

# WINDOWS FORENSICS

**01**

INTRODUCTION

**02**

WINDOWS REGISTRY

**03**

DATA ACQUISITION

**04**

REGISTRY EXPLORER

**05**

EXPLORING WINDOWS REGISTRY

**06**

CONCLUSION

# INTRODUCTION



## Computer forensics

= **gathering evidence** of activities performed on computers

The BTK (Dennis Rader) serial killer case --> floppy disk --> deleted word document --> **metadata**

Microsoft Windows is by large the most used **DOS** right now (~80%)

**Artifact** = small footprints of activity left on the computer system

The various artifacts a Windows system creates for a given activity

# WINDOWS REGISTRY

Windows Registry = collection of **databases** (system's **configuration** data)

**regedit.exe**--> Windows Registry <--> **Keys & Values**

Registry **Hive** = group of Keys, subkeys, and values stored in a single file on the disk.

**Root keys:**

**HKEY\_CURRENT\_USER** : particular to the computer (for any user)

**HKEY\_USERS**

**HKEY\_LOCAL\_MACHINE** : particular to the computer (for any user)

**HKEY\_CLASSES\_ROOT** : subkey of HKEY\_LOCAL\_MACHINE\Software

**HKEY\_CURRENT\_CONFIG** : information about the hardware profile at system startup

# WINDOWS REGISTRY

Registry Editor

File Edit View Favorites Help

Computer\HKEY\_LOCAL\_MACHINE\SECURITY

<div>Computer</div> <div><div>HKEY_CLASSES_ROOT</div><div>HKEY_CURRENT_USER</div><div><div>HKEY_LOCAL_MACHINE</div><div>BCD00000000</div><div>HARDWARE</div><div>SAM</div><div>SECURITY</div><div>SOFTWARE</div><div>SYSTEM</div></div><div>HKEY_USERS</div><div>HKEY_CURRENT_CONFIG</div></div>	<div>Name</div> <div><div>ab</div>(Default)</div>	<div>Type</div> <div>REG_SZ</div>	<div>Data</div> <div>(value not set)</div>
--	---	-----------------------------------	--

# WINDOWS REGISTRY

**running OS** --> regedit.exe

**disk image** (a static copy of system files) --> C:\Windows\System32\Config

**DEFAULT** --> HKEY\_USERS\DEFAULT

**SAM** --> HKEY\_LOCAL\_MACHINE\SAM

**SECURITY** --> HKEY\_LOCAL\_MACHINE\Security

**SOFTWARE** --> HKEY\_LOCAL\_MACHINE\Software

**SYSTEM** --> HKEY\_LOCAL\_MACHINE\System

**NTUSER.DAT** --> HKEY\_CURRENT\_USER

**USRCLASS.DAT** --> HKEY\_CURRENT\_USER\Software\CLASSES

**Transaction logs** (.LOG file) & **Registry backups**  
(C:\Windows\System32\Config\RegBack )

# DATA ACQUISITION

## Data GATHERING



KROLL

< Cyber Risk

**Kroll Artifact Parser And  
Extractor (KAPE)**

exterro®



**FTK® Imager**



# REGISTRY EXPLORER

Data VISUALIZATION & ANALYSIS

Registry Editor like

Zimmerman's Registry Explorer

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (29/0) View Help

Registry hives (1) Available bookmarks (30/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
Root	=	=	=
Console	48	3	2021-10-27 19:34:19
Control Panel	1	14	2021-10-28 08:56:41
Environment	4	0	2021-10-27 19:33:14
EUDC	0	4	2021-10-27 19:33:02
Keyboard Layout	0	3	2021-10-27 19:33:07
Microsoft	0	1	2021-10-27 19:33:02
Network	0	0	2021-10-27 19:33:02
Printers	0	6	2021-10-31 04:40:08
Software	0	23	2021-10-31 05:14:46
7-Zip	2	0	2021-10-27 19:33:15
AccessData	0	2	2021-11-04 02:06:07
AppDataLow	0	1	2021-10-27 19:33:15
Bitvise	0	6	2021-10-27 19:33:15
ChangeTracker	0	0	2021-10-28 08:56:46
Clients	0	2	2021-10-31 05:13:07
Discord	0	1	2021-10-27 19:33:15
fcd0d7f-424b-5f10-a1c7-a8f643f21adf	3	0	2021-10-27 19:33:15
Google	0	3	2021-10-31 05:28:27
Hewlett-Packard	0	4	2021-11-01 14:31:56
35e03c50-e9f4-49e0-cb96-5d48742d...	2	1	2021-10-31 04:45:39
HP Print Settings	15	1	2021-11-02 19:23:25
Default Location	1	1	2021-10-31 04:45:36
HP SSNP	3	0	2021-11-01 14:32:30
TM	0	2	2021-10-31 04:46:40
Intel	0	1	2021-10-27 19:33:15
Lenovo	0	2	2021-10-27 19:33:15

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
MystDeviceVerify	RegDword	512		<input type="checkbox"/>	<input type="checkbox"/>
ServicesTab	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>
OnlineDiagnostics	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>
OnlineSupport	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>
ProductManuals	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>
DriverUpdates	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>
OrderSupplies	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>
CurrentProfile	RegSz	Default Location	ED-E6	<input type="checkbox"/>	<input type="checkbox"/>
ReadInOldProfiles	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>
ReadInM1Profiles	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>
ChangedPorts	RegDword	0		<input type="checkbox"/>	<input type="checkbox"/>
SNPRunCount	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>
SNP-TMLastRun	RegDword	132450847		<input type="checkbox"/>	<input type="checkbox"/>
SNPTriggerMarketing	RegDword	0		<input type="checkbox"/>	<input type="checkbox"/>
SNPShowTMPrivacy	RegDword	0		<input type="checkbox"/>	<input type="checkbox"/>

Type viewer

Binary viewer

Value name

MystDeviceVerify

Value type

RegDword

Value

512

Raw value

00-02-00-00

Value: MystDeviceVerify Collapse all hives

# EXPLORING WINDOWS REGISTRY

**SI :**

**SYSTEM\CurrentControlSet\Control\TimeZoneInformation**

**SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces**

**interface <--> GUID**

**FILE/FOLDERS :**

**NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs**

**NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths**

**File Explorer**



# EXPLORING WINDOWS REGISTRY

## EVIDENCE OF EXECUTION :

**SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache**  
**ShimCache**

**SYSTEM\CurrentControlSet\Services\bam\UserSettings\{SID}**

**SYSTEM\CurrentControlSet\Services\dam\UserSettings\{SID}**

**SID <--> user account**

## EXTERNAL DEVICES :

**SYSTEM\CurrentControlSet\Enum\USB**



# CONCLUSION

