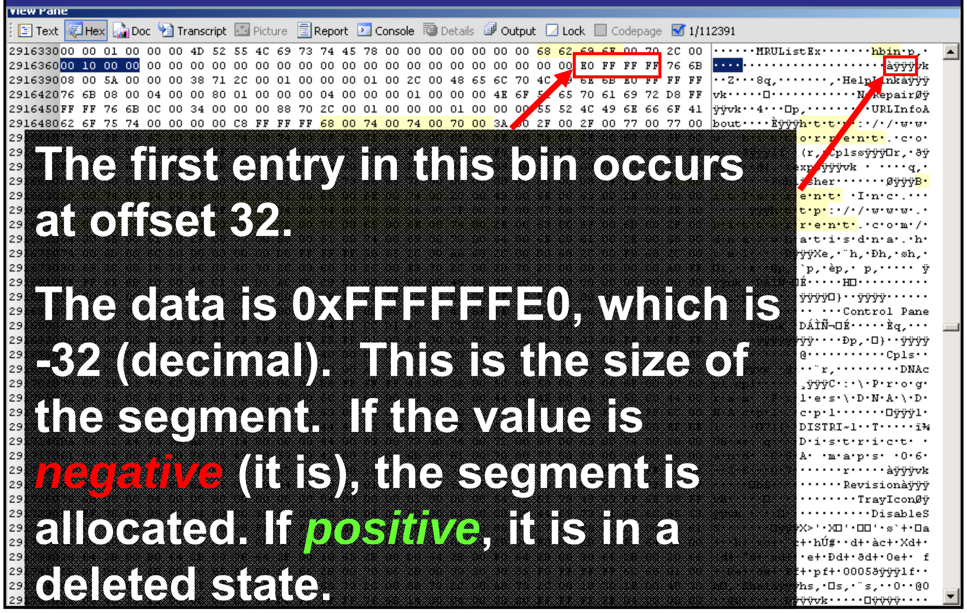
This is the beginning of the a block within the hive file.

Note the signature of the bin, "hbin"



The size of the bin is 4,096 bytes

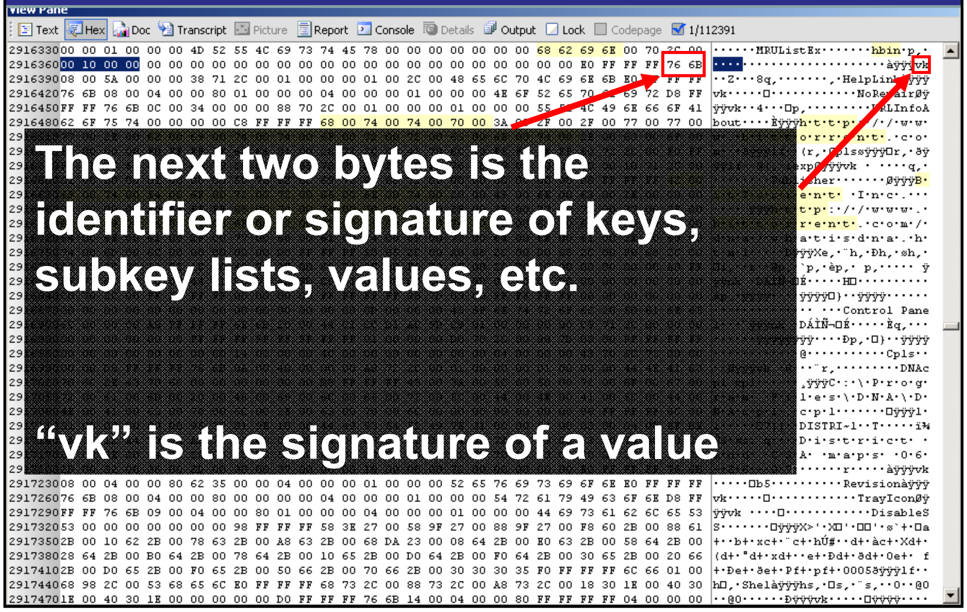
0x00001000



```
29163300 00 01 00 00 00 4D 52 55 4C 69 73 74 45 78 00 00 00 00 00 00 00 68 62 69 6E 00 70 2C 00 ······MRUListEx·······hbin·p,·
29163600 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 E0 FF FF FF 76 6B ······················àÿÿÿvk
29163908 00 5A 00 00 00 38 71 2C 00 01 00 00 00 01 00 2C 00 48 65 6C 70 4C 69 6E 6B E0 FF FF FF ··Z···8q,·······,·HelpLinkàÿÿÿ
29164276 6B 08 00 04 00 00 80 01 00 00 00 04 00 00 00 01 00 00 00 4E 6F 52 65 70 61 69 72 D8 FF vk·····□············NoRepairØÿ
291645FF FF 76 6B 0C 00 34 00 00 00 88 70 2C 00 01 00 00 00 01 00 00 00 55 52 4C 49 6E 66 6F 41 ÿÿvk··4···□p,·······URLInfoA
29164862 6F 75 74 00 00 00 00 C8 FF FF FF 68 00 74 00 74 00 70 00 3A 00 2F 00 2F 00 77 00 77 00 bout····Èÿÿÿh·t·t·p·:·/·/·w·w·
```

