College of Informatics and Virtual Education (CIVE)

IA 418: Cyber Criminology and Techniques

Windows Registry Forensics

Windows Registry

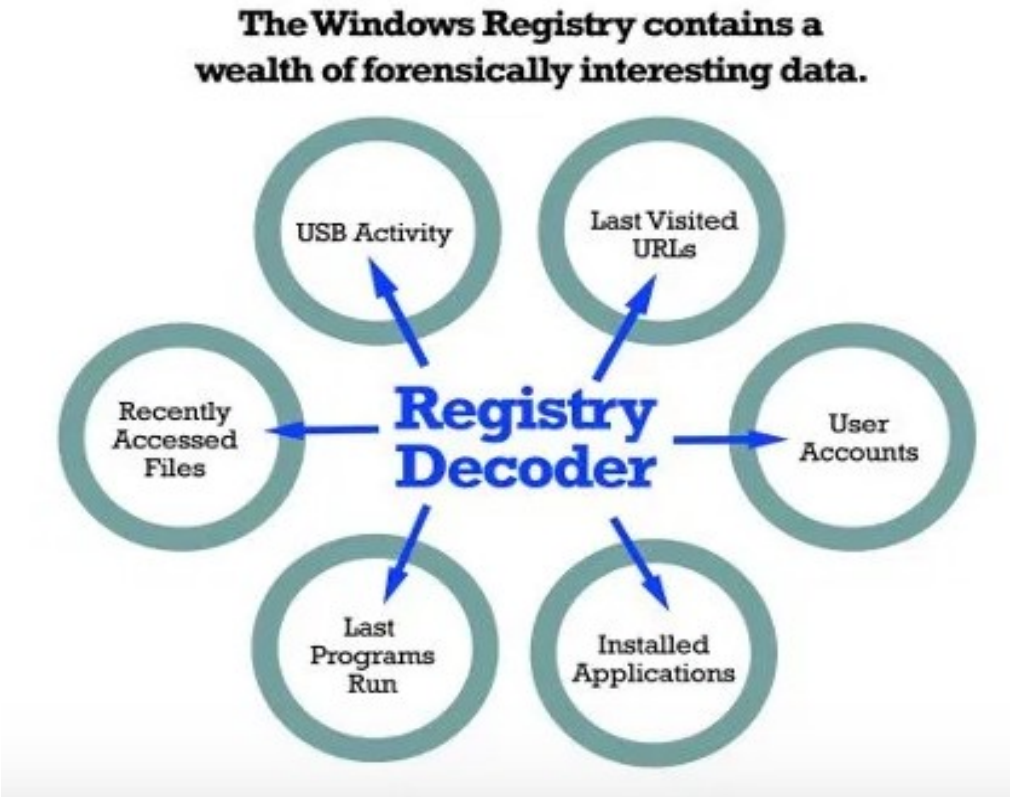
- Registry is **central database** of Windows systems
- ✓ **Configuration** of system
- ✓ Information about **user activity**
  - Applications **installed** and **opened**
  - Window positions and sizes: to provide **user with a better experience**
- ✓ Information is **time-stamped**
- It is considered the **heart** of **Windows OS.**
- ✓ It contains **critical information** needed by the operating system and installed applications in **order to function**.

Windows Registry

- It is considered the **heart** of **Windows OS.**
- ✓ It contains **critical information** needed by the operating system and installed applications in **order to function**.
- ✓ Almost **every action** conducted by a **Windows user** is **stored** in its **registry** in one way or another.
- ✓ This makes the **Windows registry** a **rich source** of **evidence** that can be extremely valuable for any **digital forensic investigation**.

