CSE3501-Information Security Analysis and Audit Lab

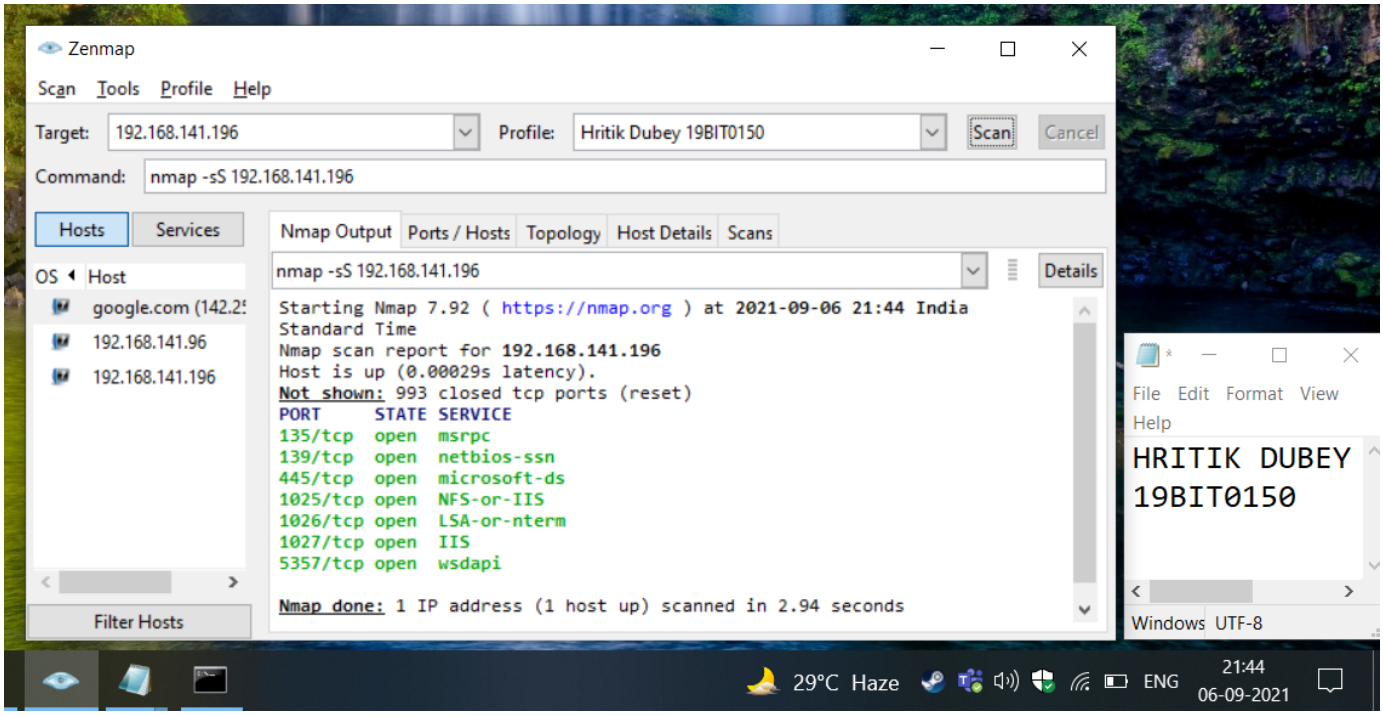
NAME- HRITIK DUBEY REG NO-19BIT0150 SLOT- L41+L42

DIGITAL ASSIGNMENT 1 Faculty : Dr. Priya V

1. A security engineer of VIT- Vellore is attempting to map a company's internal network and he wants to perform the stealth scan. Which NMAP command would the security engineer use? Show the results

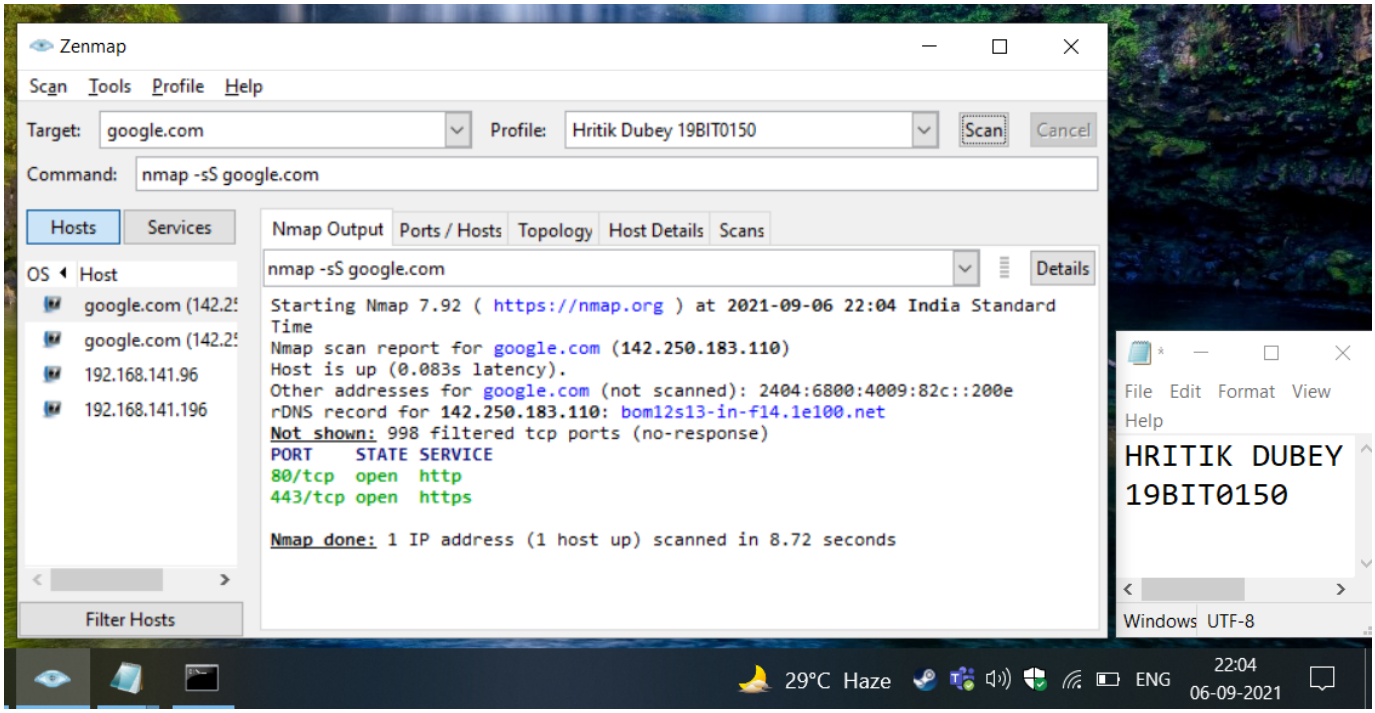
In order to perform a stealth scan we use Nmap -sS command in the format
: Nmap –Ss IP address

