**Step-by-Step Practical**

**Materials Required:**

* **Wireshark** installed on student machines
* Pre-captured PCAP file
* Internet access

**Step 1: Analysis Tasks**

Students should complete the following **tasks** by using Wireshark's filtering tools, statistical reports, and packet details.

**Task 1: Identify Basic Traffic Information**

* **Protocol Breakdown**: What protocols are being used in this capture?  
  **Traffic Volume**: Identify the **top talker IP addresses** that generate the most traffic.

**Task 2: Detect HTTP Communications**

* **HTTP Analysis**: Are there any HTTP requests to suspicious websites?
* **Inspect a GET Request**: Locate an HTTP GET request and identify:
  + Hostname of the website.
  + Type of data being requested.

**Task 3: DNS Analysis**

* **DNS Query Logs**: Filter DNS traffic using dns.
  + Are there any **unusual domain names** being queried?
  + What are the **IP addresses** resolved from those queries?

**Task 4: Analyze Network Issues**

* **Packet Loss and Latency**: Check for TCP retransmissions and high latency.
* **TCP Stream Inspection**: Choose one TCP stream with retransmissions and:
  + Examine the handshake (SYN, SYN-ACK, ACK).
  + Identify if there are delays or dropped packets.

**Task 5: Security Threat Detection**

* **Identify ARP Spoofing**: Use arp filter to look for duplicate IPs in ARP replies.
* **Find Possible DoS Attack**: Use the filter icmp and inspect if a host is receiving a large number of ICMP requests in a short time (possible ping flood).

**Step 3: Reporting and Conclusions**

1. **Prepare a Report**:  
   Write a short report with the following sections:
   * **Introduction**: Overview of your analysis.
   * **Key Findings**: Mention any suspicious behavior or network anomalies.
   * **Possible Causes/Explanations**: Explain the identified issues and what could cause them.
   * **Recommendations**: Provide suggestions to the network admin to mitigate these issues.