A Case Study

- Police were called to a disturbance at a motel
- Two men were found in a room viewing pornographic child images on a large screen
- One admitted owning the laptop but claimed the external hard drives were his mates and had never been connected to the laptop.
- Forensics examined the registry on the laptop and found the IDs for external drives with serial numbers
- On a fresh copy of Windows, they connected the drives and got identical USB details in the registry
- The suspect was convicted of possession of pornography

Week 6 - Windows Registry

Readings

Nelson - Ch 5

Objectives

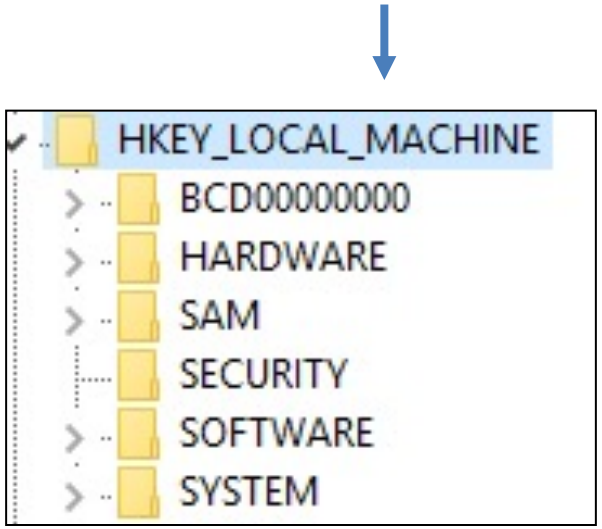
- To understand the Windows Registry
- To understand GUIDs
- To identify Registry keys of forensic interest

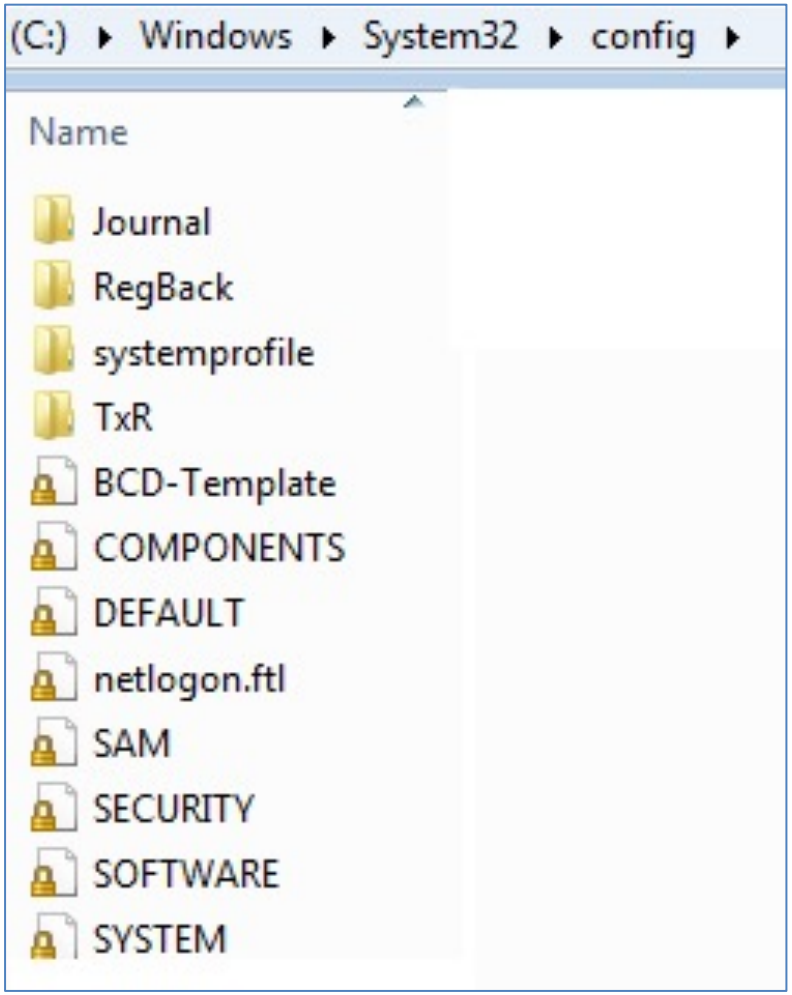
The Windows Registry

- A hierarchical database storing configuration settings
- Very fast access (like cookies)
- The brain of Windows
- Stored in C:\windows\system32\config
- Each branch or hive is called a Handle to a Key (HKey)
- Only two master keys are stored on disk
  - HKLM and HKU
- Note: Viewing a live registry can be dangerous
  - a trivial change to a registry key can cause instant failure
  - Best to view a VM that can be rebooted

