Northeastern University

Module 4
Windows Forensic Analysis
Part 2

Elton Booker, CISSP
Lead Forensic Analyst

Upcoming Deliverables

End of Module

- IA Lab 1
- Assignment 3

Upcoming Assignments

- Assignment 4
- AccessData FTK Labs

Instructor Perspective

Prefetch

Shellbags

LNK Files

Jump Lists

USB Device Analysis

Windows Prefetch

Shell Items

Type of Target Drive

- Fixed, removable, network

Path of Target File

- Drive letter, volume label and serial number

Target Metadata

- MAC timestamps
- File Size
- MFT record and sequence number

C:\Windows\Prefetch Contents

NTOSBOOT-BooDFAAD.pf

- System boot prefetch
- Only file existing on servers by default

Layout.ini

- Disk defragmenter

Appname-########.pf

- Up to 128 application-specific prefetch files*

Value of Prefetch

A record of program execution on systems

Even if the executable was deleted

Shows components and dependencies

Analysis identifies

- Application first run
- Application most recent run
- Number of times executed

PECmd Analysis

ExecutableName	Size	RunCount	LastRun	Volume0Serial
LOGONUI.EXE	115042	551	1/23/18 13:40	84CE48C6
LOCKAPP.EXE	95602	544	1/23/18 13:40	84CE48C6
WINWORD.EXE	108590	215	1/22/18 5:03	84CE48C6
POWERPNT.EXE	226804	191	1/23/18 3:08	84CE48C6
SKYPE.EXE	230116	145	1/22/18 2:33	84CE48C6
SKYPEBROWSERHOST.EXE	221646	119	1/18/18 0:30	84CE48C6
MICROSOFTEDGECP.EXE	150550	112	10/10/17 2:19	84CE48C6
CONSENT.EXE	188108	70	1/23/18 4:06	84CE48C6
EXCEL.EXE	123454	68	1/13/18 16:51	84CE48C6
FIREFOX.EXE	157432	68	9/26/17 3:31	84CE48C6
MICROSOFTEDGECP.EXE	193052	62	1/17/18 3:27	84CE48C6
G2MUPDATE.EXE	99544	60	10/12/17 23:32	84CE48C6
SNIPPINGTOOL.EXE	47824	48	1/23/18 13:38	84CE48C6
FIREFOX.EXE	101654	47	1/23/18 4:15	84CE48C6
MSIEXEC.EXE	116960	37	1/23/18 4:03	84CE48C6
DRIVERINSTALLER.EXE	160444	36	1/23/18 2:23	84CE48C6
G2MUPDATE.EXE	89084	35	10/4/17 22:31	84CE48C6
ACRORD32.EXE	86680	34	1/23/18 4:15	84CE48C6
MICROSOFTEDGE.EXE	167154	29	10/10/17 2:19	84CE48C6

PECmd –d "Directory for Prefetch Files" --csv "Directory Output\pf.csv"

Shellbag Analysis

Win7-Win10 Shellbags

Purpose

- Windows Explorer folder preferences tracked by user

Location

- **Explorer Access:**
  - USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags
  - USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU
- **Desktop Access:**
  - NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU
  - NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags

Investigations

- Identifies folders accessed on local machine, network, or removable media
- Evidence of folders after deletion or being overwritten
- Identify when certain folders were accessed

Link File Analysis

Shortcut (.lnk) Files

.LNK created in Windows Recent folder

- C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Recent

All executables create two LNK files

- 1 – Target file
- 2 – Parent folder or file

.LNK files point to:

- Target file MAC times
- Volume info (Name, type, volume SN
- Original path and location
- Creation date first opened or created (Windows 10)