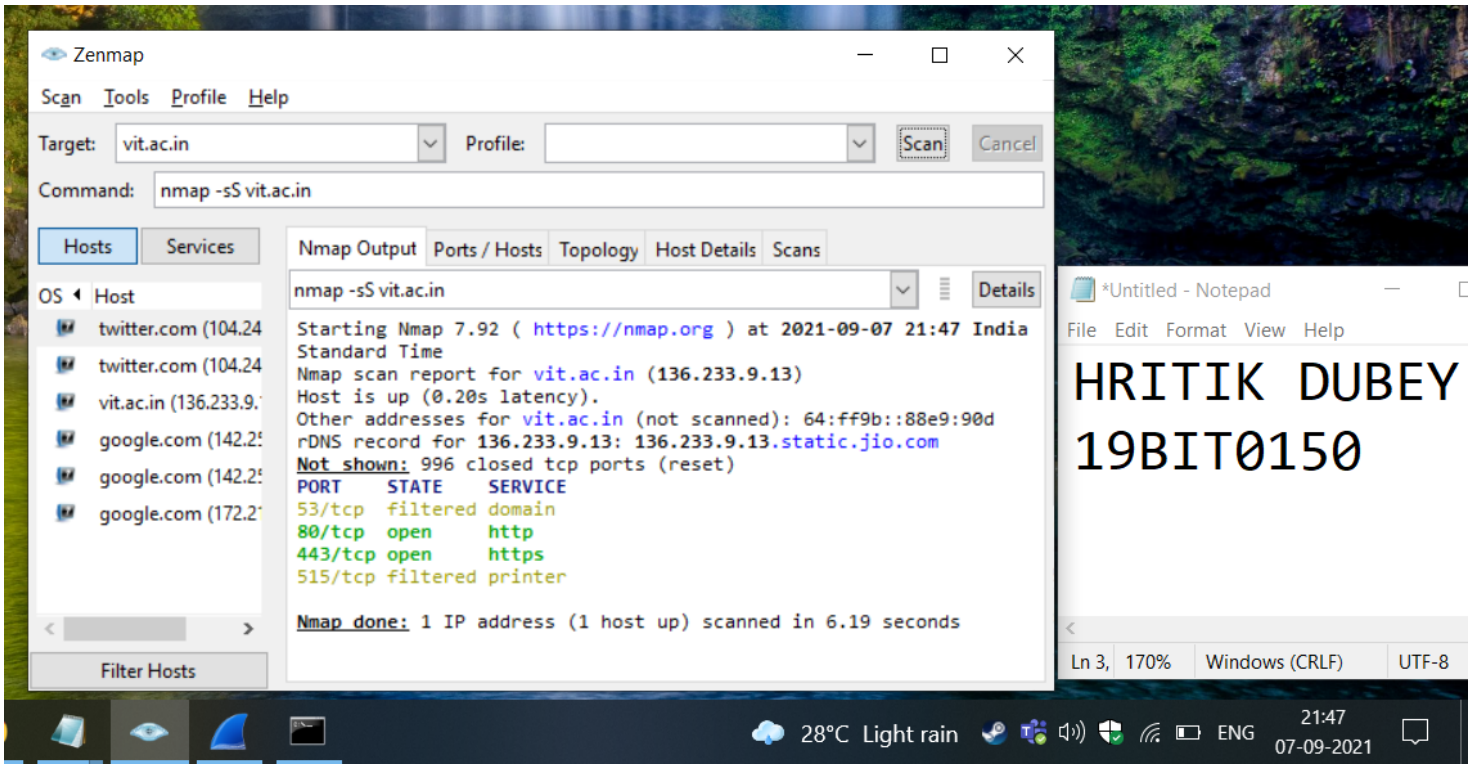
Let's set the target ip as my own IP address.



As we can see, Stealth search scan ip for port state service.