Windows Registry

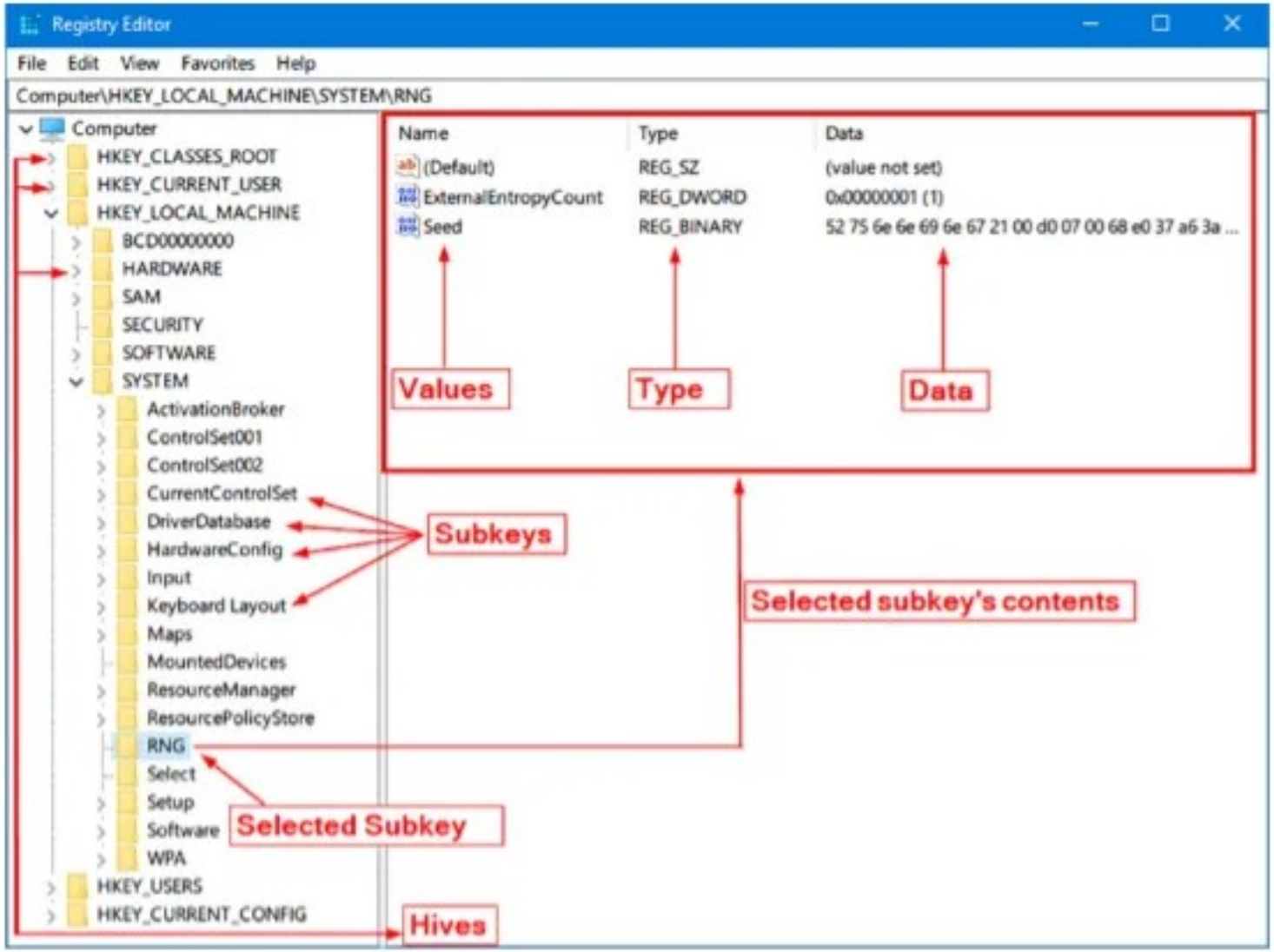
- Pieces of information that can be established:



Windows Registry: Architecture

- The registry is a **hierarchical database** that **stores** Windows system **configuration settings** for
- ✓ Hardware
- ✓ Software applications
- ✓ Operating system
- ✓ User's preferences and the computer's and applications' usage history.
- Registry data is structured in a **tree format**, where each **node** in the tree is called a **key.**
- ✓ A key can contain other keys (**subkeys**) in addition to **data values**.

Windows Registry: Architecture



Windows Registry: Architecture

- The Windows registry contains **five root folders** (also known as **hives**).
- Hives are the **first folders** in the registry and appear on the left side when you first open the registry editor and all other keys are minimized.

```
1 HKEY_CLASSES_ROOT - Contains file association information (configuration informati
2 HKEY_CURRENT_USER - Stores configuration information (related to the installed so
3 HKEY_LOCAL_MACHINE - Contains the majority of the configuration information for cu
4 HKEY_USERS - Contains configuration information (user profiles) for all active use
5 HKEY_CURRENT_CONFIG - Does not store information itself; instead, acts as a pointe
```

Windows Registry: Architecture

- HKCR stores information about **registered applications**
  - **Associations** from File Extensions and OLE Object Class IDs tying them to the applications used to handle these items.
- HKCU stores settings that are specific to the **currently logged-in user**.
  - The HKCU key is a link to the subkey of HKEY_USERS that corresponds to the user; the same information is reflected in both locations.
- HKLM **stores settings** that are **general to all users** on the computer.

Windows Registry: Architecture

- HKU contains subkeys corresponding to the HKEY_CURRENT_USER keys for **each user registered on the machine.**
- HKCC contains information gathered at runtime; information stored in this key is **not permanently** stored on the **hard disk**, but rather regenerated at boot time.
- Type **regedit.exe** at the 'search' field to see the five hives.