.lnk Time First/Last Open

| | First Opened | Last Opened |

Name	Date created	Date modified
2018_lnk2	1/30/18 2:56 PM	1/30/18 2:56 PM
RegRipper2.8	1/30/18 2:28 PM	1/30/18 2:28 PM
Cartoon Timestamp	1/30/18 12:40 PM	1/30/18 12:40 PM
Windows-Time-FILENAME2	1/30/18 12:39 PM	1/30/18 12:51 PM
FTK StandardInfo Timestamps	1/30/18 12:36 PM	1/30/18 12:36 PM
MFT Entry Req	1/30/18 12:34 PM	1/30/18 12:34 PM
MFTentry	1/30/18 12:31 PM	1/30/18 12:34 PM
NTFS MFT Attributes	1/30/18 12:30 PM	1/30/18 12:30 PM
RegEdit_OS Install	1/30/18 12:20 PM	1/30/18 12:20 PM
FTK_Quick_InstallGuide	1/30/18 12:07 PM	1/30/18 12:07 PM
FTK_Install_Guide	1/30/18 12:06 PM	1/30/18 12:06 PM
Participant-Handbook-(MSW-SM-B2C-D...	1/30/18 12:05 PM	1/30/18 12:05 PM
Participant-Handbook-Executive-(MSW-...	1/30/18 12:05 PM	1/30/18 12:05 PM
2018_JL	1/30/18 10:38 AM	1/30/18 12:04 PM
jmp_readme	1/30/18 10:35 AM	1/30/18 10:34 AM
jp_readme	1/30/18 10:25 AM	1/30/18 10:25 AM
2018_pf	1/30/18 10:24 AM	1/30/18 12:06 PM
readme	1/30/18 9:37 AM	1/30/18 10:34 AM
IA5210-TermPaperOutline	1/29/18 8:05 PM	1/29/18 8:05 PM

C:\Users\Forensic-Geek\AppData\Roaming\Microsoft\Windows\Recent

LECmd Link File Analysis

TargetCreated	TargetModified	TargetAccessed	FileSize	LocalPath	MachineID
9/16/18 2:46	9/16/18 2:46	9/17/18 4:18	38973	C:\Users\Forensic-Geek\Desktop\Accounting Module 1 Practice Quiz.docx	forensic-pc
9/23/18 22:02	9/23/18 22:02	9/26/18 10:19	46267	C:\Users\Forensic-Geek\Desktop\Accounting Module 3 Practice Quiz_Bad.docx	forensic-pc
9/17/18 4:12	9/17/18 4:12	9/23/18 19:24	14621	C:\Users\Forensic-Geek\Desktop\Accounting Quiz 1 Unanswered #8.docx	forensic-pc
5/20/17 15:54	7/17/17 21:20	7/17/17 21:20	4096	C:\Users\Forensic-Geek\Desktop\Alienware Desktop\Downloads\MGT632_SIM	forensic-pc
9/11/18 22:54	12/7/14 19:32	9/11/18 22:54	128974848	C:\Users\Forensic-Geek\Desktop\C3Proj2-2.001	forensic-pc
11/7/17 23:33	11/16/17 0:37	11/16/17 0:37	28672	C:\Users\Forensic-Geek\Desktop\Desktop_7Nov17	forensic-pc
11/8/17 0:17	11/15/17 0:21	11/15/17 0:21	160537	C:\Users\Forensic-Geek\Desktop\Desktop_7Nov17\IA5210 FA17 Week 10 Triage.pptx	forensic-pc