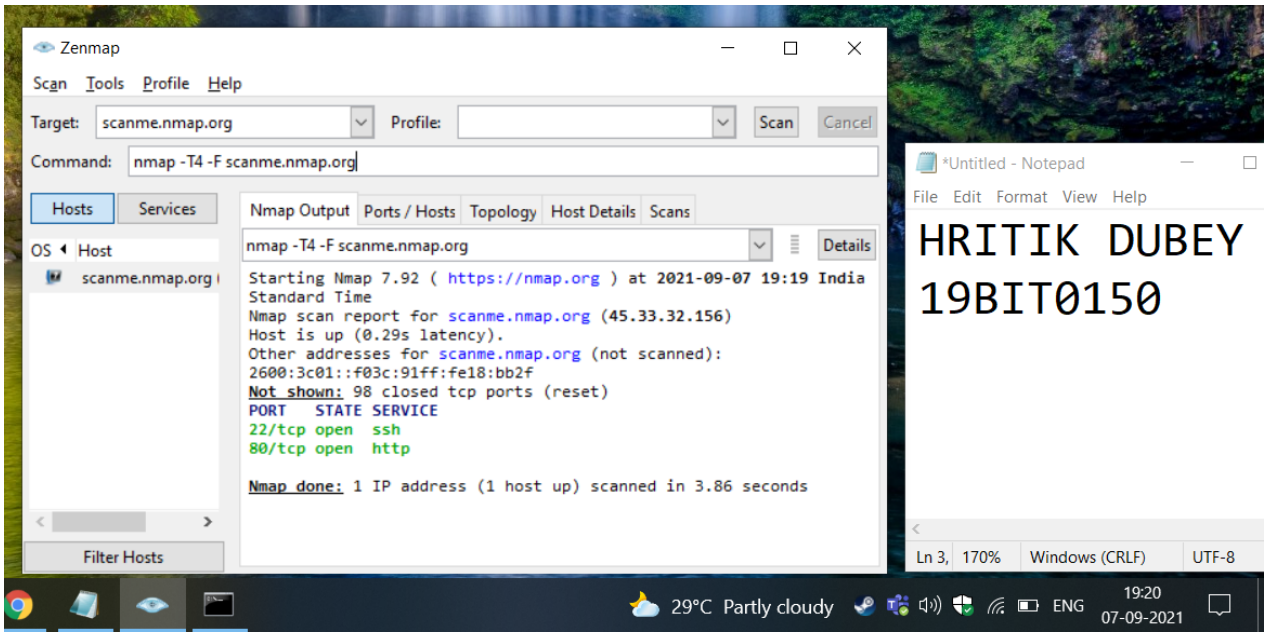
Trying with google.com



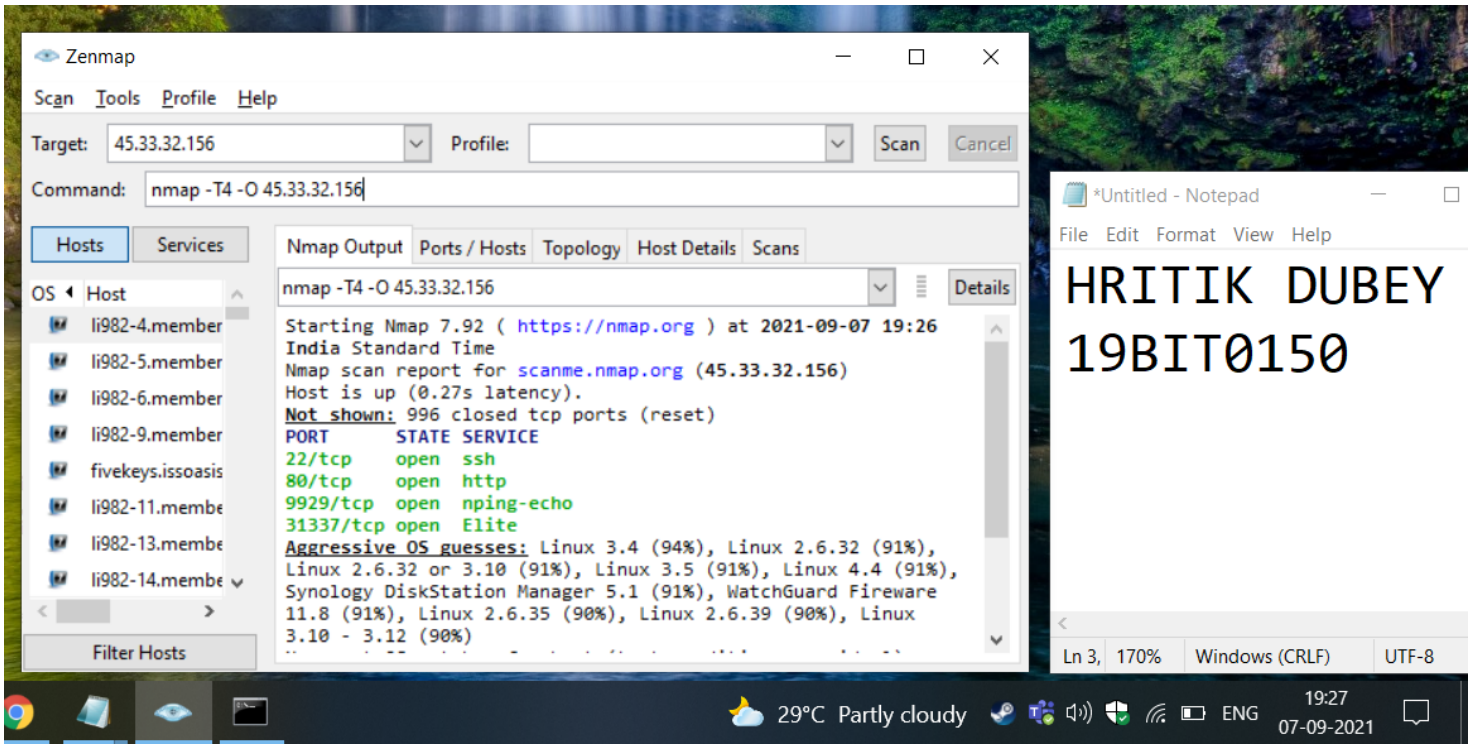


2. What is the best Nmap command to use when you want to list all devices in the same network quickly? Considering the server as scanme.nmap.org.

Nmap command - nmap -T4 -F will give us faster quick results. So it is the BEST COMMAND