Registry Files

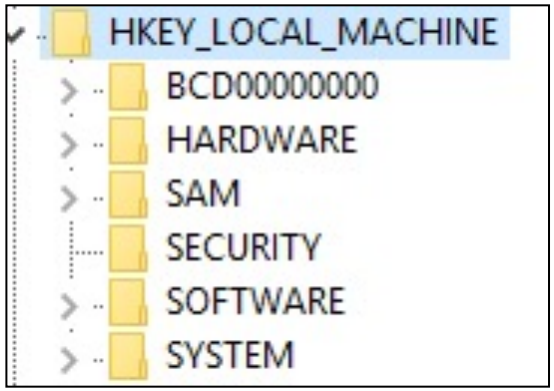
- Files On Disk ------->
- Matching Registry Keys





HKLM Windows Registry Hives

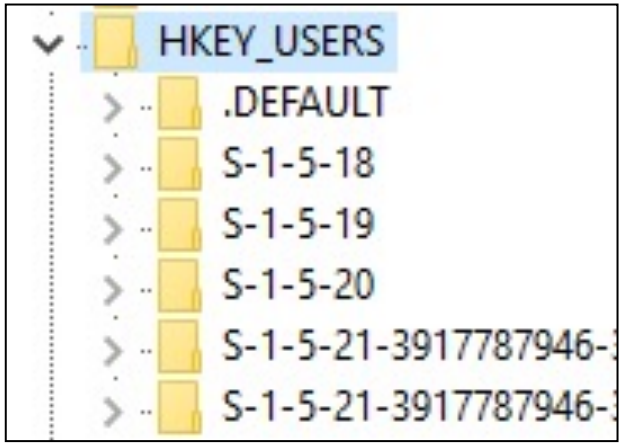
- Hkey_Classes_Root (HKCR) – Link to subkey in HKLM
  - contains file extension associations (*.exe, *.docx …)
  - Software classes
- HKey_Local_Machine (HKLM) - Master key on disk
  - hardware
  - access passwords (SAM)
  - installed software
  - device driver configs



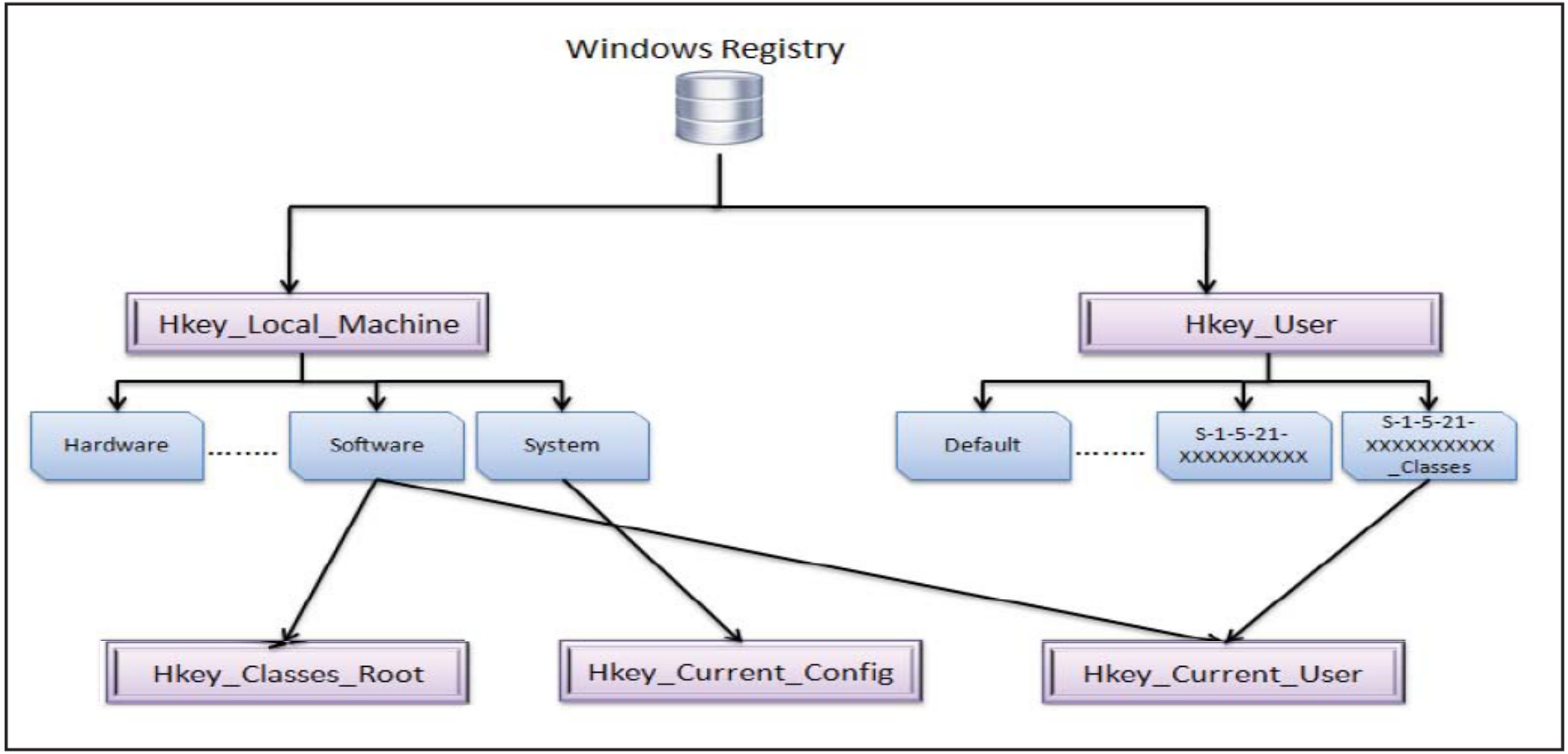
- HKey_Current_Config (HKCC) – link to subkey in HKLM
  - Hardware profiles