9/5/18 22:56	9/5/18 22:56	9/12/18 5:53	51262	C:\Users\Forensic-Geek\Desktop\Firefox Internet.jpg	forensic-pc
			0	C:\Users\Forensic-Geek\Desktop\FTK\KFF_Install.pdf	
9/17/18 4:38	9/25/18 10:27	9/26/18 10:22	4096	C:\Users\Forensic-Geek\Desktop\GCFI 6E Solutions	forensic-pc
9/17/18 4:38	9/17/18 4:39	9/17/18 4:39	4096	C:\Users\Forensic-Geek\Desktop\GCFI 6E Solutions	forensic-pc
11/2/17 19:22	9/17/18 4:38	9/26/18 10:22	29379	C:\Users\Forensic-Geek\Desktop\GCFI 6E Solutions\Solutions_05.docx	forensic-pc
			0	C:\Users\Forensic-Geek\Desktop\IA5210 - Module 3 Investigating Windows Systems 1.pptx	
			0	C:\Users\Forensic-Geek\Desktop\IA5210 FA18 Redesign_Booker.xlsx	
12/29/17 17:47	12/29/17 21:01	12/29/17 21:01	238592	C:\Users\Forensic-Geek\Desktop\IA5210 On Campus Template_NEU.ppt	forensic-pc
2/10/18 2:36	2/11/18 17:07	2/11/18 17:07	4096	C:\Users\Forensic-Geek\Desktop\IA5210 SP18	forensic-pc
			0	C:\Users\Forensic-Geek\Desktop\IA5210 Test.xlsx	
9/29/17 8:45	3/14/18 3:15	3/14/18 3:15	20185088	C:\Users\Forensic-Geek\Desktop\IA5210 Test\SYSTEM	forensic-pc
1/24/18 22:17	1/24/18 22:18	1/24/18 22:18	4096	C:\Users\Forensic-Geek\Desktop\IA5210 TZ Works Outputs	forensic-pc
1/5/18 23:11	1/7/18 6:54	1/7/18 6:54	24576	C:\Users\Forensic-Geek\Desktop\IR 3E SP2018 PPTs\PPT Images	forensic-pc
1/5/18 23:11	1/7/18 4:51	1/7/18 4:51	12288	C:\Users\Forensic-Geek\Desktop\IR 3E SP2018 PPTs\PPT Images	forensic-pc
3/7/18 2:34	3/7/18 2:41	3/7/18 2:41	4096	C:\Users\Forensic-Geek\Desktop\Markstrat Practice	forensic-pc
3/7/18 2:34	3/7/18 2:41	3/7/18 2:41	0	C:\Users\Forensic-Geek\Desktop\Markstrat Practice	forensic-pc
9/12/18 2:31	9/12/18 2:35	9/12/18 2:35	0	C:\Users\Forensic-Geek\Desktop\MGMT633 Accounting	forensic-pc
9/12/18 2:32	9/12/18 2:33	9/12/18 2:44	4096	C:\Users\Forensic-Geek\Desktop\MGMT633 Accounting\Introduction	forensic-pc
9/12/18 2:32	9/12/18 2:32	9/12/18 2:44	147897	C:\Users\Forensic-Geek\Desktop\MGMT633 Accounting\Introduction\Review - financial accounting.pdf	forensic-pc
9/12/18 2:31	9/12/18 2:31	9/12/18 2:31	0	C:\Users\Forensic-Geek\Desktop\MGMT633 Acounting	forensic-pc
			0	C:\Users\Forensic-Geek\Desktop\Networks_2	