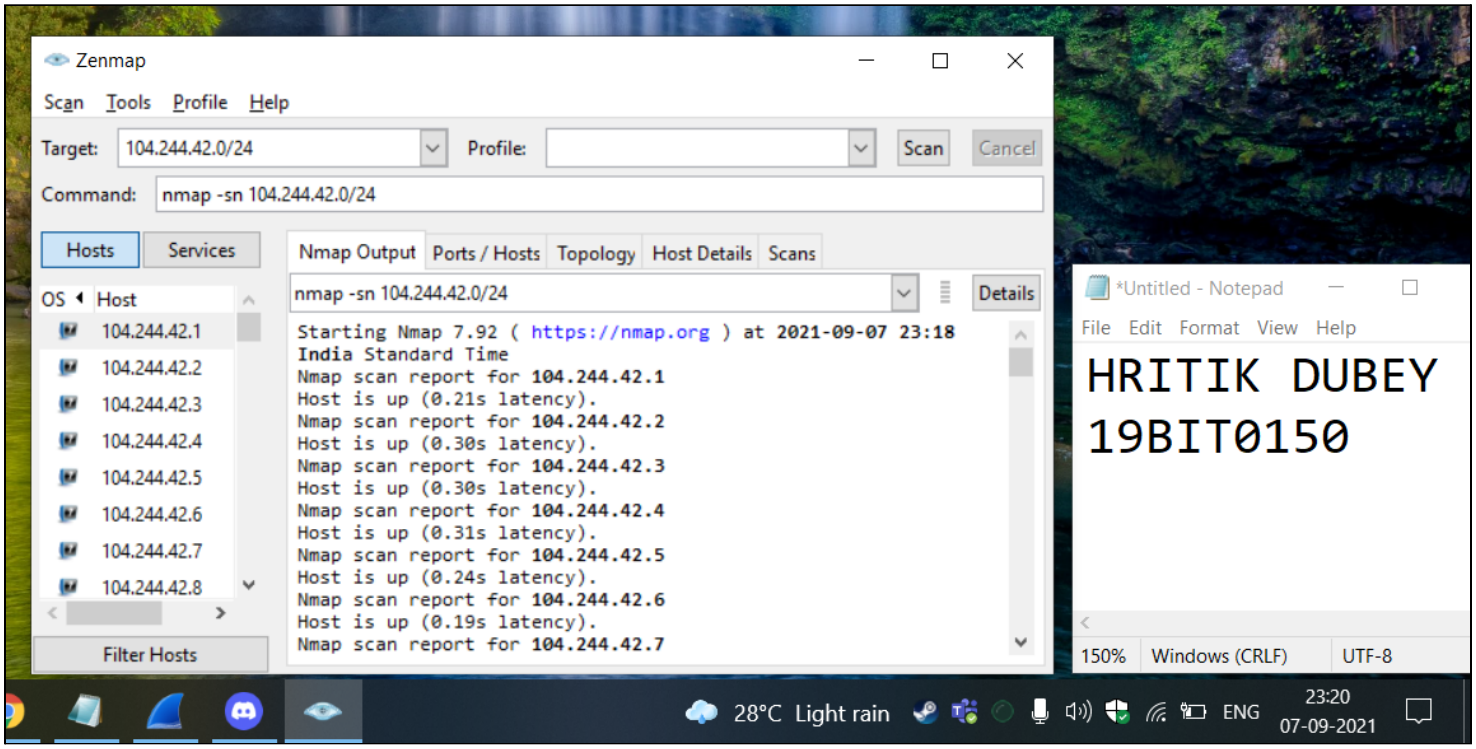


Trying with Nmap command - nmap -T4 -O IP Address - 45.33.32.156 .This gives more ports

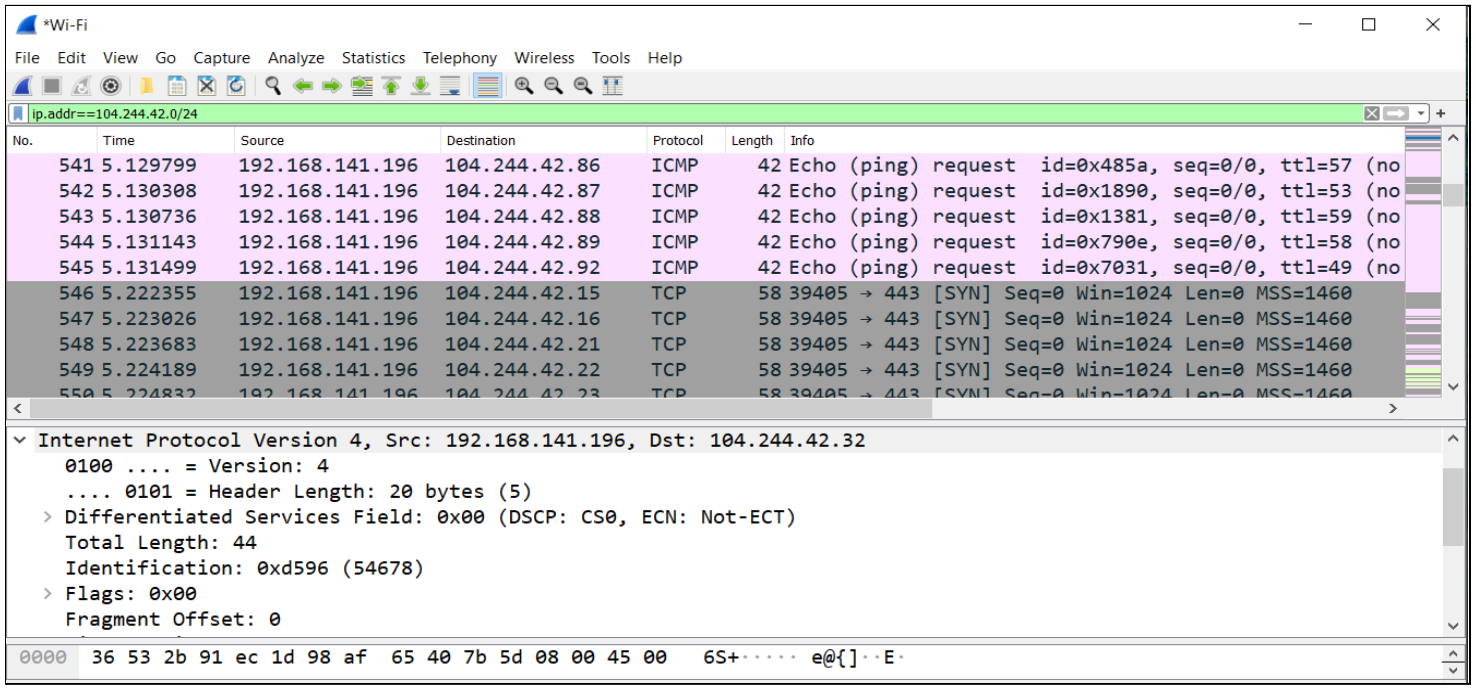


3. A hacker is attempting to see which IP addresses are currently active on the "twitter" website. Which NMAP switch would the hacker use? In Wireshark, capture the packets that contain twitter and show the results

