**1. Start capturing on your active network interface**

* Launch Wireshark, choose your active network interface (e.g., eth0), and start the packet capture session.​

**2. Browse a website or ping a server to generate traffic**

* During active capture, use a browser to visit a site or run a command like ping google.com to ensure network packets are generated and recorded.​

**3. Stop capture after a minute**

* Let the capture run for about one minute to record sufficient traffic, then click the "Stop" button or select stop from the menu.​

**4. Filter captured packets by protocol**

* Use display filter bar to enter protocols, such as tcp, tls, arp, or combinations (http or dns or tcp) to isolate different packet types in the capture window.​

**5. Identify at least 3 different protocols**

* Review the packet list window’s Protocol column: verify the presence of TCP (connection/handshake), TLSv1.2 (secure data), and ARP (local address resolution), plus others like HTTP and SSDP if present.​

**6. Export the capture as a .pcap file**

* Go to File > Save As, select. pcap format, and save your complete capture for future analysis or documentation.