**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 04**

**Total Marks: 10 CLO-03**

**Task #01**

Analyze the file named **transfer.pcap**. Answer these questions:

1. Which File Transfer Service is used in the captured traffic?
2. What was the name of the file that was transferred?
3. What was the packet number and timestamp?
4. In which packet number data (flag) was found?
5. What was the DATA?

**Task #02**

Analyze the file named **icmp.pcap**. Answer these questions:

1. What was the timestamp of the first packet sent?
2. What is the ICMP type number of the request packet?
3. What is the recovered DATA?