Lab 2

Exploring Ethernet and ARP traffic in Wireshark

What is ARP?

Address Resolution Protocol (ARP)

: A protocol for mapping an Internet Protocol Address (IP Address) to a physical machine address that is Recognized in the local network.

Step 1

: Deleting the ARP cache data

Windows: arp –a / arp –d
MacOS: sudo arp –a / sudo arp -ad

Step 2

: Deleting browser’s cache data

Step 3

: Boot up Wireshark and start capturing

Step 4

: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-lab-file3.html

Step 5

: Stop capturing

Step 6

: Apply filters to see ARP traffic

Bookmark -> Click on eth.type == 0x0806

Step 7

: Find and examine the ARP traffic