Windows Registry: Architecture

- Root hives are divided into two types with regard to their data persistence:
- ✓ **Volatile** and **nonvolatile**.
- **Non-volatile**
- ✓ **HKEY_LOCAL_MACHINE** and **HKEY_USERS** keys are nonvolatile and are stored on the **hard drive.**
- **Volatile**
- ✓ The remaining hives are volatile and **should be captured** while the **system is running** in order to acquire useful information from them.

Windows Registry: Investigation

- Digital forensic investigators can examine the Windows registry using two methods:
- ✓ The registry is contained within a **forensic image**.
  - ❑ The computer forensic program will be used to investigate registry files as you do when browsing files/folders using Windows File Explorer.
- ✓ **Live analysis** (e.g., when **booting up** from the suspect **forensic image**).
  - ❑ You can access the registry as you do with any computer using the Windows built-in registry editor.

Windows Registry: Investigation

- **Location** of registry files:

✓ When examining the Windows registry using a captured forensic image, the registry files are located in **Windows\System32\Config** folder.

✓ In the **config** folder, you will find many files

- A separate file for each root hive and a couple of supporting files for each one.
- There is an exception with the **HKEY_CURRENT_USER** hive, as this one is stored in your **profile** folder.

Windows Registry: Registry Editor

- Windows Operating Systems are equipped with a **registry editor:**
- ✓ An administrator can **view**, **edit**, and **back up** the Windows registry.
- To access the built-in registry editor, follow these steps:
- ✓ Press the **Windows button** and the **R** button (Win+R) to open the Run dialog.
- ✓ Type **regedit** and press **OK**.

Windows Registry Acquisition

- **Computer forensics** tools will acquire Windows registry files as a part of acquiring the target machine's system drive or when performing a complete **hard drive acquisition**.
- You can also extract only the **registry files** from a **live system** and store it separately for later analysis
- ✓ Usually referred to as "**Registry Image**".
- With **AccessData FTK Imager**, follow these steps:
- ✓ Attach the USB drive that contains FTK Imager to the suspect machine, open FTK Image, and go to File menu ➤ Obtain Protected Files

Windows Registry Acquisition

- With **AccessData FTK Imager**, follow these steps:

✓ Attach the USB drive that contains FTK Imager to the suspect machine, open FTK Image, and go to File menu

- Obtain Protected Files

✓ A new dialog appears; select where you want to store obtained files, and check the option “Password recovery and all registry files”.

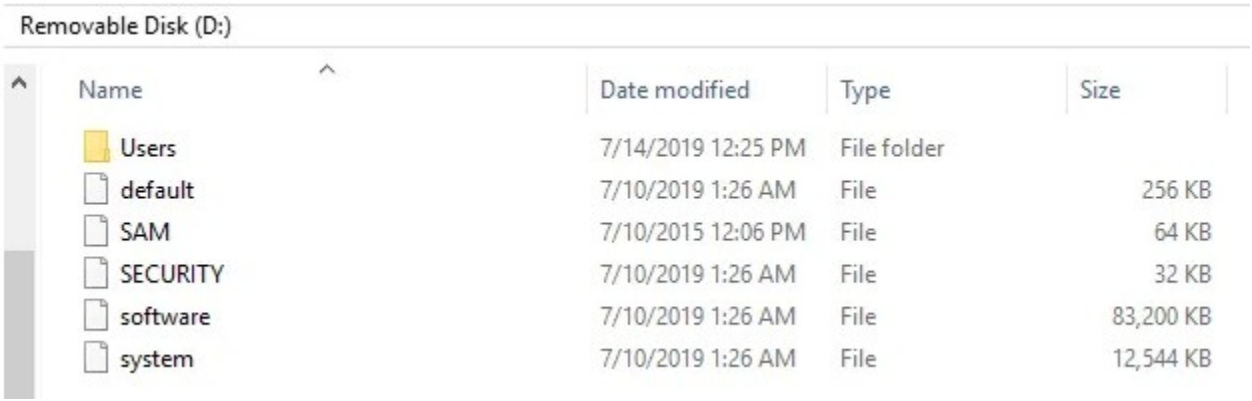
- Finally, click the “OK” button.

Windows Registry Acquisition

- With **AccessData FTK Imager**, follow these steps:

✓ A progress window will appear showing registry files' export progress; upon finishing, the window will disappear without announcing any success message.

✓ Go to the directory where you have saved your registry files to see the resultant files; you should see the five files and one folder.



Windows Registry Examination

- Installed Program Keys in the Windows Registry:

✓ Learning what programs are **currently** or were **previously installed** on the suspect machine can be of great value for forensic investigators.