Nmap -sp 104.244.42.0/24 Twitter.com Ip -104.244.42.129 from netcraft

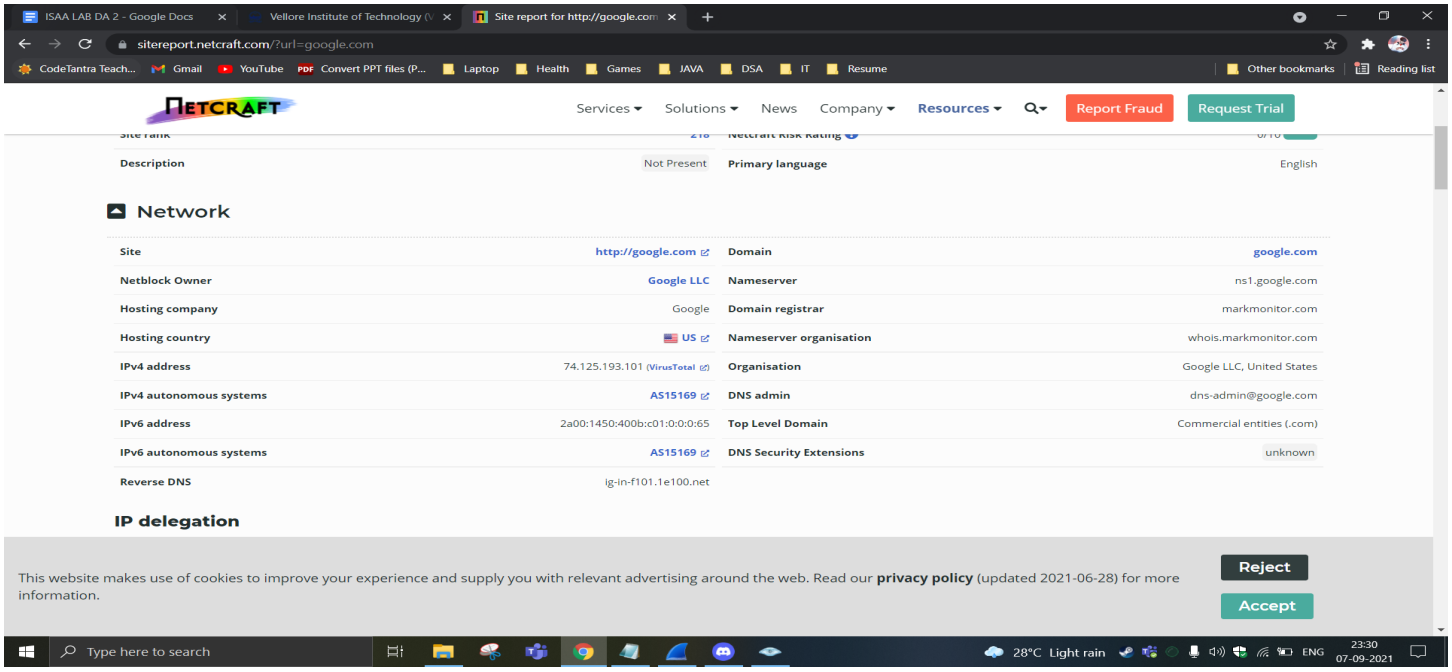


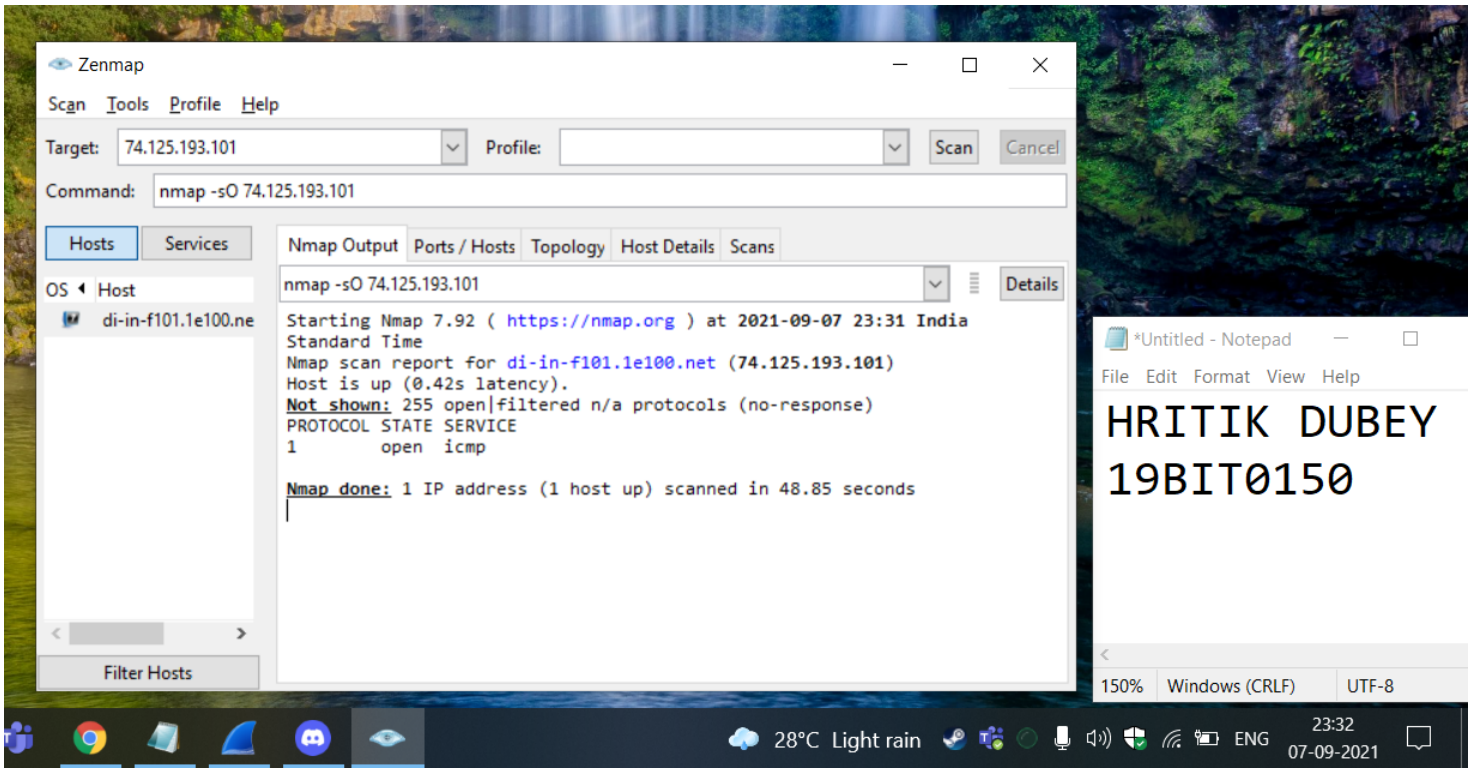
Applying filter ip.addr==104.244.42.0/24 on wireshark to get packet containing twitter