The first entry in this bin occurs at offset 32.

The data is 0xFFFFFFE0, which is -32 (decimal). This is the size of the segment. If the value is *negative* (it is), the segment is allocated. If *positive*, it is in a deleted state.



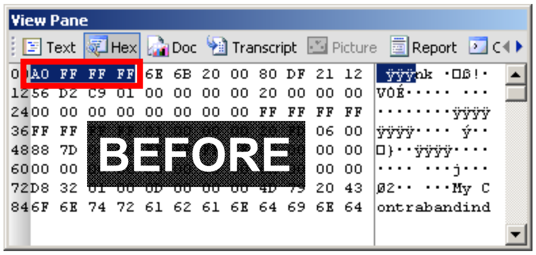
```
29163300 00 01 00 00 00 4D 52 55 4C 69 73 74 45 78 00 00 00 00 00 00 00 68 62 69 6E 00 70 2C 00 ······MRUListEx·······hbin·p,·
29163600 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 E0 FF FF FF 76 6B ······················àÿÿÿvk
29163908 00 5A 00 00 00 38 71 2C 00 01 00 00 00 01 00 2C 00 48 65 6C 70 4C 69 6E 6B E0 FF FF FF ··Z···8q,·······,·HelpLinkàÿÿÿ
29164276 6B 08 00 04 00 00 80 01 00 00 00 04 00 00 00 01 00 00 00 4E 6F 52 65 70 61 69 72 D8 FF vk·····□············NoRepairØÿ
291645FF FF 76 6B 0C 00 34 00 00 00 88 70 2C 00 01 00 00 00 01 00 00 00 55 52 4C 49 6E 66 6F 41 ÿÿvk··4···□p,·······URLInfoA
29164862 6F 75 74 00 00 00 00 C8 FF FF FF 68 00 74 00 74 00 70 00 3A 00 2F 00 2F 00 77 00 77 00 bout····Èÿÿÿh·t·t·p·:·/·/·w·w·
```

The next two bytes is the identifier or signature of keys, subkey lists, values, etc.