- For example, the existence of **steganography** and **encryption** programs —or the **leftovers** belonging to such tools— will give an indication that the suspect machine may contain hidden data or simply was used to execute such programs.

Windows Registry Examination

- Installed Program Keys in the Windows Registry:
- ✓ If the suspect's machine has **more than one user**, each user will have his/her own set of software installed on his/her own key under the (HKEY_CURRENT_USER) hive.
- ✓ Windows keeps records of **all installed applications** in the following locations in the registry:
  - ✓ HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\ WINDOWS\CURRENTVERSION\UNINSTALL
  - ✓ HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\ WINDOWS\CURRENTVERSION\UNINSTALL
  - ✓ HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432NODE\ MICROSOFT\WINDOWS\CURRENTVERSION\UNINSTALL

Windows Registry Examination

- Installed Program Keys in the Windows Registry:
- ✓ Windows keeps records of **all installed applications** in the following locations in the registry:
  - ✓ HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\UNINSTALL
  - ✓ HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\UNINSTALL
  - ✓ HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS\CURRENTVERSION\UNINSTALL
  - ✓ HKEY_CLASSES_ROOT\INSTALLER\PRODUCTS\<PRODUCTCODE>\SOURCELIST\NET
  - ✓ HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\INSTALLER\PRODUCTS\<PRODUCTCODE>\SOURCELIST\NET

Windows Registry Examination

- Automated **tools** can be used to:
- ✓ Search for a program **installed** on the Windows registry
- ✓ **Lost** information such as **parts** of installed programs, applications **leftover**,
- ✓ Any data items that could be **hidden** in the Windows registry.
- **RegScanner** which is a small tool used to search the Windows registry according to specific search criteria entered by the user

Windows Registry Examination

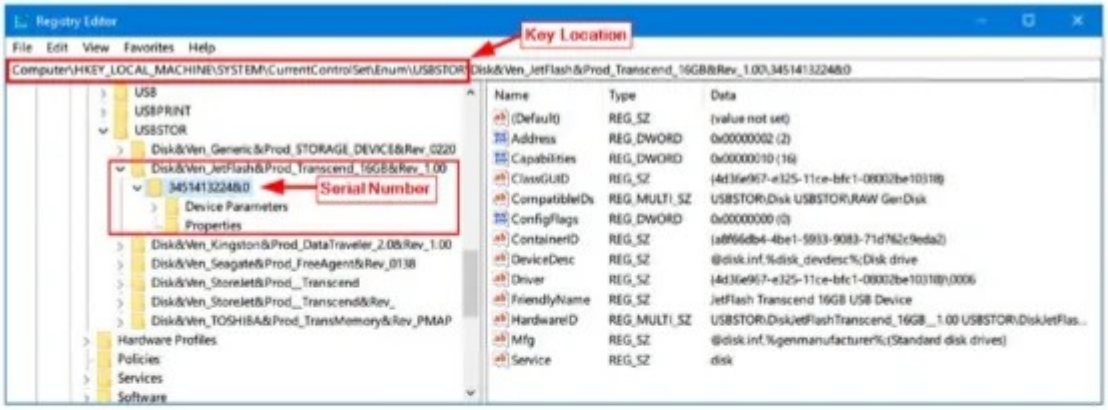
- USB Device Forensics
  - ✓ Windows keeps a **history log** of all previously connected USB devices along with their connection times in addition to the associated user account which installs them.
  - ✓ The Windows registry also stores important technical information for each connected USB device such as **vendor ID**, **product ID**, **revision**, and **serial number**.
  - ✓ Windows stores USB history-related information **using five registry keys**, where each key offers a different piece of information about the connected device.
  - ✓ By **merging this information** together, investigators will have an idea of how an offender has used removable devices—such as a USB—to conduct/facilitate his/her actions.

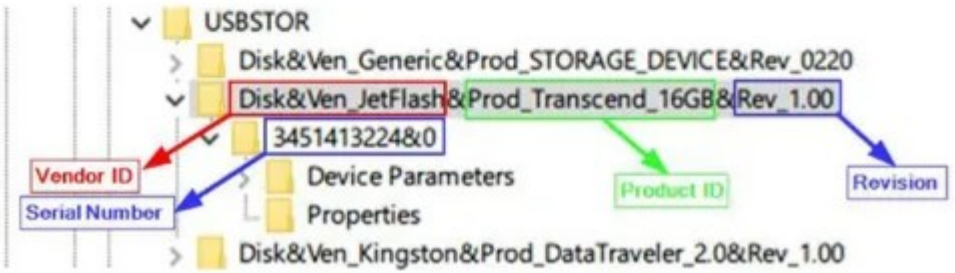
Windows Registry Examination

- USB Device Forensics
- ✓ **HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Enum\USBSTOR**
  - Find **all USB devices** that have been **plugged** into the operating system **since its installation**.
  - It shows the USB **vendor ID** (manufacturer name), **product ID**, and the **device serial number**
  - Note that if the second character of the device serial number is "&," it means the connected device does not have a serial number and the device ID has been generated by the system.

