**Digital Forensics Lab Task**



**Prepared By: Ms.Memoona Sadaf**

**Instructor: Ms.Memoona Sadaf**

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

**Air University Islamabad**

**Lab Task**

**Total Marks: 10 CLO-03**

**📝 Lab Question:**

**Objective:**  
Choose any Android APK file. Your task is to perform a **static analysis** of the APK to understand its internal structure, permissions, components, and potential security risks. You will use tools like **APKTool** and **JADX** to extract and analyze the app's code and resources.

**🧰 Instructions:**

Perform the following steps and document your findings:

1. **Decompile the APK** using **APKTool** to extract the app’s resources and AndroidManifest.xml.
   * Identify the app’s declared components (Activities, Services, Receivers).
   * List all requested permissions.
   * Check if the app is debuggable (android: debuggable="true").
2. **Analyze the Java code** using **JADX** or **JADX-GUI**:
   * Identify key Java classes and describe their purpose.
   * Search the code for hardcoded values such as:
     + API keys
     + URLs
     + User credentials
3. **Explore the res/ and assets/ folders**:
   * Identify the types of resources used (e.g., layouts, images, strings).
   * Check for any sensitive data or configuration files in assets/.
4. **Document security findings**:
   * Are there any signs of insecure coding practices?
   * Are any components exported unnecessarily?
   * Is any sensitive information stored insecurely in code or resources?
5. **Prepare a short report** summarizing your findings with screenshots and code examples where applicable.