Practical Windows Forensics CHEAT SHEET

Data Collection

Acquire a forensic copy of the digital evidence while preserving its integrity.

Methods

Write-blocker: Essential to prevent accidental modifications to the evidence (hardware or software options available).

Imaging tools:

- **FTK Imager:** GUI tool for creating forensic disk images.
- **Guymager:** Open-source tool for forensic imaging (Linux/Windows).

dd if=source_device of=image_file bs=1024

Virtualization environments:

- **VirtualBox:** Use VirtualBox for creating VMs with proper acquisition techniques. Capture memory snapshots with disk images.
- **VMware Workstation:** Consider VMware for VMs. Similar acquisition techniques apply, including memory snapshots.

Hashing

Calculate cryptographic hash (e.g., MD5, SHA-256) of the acquired image after acquisition and analysis for verification.

Data Extraction

Recover data from the acquired image for further analysis.

Methods

- **Forensic tools:** Most forensic suites offer data extraction capabilities, including file carving and undeleting functionalities.
- **File carving:** Technique to recover deleted or fragmented files based on file signatures. Consider using advanced carving techniques offered by forensic tools.

find . -name "*.txt"
grep "keyword" *.txt

Registry Hives

The Windows Registry is a hierarchical database of configuration settings.

Registry Root Keys

HKEY_CURRENT_USER	HKCU	Stores user-specific settings like software installations, network connections, and recently accessed files.
HKEY_LOCAL_MACHINE	HKLM	Holds system-wide settings for the operating system, including startup applications, loaded device drivers, and security policies.
HKEY_USERS	HKU	Contains user profile information for all accounts, allowing investigation of settings for different users and potential suspicious activity.
HKEY_CLASSES_ROOT	HKCR	Defines file associations, so examining it helps identify unusual associations that could indicate malware.
HKEY_CURRENT_CONFIG	HKCC	Stores information about the currently loaded hardware profile, allowing analysis of settings related to your computer's hardware configuration.

Location **%SystemRoot%\System32\config**

Registry file types **.hiv** extension

Registry Analysis

Examine configuration settings for potential evidence of suspicious activity.

locations

- **RunOnce keys**
- **Scheduled Tasks**
- **User startup locations**

Tools

Registry viewers and forensic tools with registry analysis capabilities.

reg query:

HKLM\SOFTWARE\Microsoft-\Windows\CurrentVersion\Run

No Extension
Registry Hive file

.alt extension
Backup copy of hive, used in Windows 2000, not XP

.log extension
Transaction log of changes to a hive

.sav extension
Backup copy of hive created at the end of text-mode(console) phrase during windows XP setup

New Technology File System (NTFS)

Dominant file system in Windows.

Key structures

- **Master File Table (MFT):** analyze it for deleted files, modifications, and access patterns.
- **$MFT:$I30:$INDEX:$I30:** stores recently used files. Use it to identify what files were accessed recently.
- **$UsnJrnl (Usn Journal):** useful for deleted file recovery. Analyze it to see what files and folders were modified.

Files

Analyze file attributes, timestamps, and data content for potential evidence.

- **File Attributes:** Examine file attributes like Read-only, Hidden, System, and Archive for suspicious behavior.
- **Timestamps:** Analyze timestamps (Created, Modified, Accessed) to understand file activity timeline.

Modified	m...	File modified
Accessed	.a..	File accessed
Changed ($MFT record)	..c.	MFT record modified
Birth (Created)	...b	File created

- **Data Content:** Utilize forensic tools to examine file content for hidden data or embedded artifacts.

Execution

Identify programs and scripts executed on the system.

Locations to examine

- **Prefetch files:** Track recently accessed applications and can reveal past program executions. Analyze prefetch files with forensic tools.

C:\Windows\Prefetch*.pf

- **Shim Cache:** Stores information about loaded DLLs (Dynamic Link Libraries). Investigate loaded DLLs for suspicious activity.
- **Command history:** Tools can analyze command history files (e.g., cmd.exe history) to identify past commands executed.
- **Memory analysis:** Can reveal evidence of recently executed processes and loaded modules.
- **Event logs:** May contain entries related to program execution, such as application startup events.

Persistence

Identify mechanisms used by malware to maintain presence on the system.

Locations to examine

- **RunOnce/Run keys:** Programs configured for automatic startup at login or system boot. Analyze listed programs for suspicious entries.
- **Scheduled Tasks:** Tasks configured to run at specific times. Investigate scheduled tasks for unauthorized activity.

HKLM\Software\Microsoft\Windows NT\Current-Version\Schedule\TaskCache\Tasks

HKLM\Software\Microsoft\Windows NT\Current-Version\Schedule\TaskCache\Tre

- **Service startup:** Programs configured as Windows services can provide persistence. Analyze startup type and service descriptions for suspicious entries.

C:\Users\[Username]\AppData\Roaming\Microsoft-\Windows\Start Menu\Programs\Startup

C:\ProgramData\Microsoft\Windows\Start Menu\Pro-grams\StartUp

- **Autoruns tools:** Help identify startup locations for programs. Utilize these tools to comprehensively identify persistence mechanisms.

Event Logs

System, Security, and Application logs track events and activities on the system.

Analysis

- **Windows Event Viewer**
- **Forensic tools**

wevtutil enum logs

Memory Analysis

Analyze volatile data in RAM for potential evidence.

vol-fwin10-memory.raw windows.info

Plugins

- **Windows.info**
- **Windows.pstree**
- **Windows.pslist**
- **Windows.registry.hivelist**
- **Windows.pslist--pid <PID>--dump**
- **Windows.dlllist--pid <PID>--dump**
- **Windows.getsids--pid <PID>**
- **Windows.registry.printkey -offset<hive_offset>--key <key_name?**

Super Timelines

Create a unified timeline of events across all evidence sources.

Qemu-img convert-O raw disk.vhd disk.raw

Forensic tools often have timeline creation functionalities.

Vol-f memory.raw timeliner-create-bodyfile