HKU Windows Registry Hives

- HKey_Current_User (HKCU) – Link to subkey in HKU
  - NTUSer.Dat in Documents and Settings
- HKey_Users (HKU) - Master key on disk
  - List of Users



Root Key Links



User Hives

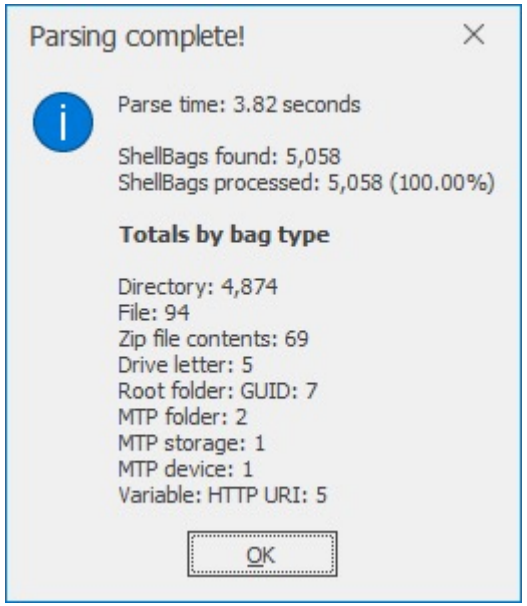
- NTUSR.DAT
- UsrClass.Dat
- Both used by ShellBags
  - You need a tool to see the ShellBags such as ShellBags Explorer

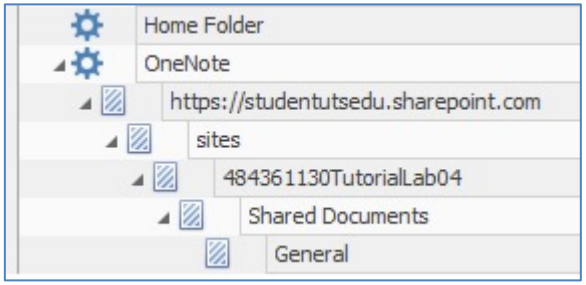
Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\hivelist