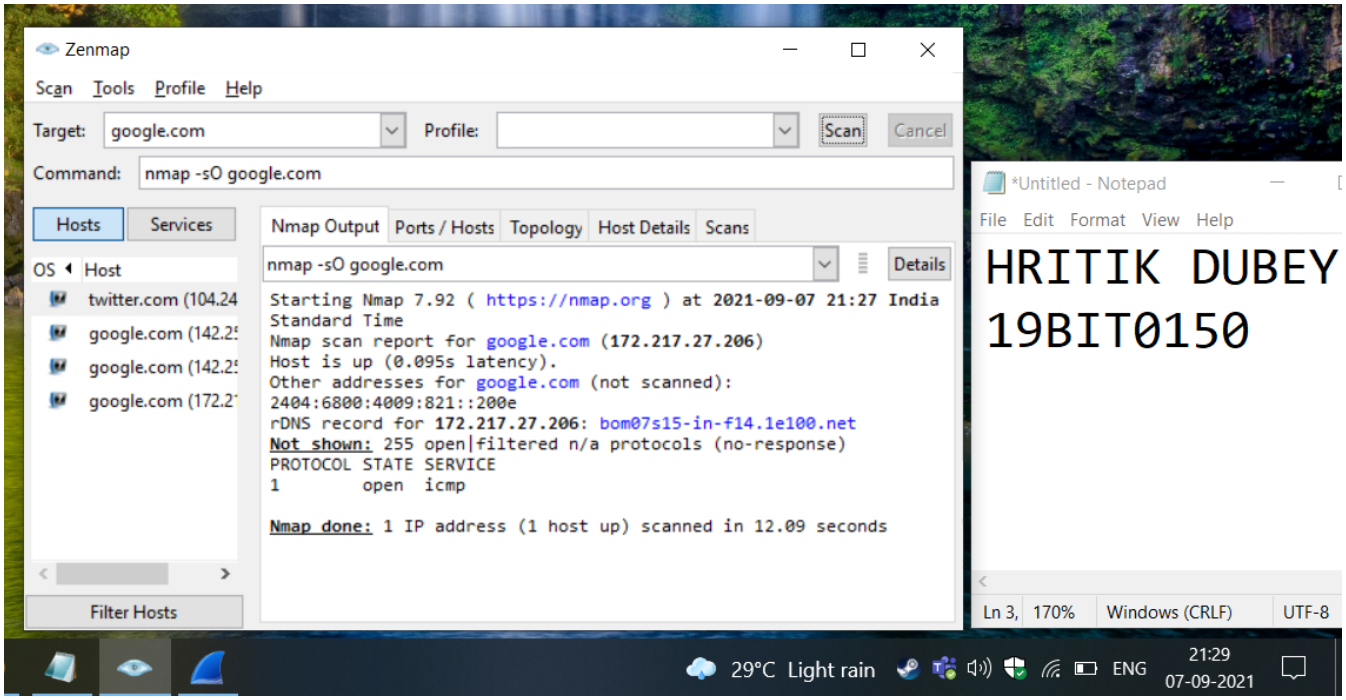


4. A hacker is attempting to see which ports have been left open on a Google.com network. Which NMAP switch would the hacker use and how can the hacker filter using Wireshark and get the packets belonging to a specific protocol like HTTP, TCP, DNS and UDP and analyze the packet structure. Show the results

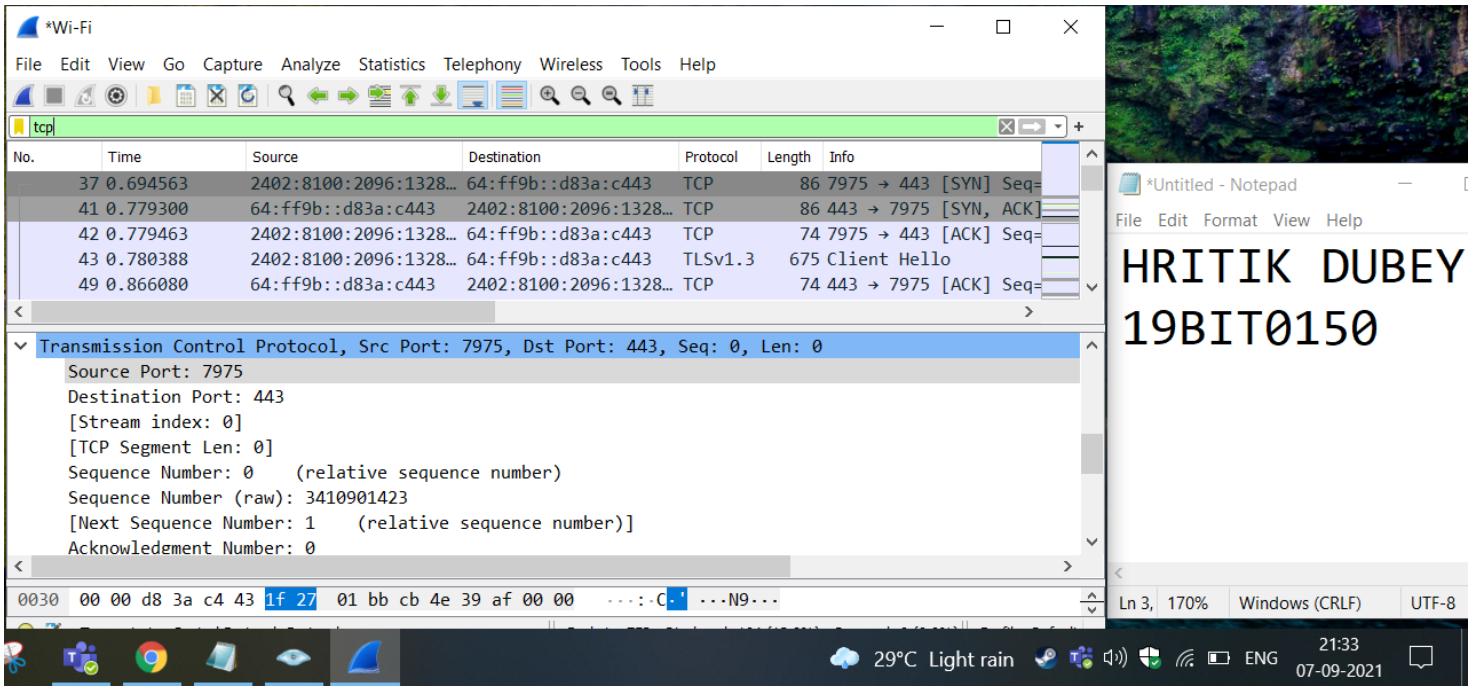
Nmap -sO command will be used to see which ports are open here. We will first use Nmap to find open ports. Getting IP from Netcraft.com as 74.125.193.101





