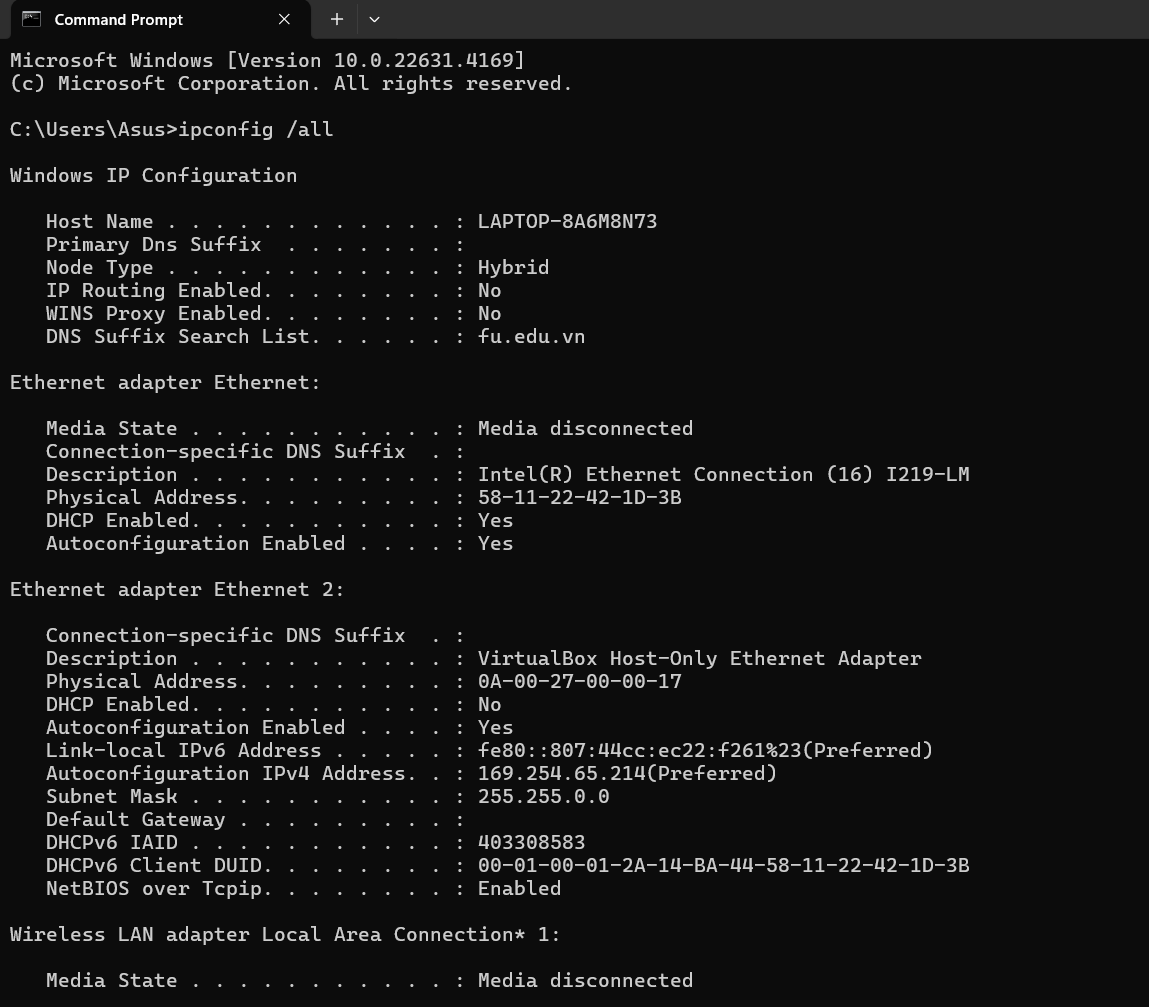
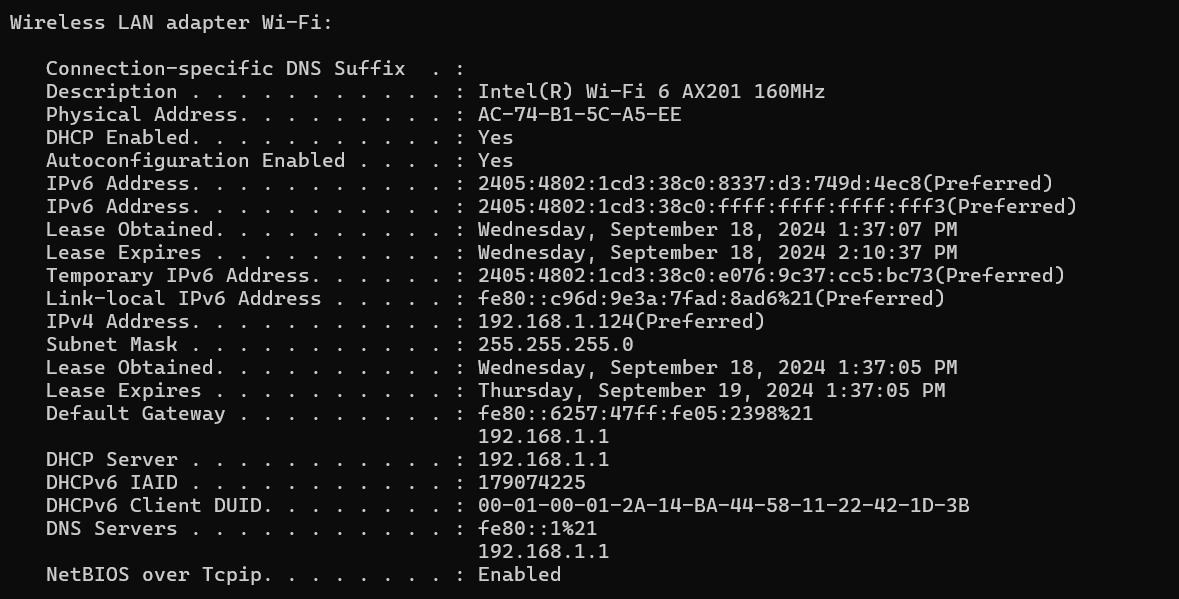