Windows Registry Examination

- USB Device Forensics
- ✓ **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR**





Windows Registry Examination

- USB Device Forensics
- **HKEY_LOCAL_MACHINE\SYSTEM\MountedDevice**
  - The MountedDevices subkey stores the **drive letter** allocations.
  - It **matches** the **serial number** of a USB device to a given **drive letter** or volume that was mounted when the USB device was inserted.
- **HKEY_CURRENT_USER\Software\Microsoft\ Windows\CurrentVersion\Explorer\ MountPoints2.**
  - Records which **user was logged** into Windows when a specific USB device was connected.
  - The key also includes the "**Last Write Time**" for each device that was connected to the system.

Windows Registry Examination

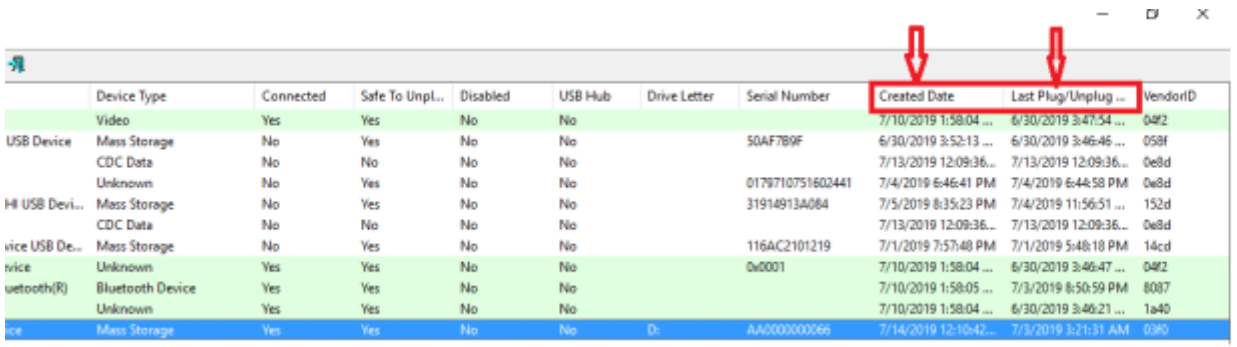
- USB Device Forensics
- **HKEY_LOCAL_MACHINE\SYSTEM\MountedDevice**
  - The MountedDevices subkey stores the **drive letter** allocations.
  - It **matches** the **serial number** of a USB device to a given **drive letter** or volume that was mounted when the USB device was inserted.
- **HKEY_CURRENT_USER\Software\Microsoft\ Windows\CurrentVersion\Explorer\ MountPoints2.**
  - Records which **user was logged** into Windows when a specific USB device was connected.
  - The key also includes the "**Last Write Time**" for each device that was connected to the system.

Windows Registry Examination

- USB Device Forensics
- ✓ **HKEY_LOCAL_MACHINE\SYSTEM\Currentcontrolset\Enum\Usb**
  - Holds **technical information** about each connected USB device in addition to the **last time** the subject USB was connected to the investigated computer.
- ✓ **Files** to identify the **first time** device was **connected:**
  - Windows Vista, Windows 7, Windows 8: **\Windows\inf\setupapi.dev.log**
  - Windows 10: **\Windows\inf\setupapi.upgrade.log**
  - Windows XP: **\Windows\setupapi. Log**
  - Search in this file for a particular USB device's serial number to learn when it was first connected to the subject system (in local time).

Windows Registry Examination

- USB Device Forensics
  - ✓ The process of finding USB information can also be automated.
  - ✓ The tool **USBDeview** automates all the tasks discussed previously.
    - **Last Plug/Unplug** Date represents the first time that the device was connected to the system. This date does not change when the same device is repeatedly reinserted.
    - The "**Created Date**" represents the last time that the same device was attached to the system.



