



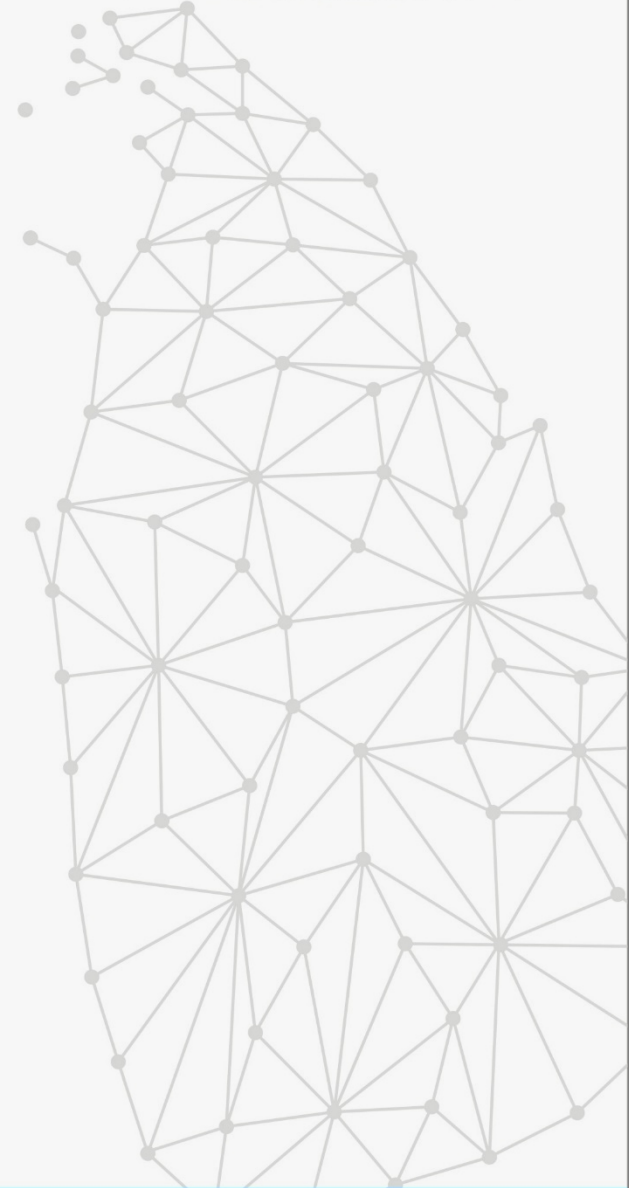
# Dark Corners of Windows Registry Analysis

by  
Ravindu W Meegasmulla  
Associate Information Security Engineer



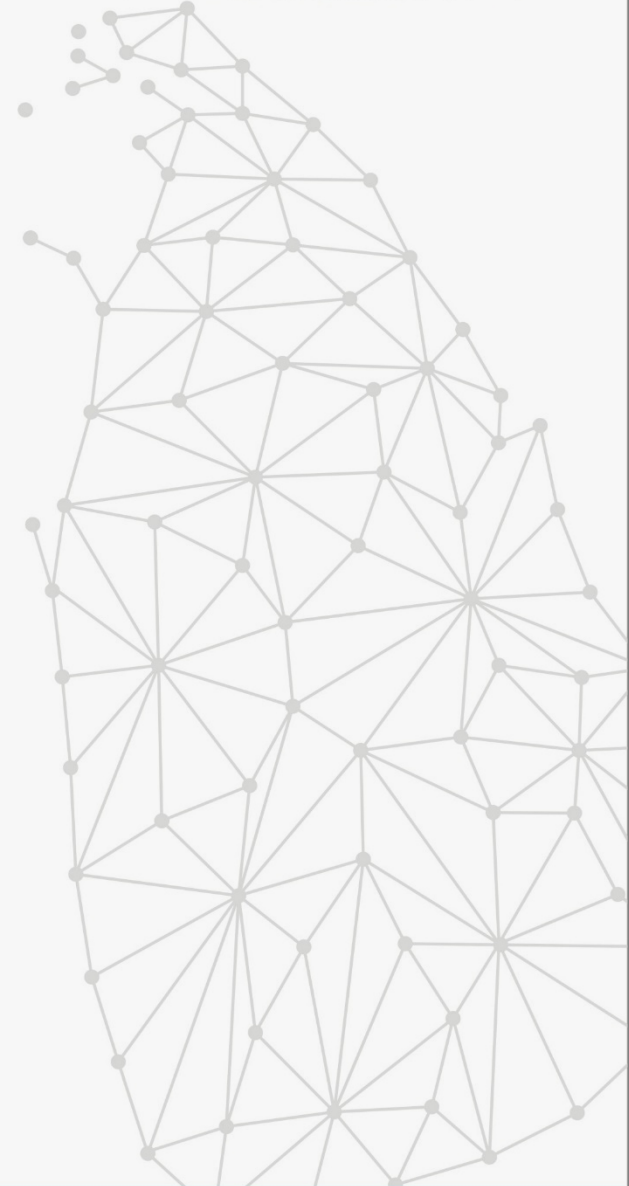
# About Me ?

- Working with Sri Lanka CERT over 4 years
- Conducted over 100 digital forensic investigations



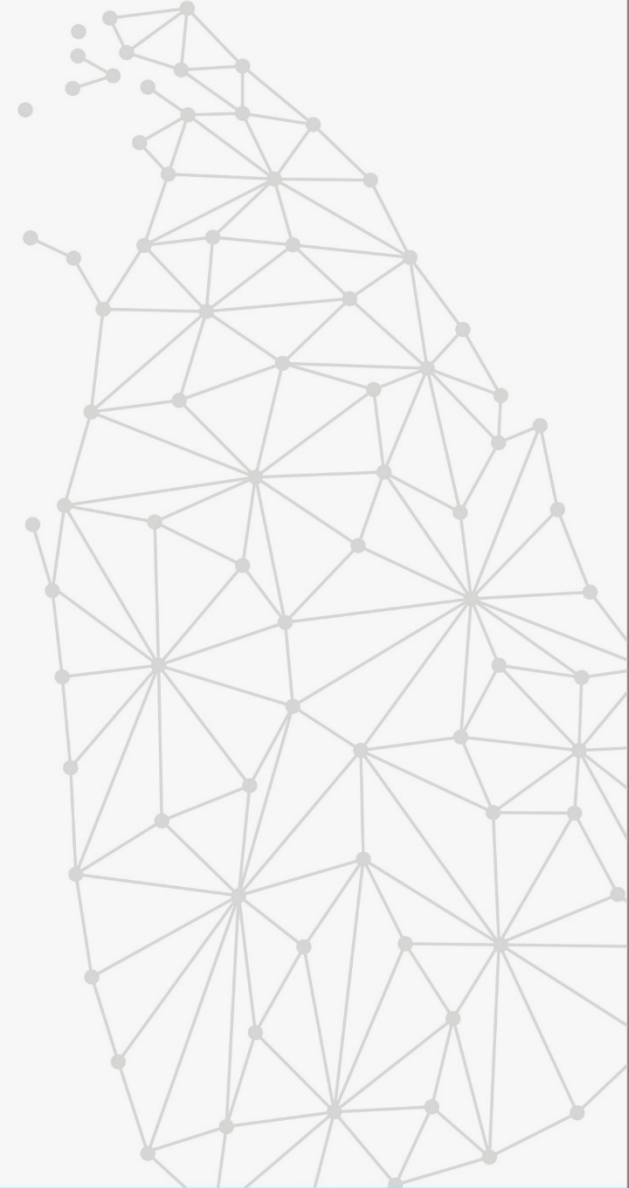
# Agenda

- Introduction to Windows Registry
  - Structure
  - Viewing the Windows registry
- Registry Analysis tools
- Registry Based Investigation
  - Time Zone Investigation
  - Last Shutdown time
  - Operating System information
  - Users in the system
  - Mounted devices
  - Connected USB devices
  - Network related investigation
  - Tracking User Activities



# Topics not Covered

- Deep analysis of Connected USB devices





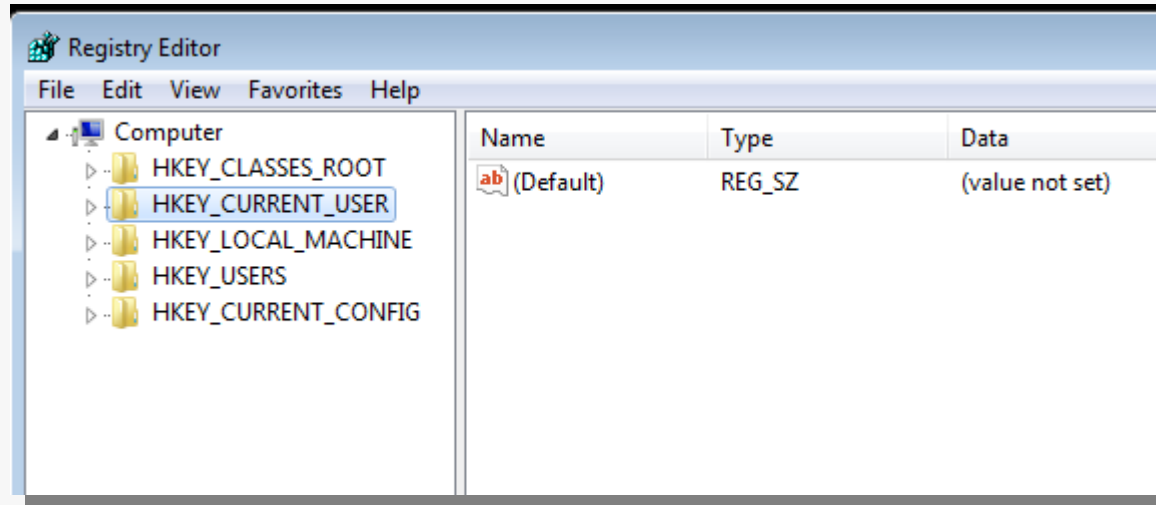
# Windows Registry?



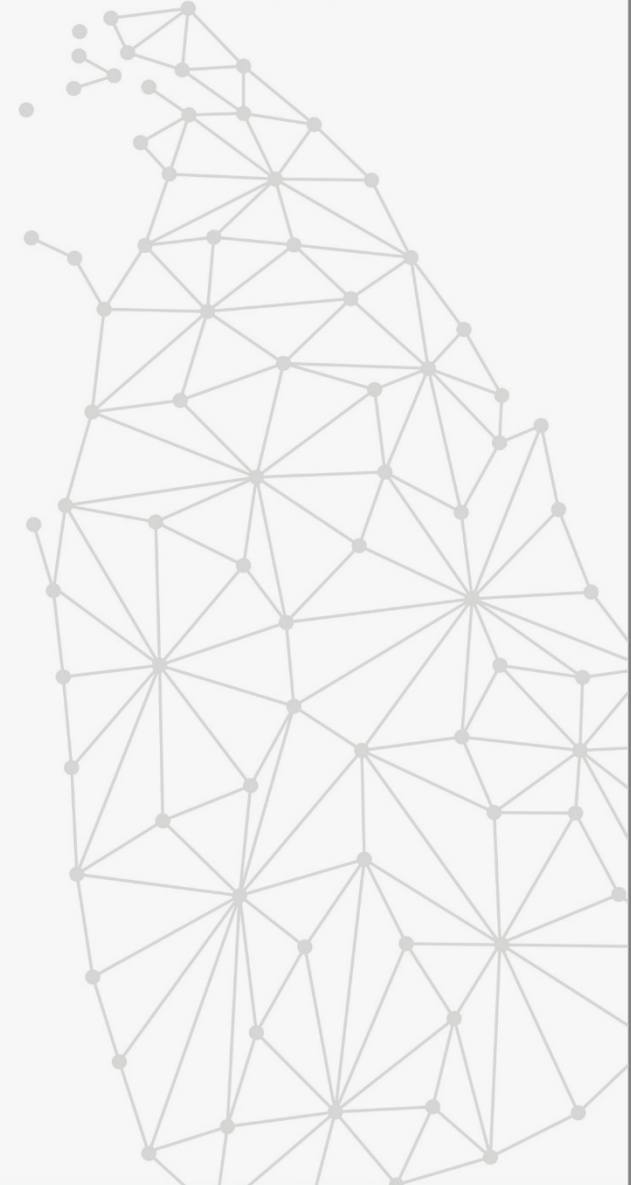
- It is a hierarchical database which contains the settings and configurations for the computer, hardware, services, security, and users etc.
- Active when operating system boots/starts
- Four main hives will read into the memory
  - Software – Information/Settings related to software installed on the system
  - System – Information/Settings related to the system
  - Security – Information/Settings related to security of the system
  - SAM – Information/Settings related to users of the system
- “NTUSER.DAT” registry file will come alive when a user authenticates to the system