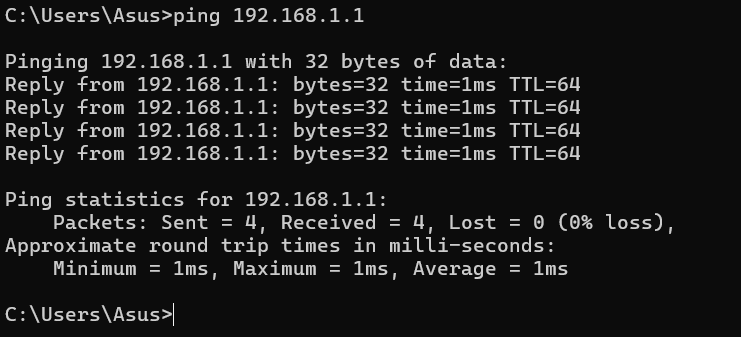
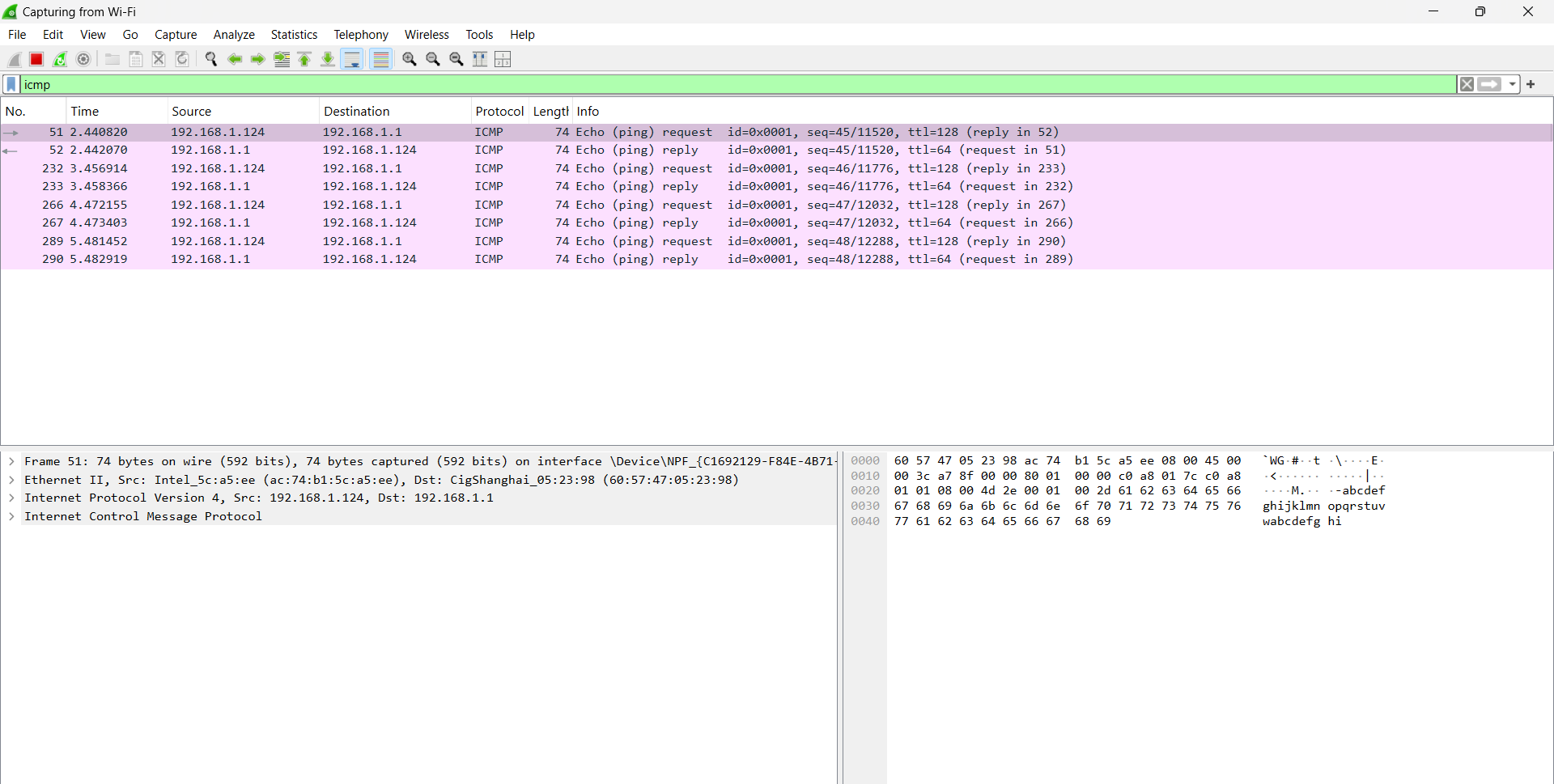
**Lab - Use Wireshark to View Network Traffic**