	Device Type	Connected	Safe To Unpl...	Disabled	USB Hub	Drive Letter	Serial Number	Created Date	Last Plug/Unplug ...	VendorID
	Video	Yes	Yes	No	No			7/10/2019 1:58:04 ...	6/30/2019 3:47:54 ...	04f2
USB Device	Mass Storage	No	Yes	No	No		50AF7B9F	6/30/2019 3:52:13 ...	6/30/2019 3:46:46 ...	058f
	CDC Data	No	No	No	No			7/13/2019 12:09:36...	7/13/2019 12:09:36...	0e8d
	Unknown	No	Yes	No	No		0179710751602441	7/4/2019 6:46:41 PM	7/4/2019 6:44:58 PM	0e8d
HI USB Devi...	Mass Storage	No	Yes	No	No		31914913A084	7/5/2019 8:35:23 PM	7/4/2019 11:56:51 ...	152d
	CDC Data	No	No	No	No			7/13/2019 12:09:36...	7/13/2019 12:09:36...	0e8d
vice USB De...	Mass Storage	No	Yes	No	No		116AC2101219	7/1/2019 7:57:48 PM	7/1/2019 5:48:18 PM	14cd
vice	Unknown	Yes	Yes	No	No		0x0001	7/10/2019 1:58:04 ...	6/30/2019 3:46:47 ...	04f2
uetooth(R)	Bluetooth Device	Yes	Yes	No	No			7/10/2019 1:58:05 ...	7/3/2019 8:50:59 PM	8087
	Unknown	Yes	Yes	No	No			7/10/2019 1:58:04 ...	6/30/2019 3:46:21 ...	1a40
ice	Mass Storage	Yes	Yes	No	No	D:	AA0000000066	7/14/2019 12:10:42...	7/3/2019 3:21:31 AM	03f0

Windows Registry Examination

- USB Device Forensics
  - ✓ **Not all types** of USB will **leave a trace** in registry files..
  - ✓ A USB device connected through an MTP connection needs special treatment to acquire its traces from a Windows machine.
- Other types of forensic tools are:
  - ✓ **USD Detective**: supports detecting USB devices that use the MTP protocol to connect to Windows.
    - It also offers rich features for thoroughly investigating connected USB devices, like creating timelines of all unique connection/disconnection and deletion timestamps for each device.

Windows Registry Examination

- Other types of USB forensic tools are:
  - ✓ **USD Detective**: supports detecting USB devices that use the MTP protocol to connect to Windows.
    - It also offers rich features for thoroughly investigating connected USB devices, like creating timelines of all unique connection/disconnection and deletion timestamps for each device.
  - ✓ **USB Forensic tracker** (USBFt) is a **free**, comprehensive suite for investigating USB devices.
    - It supports Windows, linux, and Mac and can retrieve USB device connection artifacts from live systems, mounted forensic images, or volume shadow copies.

Windows Registry Examination

- **Most Recently Used List**
  - **Windows** keep a **log** of the most **recently accessed files**.
  - There are many applications that run on Windows that have most recently used (MRU) lists such as recently opened MS Office files and recently visited web pages:
    - These applications **list** the files that have been **most recently accessed**.
  - The most common places for storing such lists are in the registry keys:
    - **HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs**

Windows Registry Examination

- **Most Recently Used List**
  - ✓ The most common places for storing such lists are in the registry keys:
    - **HKEY_CURRENT_USER\Software\Microsoft\ Office.0\Word\File MRU**
    - **KEY_CURRENT_USER\Software\Microsoft\ Windows\CurrentVersion\Explorer\ ComDlg32\ OpenSavePidlMRU**
    - **HKEY_CURRENT_USER\Software\Microsoft\ Windows\CurrentVersion\Explorer\ ComDlg32\ LastVisitedPidlMRU**
    - **HKEY_CURRENT_USER\Software\Microsoft\ Windows\CurrentVersion\Explorer\ RunMRU**

Windows Registry Examination

- **Most Recently Used List**
  - ✓ The most common places for storing such lists are in the registry keys:
    - **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs**
    - **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit**
  - ✓ Tools:
    - **ExecutedProgramsList** :list of programs and batch files that have executed previously on the target machine.
    - **OpenSaveFilesView**: list of files that have been previously opened on the target machine using the standard open/save dialog box of Windows.

Windows Registry Examination

- **Network Analysis**
  - ✓ Whenever a Windows user **connects** his/her machine to the **Internet** or **intranet**, Windows will **log** this action in the registry.
  - ✓ Knowing the **network connection** has **vital forensic value**;
    - ❑ The registry lists all **network cards** that have been used on the **suspect machine** whether it is built-in or attached (e.g., via USB port).
    - ❑ The registry will also reveal the wireless connection profile (**name**, **IP address**, **subnet mask**, **DHCP**) in addition to the date the connection was first created and the last date the connection took place.

