Windows Forensic Cheatsheet

1. Initial Response

- Isolate the system from the network to prevent tampering.
- Document the current state of the machine.
- Capture volatile data (RAM, running processes, network connections).

2. Data Acquisition

- Create a forensic image of the disk using trusted tools (FTK Imager, dd).
- Use write-blockers to avoid modifying original evidence.
- Verify image integrity with hash values (MD5/SHA1/SHA256).

3. Registry Analysis

- Examine the SAM, SYSTEM, SOFTWARE, SECURITY, and NTUSER.DAT hives.
- Check for persistence mechanisms like Run keys and Services.
- Identify recently accessed files and USB devices.

4. Log Analysis

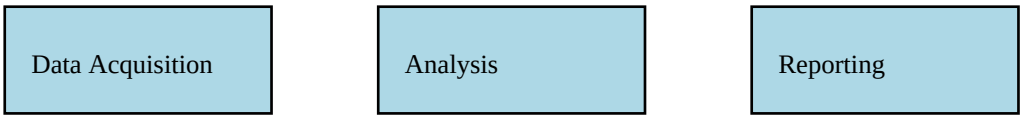
- Inspect Windows Event Logs (Application, Security, System).
- Look for failed logins, privilege escalation attempts, and unusual activities.
- Analyze Prefetch files for recently executed programs.

5. File System Examination

- Identify hidden and system files.
- Check recycle bin and shadow copies for deleted data.
- Analyze timestamps (MAC times) for anomalies.

6. Tools and Utilities

- FTK Imager – disk imaging.
- Volatility – memory analysis.
- Autopsy – GUI forensic analysis.
- Sysinternals Suite – system inspection.



AI Illustration: Imagine a cyberpunk-style forensic investigator working on holographic Windows artifacts.

Windows Registry Forensics Cheatsheet

General Commands

- reg query HKLM\Software – List subkeys under HKLM\Software
- reg query HKCU\Environment – Display user environment variables
- reg query HKLM\System\CurrentControlSet\Services – Check services configurations

User Activity

- reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run – Check startup programs
- reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU – View Run dialog history
- reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs – Recent documents

USB Device History

- reg query HKLM\System\CurrentControlSet\Enum\USBSTOR – List connected USB devices
- reg query HKLM\System\MountedDevices – Show mounted device history

Network Info

- reg query HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces – View network interfaces
- reg query HKLM\Software\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles – Check network profiles

Summary: This cheatsheet provides quick guidelines for Windows forensic investigations. It covers essential steps including initial response, data acquisition, registry and log analysis, file system examination, and common forensic tools. By following these points, investigators can maintain forensic integrity, identify critical evidence, and ensure accurate reporting.