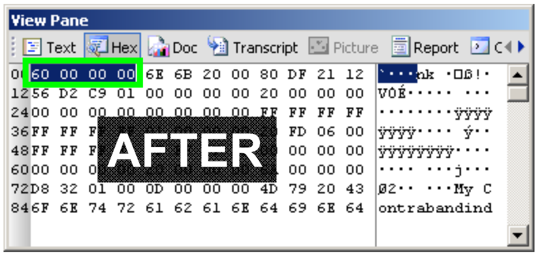
"vk" is the signature of a value

```
29172308 00 04 00 00 80 62 35 00 00 04 00 00 00 01 00 00 00 52 65 76 69 73 69 6F 6E E0 FF FF FF ·····□b5··········Revisionàÿÿÿ
29172676 6B 08 00 04 00 00 80 00 00 00 00 04 00 00 00 01 00 00 00 54 72 61 79 49 63 6F 6E D8 FF vk·····□············TrayIconØÿ
291729FF FF 76 6B 09 00 04 00 00 80 01 00 00 00 04 00 00 00 01 00 00 00 44 69 73 61 62 6C 65 53 ÿÿvk ····□············DisableS
29173253 00 00 00 00 00 00 00 98 FF FF FF 58 3E 27 00 58 9F 27 00 88 9F 27 00 F8 60 2B 00 88 61 S·······□ÿÿÿX>'·X□'·□□'·ø`+·□a
2917352B 00 10 62 2B 00 78 63 2B 00 A8 63 2B 00 68 DA 23 00 08 64 2B 00 E0 63 2B 00 58 64 2B 00 +··b+·xc+·¨c+·hÚ#··d+·àc+·Xd+·
29173828 64 2B 00 B0 64 2B 00 78 64 2B 00 10 65 2B 00 D0 64 2B 00 F0 64 2B 00 30 65 2B 00 20 66 (d+·°d+·xd+··e+·Ðd+·ðd+·0e+· f
2917412B 00 D0 65 2B 00 F0 65 2B 00 50 66 2B 00 70 66 2B 00 30 30 30 35 F0 FF FF FF 6C 66 01 00 +·Ðe+·ðe+·Pf+·pf+·0005ðÿÿÿlf··
29174468 98 2C 00 53 68 65 6C E0 FF FF FF 68 73 2C 00 88 73 2C 00 A8 73 2C 00 18 30 1E 00 40 30 h□,·Shelàÿÿÿhs,·□s,·¨s,··0··@0
2917471E 00 40 30 1E 00 00 00 00 00 D0 FF FF FF 76 6B 14 00 04 00 00 80 FF FF FF FF 04 00 00 00 ··@0······Ðÿÿÿvk·····□ÿÿÿÿ····
```

- Prior to the signature of the segment (subkey, value, etc.) is a 4 byte value
- Equals size of segment
- Convert hex to decimal
- If negative = allocated
- If positive = deleted



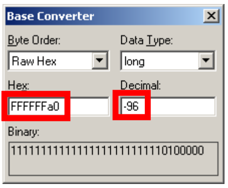
```
0 A0 FF FF FF 6E 6B 20 00 80 DF 21 12   ÿÿÿnk ·□ß!·
1256 D2 C9 01 00 00 00 00 20 00 00 00   VÒÉ····· ···
2400 00 00 00 00 00 00 00 FF FF FF FF   ········ÿÿÿÿ
36FF FF                         06 00   ÿÿÿÿ···· ý··
4888 7D                         00 00   □}··ÿÿÿÿ····
6000 00                         00 00   ···· ···j···
72D8 32                         20 43   Ø2·· ···My C
846F 6E 74 72 61 62 61 6E 64 69 6E 64   ontrabandind
```



```
00 60 00 00 00 6E 6B 20 00 80 DF 21 12   `···nk ·□ß!·
1256 D2 C9 01 00 00 00 00 20 00 00 00   VÒÉ····· ···
2400 00 00 00 00 00 00 00 FF FF FF FF   ········ÿÿÿÿ
36FF FF F                    FD 06 00   ÿÿÿÿ···· ý··
48FF FF F                    00 00 00   ÿÿÿÿÿÿÿÿ····
6000 00 0                    00 00 00   ···· ···j···
72D8 32 01 00 0D 00 00 00 4D 79 20 43   Ø2·· ···My C
846F 6E 74 72 61 62 61 6E 64 69 6E 64   ontrabandind
```