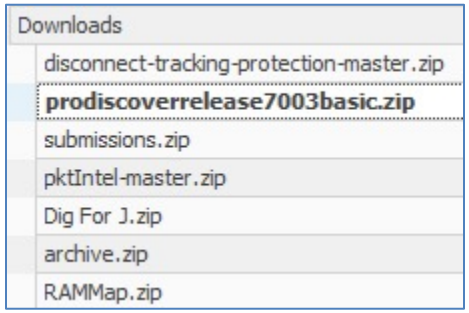
Name	Type	Data
(Default)	REG_SZ	(value not set)
\REGISTRY\MACHINE\BCD00000000	REG_SZ	\Device\HarddiskVolume1\EFI\Microsoft\Boot\BCD
\REGISTRY\MACHINE\HARDWARE	REG_SZ	
\REGISTRY\MACHINE\SAM	REG_SZ	\Device\HarddiskVolume3\Windows\System32\config\SAM
\REGISTRY\MACHINE\SECURITY	REG_SZ	\Device\HarddiskVolume3\Windows\System32\config\SECURITY
\REGISTRY\MACHINE\SOFTWARE	REG_SZ	\Device\HarddiskVolume3\Windows\System32\config\SOFTWARE
\REGISTRY\MACHINE\SYSTEM	REG_SZ	\Device\HarddiskVolume3\Windows\System32\config\SYSTEM
\REGISTRY\USER\.DEFAULT	REG_SZ	\Device\HarddiskVolume3\Windows\System32\config\DEFAULT
\REGISTRY\USER\S-1-5-19	REG_SZ	\Device\HarddiskVolume3\Windows\ServiceProfiles\LocalService\NTUSER.DAT
\REGISTRY\USER\S-1-5-20	REG_SZ	\Device\HarddiskVolume3\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
\REGISTRY\USER\S-1-5-21-215816962...	REG_SZ	\Device\HarddiskVolume3\Users\graha\NTUSER.DAT
\REGISTRY\USER\S-1-5-21-215816962...	REG_SZ	\Device\HarddiskVolume3\Users\graha\AppData\Local\Microsoft\Windows\UsrClass.dat

ShellBags Explorer

- Written by Eric Zimmerman
- Decodes the registry ShellBags
- Very handy forensic tool
  - You see exactly what the suspect did







https://ericzimmerman.github.io/#!index.md

Registry Keys

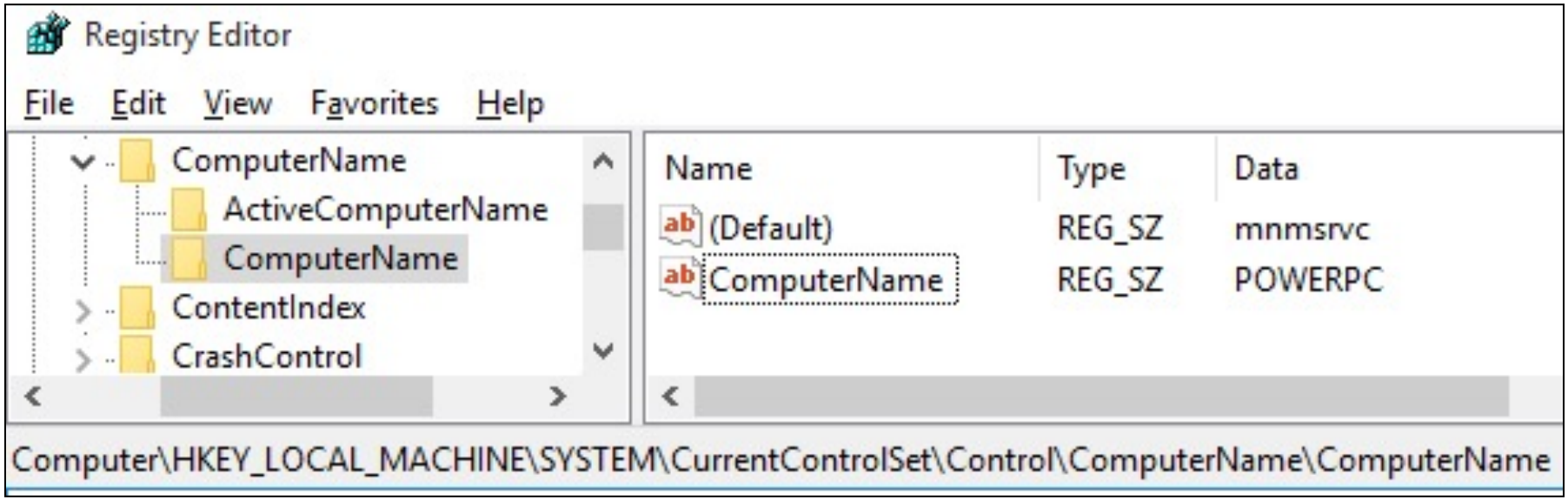
- A database of tag:value pairs
- The data in the value part can be of three types
  - REG_BINARY (data is application dependant)
  - REG_DWORD (numbers, 1 = Active, 0 = Not Active)
    (DWORD = double word = 32 bits)
  - REG_SZ (ascii string)

Sample Key

- We want to find the Computer Name
- We use the CLI for WMI (WMIC)

```
C:\Forensics>wmic computersystem get name
Name
POWERPC
```

- Where is this stored in the Registry?



