|  |  |
| --- | --- |
| **Ex. No : 6**  **Date:15/03** | **Identification ARP and capture with pcap file in wireshark** |

**Aim**

To identify ARP and save with .pcap file in wireshark

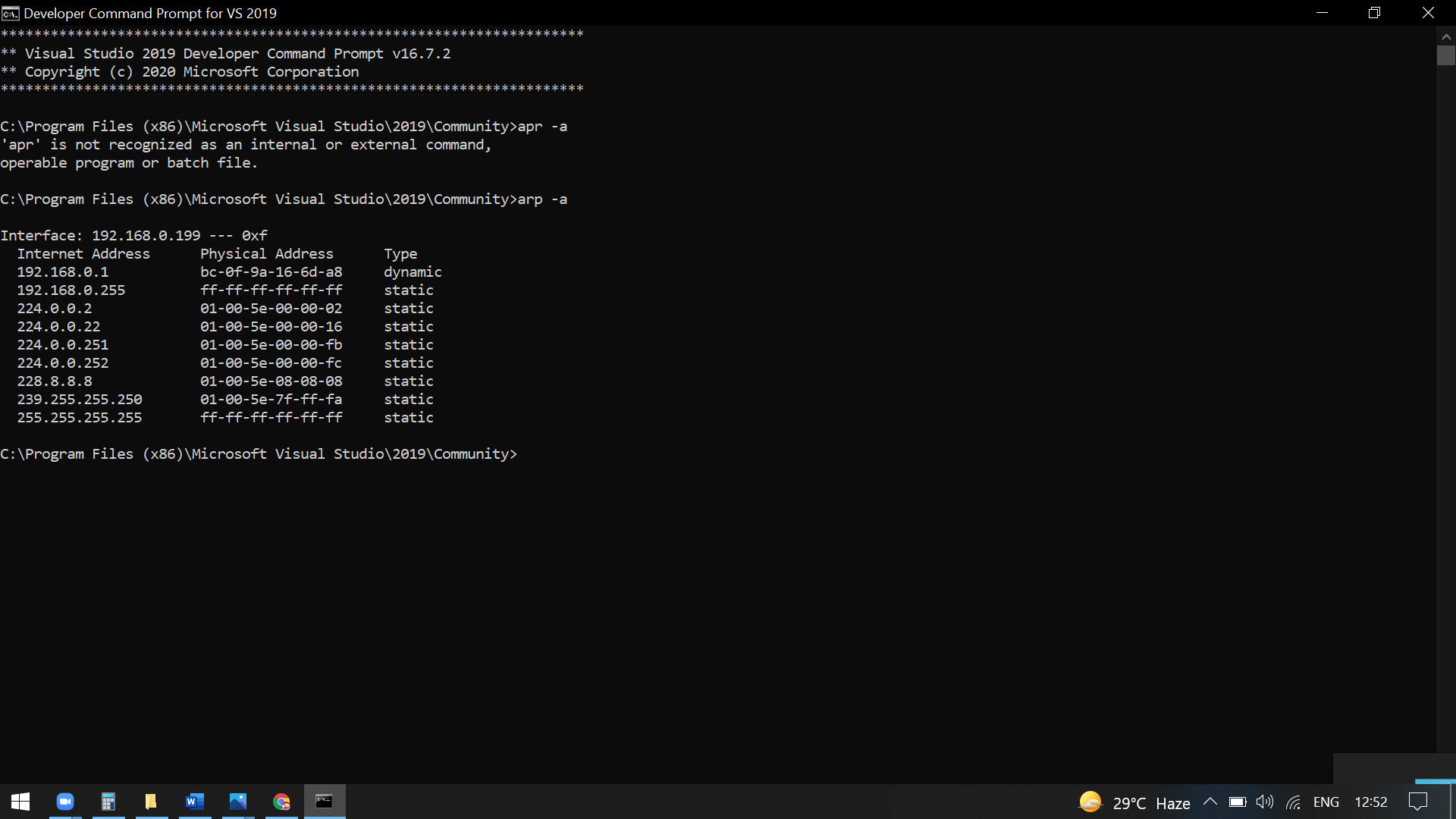
**Procedure:**

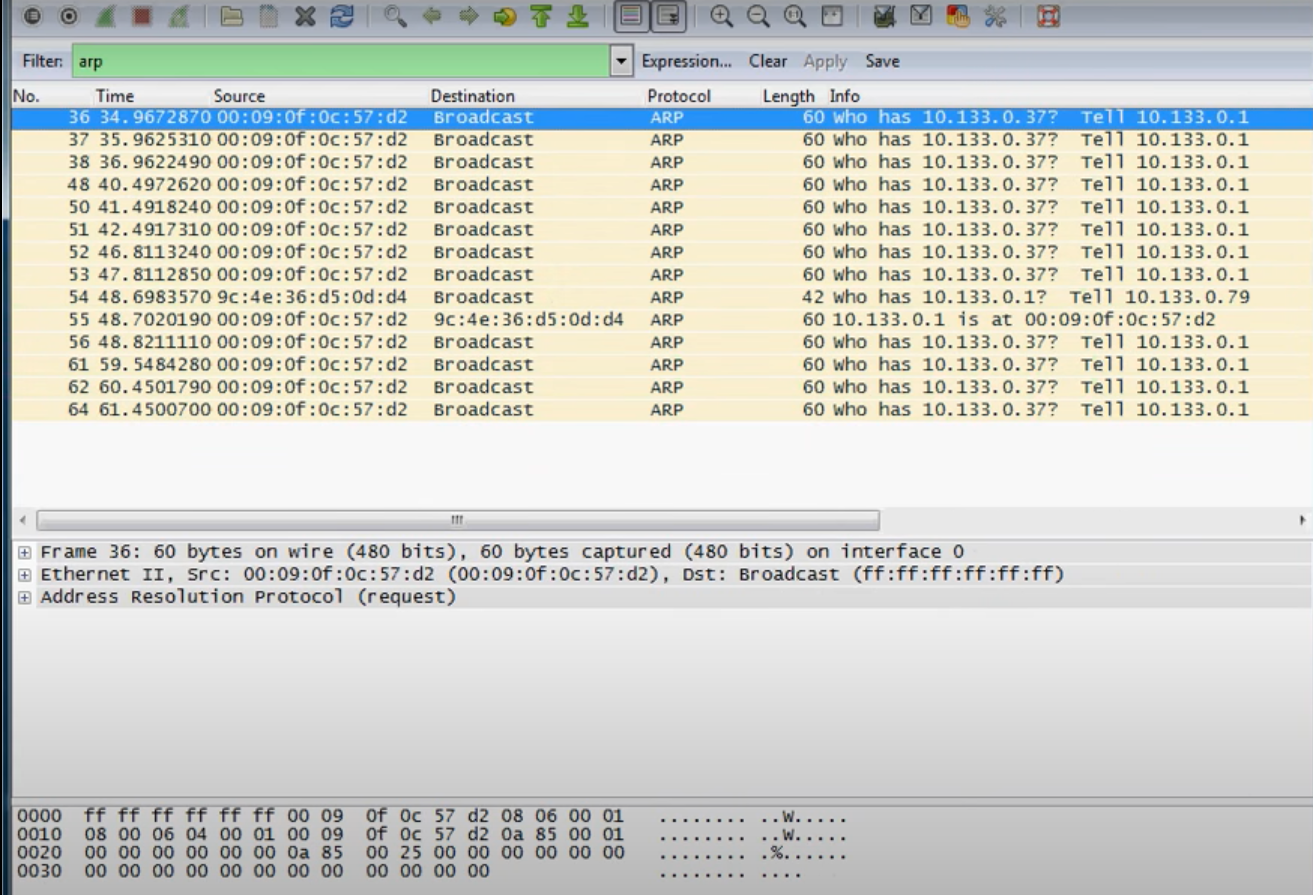
Arp -a :-

The Address Resolution Protocol (ARP) maps internet addresses to hardware addresses. TCP/IP uses ARP to collect and distribute the information for mapping

Start a Wireshark capture. Use arp -d to clear the ARP cache. Use ping <default gateway address> to ping the default gateway address. Use arp -a to view the ARP cache and confirm an entry has been added for the default gateway address.