- 0xFFFFFFA0 = -96

  allocated



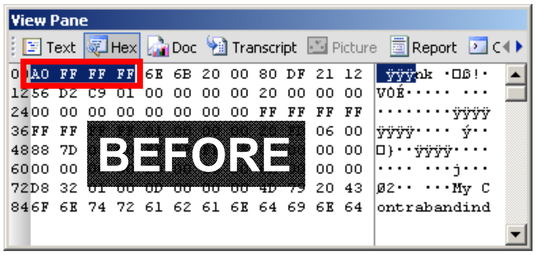
Byte Order: Raw Hex

Data Type: long

Hex: FFFFFFa0

Decimal: -96

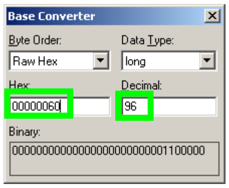
Binary: 11111111111111111111111110100000



```
0 A0 FF FF FF 6E 6B 20 00 80 DF 21 12   ÿÿÿnk ·□ß!·
1256 D2 C9 01 00 00 00 00 20 00 00 00   VÒÉ····· ···
2400 00 00 00 00 00 00 00 FF FF FF FF   ········ÿÿÿÿ
36FF FF                         06 00   ÿÿÿÿ···· ý··
4888 7D                         00 00   □}··ÿÿÿÿ····
6000 00                         00 00   ···· ···j···
72D8 32                         20 43   Ø2·· ···My C
846F 6E 74 72 61 62 61 6E 64 69 6E 64   ontrabandind
```

- 0x00000060 = +96

  deleted



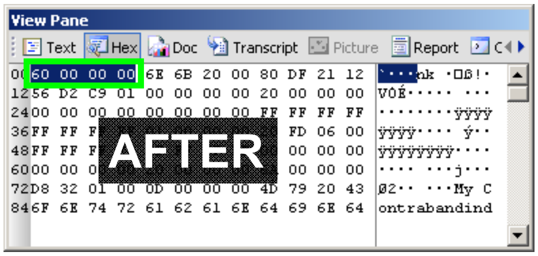
Byte Order: Raw Hex

Data Type: long

Hex: 00000060

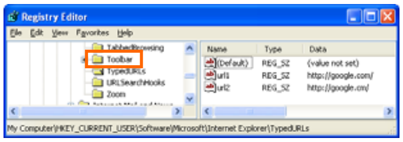
Decimal: 96

Binary: 00000000000000000000000001100000



```
00 60 00 00 00 6E 6B 20 00 80 DF 21 12   `···nk ·□ß!·
1256 D2 C9 01 00 00 00 00 20 00 00 00   VÒÉ····· ···
2400 00 00 00 00 00 00 00 FF FF FF FF   ········ÿÿÿÿ
36FF FF F                    FD 06 00   ÿÿÿÿ···· ý··
48FF FF F                    00 00 00   ÿÿÿÿÿÿÿÿ····
6000 00 0                    00 00 00   ···· ···j···
72D8 32 01 00 0D 00 00 00 4D 79 20 43   Ø2·· ···My C
846F 6E 74 72 61 62 61 6E 64 69 6E 64   ontrabandind
```

Logical view of the TypedURLs subkey



Name	Type	Data
(Default)	REG_SZ	(value not set)
url1	REG_SZ	http://google.com/
url2	REG_SZ	http://google.cm/

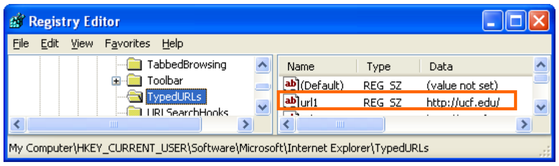
My Computer\HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs

Physical view of the subkey: Identification

- Unique signature: “kn” (little endian)
- 0x6B6E
- FILETIME date/time value follows
- FILETIME value = key/subkey last modified
- Subkey name in Unicode

```
FF FF FF 6E 6B 20 00 78 63   ÿÿÿnk ·xc
D2 D4 21 18 C9 01 00 00 00   ÒÔ!·É····
00 20 50 00 00 00 00 00 00   · P······
00 00 00 00 FF FF FF FF FF   ····ÿÿÿÿÿ
FF FF FF 05 00 00 00 78 1C   ÿÿÿ····x·
04 00 38 1D 02 00 FF FF FF   ··8···ÿÿÿ
FF 00 00 00 00 00 00 00 00   ÿ········
08 00 00 00 5A 00 00 00 00   ····Z····
00 00 00 09 00 00 00 54 79   ···  ···Ty
70 65 64 55 52 4C 73 00 00   pedURLs··
00 00 00 00 00 E0 FF FF FF   ·····àÿÿÿ
```