Another key - Windows Users

- Windows NT Network
- Windows Domain
- Default Users

```
C:\Forensics>wmic useraccount get name, sid
Name            SID
Administrator   S-1-5-21-3917787946-3202774373-1533596134-500
DefaultAccount  S-1-5-21-3917787946-3202774373-1533596134-503
Guest           S-1-5-21-3917787946-3202774373-1533596134-501

Admin01         S-1-5-21-3917787946-3202774373-1533596134-1017
user            S-1-5-21-3917787946-3202774373-1533596134-1019
```

- Added Users

Registry Issues

- The registry is complex and undocumented
- Easy to misinterpret and draw incorrect conclusions
- Many tools automate the analysis
- Need to be sure the tool is correct and complete
- Can you explain to a court which key(s) the data came from and what actions caused the data to appear?
- Deep analysis relies on three things: (see readings)
  - Timelining
  - Baselining
  - Backup Analysis

Objectives

- To understand the Windows Registry
- To understand GUIDs
- To identify Registry keys of forensic interest

GUIDs and UUIDs

- A **universally unique identifier** (**UUID**) is a 128-bit number used to identify information in Linux file systems.
- The term **globally unique identifier** (**GUID**) is used in Windows file systems.
- Many versions, here is version 1
- {4d36e967-e325-11ce-bfc1-08002be10318}
- {time of day-month-year-variant-MAC address}

UUID Decoder
https://www.uuidtools.com/decode

UUID/GUID types

- v1 GUIDs
  - Have a ‘1’ at the start of the third group
  - {72631e54-78a4-11d0-bcf7-00aa00b7b32a}
  - use the Gregorian calendar time (0=15 Oct 1582)
  - The third group = 1xxx where xxx is the date code
  - use the users NIC MAC address as the last 6 bytes
- v4 GUIDs
  - Have a ‘4’ at the start of the third group
  - Have 8,9,A,or B at the start of the fourth group
  - {53d29ef7-377c-4d14-864b-eb3a85769359}
  - Use a Pseudo Random Number Generator for all other bits

UUID/GUID Version 1 Date codes

UUID Dates - Version 1		
Third Group	Date low	Date high
11b2	1/01/1970	15/10/1970
11b8	1/04/1975	14/05/1982
11c0	20/05/1982	11/04/1983
11c8	9/07/1989	31/05/1990
11d0	27/08/1996	19/07/1997
11d8	16/10/2003	6/09/2004
11e0	4/12/2010	20/10/2011
11e3	8/08/2013	30/06/2014
11e6	11/04/2016	3/03/2017

UUID/GUID Version 1 MAC OUI codes

```
MAC OUIs
--------
00:0C:29 VMware, Inc.(VM)
00:1d:7d GIGA-BYTE TECHNOLOGY CO.,LTD.(Motherboard)
00:aa:00 Intel (NIC or CPU)
08:00:2b DEC (Digital Equipment Corporation - Unix)
2C:44:FD Hewlett Packard (PC)
```

- https://www.wireshark.org/tools/oui-lookup.html

Windows GUIDs

- Used to identify components in Windows hardware
  - disk drives and partitions
- Used to identify software
  - Drivers
  - class objects

```
typedef struct _GUID {
  DWORD Data1;          # 4 bytes = 32 bits
  WORD  Data2;          # 2 bytes = 16 bits
  WORD  Data3;          # 2 bytes = 16 bits
  BYTE  Data4[8];       # 8 byte array = 64 bits
} GUID;
Total Length = 128 bits (like IPv6)
```

Sample v1 GUIDs

```
Class = GPS
ClassGuid = {6bdd1fc3-810f-11d0-bec7-08002be2092f}

Class = DiskDrive
ClassGuid = {4d36e967-e325-11ce-bfc1-08002be10318}

Class = Net (Network Adapter)
ClassGuid = {4d36e972-e325-11ce-bfc1-08002be10318}

Class = Printer
ClassGuid = {4d36e979-e325-11ce-bfc1-08002be10318}
```

Linux UUIDs

- Used to identify block devices (disks)
- Look in /dev/disk

```
root@kali:~#ls /dev/disk
by-id   by-label    by path     by-uuid

root@kali:~# ls -l /dev/disk/by-label/
total 0
lrwxrwxrwx 1 root root 10 Aug 19 04:03 FORENSICS -> ../../sdb1
lrwxrwxrwx 1 root root  9 Aug 19 03:55 Kali\x20Live -> ../../sr0

root@kali:~# ls -l /dev/disk/by-uuid/
total 0
lrwxrwxrwx 1 root root 10 Aug 19 04:03 24D7-B629 -> ../../sdb1
lrwxrwxrwx 1 root root 10 Aug 19 03:55 8a833949-3596-4c15-932b-0573f630307c -> ../../sda1
lrwxrwxrwx 1 root root 10 Aug 19 03:55 ebfc84f5-4e38-47ab-b451-2f683c549b6d -> ../../sda5
```