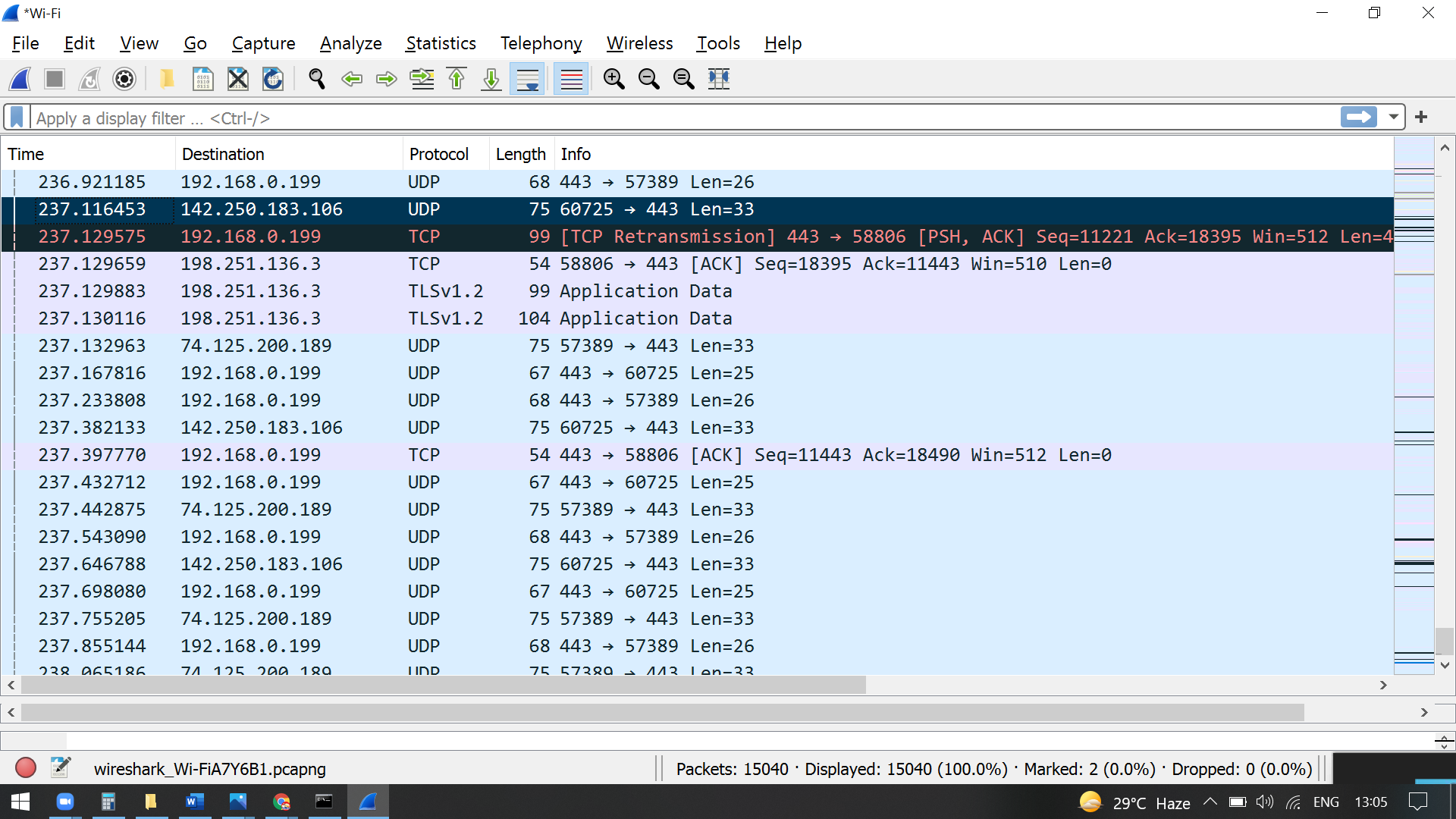






There are several ways to mark and unmark packets. From the Edit menu you can select from the following:

* Mark/Unmark Packet toggles the marked state of a single packet. This option is also available in the packet list context menu.
* Mark All Displayed set the mark state of all displayed packets.
* Unmark All Displayed reset the mark state of all packets.



