Windows Forensics 1

## **Windows Forensics 1 – Notes**

### **Task 1 – Introduction to Windows Forensics**

* **Goal**: Investigate Windows systems for digital evidence.
* Focus areas:
  + **Registry analysis**
  + **System artifacts**
  + **Evidence of execution**
  + **USB/device forensics**
* Key principle: Preserve evidence integrity (use forensic images / offline analysis).

### **Task 2 – Windows Registry and Forensics**

* **Windows Registry**: Hierarchical database storing configuration, preferences, and user/system activity.
* **Hive files**: Main registry database files stored in %SystemRoot%\System32\Config and user profile folders.
* **Registry Keys for Forensics**:
  + **SAM** – Security Account Manager (user accounts, password hashes).
  + **SYSTEM** – System config, time zone, control sets.
  + **SOFTWARE** – Installed programs, system-wide settings.
  + **SECURITY** – Local security policy.
  + **NTUSER.DAT** – User-specific settings, run history, typed URLs.
  + **USRCLASS.DAT** – File association info, recent activity.

### **Task 3 – Accessing Registry Hives Offline**

* Acquire hives from:
  + Live systems (careful—possible contamination).
  + Forensic disk images (preferred).
* Tools:
  + **RegRipper** – Automated registry parsing.
  + **Registry Explorer** – Manual exploration.
  + **FTK Imager** – Extraction.
* Offline analysis avoids altering original evidence.

### **Task 4 – Data Acquisition**

* **Live Acquisition**: Collect volatile + non-volatile data from a running system (risky—changes state).
* **Dead Acquisition**: From powered-off system or forensic image (safer for integrity).
* Tools: FTK Imager, EnCase, Magnet AXIOM.
* Follow **chain of custody** and maintain **hash verification**.

### **Task 5 – Exploring Windows Registry**

* Common forensic registry areas:
  + **Run / RunOnce Keys** – Auto-start programs.
  + **UserAssist** – GUI program execution counts & last run times.
  + **RecentDocs** – Recently opened files.
  + **Shellbags** – Folder view history.
  + **TypedURLs / TypedPaths** – Browser and Explorer input history.
* Registry timestamps help build an **activity timeline**.

### **Task 6 – System Information and System Accounts**

* Registry stores:
  + OS install date, version, last shutdown time.
  + Time zone settings.
  + User account list & group memberships (from SAM hive).
  + Last login times.
* Useful for attribution and system profiling.

### **Task 7 – Usage or Knowledge of Files/Folders**

* Artifacts showing file/folder access:
  + **RecentDocs** (NTUSER.DAT).
  + **OpenSaveMRU** – Files opened/saved in common dialogs.
  + **Shellbags** – Directories viewed in Explorer.
* Helps prove knowledge/possession of specific files.

### **Task 8 – Evidence of Execution**

* Key registry sources:
  + **UserAssist** – Tracks GUI program execution.
  + **ShimCache (AppCompatCache)** – Stores program execution history.
  + **Prefetch Files** (C:\Windows\Prefetch) – Contains execution counts & last run times.
  + **Amcache.hve** – Installed program metadata.
* Correlate with file system timestamps for accuracy.

### **Task 9 – External Devices / USB Device Forensics**

* Identify connected devices from registry:
  + **SYSTEM hive** → USBSTOR – Vendor IDs, product IDs, serial numbers.
  + **MountedDevices** – Drive letter to volume mapping.
  + **SetupAPI.dev.log** – Installation timestamps.
* Useful for tracking unauthorized data exfiltration via USB.

### **Task 10 – Hands-on Challenge**

* Apply registry and artifact analysis skills to extract:
  + Last plugged-in USB device.
  + Most recently executed programs.
  + Files/folders recently accessed.
  + System/user account information.

### **Task 11 – Conclusion**

* **Windows registry** is a rich source of forensic evidence.
* Offline analysis ensures evidence integrity.
* Correlating multiple artifacts increases confidence in findings.
* Crucial for **incident response, legal investigations, and insider threat cases**.