Linux UUIDs #2

- You can generate your own UUIDs

```
bash-4.1$ uuidgen -t
5c15d34e-879c-11e7-9cd3-2c44fd18e75f
bash-4.1$
```

Objectives

- To understand Windows Registry
- To understand GUIDs
- To identify Registry keys of forensic interest

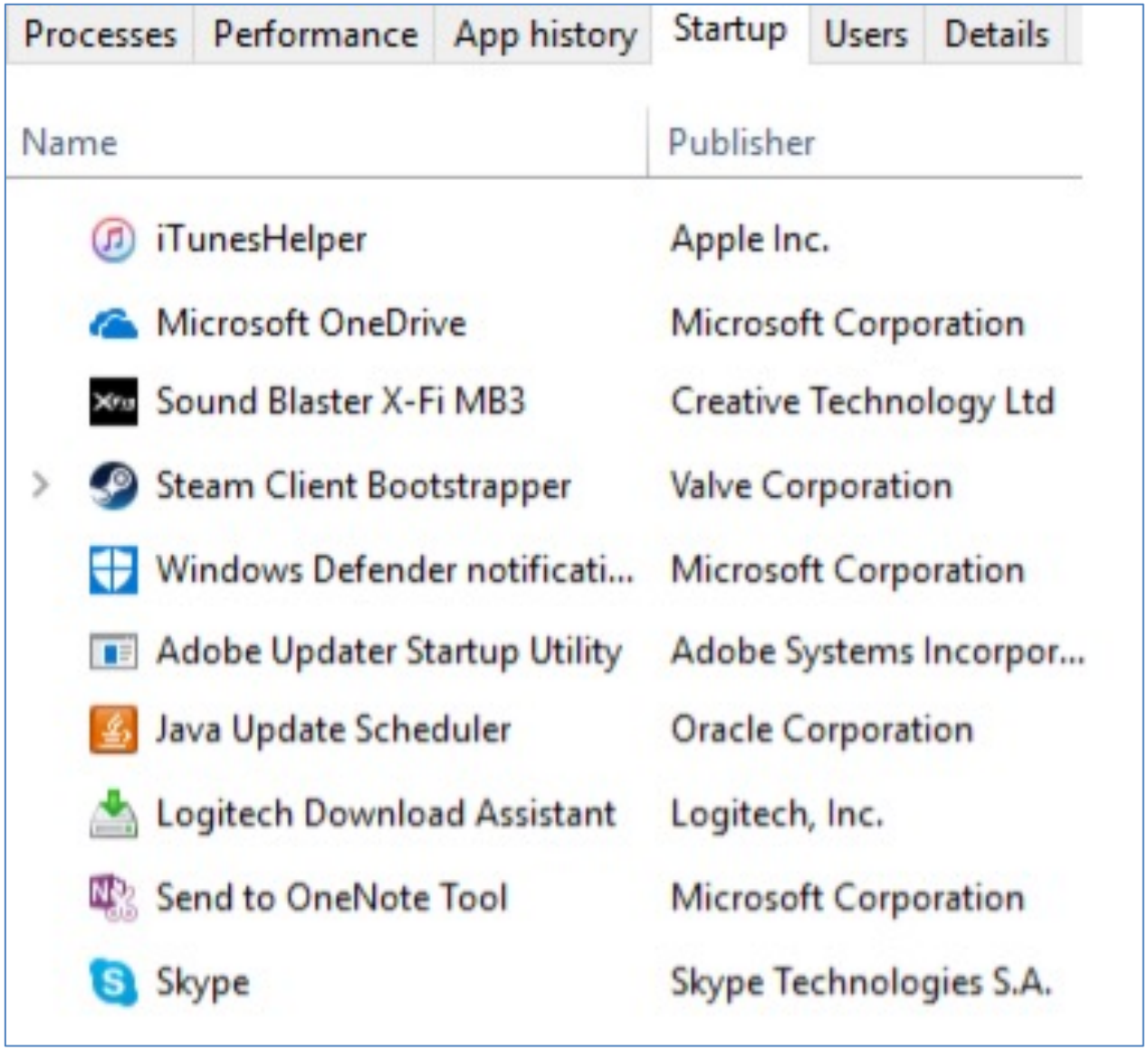
Useful registry keys

- There are many such keys
- Investigators use a tool to check most of them
- The following slides list a few of the more important ones