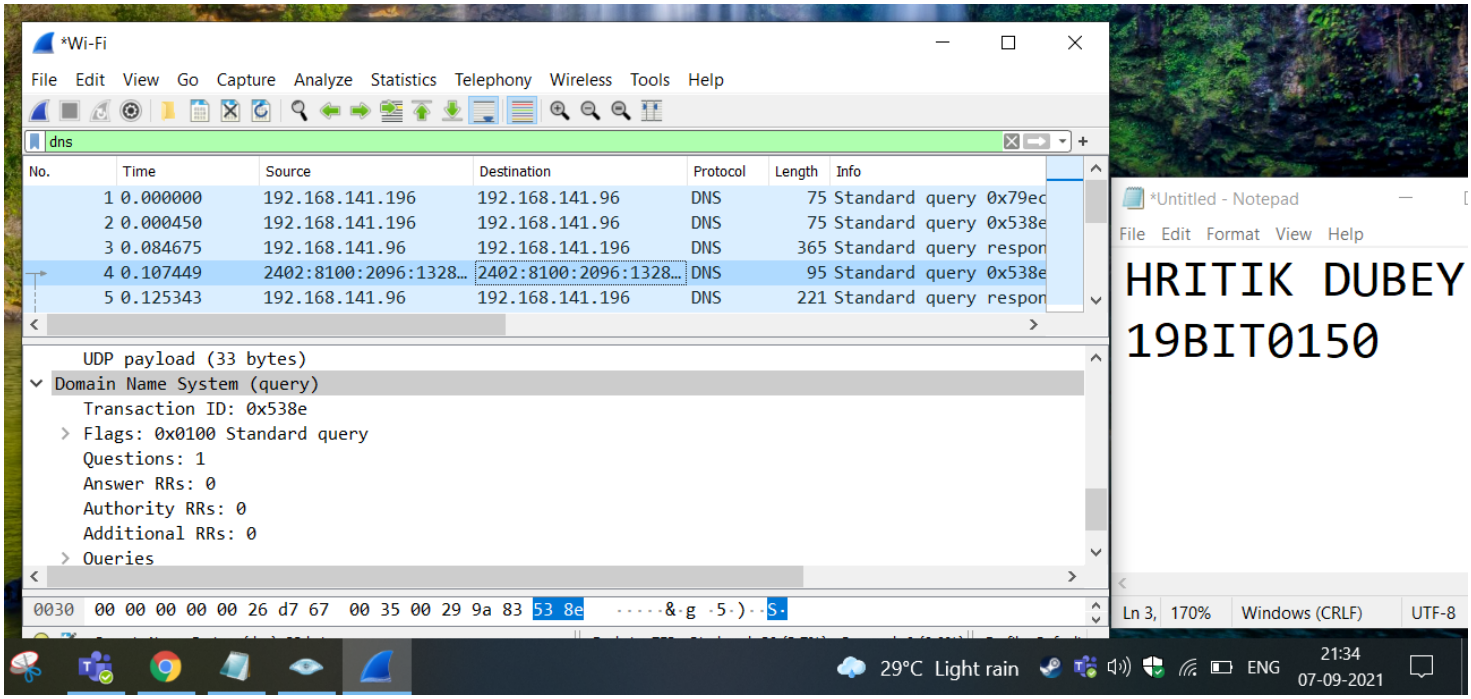


Now we will use Wire shark filter, TCP, UDP, DNS to filter the packets.

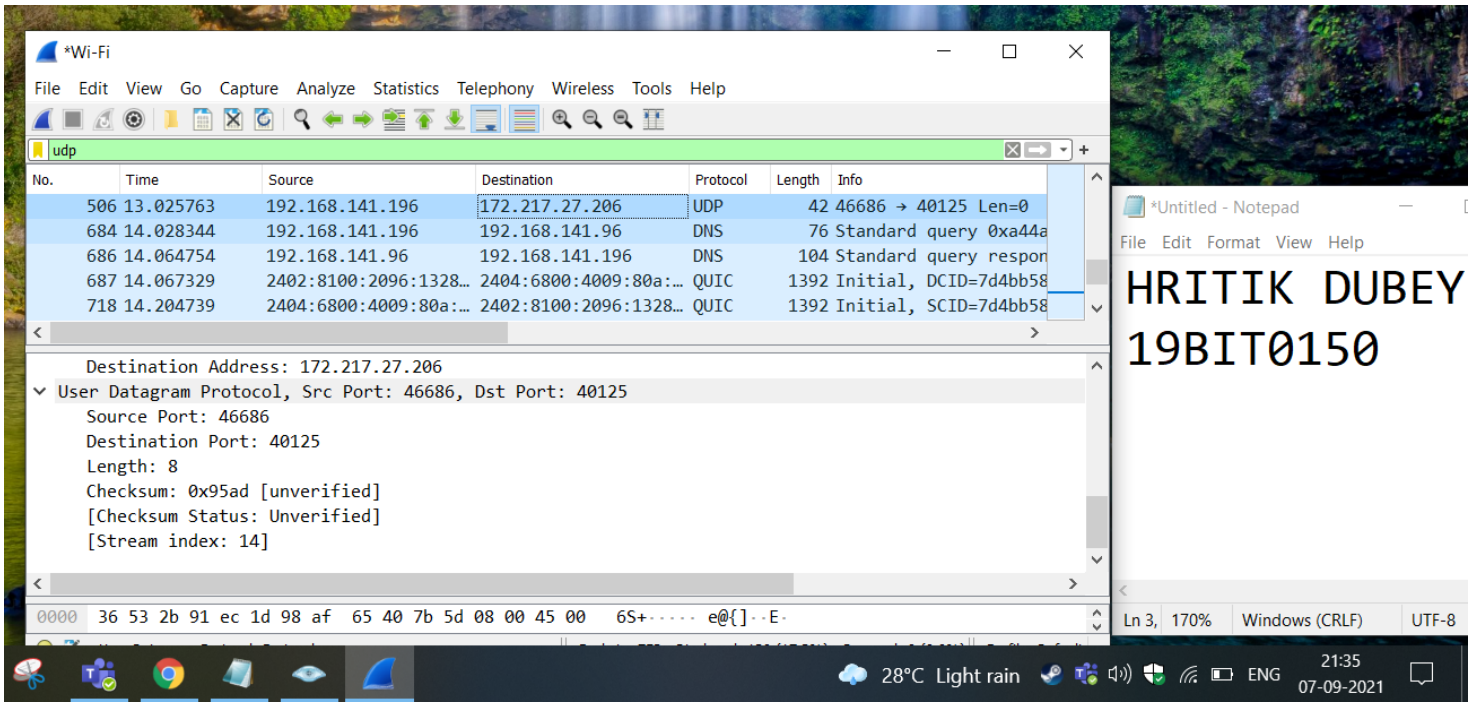


For the TCP protocol as we can see in the packet structure, Transmission control protocol section we are provided with source Port & Destination Port.