# 2-Ways of viewing the registry

- Using a run command “regedit”



- Using a digital forensic investigation tool
  - Mount the 4 main hives located in below locations to the tool
    - windir\system32\config\System
    - windir\system32\config\Software
    - windir\system32\config\Security
    - windir\system32\config\SAM



# View from a forensic tool - EnCase



Name	File Ext	Physical Size	Logical Size	Item Path
system		2,359,296	2,359,296	CBARROW\WINDOWS\system32\config\system
software		11,272,192	11,272,192	CBARROW\WINDOWS\system32\config\software
userdiff		262,144	262,144	CBARROW\WINDOWS\system32\config\userdiff
system.LOG	LOG	2,048	1,024	CBARROW\WINDOWS\system32\config\system.LOG
software.LOG	LOG	2,048	1,024	CBARROW\WINDOWS\system32\config\software.LOG
default.LOG	LOG	2,048	1,024	CBARROW\WINDOWS\system32\config\default.LOG
userdiff.LOG	LOG	2,048	1,024	CBARROW\WINDOWS\system32\config\userdiff.LOG
system.sav	sav	376,832	376,832	CBARROW\WINDOWS\system32\config\system.sav
TempKey.LOG	LOG	2,048	1,024	CBARROW\WINDOWS\system32\config\TempKey.LOG
software.sav	sav	606,208	606,208	CBARROW\WINDOWS\system32\config\software.sav
default.sav	sav	90,112	90,112	CBARROW\WINDOWS\system32\config\default.sav
SECURITY		262,144	262,144	CBARROW\WINDOWS\system32\config\SECURITY
SAM		262,144	262,144	CBARROW\WINDOWS\system32\config\SAM
SECURITY.LOG	LOG	2,048	1,024	CBARROW\WINDOWS\system32\config\SECURITY.LOG
SAM.LOG	LOG	2,048	1,024	CBARROW\WINDOWS\system32\config\SAM.LOG
AppEvent.Evt	Evt	65,536	65,536	CBARROW\WINDOWS\system32\config\AppEvent.Evt

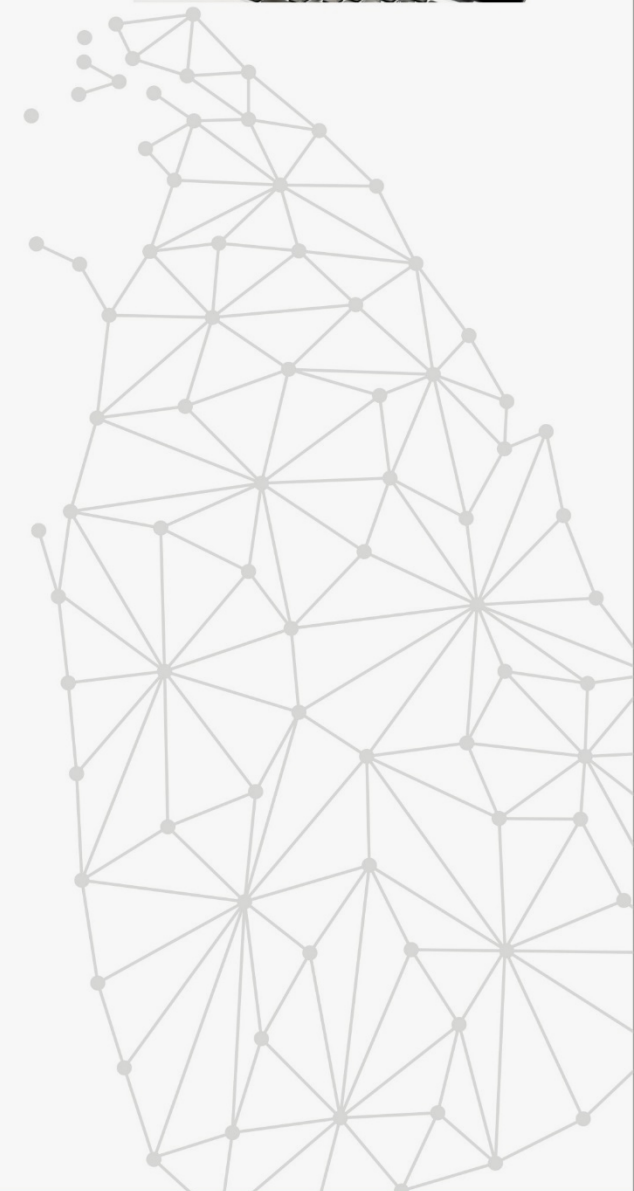
WINDOWS		144	144	CBARROW\C\Documents and Settings\Clyde\WINDOWS
Work		4,096	4,096	CBARROW\C\Documents and Settings\Clyde\Work
NTUSER.DAT	DAT	1,048,576	1,048,576	CBARROW\C\Documents and Settings\Clyde\NTUSER.DAT
NTUSER.DAT.LOG	LOG	2,048	1,024	CBARROW\C\Documents and Settings\Clyde\NTUSER.DAT...
ntuser.ini	ini	180	180	CBARROW\C\Documents and Settings\Clyde\ntuser.ini



# Confusing?



Subtree/Key	Filename
HKEY_LOCAL_MACHINE	windir\system32\config\System\
HKEY_LOCAL_MACHINE	windir\system32\config\Software
HKEY_LOCAL_MACHINE	windir\system32\config\Security
HKEY_USERS	windir\system32\config\SAM
HKEY_LOCAL_MACHINE\BCD00000000	\Boot\BCD
HKEY_CURRENT_USERS	NTUSER.DAT





# Structure of the Registry



Registry Editor

File Edit View Favorites Help

Computer

- HKEY\_CLASSES\_ROOT
- HKEY\_CURRENT\_USER
- HKEY\_LOCAL\_MACHINE
  - BCD00000000
  - HARDWARE
  - SAM
  - SECURITY
  - SOFTWARE
  - SYSTEM
    - ControlSet001
    - ControlSet002
    - CurrentControlSet
    - MountedDevices
    - RNG
    - Select
    - Setup
    - Software
    - WPA
- HKEY\_USERS
- HKEY\_CURRENT\_CONFIG

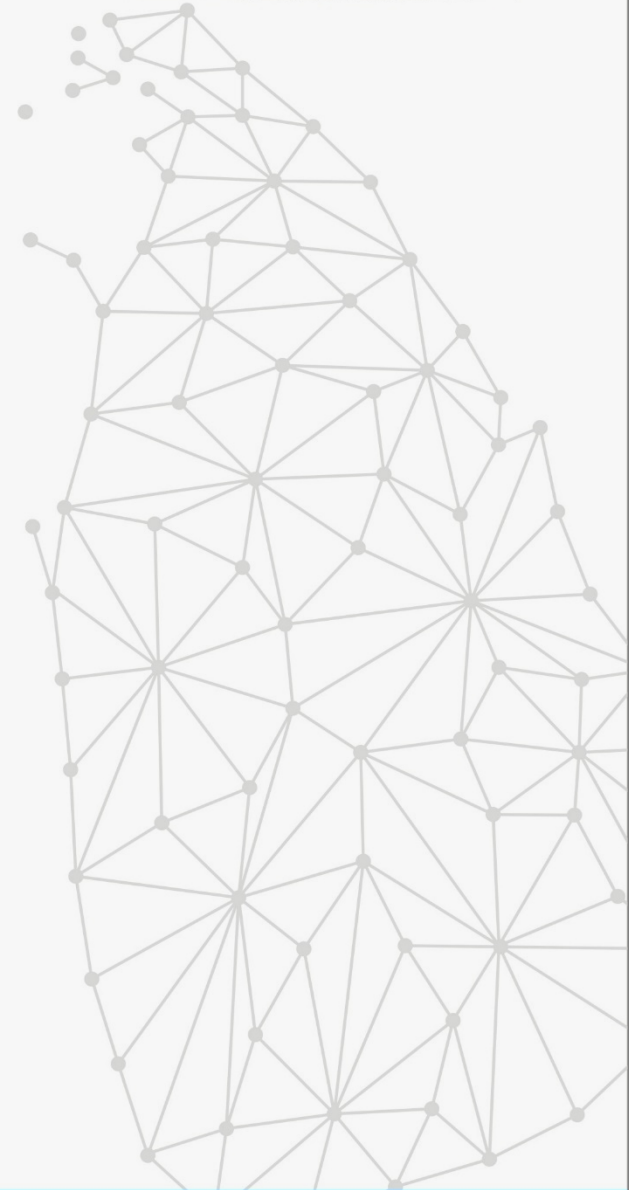
Name	Type	Data
(Default)	REG_SZ	(value not set)
Current	REG_DWORD	0x00000001 (1)
Default	REG_DWORD	0x00000001 (1)
Failed	REG_DWORD	0x00000000 (0)
LastKnownGood	REG_DWORD	0x00000002 (2)

Registry Key Hives

Values

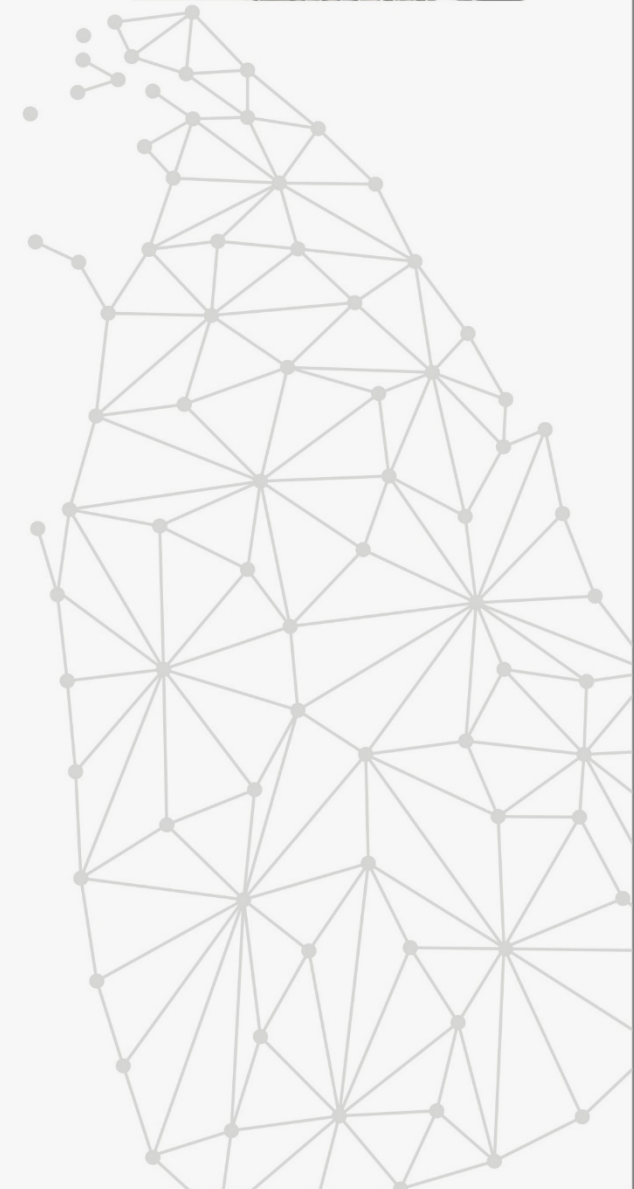
Registry Keys

Registry Sub Keys



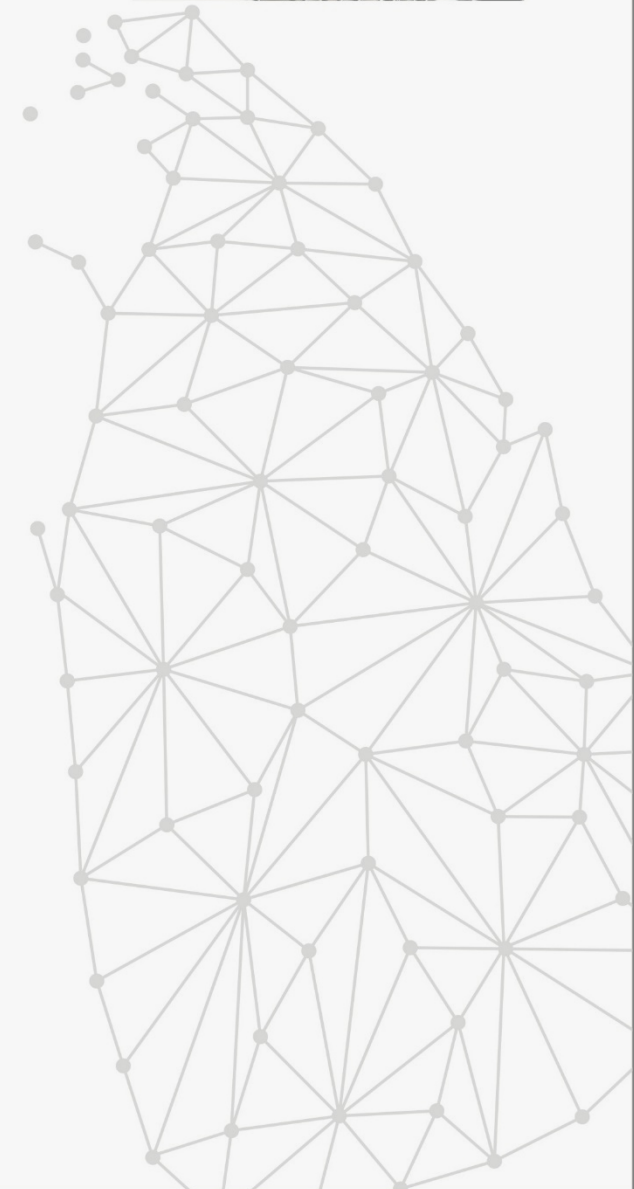
# Registry Analysis Tools

- Regedit.exe
- Reg.exe
- Autoruns.exe
- Scripting tools
  - Ex: Perl Win32::TieRegistry
- Regshot
- RegMon
- Build into tools Encase, F-Response, FTK
- RegRipper, RIP.pl, regslack