Windows GUIDs

- **Windows 7**
- {F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
- {CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
- **Windows 8**
- {FA99DFC7-6AC2-453A-A5E2-5E2AFF4507BD}
- {F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
- {F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}
- {CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
- {CAA59E3C-4792-41A5-9909-6A6A8D32490E}
- {B267E3AD-A825-4A09-82B9-EEC22AA3B847}
- {A3D53349-6E61-4557-8FC7-0028EDCEEBF6}
- {9E04CAB2-CC14-11DF-BB8C-A2F1DED72085}

Autostart in Task Manager



Autostart/Autorun - Registry

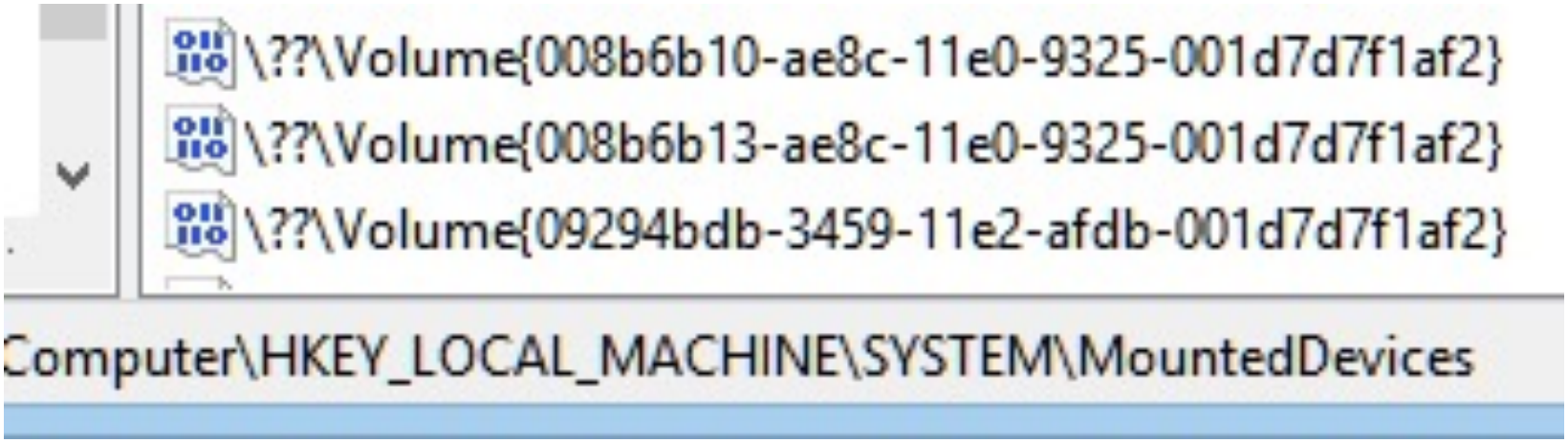
- use regedit to see these

```
HKEY_LOCAL_MACHINE\SOFTWARE
\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE
\Microsoft\Windows\CurrentVersion\RunOnce

HKEY_LOCAL_MACHINE\SOFTWARE
\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE
\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce
```

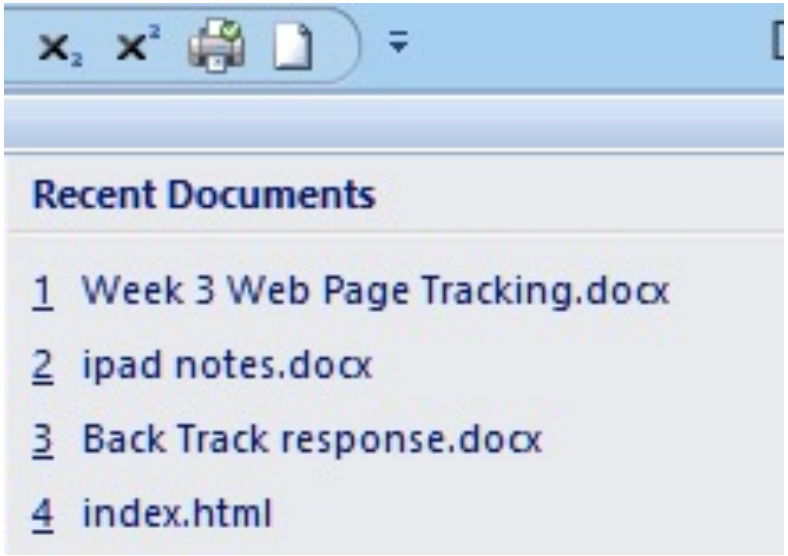
Disk GUIDs

- kept in the registry to map drive letters (C:)
- HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices\



