Windows Forensics 2

# 🕵 Windows Forensics 2 – Notes

### **Task 1 – Introduction**

* Focuses on file system forensics in Windows.
* Covers **FAT (File Allocation Table)** and **NTFS (New Technology File System)**.
* Learn how files are stored, deleted, and recovered.
* Helps investigators **recover evidence** (deleted files, execution history, USB activity).

### **Task 2 – The FAT File Systems**

* Used in older systems and removable media (USB, SD cards).
* Variants: **FAT12, FAT16, FAT32, exFAT**.
* Structure:
  + **Boot Sector** – metadata (system info, file system type).
  + **File Allocation Table** – keeps track of clusters used by files.
  + **Root Directory Region** – contains file and folder metadata.
  + **Data Region** – actual contents of files.
* **Forensic importance**: Easy to recover deleted files since FAT only marks entries as deleted.

### **Task 3 – The NTFS File System**

* Default Windows file system (more advanced than FAT).
* Uses **Master File Table (MFT)** to store metadata.
* Features:
  + Journaling (keeps logs of changes).
  + File permissions (ACLs).
  + Alternate Data Streams (ADS) – can hide malicious data.
* **Forensic importance**:
  + Every file has an MFT entry.
  + Deleted files may leave traces in unallocated MFT records.
  + ADS often used by malware to hide payloads.

### **Task 4 – Recovering Deleted Files**

* Deletion doesn’t remove data immediately – only marks space as "available".
* Recovery depends on:
  + File system type (FAT easier than NTFS).
  + Whether data clusters have been overwritten.
* Tools used:
  + **Autopsy**, **FTK Imager**, **Recuva**, **Sleuth Kit**.
* Investigators must preserve evidence before it gets overwritten.

### **Task 5 – Evidence of Execution**

* Detecting if and when a file/application was executed.
* Sources of evidence:
  + **Prefetch files** (.pf) – record program execution details (location, time, frequency).
  + **AmCache.hve** – registry hive storing app execution metadata.
  + **Shimcache (AppCompatCache)** – registry artifact logging executed applications.
* Forensics tools can parse these to prove program execution.

### **Task 6 – File/Folder Knowledge**

* Windows records when users access files/folders.
* Key artifacts:
  + **Jump Lists** – track recently accessed documents.
  + **Recent Files (LNK files)** – shortcuts created when files are opened.
  + **Shellbags** – registry keys showing folder browsing history.
* Useful in showing user awareness/knowledge of files.

### **Task 7 – External Devices/USB Device Forensics**

* Traces of USB connections remain in Windows.
* Important registry locations:
  + SYSTEM\CurrentControlSet\Enum\USBSTOR – device details.
  + SYSTEM\MountedDevices – drive letters assigned.
  + SOFTWARE\Microsoft\Windows Portable Devices – connected devices.
* Investigators can determine:
  + Which devices were connected.
  + When they were connected.
  + What data may have been transferred.

### **Task 8 – Conclusion & Further Material**

* Windows file systems (FAT/NTFS) leave **plenty of forensic artifacts**.
* Deleted files can often be recovered if not overwritten.
* Execution evidence (prefetch, AmCache, Shimcache) helps prove malicious activity.
* USB artifacts confirm external device usage.
* Recommended for deeper learning: **SANS Windows Forensics Courses**, **DFIR blogs**, and **Practical Forensics labs**.