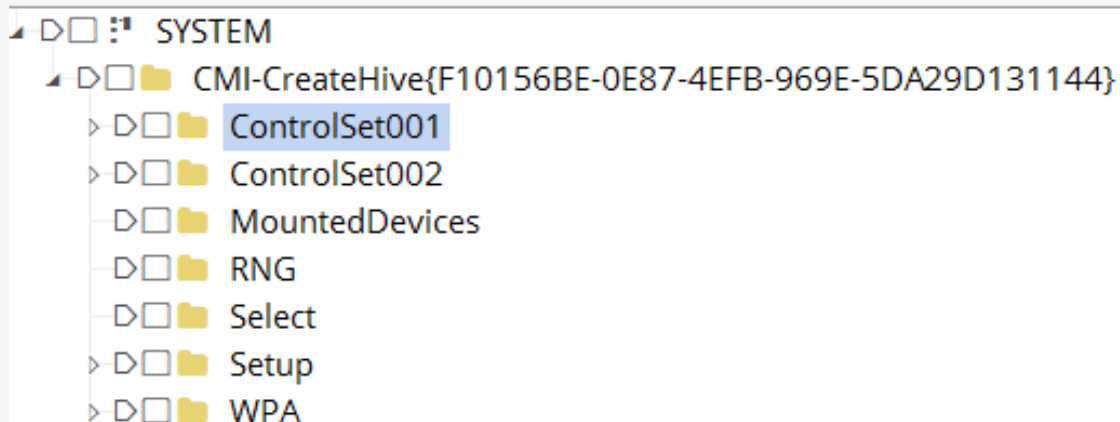
# When to use registry analysis

- Network related investigations
- Malware infections
- Suspicious user activities
- Fake document forgery investigations
- And many more



# Registry Investigation

- Finding out the Time Zone
  - Located in SYSTEM Hive
  - What are ControlSets?
    - Contains system configuration information (Devices, Drivers and Services)
    - System:NTRegistry\CMI-CreateHive[xxxxxx]/ControlSet001/Control/TimeZoneinformation
    - Regedit location - HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control
    - Values are stored in little-endian format(least significant bytes are processed first) 32-bit integer and displayed as hex values



```
SYSTEM
├── CMI-CreateHive{F10156BE-0E87-4EFB-969E-5DA29D131144}
│   ├── ControlSet001
│   ├── ControlSet002
│   ├── MountedDevices
│   ├── RNG
│   ├── Select
│   ├── Setup
│   └── WPA
```





# Registry Investigation

- Time Zone Contd.



SYSTEM

- ROOT
  - ActivationBroker
  - ControlSet001
  - DriverDatabase
  - HardwareConfig
  - Input
  - Keyboard Layout
  - Maps
  - MountedDevices
  - ResourceManager
  - ResourcePolicyStore
  - RNG
  - Select
  - Setup
  - Software
  - WaaS
  - WPA

	Name	File Ext	Physical Size	Logical Size	Item Path
1	Default		4	4	ROOT>Select\Default
2	Failed		4	4	ROOT>Select\Failed
3	LastKnownGood		4	4	ROOT>Select\LastKnownGood
4	Current		4	4	ROOT>Select\Current

Fields Report Text Hex Doc Transcript Picture Console File Extents Permissions Hash Sets Lock Condition Filter EnScript Decode Tag

Options Codepage Text Style Find Compressed View

01 00 00 00

Integers

- 8-bit integer
- 16-bit integer
- 16-bit big-endi
- 32-bit integer
- 32-bit big-endi
- 64-bit integer

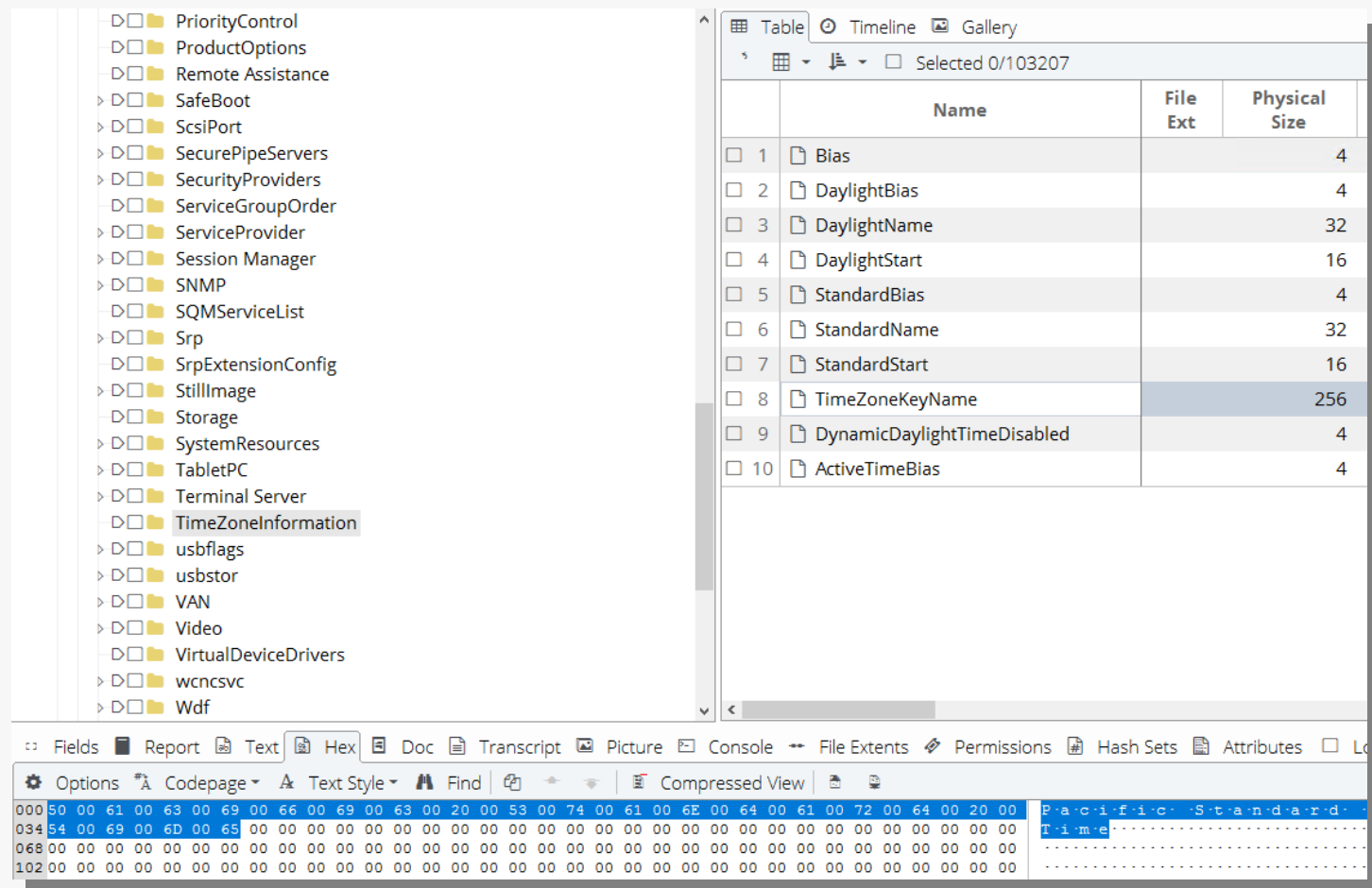
32-bit integer

Hex	UInt32	Int32
00000001	1	1



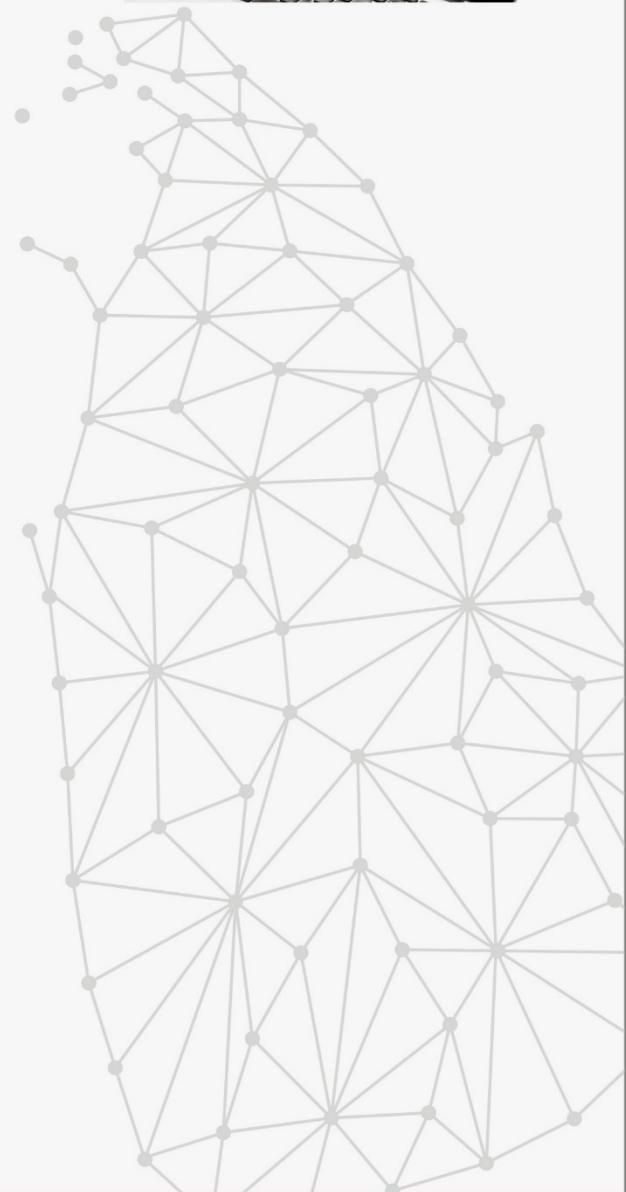
# Registry Investigation

- Time Zone Contd.



	Name	File Ext	Physical Size
1	Bias		4
2	DaylightBias		4
3	DaylightName		32
4	DaylightStart		16
5	StandardBias		4
6	StandardName		32
7	StandardStart		16
8	TimeZoneKeyName		256
9	DynamicDaylightTimeDisabled		4
10	ActiveTimeBias		4

Below the table, the hex data for the selected 'TimeZoneKeyName' is displayed in a hex editor view. The data is shown in hexadecimal and ASCII format. The ASCII column shows the text 'Pacific Standard Time'.



# Registry Investigation

- Identify last shutdown time period
- System\ControlSet001\Control\TimeZoneInformation\Windows

The screenshot displays the Windows Registry Editor with the path `System\ControlSet001\Control\TimeZoneInformation\Windows` selected. The right pane shows a list of registry values, with `ShutdownTime` highlighted. Overlaid on this is the DCode v4.02a utility window, which is used for converting hex data to date and time. The utility shows the following settings:

- Add Bias: UTC -08:00
- Decode Format: Windows: 64 bit Hex Value - Little Endian
- Example: FF03D2315FE1C701
- Value to Decode: 2A69C31B42C3CB01
- Date & Time: Wed, 02 February 2011 17:31:41 -0800

The utility also includes a 'Decode' button and a 'www.digital-detective.co.uk' link.