MRUs

- Windows keeps several Most Recently Used lists (MRUs)
- Apps started
- Web Pages visited
- Office docs opened



- These indicate what the suspect did recently
- MRUs are found in the registry

See readings

Time Zone

- You need to know the time zone when the suspect's disk was seized.
- Then you can build a time line around the suspicious event
- HKLM\SYSTEM\CurrentControlSet\Control\TimeZone Information

TimeZoneKeyName	REG_SZ	AUS Eastern Standard Time

The USBStor Key

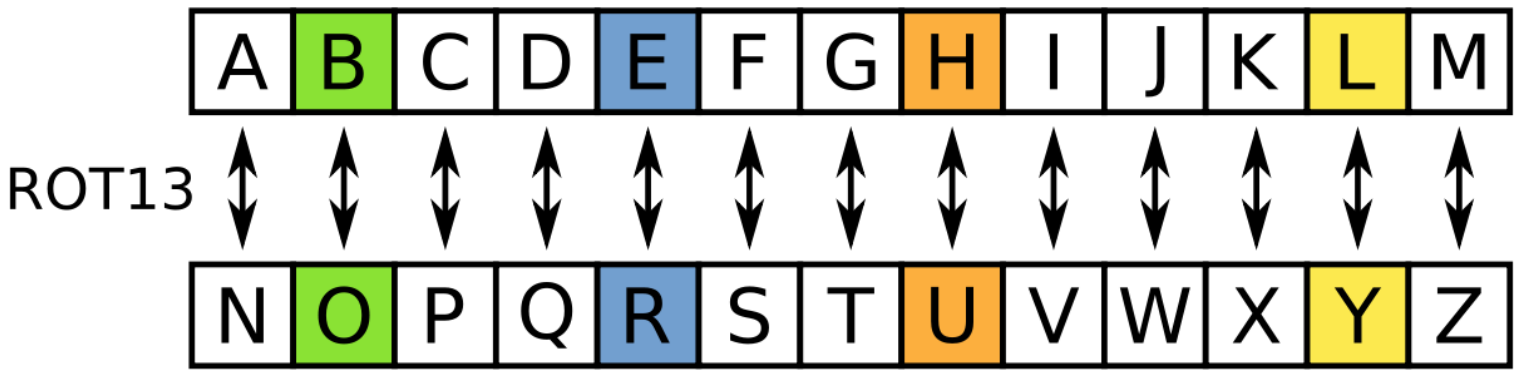
- Records every device connected by USB
- Backed up at each restore point

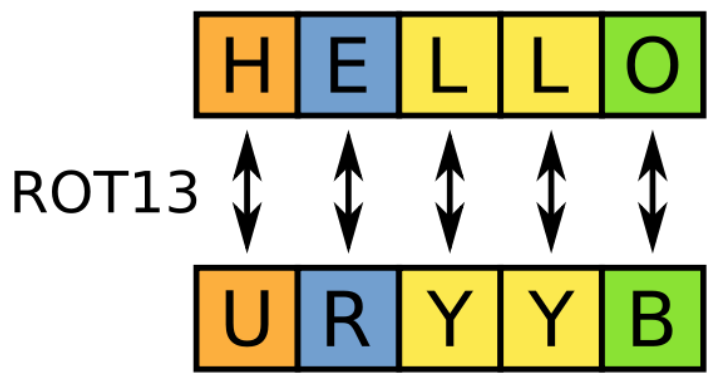
Userassist keys

- User assist tracks programs executed.
- The count and last use date are stored
- Does not count exes run from the cmdline
- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
- The key is ROT13 encoded.
-

```
pzq.rkr = cmd.exe, ertrqvg.rkr = regedit.exe
\Nppprffbevrf\Cnvag.yax = \Accessories\Paint.lnk
```

Rotate by 13 Chars – ROT13





Sample Userassist keys

PnabavpnyTebhcYvzvgrq.HohaghbaJvaqbjf_79euxc1saqtfp!hohagh

CanonicalGroupLimited.UbuntuonWindows_79rhkp1fndgsc!ubuntu

{6D809377-6AF0-444B-8957-A3773F02200E}\Wireshark\Wireshark.exe

{6Q809377-6NS0-444O-8957-N3773S02200R}\Jverfunex\Jverfunex.rkr

C:\Users\graha\Desktop\putty.exe
{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Nmap\zenmap.exe
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\msiexec.exe

P:\Hfref\tenun\Qrfxgbc\chggl.rkr
{7P5N40RS-N0SO-4OSP-874N-P0S2R0O9SN8R}\Aznc\mraznc.rkr
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\zfvrkrp.rkr

FIN

- Haere rā