CYBER502x Computer Forensics

Unit 6: Windows Registry Analysis

Forensics involves

- Discover and Collect
- Preserve
- Analyze
- Present / Report

Registry

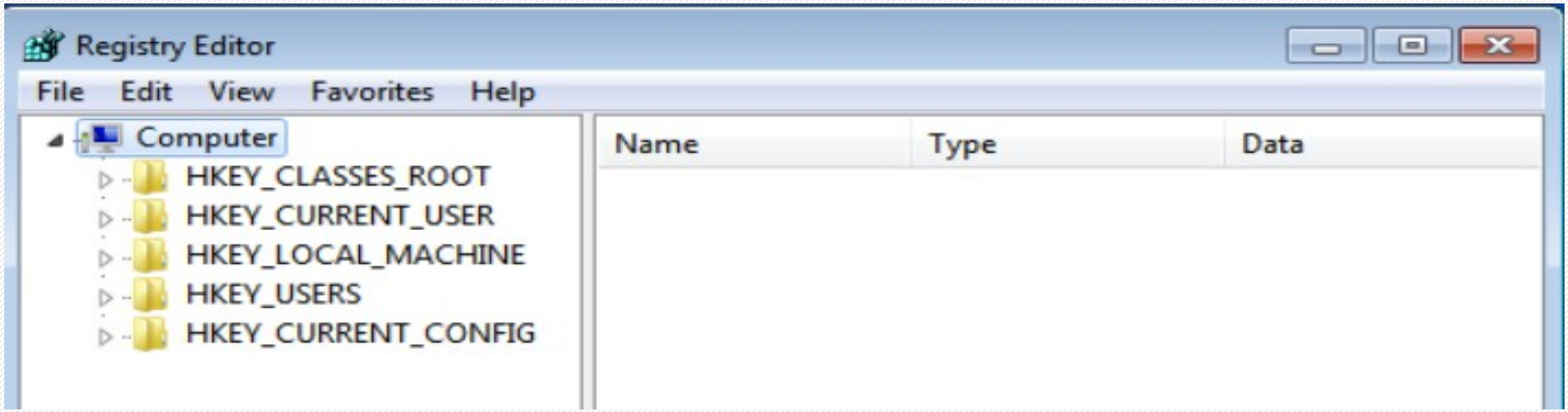
- Central hierarchical, configuration database
- Operating system relies on it
- Contains information about
  - Hardware including plug and play devices
  - Users information, preferences
    - Support multiple users
  - Application information
  - Network information

What can you possibly find from registry files?

- Usernames and passwords for programs
- Visited Internet sites including date and time
- A record of Internet searches via Google, Yahoo
- Lists of recently accessed files
- A list of programs installed on the system

Registry Tree

- HKEY_CLASSES_ROOT, HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE, HKEY_USERS
- HKEY_CURRENT_CONFIG



Glean evidence from Registry

- Make sure that your registry is backed up
- On Win95/98, registry is comprised of
  - Windows\System.dat
  - Windows\User.dat
- WinNT and later, registry is comprised of
  - Several hive files
    - HKEY_LOCAL_MACHINE \SYSTEM : SYSTEM
    - HKEY_LOCAL_MACHINE \SAM: SAM
    - HKEY_LOCAL_MACHINE \SECURITY: SECURITY
    - HKEY_LOCAL_MACHINE \SOFTWARE: SOFTWARE
  - NTUSER.dat files related to each user account

What can you find from SAM?

- SAM
  - Contains user account information for users and groups on the system
  - Also contains hashed logon passwords
- Use of SAM
  - Resolve user to SID
  - Find out who is the last one logged in

SID

SIDs in a typical multiuser system:

- HKU\.DEFAULT
- HKU\S-1-5-18
- HKU\S-1-5-19
- HKU\S-1-5-20

System Accounts

- HKU\S-1-5-21-1116317227-3122546243-4014252641-1000
- HKU\S-1-5-21-1116317227-3122546243-4014252641-1002

Individual User Accounts

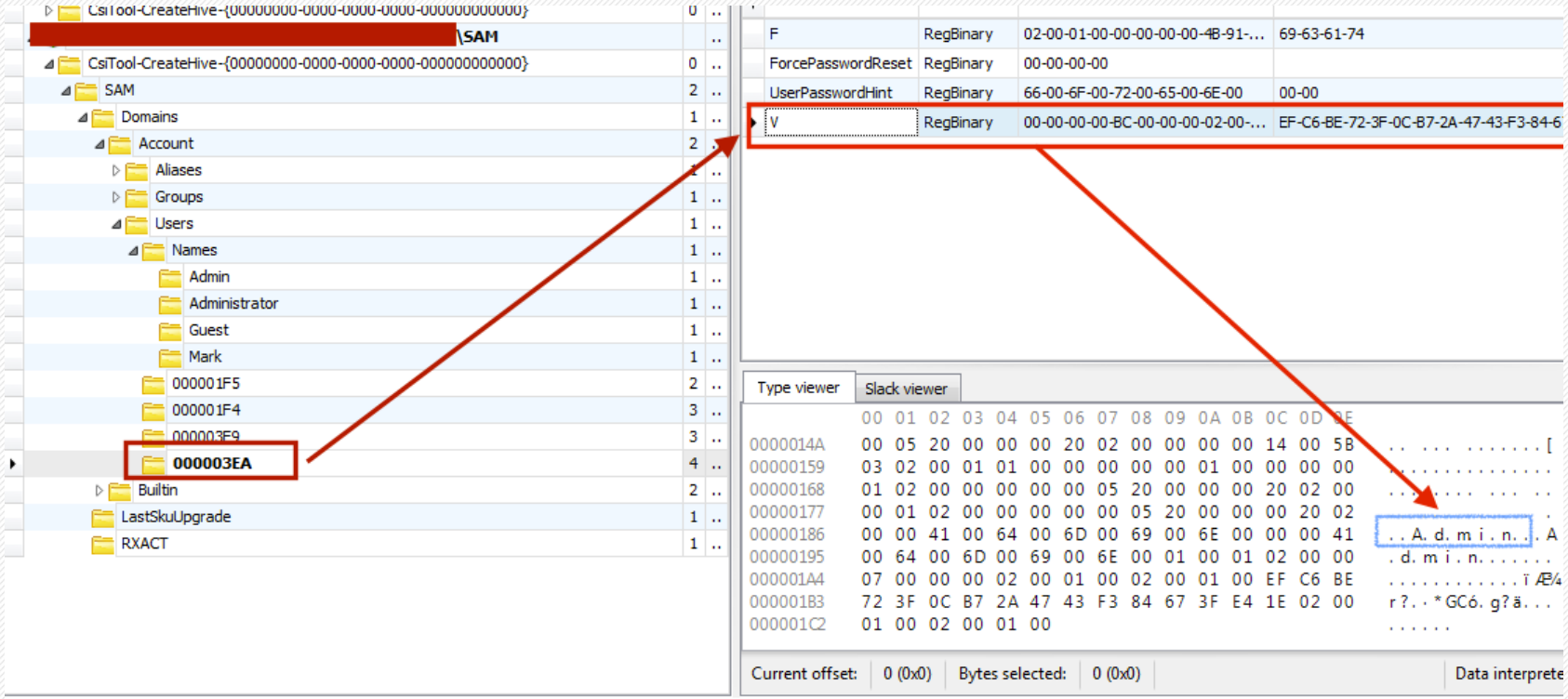
- "S" identifies the string as SID.
  "1" SID specification version.
- "5" is the identifier authority value.
- "21-1116317227-3122546273-4014252641" Domain identifier.
  "1000" or "1002" is the Relative ID (RID).

Identifying last logon using RID

- Windows stores the last logon time for a user at:
  - SAM\Domains\Account\Users\%RID%\F
- Finding Usernames from RID (V-values)
- Determine last logon time for the RID (F-values)