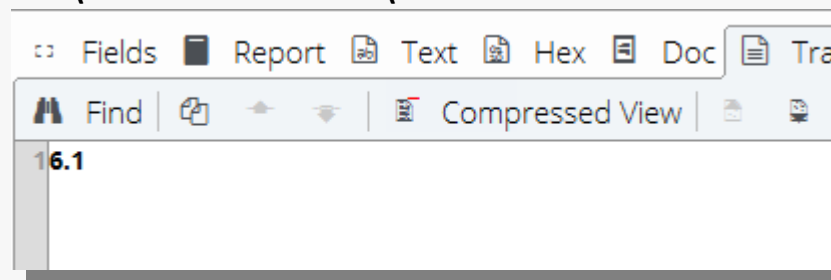
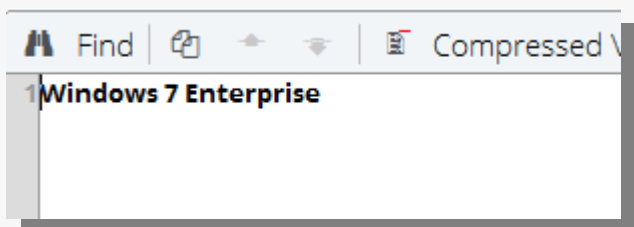
# Registry Investigation



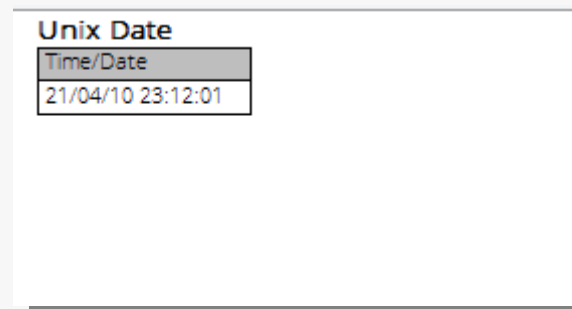
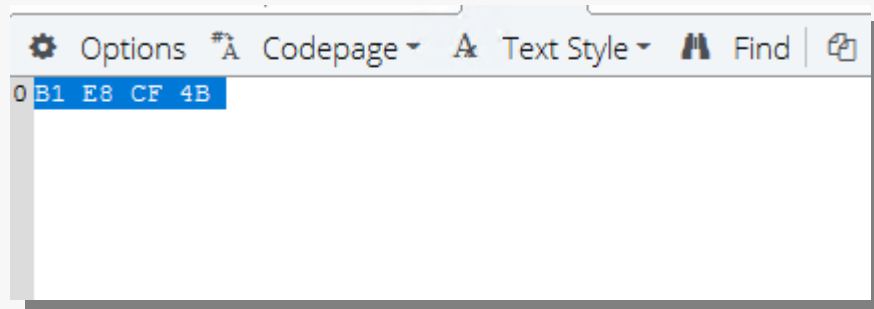
- Identifying the OS information and OS installed date/time

- Information can be found in the SOFTWARE Hive

- Software Hive\Microsoft\Windows NT\CurrentVersion\ProductName
- Software Hive\Microsoft\Windows NT\CurrentVersion\CurrentVersion



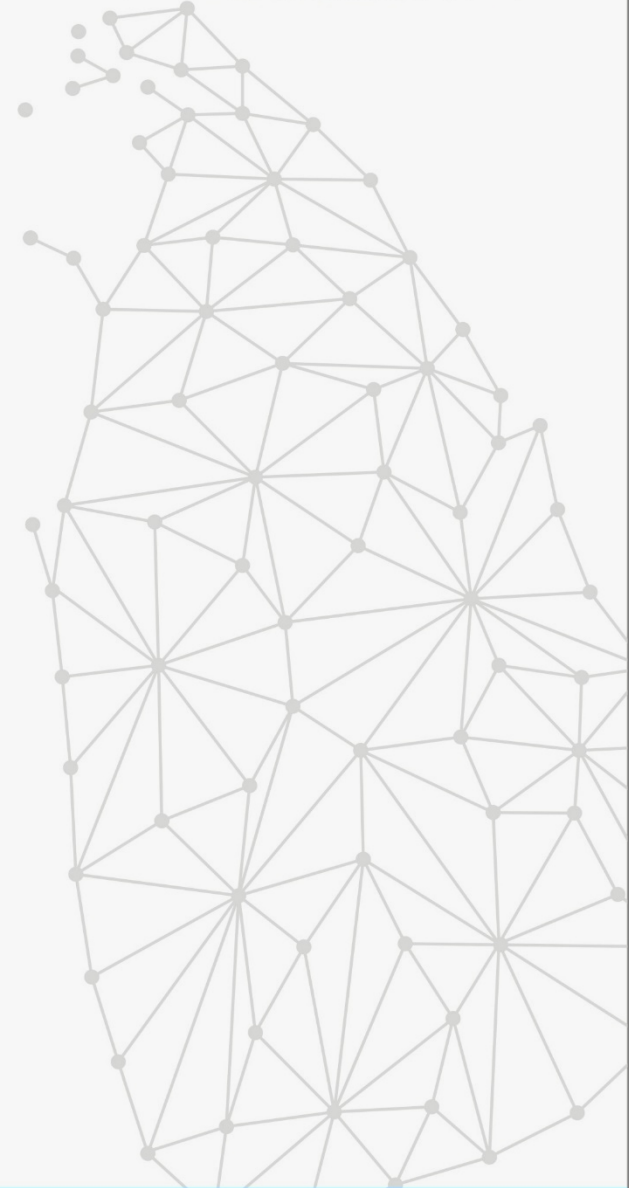
- Software Hive\Microsoft\Windows NT\CurrentVersion\InstallDate





# Registry Investigation

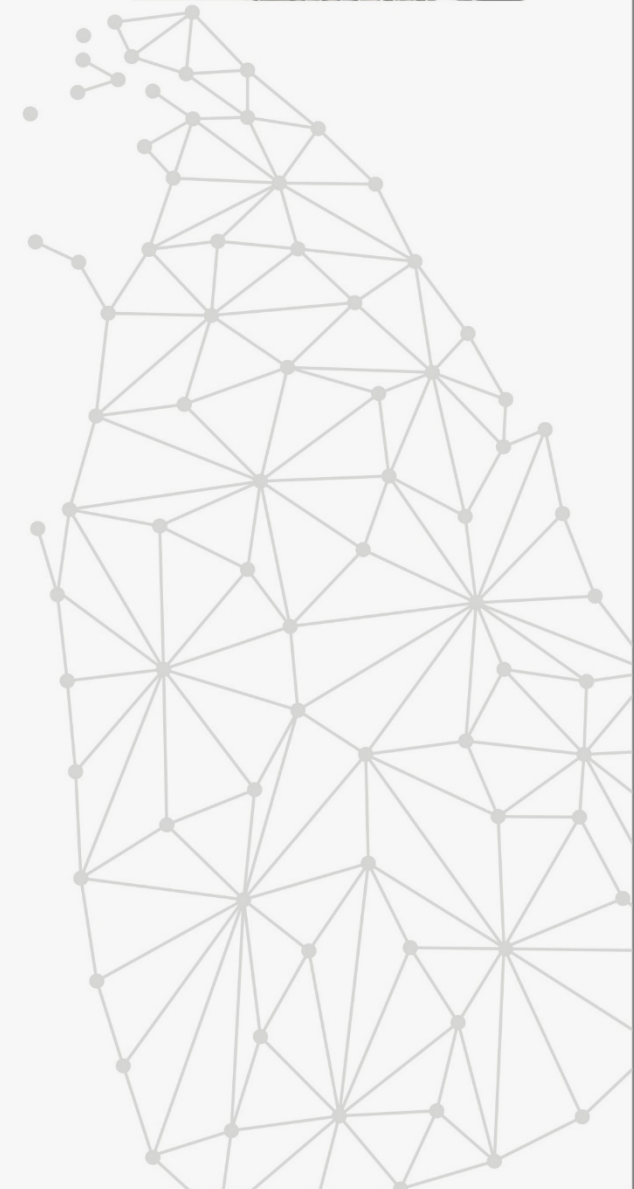
- Users in the system
- Our goal is to:
  - Identify the domain users and local users in the system



# Registry Investigation



- Users in the system contd.
  - Windows Security and Relative ID
  - SID is used to identify the computer system
  - RID is used to identify the specific user
  - SID appears as:
    - S-1-5-21-3774130484-663992614-3010368698-1000
  - USER ID (RID)
    - Administrator – 512
    - Guest – 501
    - Custom users – 1000 onward



# Registry Investigation



- Users in the system contd.

- SAM Hive

The screenshot shows the SAM hive structure in a registry viewer. The tree view is expanded to show the 'Users' subkey, which contains several user entries: 000001F4, 000001F5, 000003E8, 000003E9, and a 'Names' subkey. The 'Names' subkey contains 'Administrator', 'Guest', 'Sam.Malone', and 'Zerobit Admin'. To the right, a 'Hexadecimal to Decimal converter' tool is shown. It has a 'From' dropdown set to 'Hexadecimal' and a 'To' dropdown set to 'Decimal'. The 'Enter hex number:' field contains '3e8', and the 'Decimal number:' field contains '1000'. There are 'Convert', 'Reset', and 'Swap' buttons.

The screenshot shows the HKEY\_USERS registry hive. The tree view is expanded to show the 'HKEY\_USERS' subkey, which contains several user entries: .DEFAULT, S-1-5-18, S-1-5-19, S-1-5-20, S-1-5-21-291283512-199042653-2173327418-500, S-1-5-21-291283512-199042653-2173327418-500\_Classes, and HKEY\_CURRENT\_CONFIG.

- Finding SID using terminal

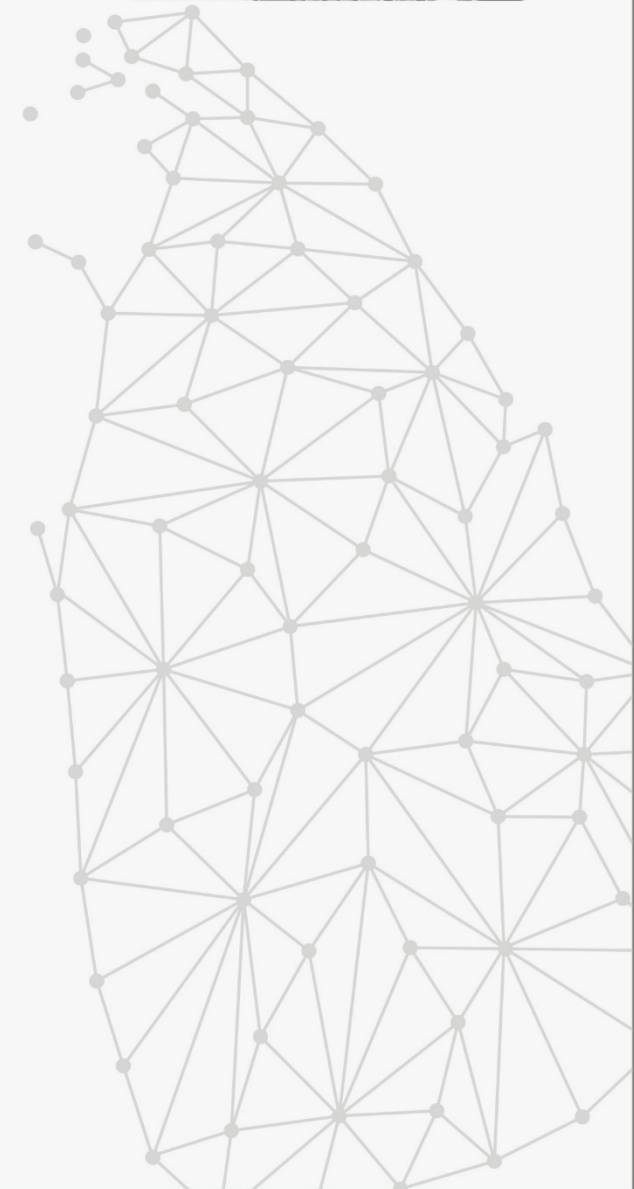
```
C:\Windows\system32\cmd.exe
Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>wmic useraccount get name,sid
Name                SID
Administrator       S-1-5-21-291283512-199042653-2173327418-500
DefaultAccount       S-1-5-21-291283512-199042653-2173327418-503
Guest                 S-1-5-21-291283512-199042653-2173327418-501

C:\Users\Administrator>_
```

# Registry Investigation

- Mounted Devices & USB Devices
- Our goal is to
  - Identify the mounted devices
  - Gather more information on each mounted devices
  - Finding the HardwareID
  - Map the hardwareID with the USB devices found in the crime scene





# Registry Investigation

- Mounted Devices

- List of Mounted devices on a system
- SYSTEM\MountedDevices

The screenshot displays the Windows Registry Editor at the path `SYSTEM\MountedDevices`. The left pane shows the tree structure with `MountedDevices` selected. The right pane shows a list of devices with their GUIDs and names. The bottom pane shows the hex data for the selected device, which is a Kingston DataTraveler 2.0 USB drive.