LECmd –d "Directory for Link Files" --csv "Directory Output\lnk.csv"

Northeastern University

Jump List Analysis

Jump Lists

Jump List Types

- Automatic Destinations
- Custom Destinations

AppIDs

- Universal across Windows versions

Location

- C:\Users\[Profile]\AppData\Roaming\Microsoft\Windows\Recent\

TZWorks Jumplist Parsing Utility

Last Opened   **First Opened**

appid	MRU/MFU	MRU date	MRU-UTC	file mdate	time-UTC	file cdate	time-UTC2	local path
5f7b5f1e01b83767	1	1/30/18	15:34:59.867	1/30/18	15:34:59	11/11/15	16:39:51	C:\Users\Forensic-Geek\Desktop\TZ Works 2017\readme\jmp_readme.htm
5f7b5f1e01b83767	2	1/30/18	15:31:37.535	1/30/18	15:34:59	11/11/15	16:39:51	C:\Users\Forensic-Geek\Desktop\IA5210 TZ Works Outputs\2018_JumpList.csv
5f7b5f1e01b83767	3	1/30/18	15:25:32.373	1/30/18	15:34:59	11/11/15	16:39:51	C:\Users\Forensic-Geek\Desktop\TZ Works 2017\readme\jp_readme.htm
5f7b5f1e01b83767	4	1/30/18	15:24:14.182	1/30/18	15:34:59	11/11/15	16:39:51	C:\Users\Forensic-Geek\Desktop\IA5210 TZ Works Outputs\2018_pf.csv
5f7b5f1e01b83767	5	1/30/18	15:20:53.116	1/30/18	15:34:59	11/11/15	16:39:51	C:\Users\Forensic-Geek\Desktop\IA5210 TZ Works Outputs\2018_lnk.csv
5f7b5f1e01b83767	6	1/30/18	14:40:19.633	1/30/18	15:34:59	11/11/15	16:39:51	C:\Users\Forensic-Geek\Desktop\IA5210 TZ Works Outputs\2018_USB.csv
5f7b5f1e01b83767	7	1/30/18	14:40:15.085	1/30/18	15:34:59	11/11/15	16:39:51	C:\Users\Forensic-Geek\Desktop\IA5210 TZ Works Outputs\2018_USB.xlsx
5f7b5f1e01b83767	8	1/30/18	14:37:31.334	1/30/18	15:34:59	11/11/15	16:39:51	C:\Users\Forensic-Geek\Desktop\TZ Works 2017\readme\lp_readme.htm
5f7b5f1e01b83767	9	1/30/18	13:54:16.767	1/30/18	15:34:59	11/11/15	16:39:51	C:\Users\Forensic-Geek\Desktop\IA5210 TZ Works Outputs\2018_prefetch.csv
5f7b5f1e01b83767	10	1/30/18	01:25:51.876	1/30/18	15:34:59	11/11/15	16:39:51	D:\NEU IA5210\SFIR 3E\Forensics_v03_Lab_Worksheets\Self-Concept - Low.pdf
5f7b5f1e01b83767	11	1/30/18	01:25:17.219	1/30/18	15:34:59	11/11/15	16:39:51	C:\Users\Forensic-Geek\Downloads\activity_results_20180129074802.csv
5f7b5f1e01b83767	12	1/30/18	01:05:48.445	1/30/18	15:34:59	11/11/15	16:39:51	C:\Users\Forensic-Geek\Downloads\MathewSylvia_IA5210-TermPaperOutline.doc

C:\>dir "C:\Users\Forensic-Geek\AppData\Roaming\Microsoft\Windows\Recent*.ions-ms"/b /s | jmp64 –pipe –csv –no_whitespace –timeformat hh:mm:ss > c:\2018_jmp.csv