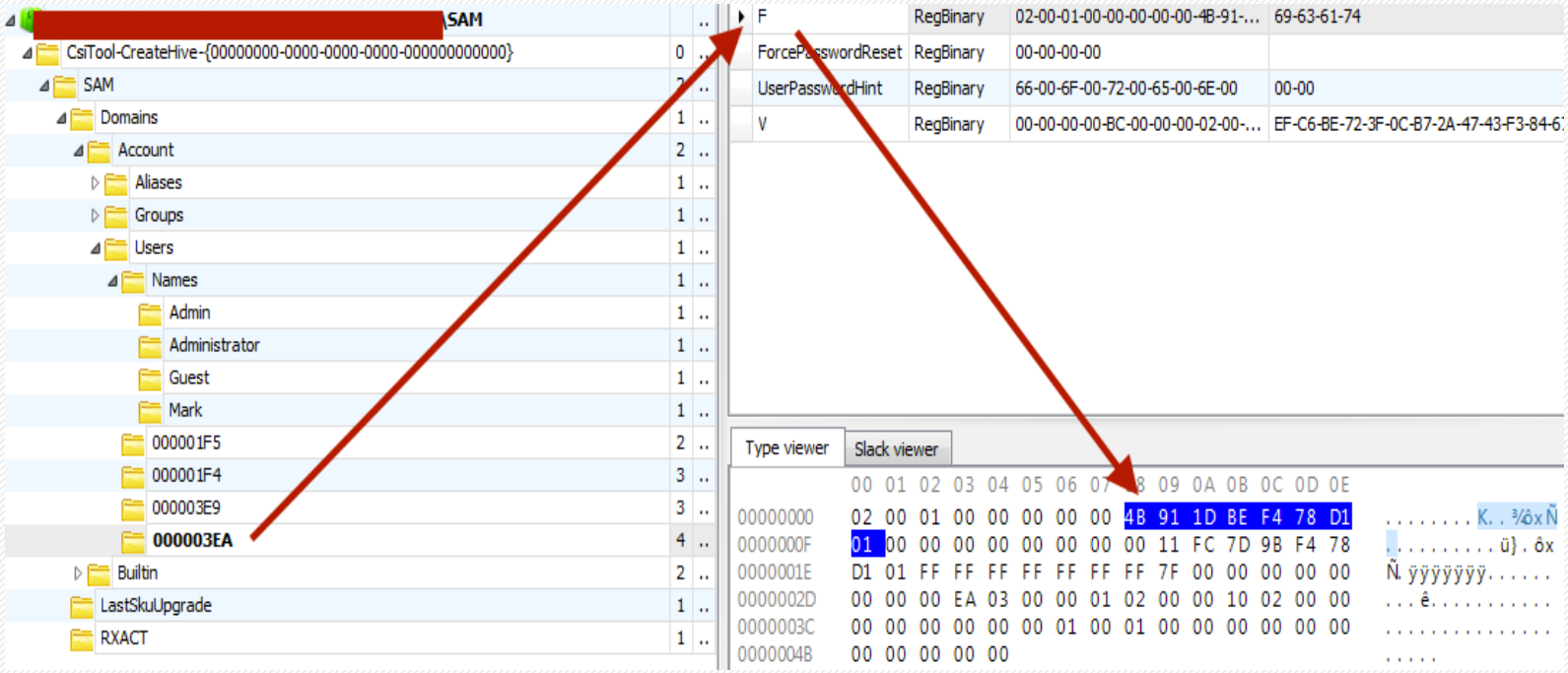
Finding Username from RID

- Select RIDs under SAM\Domains\Account\Users
- Select V entry and scroll the hex values till the end.



Determining Last logon

- Select the F value for RID.
- Bytes 9-16 are Last logon time in FILETIME format for the associated user.
- Convert the FILETIME to Date & Time. (Use Dcode).



What can you find from SYSTEM?

- SYSTEM
  - Computer Name
  - Device Drivers and driver letter mappings
  - The Last Known Good Configuration
  - Setup information
  - Hardware profile
- Use of SYSTEM
  - Determine which control set is active
  - Find out timezone, Mounted devices

What can you find from SYSTEM (Cont'd)?

- Finding USB last insertion and removal time
  - In USBSTOR under \ControlSet00x\Enum\USBSTOR
  - Windows 8 new registry artifacts
    - Device last insertion date
    - Device last removal date

Windows 7 Event Log and USB Device Tracking

- Identify the connection and disconnection events associated with the device.
- Event ID 2003 associates with USB connected
- Event ID 2100/2102 associates with USB disconnected.

What can you find from SOFTWARE?

- Contains a list of all installed programs and their settings
- Paths to application files and dirs
- Use of SOFTWARE
  - RigisteredOwner
  - RegisteredOrganization
  - ProductID
  - ProductName
  - InstallDate

What can you find from NTUSER?