Logical view of a TypedURL value



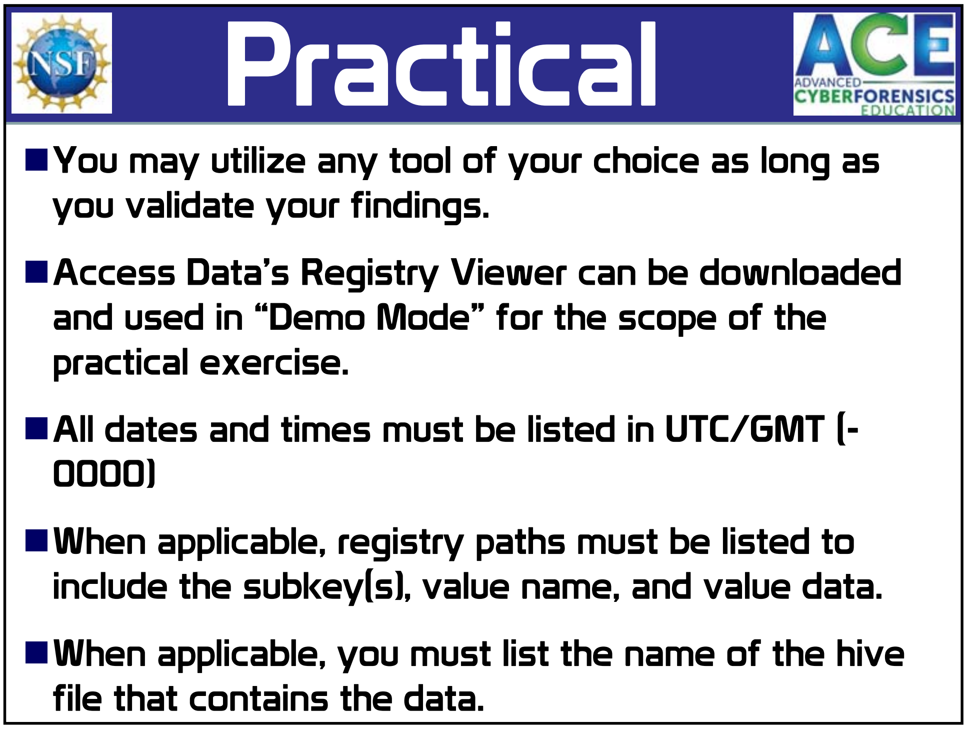
Name	Type	Data
(Default)	REG_SZ	(value not set)
url1	REG_SZ	http://ucf.edu/

My Computer\HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs

Physical view of the value: Identification

- Unique signature: “kv” (little endi
- 0x6B76
- Value name “URL1” in ASCII
- Value data http://ucf.edu in Unicode

```
76 6B 04 00 20 00 00 00 10 9F 02 00   vk·· ····□··
01 00 00 00 01 00 00 00 75 72 6C 31   ········url1
00 00 00 00 A0 FF FF FF 68 00 74 00   ···· ÿÿÿh·t·
74 00 70 00 3A 00 2F 00 2F 00 75 00   t·p·:·/·/·u·
63 00 66 00 2E 00 65 00 64 00 75 00   c·f·.·e·d·u·
```



Practical

- You may utilize any tool of your choice as long as you validate your findings.
- Access Data’s Registry Viewer can be downloaded and used in “Demo Mode” for the scope of the practical exercise.
- All dates and times must be listed in UTC/GMT (-0000)
- When applicable, registry paths must be listed to include the subkey(s), value name, and value data.
- When applicable, you must list the name of the hive file that contains the data.

Windows Registry