Windows Registry Examination

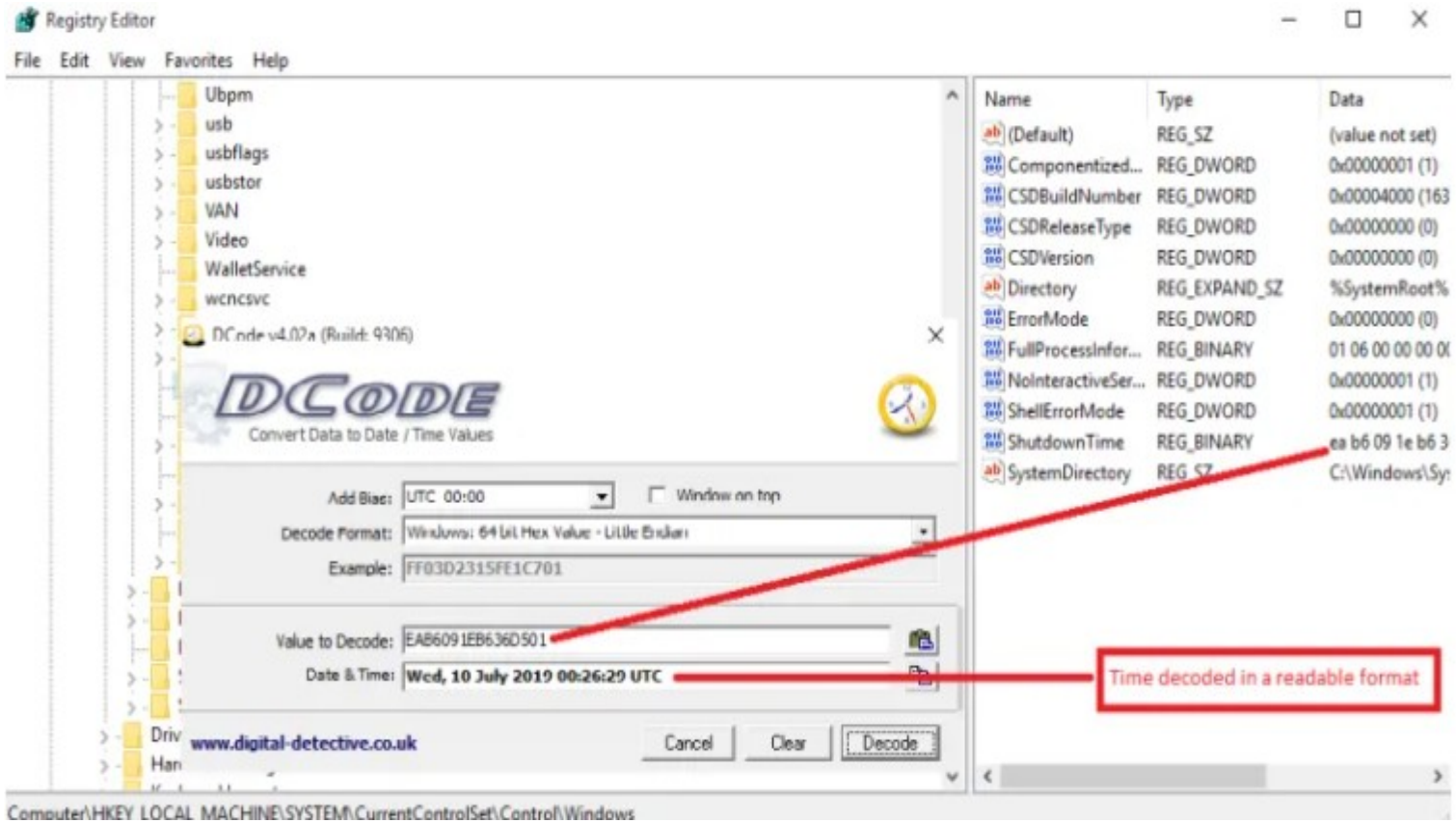
- **Network Analysis**
  - Registry keys for investigating network connection information:
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows NT\CurrentVersion\NetworkCards
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows NT\CurrentVersion\NetworkList\Nla\ Cache\Intranet
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows NT\CurrentVersion\NetworkList\Nla\ Wireless
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows NT\CurrentVersion\NetworkList\ Signatures\Unmanaged
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows NT\CurrentVersion\NetworkList\ Profiles

Windows Registry Examination

- **Windows Shutdown Time**
  - ✓ The Windows registry records when the system was **last closed down** in the following registry key:
    - **HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control\Windows**
    - Under the **ShutdownTime** value.
    - The shutdown value is stored using a **binary value**; to decode it to a readable form, use a tool called **DCode** from Digital Detective.