- Protected storage information
  - An access-restricted area of the registry that stores confidential user information
- The recently run programs
- The recently used (open or save) files
- Recently accessed networks
- Internet Explorer usages and password
- User preference settings

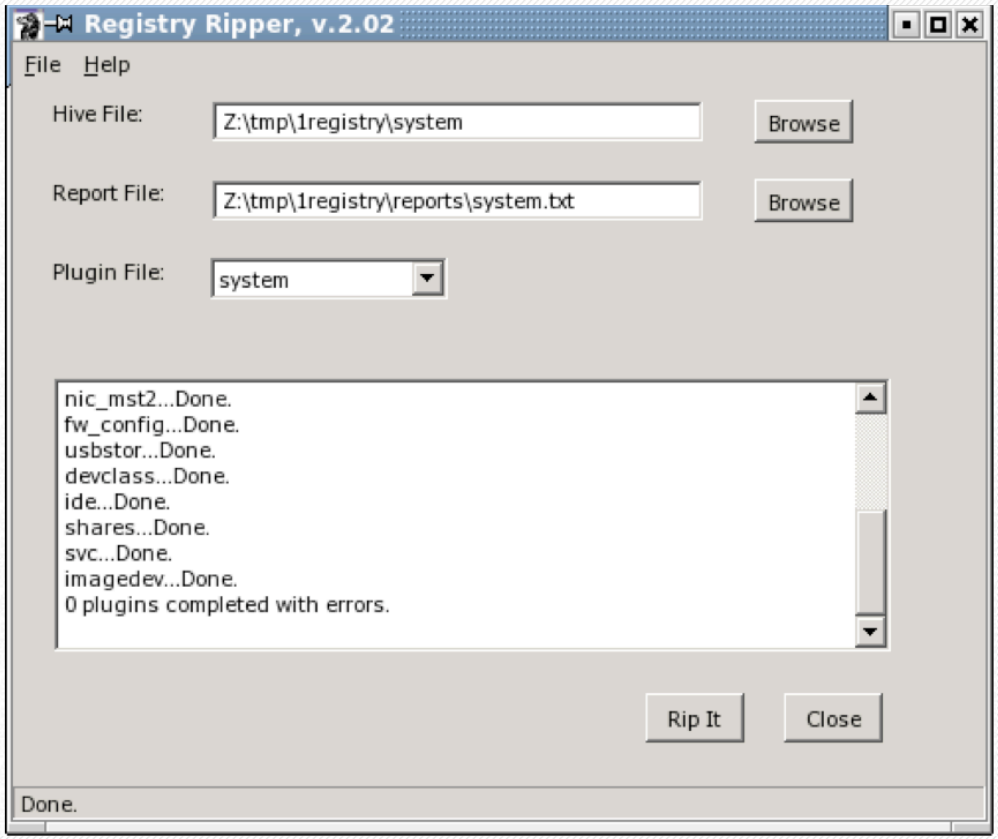
Information from the registry.9

- Registry quick find chart from AccessData
  - wp.Registry_Quick_Find_Chart.en_us.pdf

How to view the registry files

- FTK imager – extract registry hives from a running machine
- Volatility – extract registry hives from memory
- Registry Viewer – view registry key and values
- EnCase parses the registry files and presents them in a familiar tree-structured view.
  - Examine C:\Windows\system32\config\system
  - C:\Documents and Settings\%USER% or C:\%USER%

RegRipper – Reg Analyzer




```
ComputerName = testbox
---------------------------------------
ShutdownCount
ControlSet002\Control\Watchdog\Display
LastWrite Time Mon Jan 19 23:03:52 2009 (UTC)
   ShutdownCount = 218
---------------------------------------
TimeZoneInformation key
ControlSet002\Control\TimeZoneInformation
LastWrite Time Sun Nov  2 14:14:54 2008 (UTC)
   DaylightName   -> Eastern Daylight Time
   StandardName   -> Eastern Standard Time
   Bias           -> 300 (5 hours)
   ActiveTimeBias -> 300 (5 hours)
---------------------------------------
ControlSet002\Control\Terminal Server key,
fDenyTSConnections value
LastWrite Time Fri Oct 24 20:53:51 2008 (UTC)
   fDenyTSConnections = 1
---------------------------------------
```

Registry Recon

- By Arsenal Recon, http://arsenalrecon.com/
- Show how Windows Registries have changed over time
- Analyze Registry live, backed up or deleted data
- 14-day Trial download:
  - http://ArsenalRecon.com/apps