USB Device Analysis

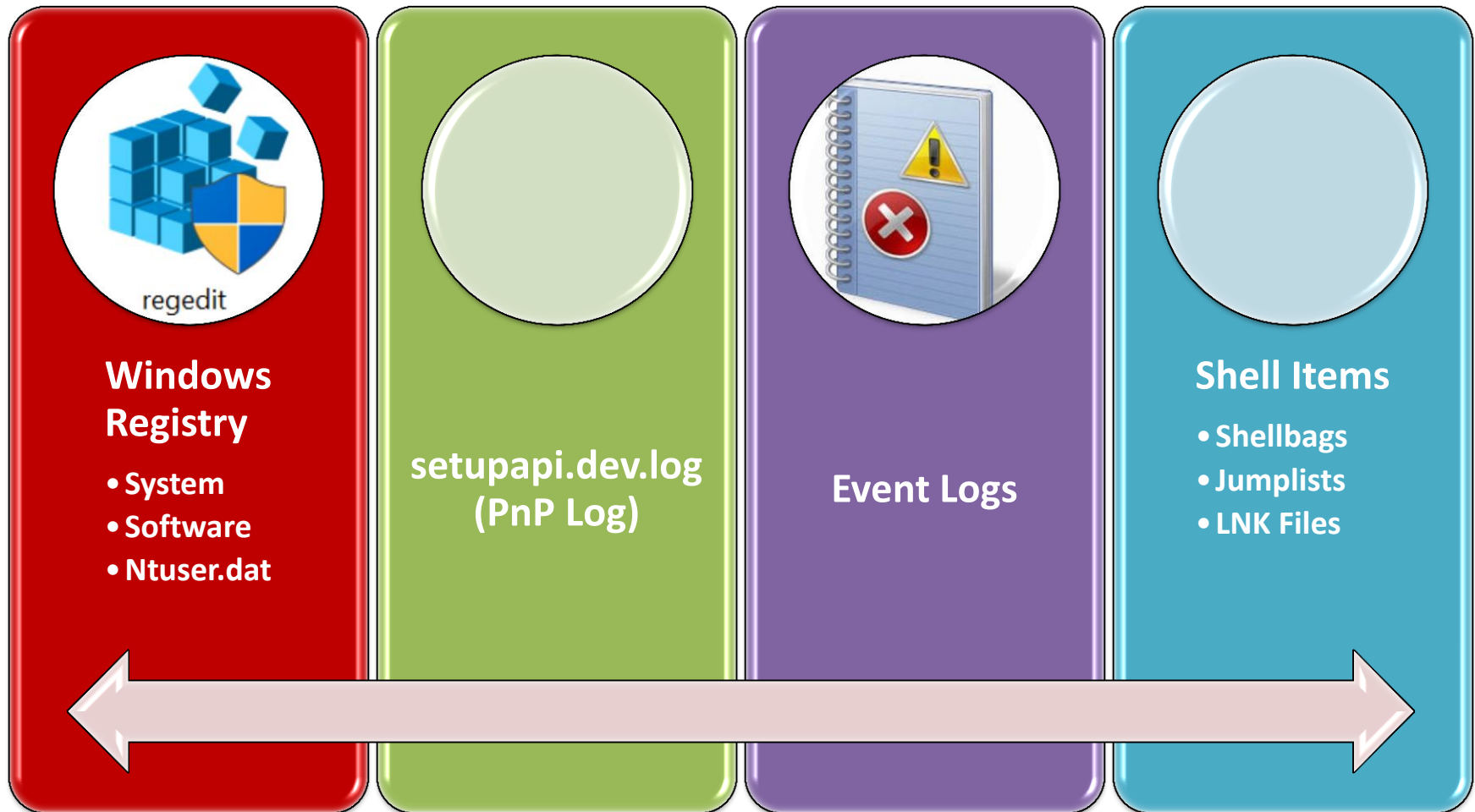# Purpose of USB Device Forensics

USB Information

- Vendor/Make/Model
- Unique Serial Number

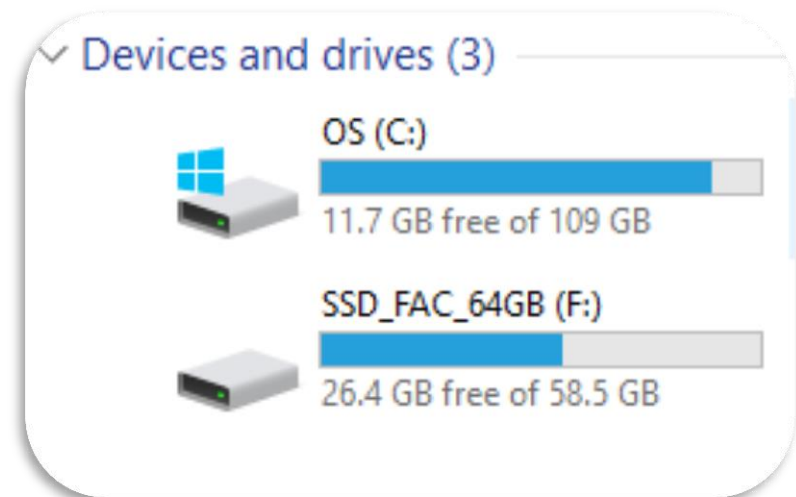## User Information and USB Activity

- Identify drive letter and volume name
- Attribute to a specific user
- Identify first time connected
- Determine last time connected
- Determine time device removed

Identifying USB Information

Windows Registry

- System
- Software
- Ntuser.dat

setupapi.dev.log (PnP Log)

Event Logs

Shell Items

- Shellbags
- Jumplists
- LNK Files

Mass Storage Class (MSC)

- USB Mass Storage
  - Supported since 2000
  - Physical access
  - Supported devices:
    - Thumb and ExHDs
    - MP3 Players
    - Smartphones

- Windows – mount as:
  - HDDs
  - Devices with removable storage

Devices and drives (3)