Windows Registry Examination

- **Windows Shutdown Time**



Windows Registry Examination

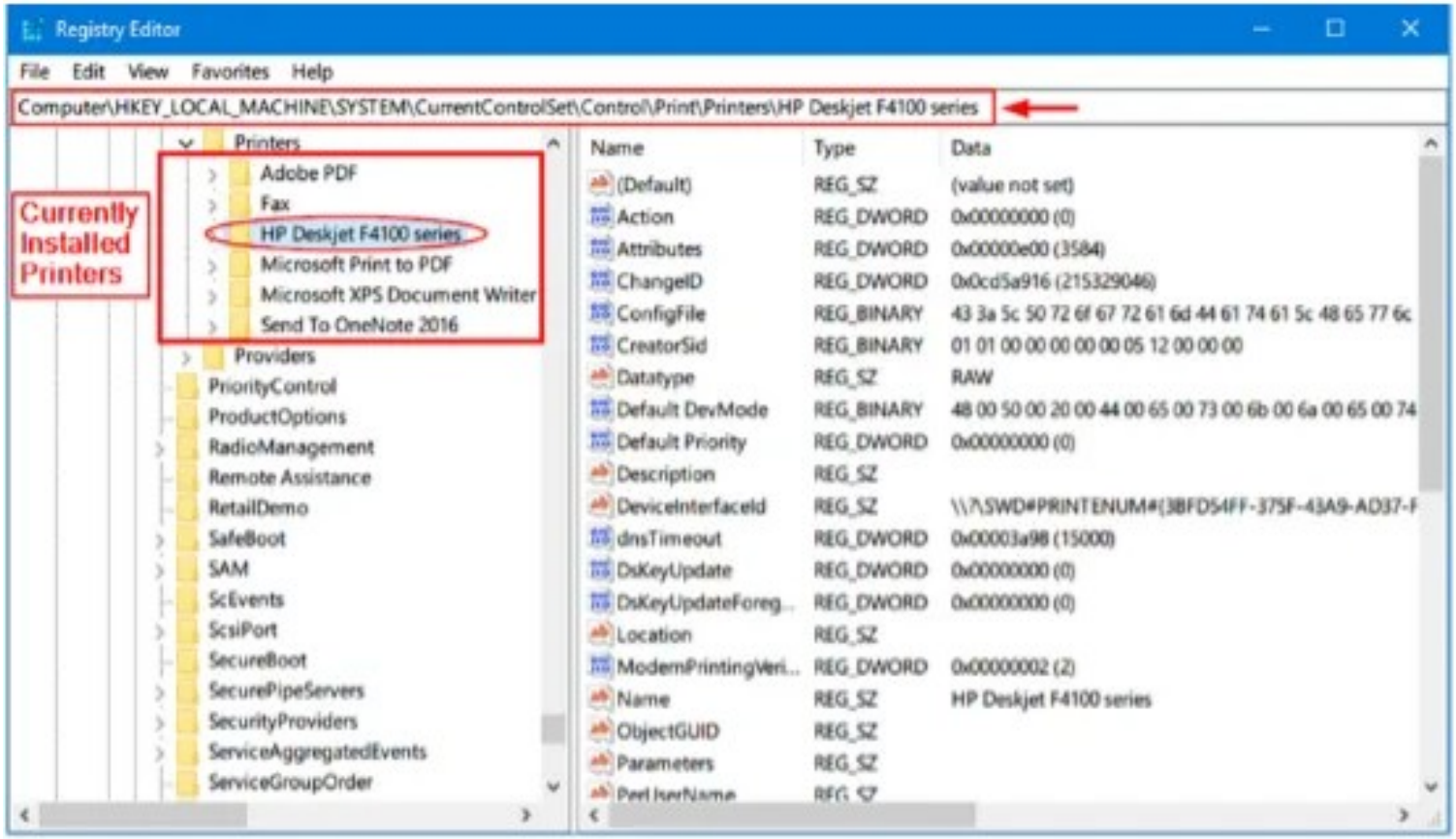
- **UserAssistsForensics**
  - ✓ Keeps a record of **all executable programs recently launched** in addition to the **frequency of usage** (number of executions) for each recorded program.
  - ✓ UserAssist information can be found in the following registry key:
    - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
  - ✓ Information stored in UserAssist keys is **encoded using ROT-13 encoding schema**.
    - To decode this information, use **UserAssist-View** tool

Windows Registry Examination

- **Printer Registry Information**
  - ✓ The Windows registry contains the entries for printing as follows:
    - HKEY_CURRENT_USER\Printers: holds **settings** of the current **default printer**.
    - HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control\Print : contains additional subkeys that hold information about installed printer.

Windows Registry Examination

- **Printer Registry Information**



Windows Registry Examination

- **Deleted Registry Key Recovery**
  - ✓ **Recovering** deleted Windows registry keys can be forensically valuable in many cases.
  - ✓ There is a simple, portable tool developed by Eric Zimmerman to handle this task and more.
    - ❑ **Registry Explorer/RECmd**