**Digital Forensics Lab-Tasks**



**Prepared By: Ms.Memoona Sadaf**

**Instructor: Ms.Memoona Sadaf**

**Lab/Teaching Assistant: Muhammad Ahmad Ali Qureshi**

**Air University Islamabad**

**Lab Task 03**

**Total Marks: 10 CLO-03**

**1. Analyze the Disk Image**

* **Explore File System:**
  + Navigate the file structure to check for suspicious or interesting files.
* **Check Deleted Files:**
  + Look for **deleted files** that can be recovered.
* **Keyword Search:**
  + Run searches for relevant terms (e.g., "password," "confidential," "logs").
* **Metadata Analysis:**
  + Extract file metadata (timestamps, user info, etc.).
* **USB and External Devices:**
  + Identify if any external devices (USBs, hard drives) were connected.

**2. Use Additional Analysis Modules**

* **Hash Lookup:** Compare files with known forensic databases.
* **EXIF Data Extraction:** Retrieve metadata from images.
* **Web History & Cookies:** Identify browsing activities.
* **Email Analysis:** Look for stored email files.
* **Registry Analysis:** Extract user accounts and OS information.

**3. Report Findings**

* Document **important discoveries** (e.g., deleted files, suspicious programs, registry changes).
* Summarize key evidence in a **forensic report**.