Windows Forensic Artifacts Cheat Sheet

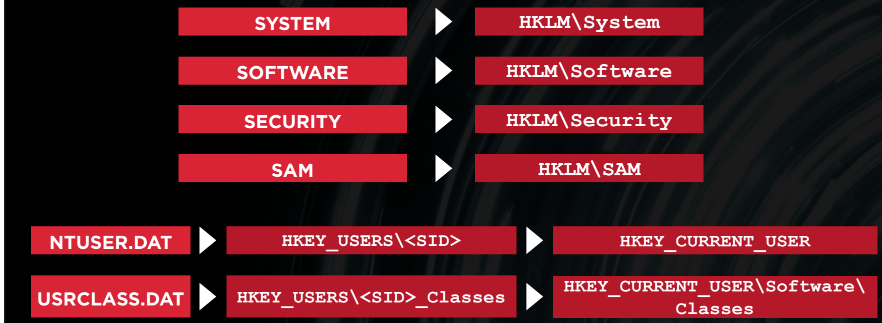
Registry Hives

Hierarchical databases that store system, application, and user configuration data

- **System Hives:** SYSTEM, SECURITY, SOFTWARE, SAM
- **System Hives Path:** %Systemroot%\System32\config\
- **User Hives:** NTUSER.DAT, USRCLASS.DAT
- **User Hives Paths:**
  \Users\<user>\NTUSER.DAT,
  \Users\<user>\AppData\Local\Microsoft\Windows\USRCLASS.DAT

Tools: *Regripper, Regedit (built-in), Registry Explorer*

Registry Hive Mappings



SYSTEM → HKLM\System

SOFTWARE → HKLM\Software

SECURITY → HKLM\Security

SAM → HKLM\SAM

NTUSER.DAT → HKEY_USERS\<SID> → HKEY_CURRENT_USER

USRCLASS.DAT → HKEY_USERS\<SID>_Classes → HKEY_CURRENT_USER\Software\Classes

System Configuration Registry Keys

- **Computer Name**
  HKLM\System\ControlSet###\Control\Computername\
- **Domain, Hostname, IP Address, DHCP Server**
  HKLM\System\ControlSet###\Services\Tcpip\Parameters\
- **Firewall Configuration**
  HKLM\System\ControlSet###\Services\Sharedaccess\Parameters\Firewallpolicy\
- **Map SIDs to Users**
  HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\
- **Network Shares**
  HKLM\System\ControlSet###\Services\Lanmanserver\Shares
- **OS Version and Product Name**
  HKLM\Software\Microsoft\Windows NT\Currentversion
- **System Time Zone**
  HKLM\System\ControlSet###\Control\Windows
- **Users that Logged On to the System**
  HKLM\Software\Microsoft\Windows NT\Currentversion\Winlogon\Defaultusername, Altdefaultusername
- **Users Active Directory Group Membership**
  HKLM\Microsoft\Windows\CurrentVersion\Group Policy\[USER_SID]\GroupMembership
- **USB Storage Devices**
  HKLM\System\ControlSet###\Enum\USBSTOR\

Application Compatibility Artifacts

- "Shim Cache" – Contains path and time metadata for files that ran on the system
  HKLM\SYSTEM\ControlSet###\Control\Session Manager\AppCompatCache\AppCompatCache
- "Amcache" – Contains path, time, and SHA1 hash metadata for files that ran on the system
  "Amcache" Path: %Systemroot%\AppCompat\Programs\Amcache.hve
- "Recent File Cache" – Contains file path for files that ran on the system
  "Recent File Cache" Path: %Systemroot%\AppCompat\Programs\RecentFileCache.bcf

Tools: *Mandiant ShimCacheParser.py, AppCompatCacheParser, AmcacheParser, rfcparse.py*

Common Autorun Registry Keys

- **Active Setup**
  HKLM\Software\Microsoft\Active Setup\Installed Components\%APPGUID%
- **AppInit DLLs**
  HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs
- **Run Keys**
  HKLM\Software\Microsoft\Windows\CurrentVersion\Run, RunOnce
- **Services and ServiceDLLs**
  HKLM\System\ControlSet###\Services\<Servicename>,<ImagePath>
  HKLM\System\ControlSet###\Services\<Servicename>\Parameters,<servicedll>
- **Shell Extensions**
  HKLM\Software\Microsoft\Windows\CurrentVersion\Shell Extensions
- **UserInit**
  HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\UserInit