Index	Device Name	Value
85	\DosDevices\C:	24
86	\DosDevices\D:	194
87	\DosDevices\E:	24
88	\DosDevices\F:	24
89	\DosDevices\G:	12
90	\DosDevices\H:	218
91	\DosDevices\I:	238
92	\DosDevices\J:	252
93	\??\Volume{b3a55054-70ba-11e8-b...	214
94	\??\Volume{b3a55055-70ba-11e8-b...	216
95	\??\Volume{b3a55094-70ba-11e8-b...	212

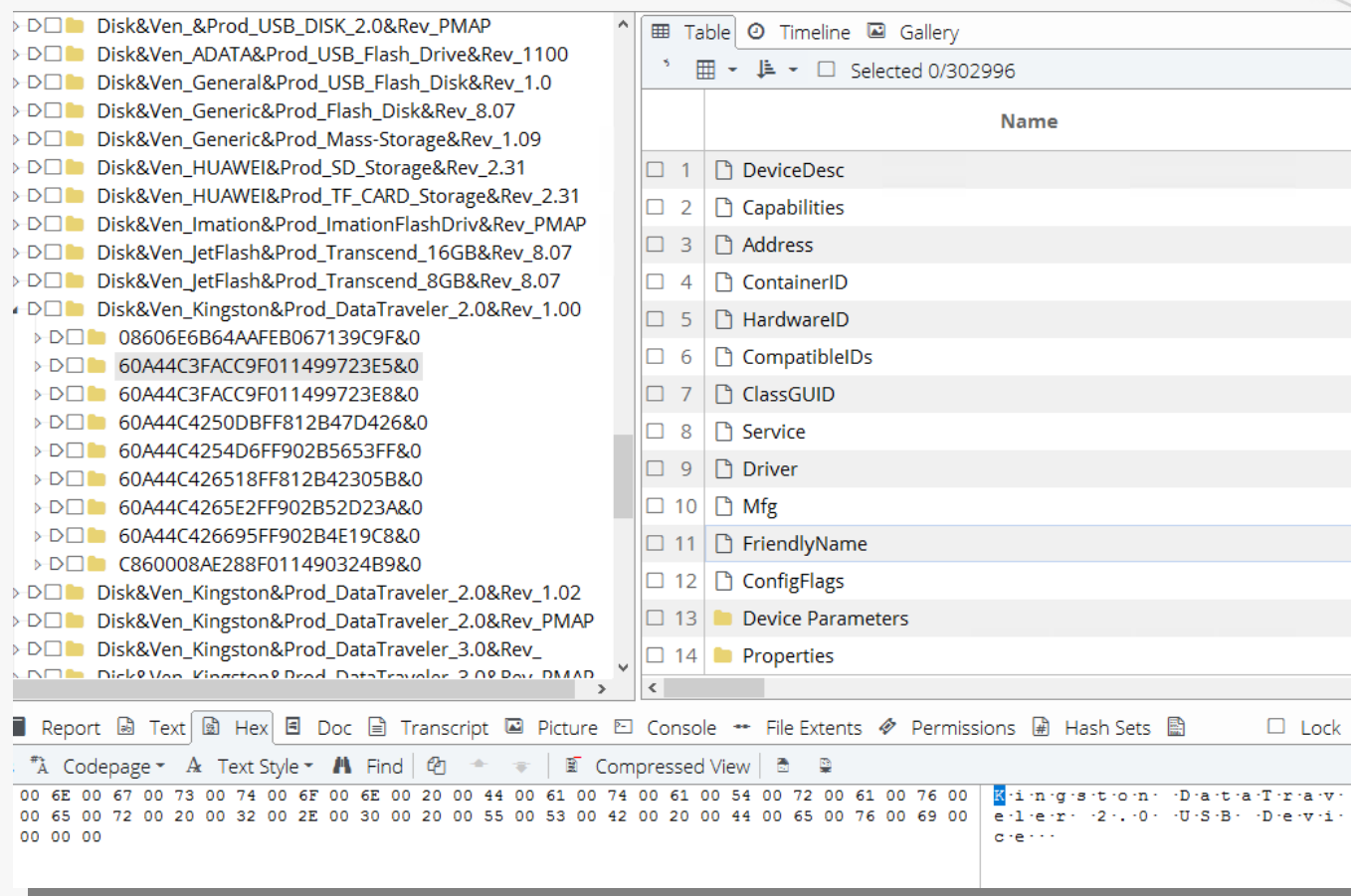
The bottom pane shows the hex data for the selected device, which is a Kingston DataTraveler 2.0 USB drive. The data is displayed in a hex editor view, showing the device's GUID and other identifying information.

```
000 5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4F 00 52 00 23 00 44 00 69 00 73 00 6B 00 26 00  
034 56 00 65 00 6E 00 5F 00 4B 00 69 00 6E 00 67 00 73 00 74 00 6F 00 6E 00 26 00 50 00 72 00 6F 00 64 00  
068 5F 00 44 00 61 00 74 00 61 00 54 00 72 00 61 00 76 00 65 00 6C 00 65 00 72 00 5F 00 32 00 2E 00 30 00  
102 26 00 52 00 65 00 76 00 5F 00 31 00 2E 00 30 00 30 00 23 00 30 00 38 00 36 00 30 00 36 00 45 00 36 00  
136 42 00 36 00 34 00 41 00 41 00 46 00 45 00 42 00 30 00 36 00 37 00 31 00 33 00 39 00 43 00 39 00 46 00  
170 26 00 30 00 23 00 7B 00 35 00 33 00 66 00 35 00 36 00 33 00 37 00 2D 00 62 00 36 00 62 00 66 00  
204 2D 00 31 00 31 00 64 00 30 00 2D 00 39 00 34 00 66 00 32 00 2D 00 30 00 30 00 61 00 30 00 63 00 39 00  
238 31 00 65 00 66 00 62 00 38 00 62 00 7D 00
```

# Registry Investigation

- USB Devices

- SYSTEM\ControlSet001\Enum\USBSTOR\



The screenshot displays the Windows Registry Editor. The left pane shows the tree structure expanded to `SYSTEM\ControlSet001\Enum\USBSTOR\`. A list of USB storage devices is shown, including various Kingston DataTraveler drives. The right pane shows the properties for the selected device, `Disk&Ven_Kingston&Prod_DataTraveler_2.0&Rev_1.00`. The properties include:

Name
1 DeviceDesc
2 Capabilities
3 Address
4 ContainerID
5 HardwareID
6 CompatibleIDs
7 ClassGUID
8 Service
9 Driver
10 Mfg
11 FriendlyName
12 ConfigFlags
13 Device Parameters
14 Properties

The bottom pane shows the hex data for the selected device, with the text `Kingston DataTraveler 2.0 USB Device` visible in the right column.



# Registry Investigation

- Network related investigations.
- Our goal is to:
  - Identifying Network Interface Cards
  - Identifying IP addresses, DHCP Server, LeaseObtainedTime, LeaseTerminatedTime, etc.
  - Identifying the SSID
  - Identifying the MAC address of the Wireless access point.



# Registry Investigation

- Network related investigations Contd.

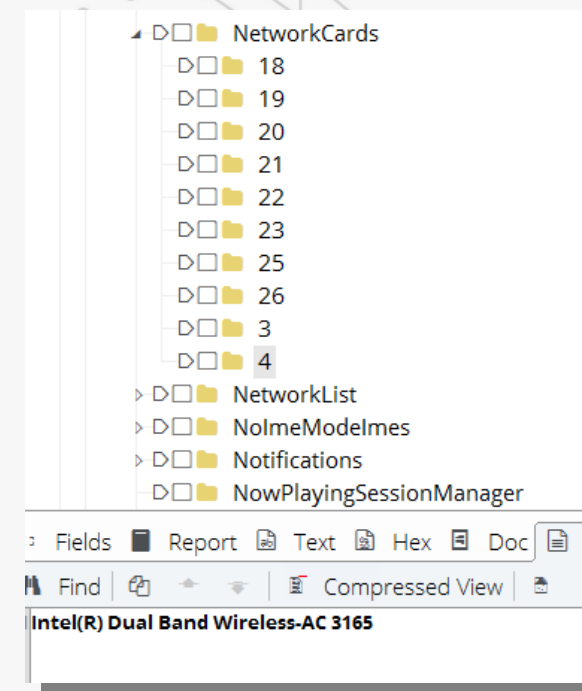
- Finding the NIC's

- SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkCards
    - GUID is important

{7559DD84-DB7A-42AE-9A0B-9AA7AB1A8660}

- Finding more information

- SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{GUID}





# Registry Investigation

- Network related investigations Contd.

Adapters	1	EnableDHCP	4
DNSRegisteredAdapters	2	MTU	4
Interfaces	3	UseZeroBroadcast	4
{11d2a2b8-0ee2-4e13-9f57-c26cbd6ec6b8}	4	Domain	2
{13a9fda3-877a-4bdb-aad5-b9c51ba584d6}	5	NameServer	2
{1b1a660e-536c-4af0-b0e6-7512d649a553}	6	DhcpIPAddress	24
{226AC763-C689-4048-93D0-5452D61BFA3A}	7	DhcpSubnetMask	28
{275dd3d2-f87b-4664-8e15-48beb86b4f0f}	8	DhcpServer	24
{37c27747-aaa7-40a7-93c3-100e5052f2fa}	9	Lease	4
{38cd87c3-e1cc-4402-b217-73fae61ce381}	10	LeaseObtainedTime	4
{3efb8523-b8e8-441e-b7a1-eb072bf9f10b}	11	T1	4
{3f33a990-b4da-4a2c-8640-b4ec8721570a}	12	T2	4
{421029f3-35af-430a-88b5-c122fe3fb21f}	13	LeaseTerminatesTime	4
{43b45b91-ec60-11e7-88a2-806e6f6e6963}	14	AddressType	4
{51f8a38e-dcb1-4281-b406-77abb12e941a}	15	IsServerNapAware	4
{6bb1ddf5-c82c-4305-beb7-da9fd17453fd}	16	DhcpConnForceBroadcastFlag	4
{7559dd84-db7a-42ae-9a0b-9aa7ab1a8660}			
055726C69636027596D26496			
055726C69636F575966496			
2514E444949514D2E414E4F4			
2556463627F63737F525F6F66647F607			
35C42534352364C425			



# Registry Investigation

- Network related investigations Contd.

- LeaseObtainedTime

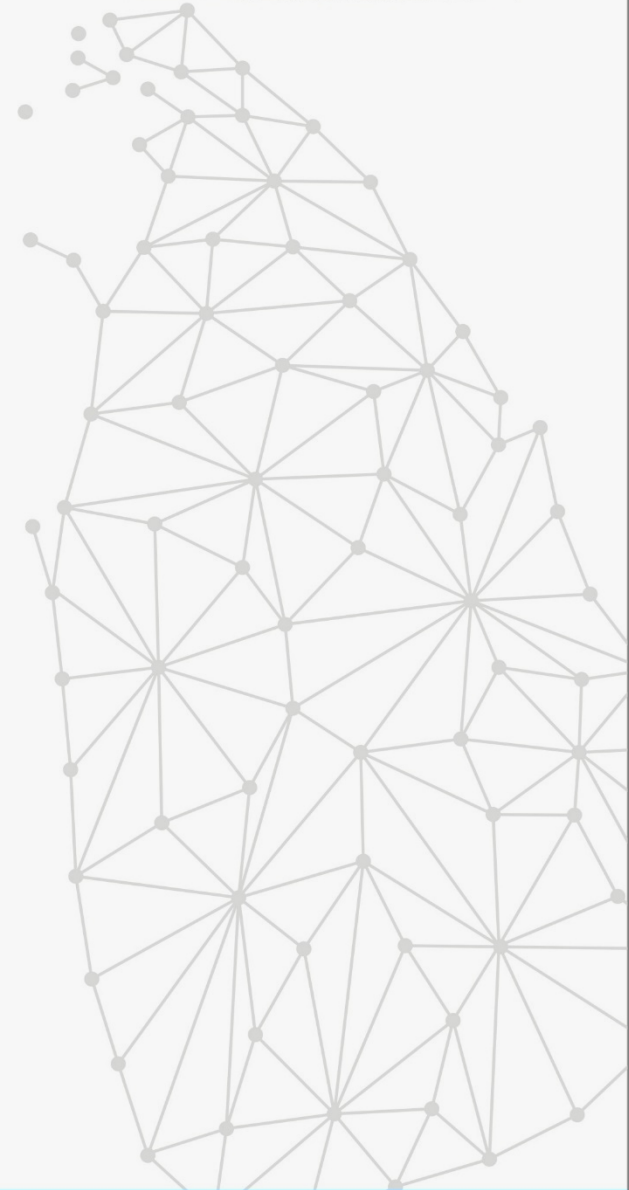
ark

Unix Date
Time/Date
12/08/19 13:19:32

- LeaseTerminatedTime

Unix Date
Time/Date
13/08/19 13:19:32

- Identified what time frame this interface connected to the network.
  - Which network is connected to remains to be discovered.