OS (C:)
11.7 GB free of 109 GB

SSD_FAC_64GB (F:)
26.4 GB free of 58.5 GB

Media Transfer Protocol (MTP)

Replaced PTP

Files can be moved to/from the device

MTP mounted as portable devices

Supportd Devices

- MP3 players
- Android 4.0+
- Windows Phone 8+

∨ Devices and drives (3)

iPhone 542981

USB MSC Device Forensics

1. Vendor, Product, Version

2. Serial Number

3. Vendor-ID (VID) and Product-ID (PID)

4. Volume GUIDs

5. Drive Letter and Volume Name

6. Volume Serial Number

7. Identify Specific User

8. First Time Connected

9. Last Time Connected

10. Time Device Removed

USBSTOR

Intent

- Identify MSC USB devices connected to a system

Location

- SYSTEM\CurrentControlSet\Enum\USBSTOR

Investigations

- Identify the vendor, product, and version of each USB device
- Identify unique devices connected to system by serial number
- Determine the time of connection

Win7-10 USB Devices


```
SYSTEM - Notepad
File  Edit  Format  View  Help
------------------------------------------
usb v.20141111
(System) Get USB key info

USBStor
ControlSet001\Enum\USB

Hasp [Fri Feb  9 15:44:03 2018]
  S/N: 6&289d236&0&00 [Fri Feb  9 15:44:03 2018]
  Device Parameters LastWrite: [Fri Feb  9 15:44:03 2018]
  Properties LastWrite      : [Fri Feb  9 15:44:03 2018]
  S/N: 6&3431b5af&0&00 [Wed Feb 14 00:58:17 2018]
  Device Parameters LastWrite: [Tue Feb  6 21:30:42 2018]
  Properties LastWrite      : [Tue Feb  6 21:30:42 2018]
  S/N: 6&cc22657&0&00 [Fri Feb  9 15:44:03 2018]
  Device Parameters LastWrite: [Wed Feb  7 00:41:05 2018]
  Properties LastWrite      : [Wed Feb  7 00:41:06 2018]

ROOT_HUB20 [Wed Jan 31 05:29:11 2018]
  S/N: 4&2d45bba3&0 [Wed Mar 14 03:15:27 2018]
  Device Parameters LastWrite: [Thu Feb  8 00:05:03 2018]
  Properties LastWrite      : [Wed Jan 31 05:38:33 2018]
    ParentIdPrefix: 5&5bbd58b&0
  S/N: 4&325238e9&0 [Wed Mar 14 03:15:27 2018]
  Device Parameters LastWrite: [Thu Feb  8 00:05:03 2018]
  Properties LastWrite      : [Wed Jan 31 05:38:33 2018]
    ParentIdPrefix: 5&2b786412&0

ROOT_HUB30 [Wed Jan 31 05:29:11 2018]
  S/N: 4&13f24155&0&0 [Wed Mar 14 03:15:27 2018]
  Device Parameters LastWrite: [Fri Mar 16 12:32:09 2018]
  Properties LastWrite      : [Wed Jan 31 05:38:33 2018]
    ParentIdPrefix: 5&37adfd2&0
```

```
SYSTEM - Notepad                                    —   □   ×
File  Edit  Format  View  Help
VID_05AC&PID_12A8 [Wed Feb 14 01:02:44 2018]
  S/N: 1b69edfa4397102b94c7a1b643dacae2a03cafd3 [Wed Feb 14 01:02:44
2018]
  Device Parameters LastWrite: [Wed Feb 14 01:02:44 2018]
  Properties LastWrite      : [Wed Feb 14 01:02:44 2018]
    FriendlyName      : @oem89.inf,%iPhone.DeviceDesc%;Apple Mobile
```

Device serial numbers are unique unless the second character is an "&."

USB Enumeration

SYSTEM\CurrentControlSetXX\Enum\USB

Volume Name

Intent

- Identify the volume name of each USB device

Location

- SOFTWARE\Microsoft\Windows Portable Devices\Devices

Investigations

- Identify the USB device volume name

Identify Volume Name

User That Connected Device

IA5210 Information System Forensics

Open Discussion