User Hive Registry Keys

- **Shellbags:** Keys in User Hives that track Explorer usage. Analysis can yield accessed file metadata.
  HKCU\Local Settings\Software\Microsoft\Windows\Shell\
  Tools: *Shellbags.py, Shellbags Explorer*
- **"Most Recently Used" or "MRU" keys**
  HKCU\Software\Microsoft\Windows\CurrentVersion\ Explorer\RunMRU
  HKCU\Software\Microsoft\Windows\CurrentVersion\ Explorer\ComDlg32\OpenSaveMRU
- **MUICache (Recently Executed Applications)**
  HKCU\Software\Microsoft\Windows\ShellNoRoam\MUICache
  HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache
- **Mounted Volumes & Mapped Network Drives**
  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\<drive/GUID>
  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU
- **Opened Documents**
  HKCU\Software\Microsoft\Windows\CurrentVersion\ Explorer\RecentDocs
- **Remote Desktop – Last Accessed History**
  HKCU\Software\Microsoft\Terminal Server Client\Default
- **TypedURLs (Manually inputted into Internet Explorer)**
  "HKCU\Software\Microsoft\Internet Explorer\TypedURLs" OR "…\TypedPaths" (Vista & later)
- **UserAssist (Frequently Executed Applications)**
  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

***Note: Locations assume use of Vista/2008+ systems**

MANDIANT®
A FireEye® Company

Master File Table (MFT)

Stores information about every file and directory on an NTFS Volume.

Location: `<drive>\$MFT`

Tools: *Acquire with FTK Imager, other raw disk access. Parse with MFT2CSV*

INDX Attributes

Contains metadata about files stored within a directory

Location: $I30 files (a.k.a. “INDX” files) within each directory

Tools: *Acquire with FTK Imager or other raw disk access. Parse with INDXParse.py*

Windows Management Instrumentation

WMI can provide malware persistence and record evidence of program execution

Location: `%systemroot%\System32\wbem\Repository\OBJECTS.DATA`

Tools: *https://github.com/fireeye/flare-wmi/tree/master/python-cim*

Browser History

- **Internet Explorer 10 & 11**
  `C:\Users\<user>\AppData\Local\Microsoft\Windows\WebCache`
- **Google Chrome**
  `C:\Users\<user>\AppData\Local\Google\Chrome\User Data`
- **Mozilla Firefox**
  `C:\Users\<user>\AppData\Roaming\Mozilla\Firefox\Profiles\<profile>`

Scheduled Tasks

“SchedLgU.txt” Log: History of scheduled tasks that previously ran on the system

`%systemroot%\tasks\SchedLgU.txt, Microsoft-Windows-TaskScheduler%4Operational.evtx`

“.job” file path: `%systemroot%\tasks\*.job`

Tools: *Text editor for “SchedLgU.txt”, hex editor or “jobparser.py” for “.job” files*

Prefetch

Cached data for files that have previously executed on a system.

Location: `%systemroot%\prefetch\*.pf`

Tools: *WinPrefetchView, strings*

Common A/V Log Locations

- **McAfee:** `%allusersprofile%\McAfee\DesktopProtection\*.txt`
- **Symantec:** `%allusersprofile%\Symantec\Symantec EndpointProtection\Logs\AVMan.log`
- **Trend Micro:** Path listed at `HKLM\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\`
- **Sophos:** `C:\ProgramData\Sophos\Sophos Anti-Virus\logs\sav.txt`
- **Windows Defender:** `C:\ProgramData\Microsoft\Windows Defender\Support\*.log`

Event Logs

Windows’ built-in logging mechanism

Key Logs: Application, Security, System, Terminal Services Logs for evidence of RDP access (Microsoft-Windows-TerminalServices-LocalSessionManager, Microsoft-Windows-TerminalServices-RemoteconnectionManager); Task Scheduler log for evidence of scheduled tasks (Microsoft-Windows-TaskScheduler)

Location: `%systemroot%\System32\winevt\Logs\*.evtx`

Tools: *Event Viewer (built-in), Microsoft Log Parser, Event Log Explorer (commercial)*

Windows Logon Types

Type	Code
Interactive	2
Network Logons	3
Batch	4
Service	5
Unlock	7

Type	Code
NetworkCleartext	8
NewCredentials	9
RemoteInteractive	10
CacheInteractive	11

Windows Event Log Codes

Status Message	Windows Vista/2008+
Scheduled Task Registered	106
Remote Desktop Auth Succeeded	1149
Audit Logs Clearedz	1102
Powershell Scriptblock contents	4104
Powershell Scriptblock start	4105
Powershell Scriptblock stop	4106
Network Logons	4624
Logon Using Explicit Credentials	4648

Status Message	Windows Vista/2008+
New Process	4688
Process Exit	4689
Scheduled Task Created	4698
Scheduled Task Deleted	4699
Scheduled Task Updated	4702
Service Start / Stop Control	7035
Service Running / Stopped	7036
Service Installation	7045

Windows Timestamps

$STD_INFORMATION	Rename	Local Move	Volume Move	Copy	Access	Modify	Create	Delete
Modified						X	X	
Accessed			X	X			X	
Created				X			X	
Entry Modified	X	X				X	X	

$FN_NAME	Rename	Local Move	Volume Move	Copy	Access	Modify	Create	Delete
Modified	X	X	X	X			X	
Accessed			X	X			X	
Created			X	X			X	
Entry Modified	X	X	X	X			X	