# Registry Investigation

- Network related investigations Contd.

- Identifying the network profiles

- Software\Microsoft\WindowsNT\CurrentVersion\NetworkList\Profiles
    - Each Profile has unique GUIDs

NetworkList

- DefaultMediaCost
- NewNetworks
- Nla
- Permissions
- Profiles
  - {0807BC91-E4C1-42D9-9BE5-479B9A7FDDDB9}
  - {098B1B53-BEB3-4F0F-B7DD-C8FDB924FBD3}
  - {15E99C9C-93BE-4230-83A5-7B12561725A2}
  - {16B94773-F897-45BB-A192-EA74C849133B}
  - {1D4BB7F8-CCB2-4BB9-9FB4-79A822B7314D}
  - {2977D5BF-8642-440B-8B4A-CF4242A29632}
  - {2A9917EE-ACF4-4DCE-AB7B-C42B13A88EC5}
  - {2F1035ED-6922-4B61-8F23-83B36B721561}
  - {3FB60C92-4C3F-4E0B-9309-E6EAB24738D2}
  - {4075C7D2-7191-4AD0-8E9D-8B4588A8C27B}
  - {461B1324-A417-4B97-A67C-5F79E53D2BDE}
  - {4A0AF03A-F15A-4EFB-83C1-4FDC349CB77D}
  - {50996703-F8E2-4991-BE6A-22C466C58898}
  - {52892781-383B-40FD-869A-528299718DED}

DCode v4.02a (Build: 9306)

Convert Data to Date / Time Values

Add Bias: UTC +05:30 ☐ Window on top

Decode Format: Windows: 128 bit SYSTEM Structure

Example: D9070800010002000600090013000000

Value to Decode: E307080001000C000D0013002000F501

Date & Time: Mon, 12 August 2019 13:19:32.501

www.digital-detective.co.uk

Cancel Clear Decode

00E3 07 08 00 01 00 0C 00 0D 00 13 00 20 00 F5 01

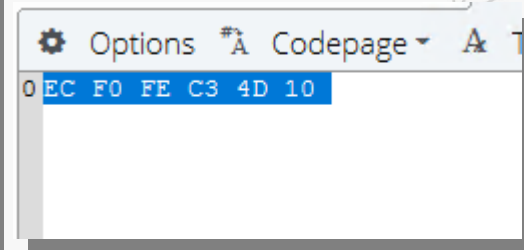
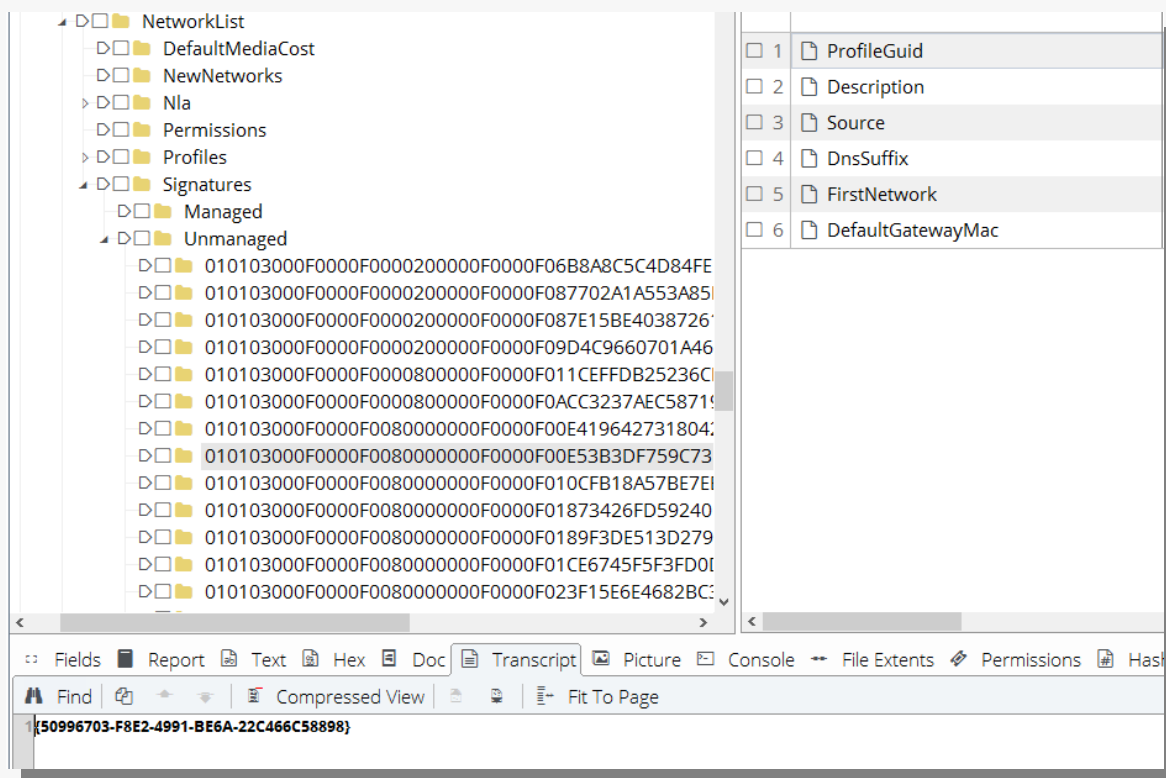
1SLT\_FIBRE

# Registry Investigation

- Network related investigations Contd.

- Finding the MAC address of the wireless access point

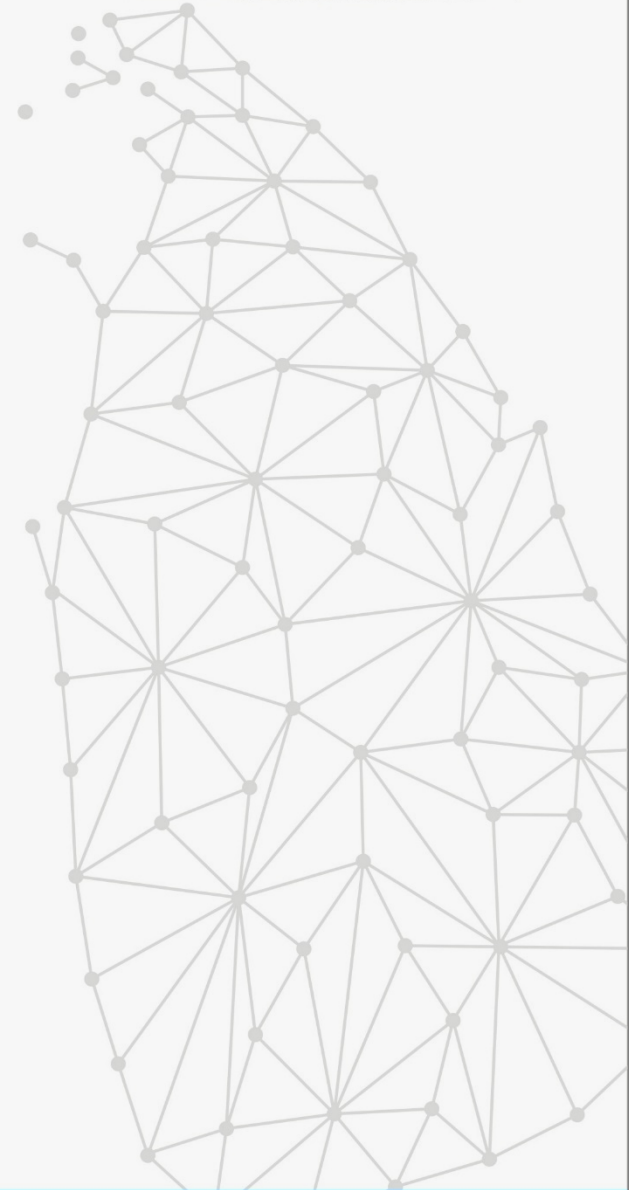
- Software\Microsoft\Windows\WindowsNT\CurrentVersion\NetworkList\Signatures\Unmanaged





# Registry Investigation

- Tracking User Activities
- Our goal is to:
  - Identifying the user behavior





# Registry Investigation



- Identifying MRU (Most Recently Used) files on a suspect computer system (Tracking User activities) - NTUSER.DAT
  - Contains User-specific data
  - Located at root of each user account on the system
  - Typed Url's
    - NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURLs
  - Opened Recent Documents
    - NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
      - MRUListEx will record the order in which the files were accessed
      - Each file number is represented in 8 bytes hexadecimal format. Convert each to 32-bit integer
      - Each file extension has its own folder.
        - Contains MRUListEx
        - File name

# Registry Investigation

- Tracking User activities Contd.

The screenshot displays a forensic analysis tool interface. On the left, a tree view shows the structure of an NTUSER.DAT file, with 'RecentDocs' expanded. The main pane shows a table of files and folders within 'RecentDocs'.

	Name	File Ext	Physical Size	Logical Size
214	91		216	
215	92		312	
216	93		262	
217	94		176	
218	95		332	
219	96		220	
220	97		106	
221	98		280	
222	99		222	
223	Folder		6	
224	MRUListEx		600	600

Below the table, a hex view shows the raw data of a file. The hex data is displayed in a grid, with the first few lines showing:

```
0000 3a 00 00 00 78 00 00 00 85 00 00 00 5b 00 00 00 1d 00 00 00 83 00 00 00 3b 00 00 00 14 00 00 00 0a 00 00
0340 00 00 03 00 00 72 00 00 00 23 00 00 00 8b 00 00 00 53 00 00 00 4b 00 00 00 08 00 00 00 15 00 00 00 00
0680 47 00 00 00 4c 00 00 00 21 00 00 00 05 00 00 00 00 00 00 00 69 00 00 00 5f 00 00 00 63 00 00 00 70 00 00
1020 00 00 66 00 00 00 50 00 00 00 52 00 00 00 55 00 00 00 3d 00 00 00 89 00 00 00 04 00 00 00 45 00 00 00 00
```

On the right, a file explorer shows the contents of a folder named 'RecentDocs', listing various files and folders, including '.0"', '.06162019', '.2017', '.2018', '.2019', '.39&sharedAccessToken=AAAC5E45-982F-4D74-A4', '.3gp', '.aac', '.avi', '.bmp', and 'bin'.

