WINDOWS FORENSICS

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%)

Atifact = 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)

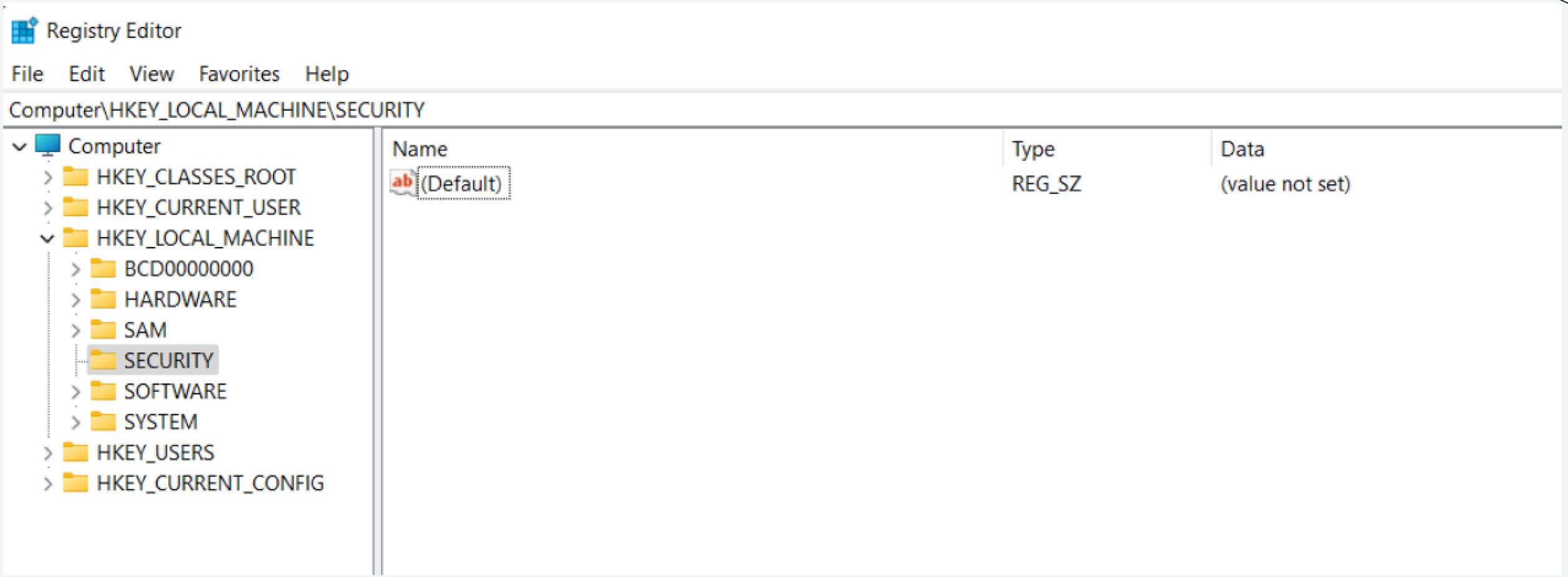
HKEY_USERS

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



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

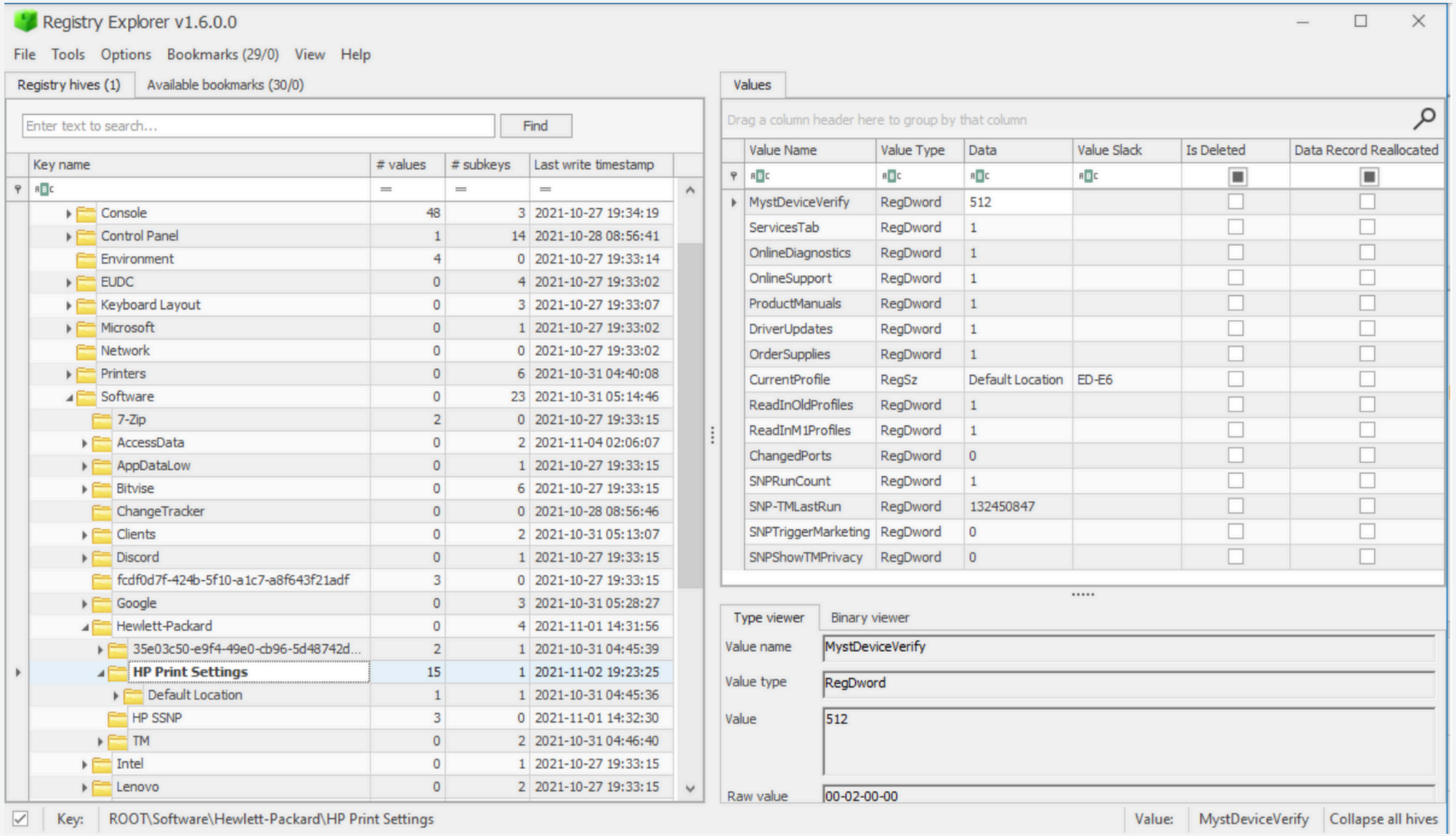
FTK® Imager

REGISTRY EXPLORER

Data VISUALIZATION & ANALYSIS

Registry Editor like

Zimmerman's Registry Explorer



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