**ARP Spoofing**

* The ARP protocol was not designed for security, so it does not verify that a response to an ARP request really comes from an authorized party.
* It also lets hosts accept ARP responses even if they never sent out a request. This is a weak point in the ARP protocol, which opens the door to ARP [spoofing attacks](https://www.imperva.com/learn/ddos/ip-spoofing/).

An ARP spoofing, also known as ARP poisoning, is a [Man in the Middle](https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/) (MitM) attack that allows

# **Saving Captured Packets in Wireshark**

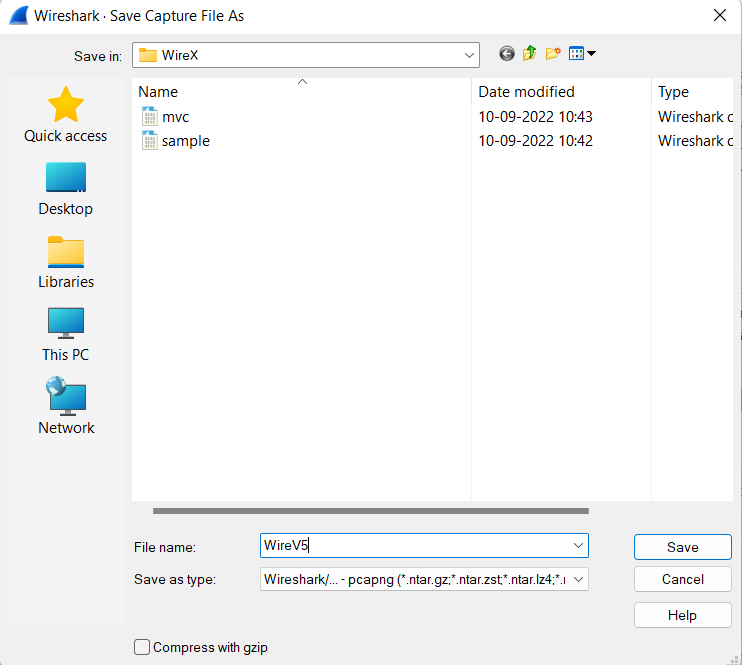
In Wireshark, after capturing some traffic of a network we can save the capture file on our local device so that it can be analyzed thoroughly in the future. We can save captured packets by using the**File → Save or File → Save As**…​ menu items. This will bring up the **“Save Capture File As”** dialogue box. While saving, we can select some specific packets and also choose different file formats according to our use. But most of the file formats don’t record the number of dropped packets.

If we are exiting without saving the current capture file then we will be prompted with a message to save the file first to prevent data loss. This warning can be disabled in the preferences. Wireshark uses the **pcapng** file format as the default format to save captured packets.

**Save Capture File As Dialogue Box:**

The “Save Capture File As” dialogue box allows us to save the current capture to a file in our local system. The appearance of this dialogue box varies from system to system, but the functionality is the same across all systems.

* Windows:



While saving, we can decide on many formats of the capture file by clicking on the **“Save as”** drop-down box. Below are the following file formats in which a capture file can be saved by Wireshark :

* **pcap:**The libpcap packet capture library uses pcap as the default file format.  The tcpdump, \_Snort, Nmap, and Ntop also use pcap as the default file format.
* **pcapng:** Wireshark 1.8 or later uses the pcapng file format as the default format to save captured packets.
* **Microsoft Network Monitor:**NetMon (\*.cap)
* **Network Associates Sniffer:** DOS (\*.cap,\*.enc,\*.trc,\*.fdc,\*.syc),Windows (\*.cap)
* Cinco Networks NetXray captures (\*.cap
* Novell LANalyzer (\*.tr1)
* Oracle (previously Sun) snoop (\*.snoop,\*.cap)
* Visual Networks Visual UpTime traffic (\*.\*)
* Symbian OS btsnoop captures (\*.log)

Some file formats may not be available depending on the packet types captured. The **“Compress with gzip”** option will compress the capture file as it is being written to disk. We can also convert a capture file format to another format by opening it and saving it in a different format.

**Result:**

Hence to identify ARP and save with .pcap file in wireshark is done and output is verified.