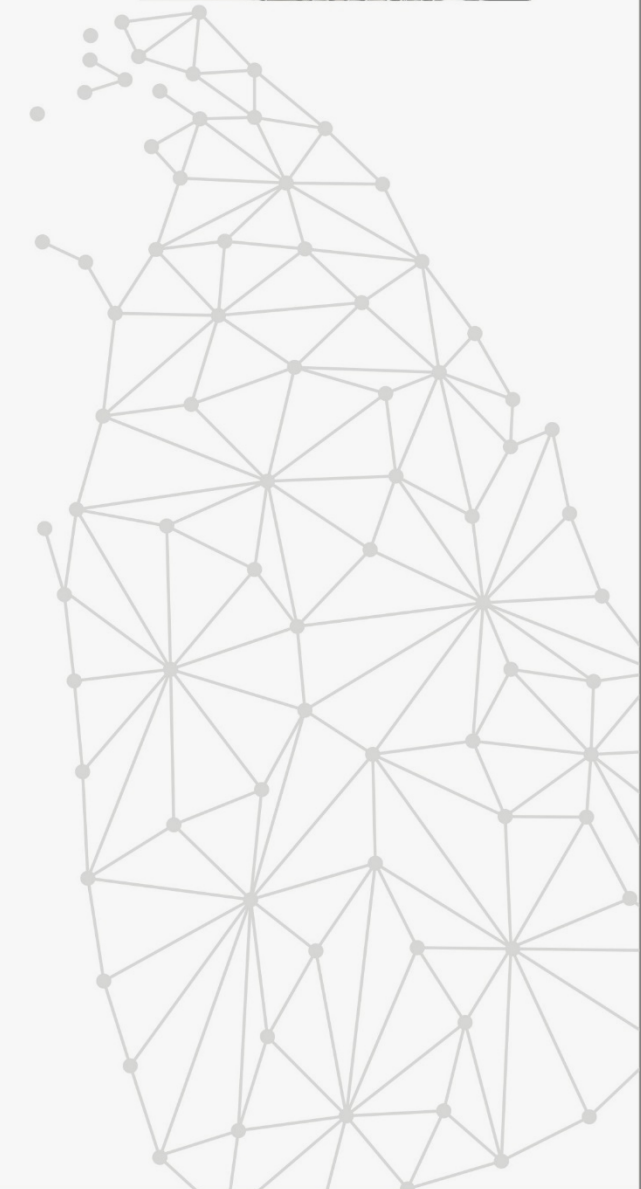
At the bottom, a '32-bit integer' field is shown with a value of 58.

# Registry Investigation

- Tracking User activities Contd.



Table Timeline Gallery					
Selected 0/60120					
	Name	File Ext	Physical Size	Logical Size	
<input type="checkbox"/> 191	.msg	msg	4	4	ROOT\Soft
<input type="checkbox"/> 192	.MTS	MTS	4	4	ROOT\Soft
<input type="checkbox"/> 193	.nomedia	nome...	8	8	ROOT\Soft
<input type="checkbox"/> 194	.odt	odt	4	4	ROOT\Soft
<input type="checkbox"/> 195	.opdownload	opdo...	11	11	ROOT\Soft
<input type="checkbox"/> 196	.pdf	pdf	4	4	ROOT\Soft
<input type="checkbox"/> 197	.PL	PL	3	3	ROOT\Soft
<input type="checkbox"/> 198	.png	png	4	4	ROOT\Soft
<input type="checkbox"/> 199	.ppsx	ppsx	5	5	ROOT\Soft
<input type="checkbox"/> 200	.ppt	ppt	4	4	ROOT\Soft
<input type="checkbox"/> 201	.pptm	pptm	5	5	ROOT\Soft
<input type="checkbox"/> 202	.pptx	pptx	5	5	ROOT\Soft
<input type="checkbox"/> 203	.pst	pst	4	4	ROOT\Soft
<input type="checkbox"/> 204	.rar	rar	4	4	ROOT\Soft



# Registry Investigation



- Tracking User activities Contd.

- User Assist Keys

- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{GUID}\Count
    - Mostly frequently opened EXE and LNK files
    - Keys are encrypted with ROT-13
    - What action user took through shell
    - Also shows when it has happened
    - Encase Provides Encrpt to decode
    - UserAssistView tool can be used - [https://www.nirsoft.net/utls/userassist\\_view.html](https://www.nirsoft.net/utls/userassist_view.html)

# Registry Investigation

- Tracking User activities Contd.

- User Assist Keys contd.

The screenshot displays a forensic tool interface with three main components:

- File List (Left):** A tree view showing a directory structure. The 'UserAssist' folder is expanded, revealing several subfolders with GUIDs. The 'Count' subfolder under the GUID {BCB48336-4DDD-48FF-BB0B-D3190DACB3E2} is selected.
- Table (Middle):** A table with columns 'Name' and 'File Ext'. It lists files with GUIDs and their extensions. The file 'U:\BVafgnyy.rkr' is highlighted in row 90.
- Cipher Decoder (Bottom):** A panel with three tabs: 'Ciphertext', 'ROT13', and 'Plaintext'. The 'Ciphertext' tab is active, showing the file path 'U:\BVafgnyy.rkr'. The 'ROT13' tab is also visible, showing the variant 'ROT13 (A-Z, a-z)' and the decoded output 'H:\0Install.exe'.

	Name	File Ext
86	{6Q809377-6NS0-444O-8957-N377...	RKR
87	{6Q809377-6NS0-444O-8957-N377...	RKR
88	{6Q809377-6NS0-444O-8957-N377...	rkr
89	P:\Hfref\Grfg\NccQngn\Ybpny\Grzc...	rkr
90	U:\BVafgnyy.rkr	rkr

**Cipher Decoder Interface:**

- VIEW** (plus icon)
- Ciphertext** (dropdown arrow)
- U:\BVafgnyy.rkr
- VIEW** (plus icon)
- ROT13** (dropdown arrow)
- VARIANT**
- ☐ ROT5 (0-9)
- ☒ ROT13 (A-Z, a-z)
- ☐ ROT18 (0-9, A-Z, a-z)
- ☐ ROT47 (!~)
- Decoded 15 chars in 4ms
- VIEW** (plus icon)
- Plaintext** (dropdown arrow)
- H:\0Install.exe





# Registry Investigation

- Tracking User activities Contd.

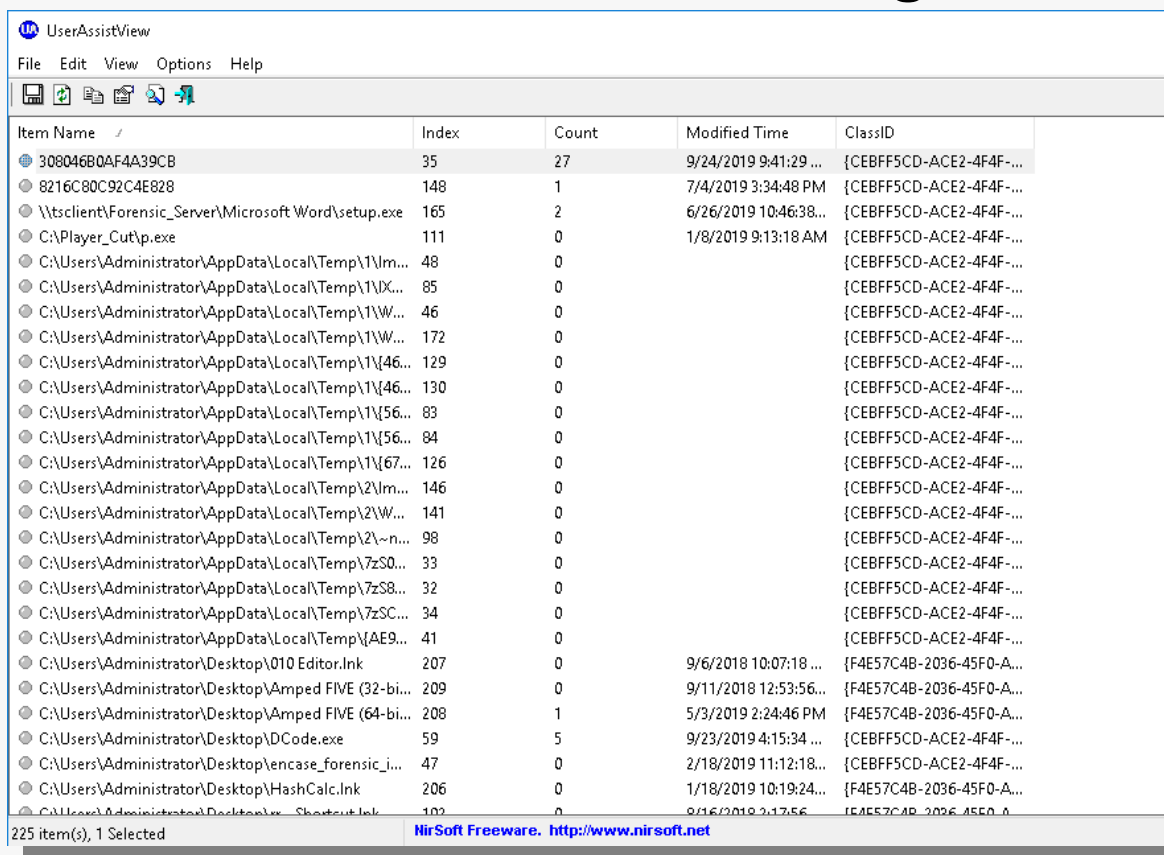
- Enscript

	A	B
1	Decoded Name	
2	<u>UEME_CTLSESSION</u>	
3	<u>UEME_CTLSESSION</u>	
4	<u>UEME_CTLSESSION</u>	
5	<u>UEME_CTLSESSION</u>	
6	<u>UEME_CTLCUACount:ctor</u>	<invalid>
7	<u>Microsoft.Getstarted_8wekyb3d8bbwe!App</u>	30/04/19 10:05:53
8	<u>UEME_CTLSESSION</u>	
9	<u>{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\mspaint.exe</u>	29/03/19 10:05:02
10	<u>Microsoft.Windows.Explorer</u>	12/08/19 13:30:41
11	<u>windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel</u>	29/03/19 15:08:25
12	<u>Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge</u>	12/08/19 13:44:33
13	<u>KasperskyLab.Kis.UI.Toasts</u>	14/02/19 16:26:54
14	<u>{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cmd.exe</u>	<invalid>
15	<u>Microsoft.Windows.ControlPanel</u>	30/07/19 10:01:33
16	<u>Microsoft.WindowsStore_8wekyb3d8bbwe!App</u>	28/07/19 08:30:15
17	<u>Microsoft.ZuneMusic_8wekyb3d8bbwe!Microsoft.ZuneMusic</u>	12/08/19 08:11:37
18	<u>Microsoft.Windows.Photos_8wekyb3d8bbwe!App</u>	12/08/19 13:44:18
19	<u>{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\msdt.exe</u>	14/10/18 19:40:15
20	<u>Microsoft.ZuneVideo_8wekyb3d8bbwe!Microsoft.ZuneVideo</u>	12/08/19 13:44:44
21	<u>Microsoft.Office.OUTLOOK.EXE.15</u>	12/08/19 08:48:29
22	<u>{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\OpenWith.exe</u>	<invalid>
23	<u>Microsoft.Windows.MediaPlayer32</u>	11/08/19 23:37:56
24	<u>{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\fsquirt.exe</u>	<invalid>
25	<u>OperaSoftware.OperaWebBrowser.1495693551</u>	12/08/19 08:35:49
26	<u>{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\GreenTree Applications\YTD Video Downloader\ytd.exe</u>	27/07/19 17:48:01
27	<u>Microsoft.Windows.Cortana_cw5n1h2txyewy!CortanaUI</u>	09/08/17 14:28:29
28	<u>Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy!App</u>	<invalid>
29	<u>Microsoft.MicrosoftEdge_8wekyb3d8bbwe!ContentProcess</u>	<invalid>
30	<u>Microsoft.MSPaint_8wekyb3d8bbwe!Microsoft.MSPaint</u>	20/02/19 13:36:56
31	<u>Microsoft.LockApp_cw5n1h2txyewy!WindowsDefaultLockScreen</u>	<invalid>
32	<u>{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\WFS.exe</u>	18/04/19 12:27:39
33	<u>Microsoft.WindowsScan_8wekyb3d8bbwe!App</u>	11/08/19 18:37:01
34	<u>Chrome</u>	21/07/19 16:06:39
35	<u>{6D809377-6AF0-444B-8957-A3773F02200E}\CONEXANT\SA3\HP-NB-AIO\SmartAudio3.exe</u>	<invalid>
36	<u>Microsoft.SkypeApp_kzf8qxf38zg5c!App</u>	11/09/18 14:26:10
37	<u>Microsoft.Windows.SecHealthUI_cw5n1h2txyewy!SecHealthUI</u>	<invalid>
38	<u>Microsoft.Windows.PeopleExperienceHost_cw5n1h2txyewy!App</u>	<invalid>
39	<u>Microsoft.MicrosoftEdge_8wekyb3d8bbwe!PdfReader</u>	<invalid>
40	<u>C:\Users\Test\Desktop\YTDSetup.exe</u>	21/11/18 15:37:45
41	<u>Microsoft.Office.OUTLOOK.EXE.16</u>	27/05/19 08:41:47