**Part 1**

****

****

* My Mac address: AC-74-B1-5C-A5-EE
* Ip address: 192.168.1.124
* Default gateway: 192.168.1.1
* Router MAC address: 60:57:47:05:23:98



Questions

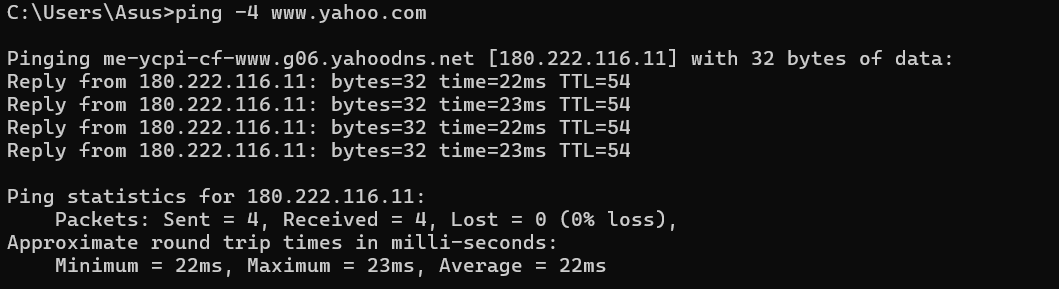
* **Does the source MAC address match your PC interface?**
* Yes
* **Does the destination MAC address in Wireshark match your team member MAC address?**

Yes

* **How is the MAC address of the pinged PC obtained by your PC?**

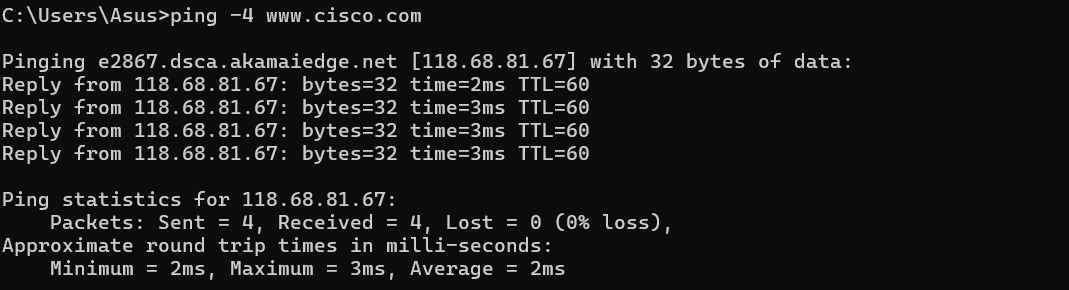
The MAC address of the pinged PC is obtained by your PC using the Address Resolution Protocol (ARP)

**Part 2**

****

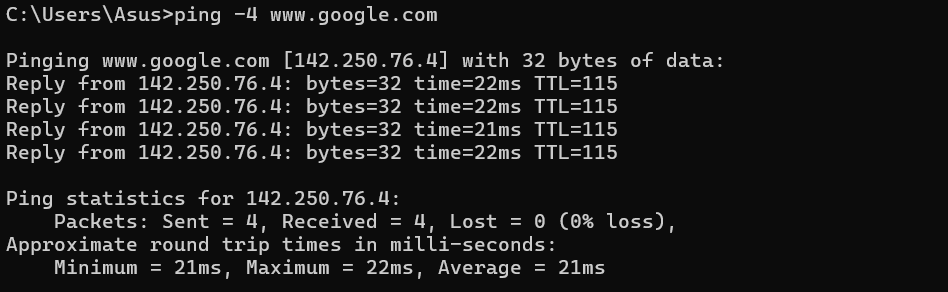
**IP address for www.yahoo.com:** 188.222.116.11

**MAC address for www.yahoo.com:** 60:57:47:05:23:98



**IP address for www.cisco.com:** 118.68.81.67

**MAC address for www.cisco.com:** 60:57:47:05:23:98



**IP address for www.google.com:** 142.250.76.4

**MAC address for www.google.com:** 60:57:47:05:23:98

**What is significant about this information?**

The significant point is that in Part 2, the MAC address is the same for all remote websites: 60:57:47:05:23:98

**How does this information differ from the local ping information you received in Part 1?**

**Part 1** shows correct local network information, while **Part 2** shows MAC addresses that are likely not from the external servers but from a local or intermediary device. This is because MAC addresses are not transmitted beyond local network boundaries.

**Why does Wireshark show the actual MAC address of the local hosts, but not the actual MAC address for the remote hosts?**

Wireshark shows the actual MAC addresses of local hosts because MAC addresses are only used for communication within the local network. Once data leaves the local network, it travels across routers, which replace the MAC address with their own, making remote hosts' MAC addresses inaccessible beyond the local network.