# Registry Investigation

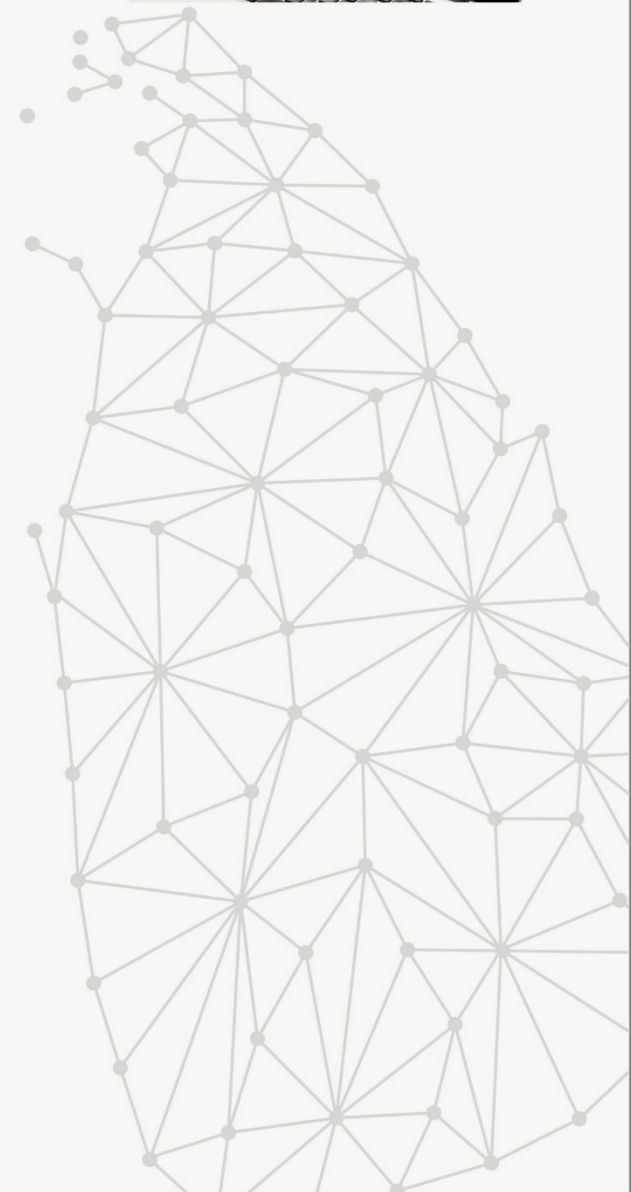
- Tracking User activities Contd.
  - UserAssistViewer – On a running machine



Item Name	Index	Count	Modified Time	ClassID
308046B0AF4A39CB	35	27	9/24/2019 9:41:29 ...	{CEBFF5CD-ACE2-4F4F-...
8216C80C92C4E828	148	1	7/4/2019 3:34:48 PM	{CEBFF5CD-ACE2-4F4F-...
\\tsclient\Forensic_Server\Microsoft Word\setup.exe	165	2	6/26/2019 10:46:38...	{CEBFF5CD-ACE2-4F4F-...
C:\Player_Cut\p.exe	111	0	1/8/2019 9:13:18 AM	{CEBFF5CD-ACE2-4F4F-...
C:\Users\Administrator\AppData\Local\Temp\1\Wm...	48	0		{CEBFF5CD-ACE2-4F4F-...
C:\Users\Administrator\AppData\Local\Temp\1\DX...	85	0		{CEBFF5CD-ACE2-4F4F-...
C:\Users\Administrator\AppData\Local\Temp\1\W...	46	0		{CEBFF5CD-ACE2-4F4F-...
C:\Users\Administrator\AppData\Local\Temp\1\W...	172	0		{CEBFF5CD-ACE2-4F4F-...
C:\Users\Administrator\AppData\Local\Temp\1\{46...	129	0		{CEBFF5CD-ACE2-4F4F-...
C:\Users\Administrator\AppData\Local\Temp\1\{46...	130	0		{CEBFF5CD-ACE2-4F4F-...
C:\Users\Administrator\AppData\Local\Temp\1\{56...	83	0		{CEBFF5CD-ACE2-4F4F-...
C:\Users\Administrator\AppData\Local\Temp\1\{56...	84	0		{CEBFF5CD-ACE2-4F4F-...
C:\Users\Administrator\AppData\Local\Temp\1\{67...	126	0		{CEBFF5CD-ACE2-4F4F-...
C:\Users\Administrator\AppData\Local\Temp\2\Wm...	146	0		{CEBFF5CD-ACE2-4F4F-...
C:\Users\Administrator\AppData\Local\Temp\2\W...	141	0		{CEBFF5CD-ACE2-4F4F-...
C:\Users\Administrator\AppData\Local\Temp\2\~n...	98	0		{CEBFF5CD-ACE2-4F4F-...
C:\Users\Administrator\AppData\Local\Temp\7zS0...	33	0		{CEBFF5CD-ACE2-4F4F-...
C:\Users\Administrator\AppData\Local\Temp\7zS8...	32	0		{CEBFF5CD-ACE2-4F4F-...
C:\Users\Administrator\AppData\Local\Temp\7zSC...	34	0		{CEBFF5CD-ACE2-4F4F-...
C:\Users\Administrator\AppData\Local\Temp\{AE9...	41	0		{CEBFF5CD-ACE2-4F4F-...
C:\Users\Administrator\Desktop\010 Editor.lnk	207	0	9/6/2018 10:07:18 ...	{F4E57C4B-2036-45F0-A...
C:\Users\Administrator\Desktop\Amped FIVE (32-bi...	209	0	9/11/2018 12:53:56...	{F4E57C4B-2036-45F0-A...
C:\Users\Administrator\Desktop\Amped FIVE (64-bi...	208	1	5/3/2019 2:24:46 PM	{F4E57C4B-2036-45F0-A...
C:\Users\Administrator\Desktop\DCcode.exe	59	5	9/23/2019 4:15:34 ...	{CEBFF5CD-ACE2-4F4F-...
C:\Users\Administrator\Desktop\encase_forensic_i...	47	0	2/18/2019 11:12:18...	{CEBFF5CD-ACE2-4F4F-...
C:\Users\Administrator\Desktop\HashCalc.lnk	206	0	1/18/2019 10:19:24...	{F4E57C4B-2036-45F0-A...
C:\Users\Administrator\Desktop\... Shortcut.lnk	102	0	9/16/2019 3:17:56	{F4E57C4B-2036-45F0-A...

225 item(s), 1 Selected

NirSoft Freeware. <http://www.nirsoft.net>



# Registry Investigation



- Tracking User activities Contd.

- RunMRU

- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
- Most recently used typed items. (Start button, Run commands, etc.)
- MRUList will show the order

	Name	Type	Data
	(Default)	REG_SZ	(value not set)
	a	REG_SZ	gpedit.msc\1
	b	REG_SZ	cmd\1
	c	REG_SZ	notepad\1
	d	REG_SZ	mspaint\1
	e	REG_SZ	explorer\1
	f	REG_SZ	regedit\1
	MRUList	REG_SZ	fbceda

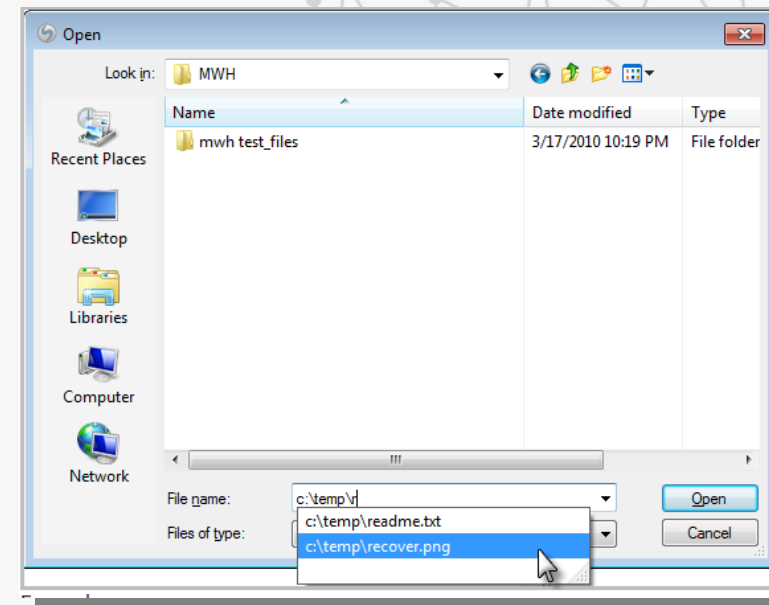


# Registry Investigation

- Tracking User activities Contd.

- OpenSaveMRU

- Files that have been opened or saved with a windows shell dialog box
    - NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDMRU





# Registry Investigation



- Tracking User activities Contd.

- OpenSaveMRU Contd.

- Each file extension have a folder
- Each folder have a MRUListEx to order
- \* folder will contain information about the latest 10 files regardless of the file extension
- File Name and location

7 5		497																																	
00 00 00 00 00 00 00 00 00 00 00 00 00 00 87 F9 E8 00 54 00 65 00 73 00 74																		..@.... ..tùè·T·e·s·t																	
00 00 00 00 00 00 F2 4E 10 26 11 00 44 65 73 6B 74 6F 70 00 68 00 09 00 04 00 EF																		.....~1.....òN·&·Desktop·h· ...i																	
26 2E 00 00 00 00 F6 D3 00 00 00 00 17 00 00 00 00 00 00 00 00 00 00 00 3E 00 00 00 00																		·%·I),òN·&·...ôÓ.....>....																	
00 73 00 6B 00 74 00 6F 00 70 00 00 00 00 40 00 73 00 68 00 65 00 6C 00 6C 00 33																		·i/·D·e·s·k·t·o·p·...@·s·h·e·l·l·3																	
00 6C 00 2C 00 2D 00 32 00 31 00 37 00 36 00 39 00 00 00 16 00 7E 00 32 00 00																		·2·..d·l·l·,·--2·1·7·6·9·.....~2·..																	
00 4A 52 43 20 50 72 65 73 65 6E 74 61 74 69 6F 6E 2E 70 64 66 00 00 5A 00 09																		.....€·J·R·C·P·r·e·s·e·n·t·a·t·i·o·n·.p·d·f·-2·																	
00 00 00 00 00 00 2E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00																		...i%.....																	
00 4A 00 52 00 43 00 20 00 50 00 72 00 65 00 73 00 65 00 6E 00 74 00 61 00 74																		.....J·R·C·P·r·e·s·e·n·t·a·t																	
00 70 00 64 00 66 00 00 00 24 00 00 00																		·i·o·n·.p·d·f·...\$...																	



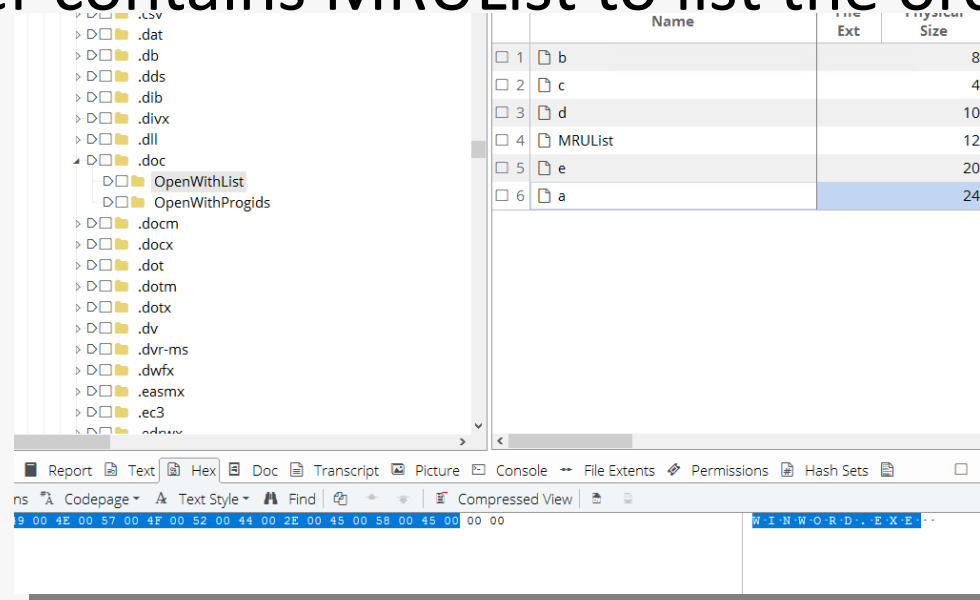


# Registry Investigation



- Tracking User activities Contd.

- FileExts - NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts
  - Tell the system what application to use to open a file
  - Folders with each file extension
  - Each folder contains MRUList to list the order of applications



# Registry Investigation

- What if there are no values?
  - “Absence of evidence is not evidence of absence”
    - Windows washer removes the registry entries
      - Last run times of windows washer becomes evidence



Thank You !  
&  
Any Questions?