For DNS we can see in the packet structure, Domain Name System containing queries.



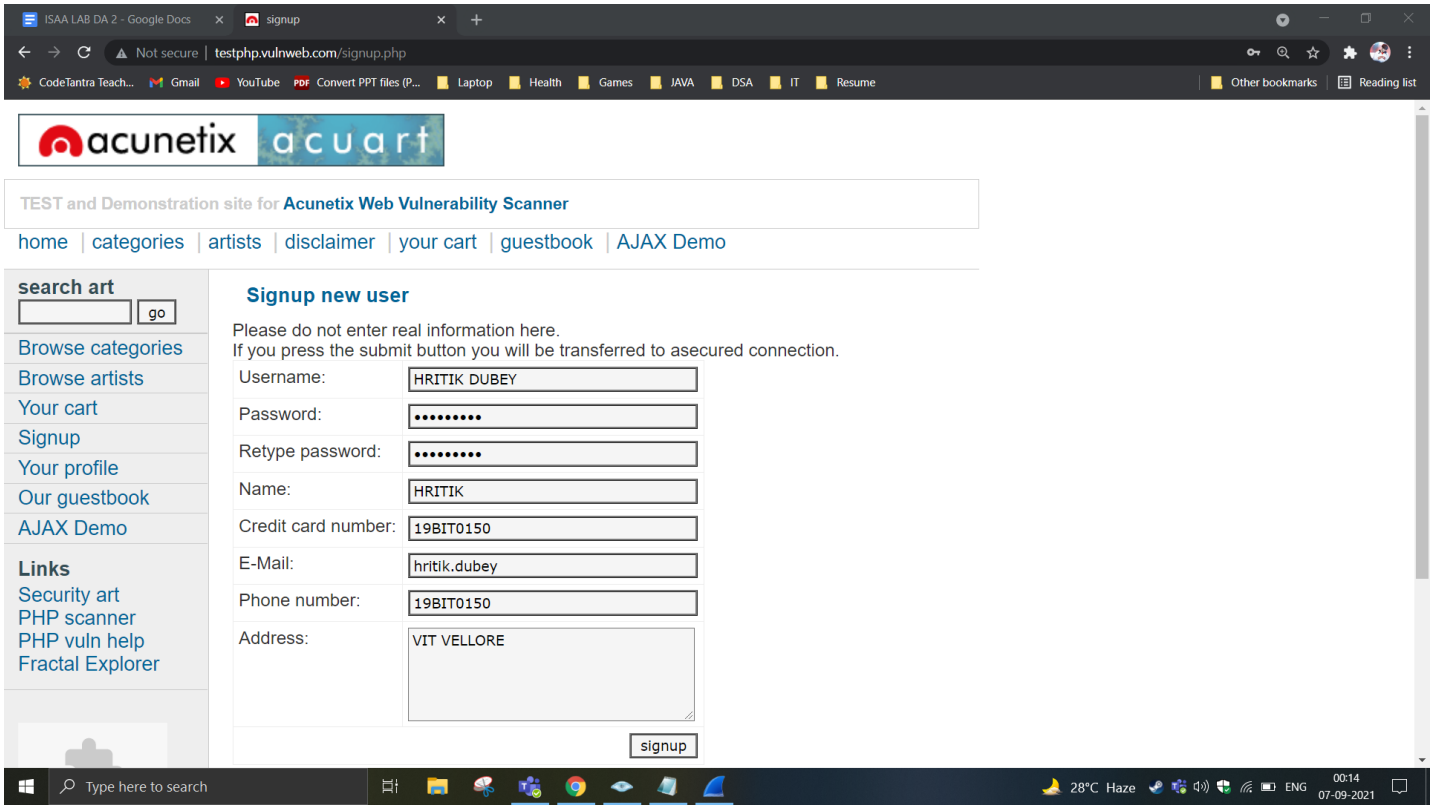
For the UDP protocol in the packet structure User Datagram Protocol we are given Source/Dest Port



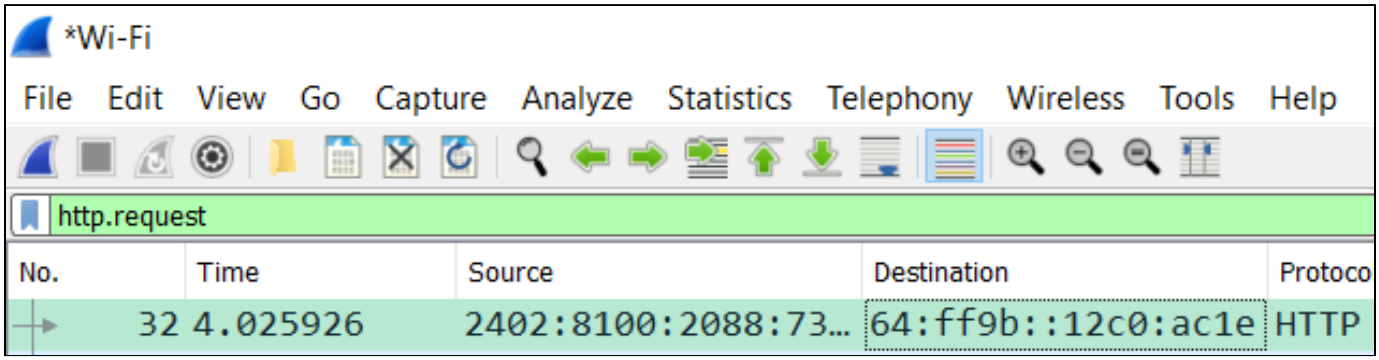
Hence for each protocol we have filtered the packets UDP,TCP & DNS while using -sO command on Nmap.

5.Choose any vulnerable website from "http://www.vulnweb.com/". Create an account having the username with your name and register number. Grab the username and password in Wireshark.

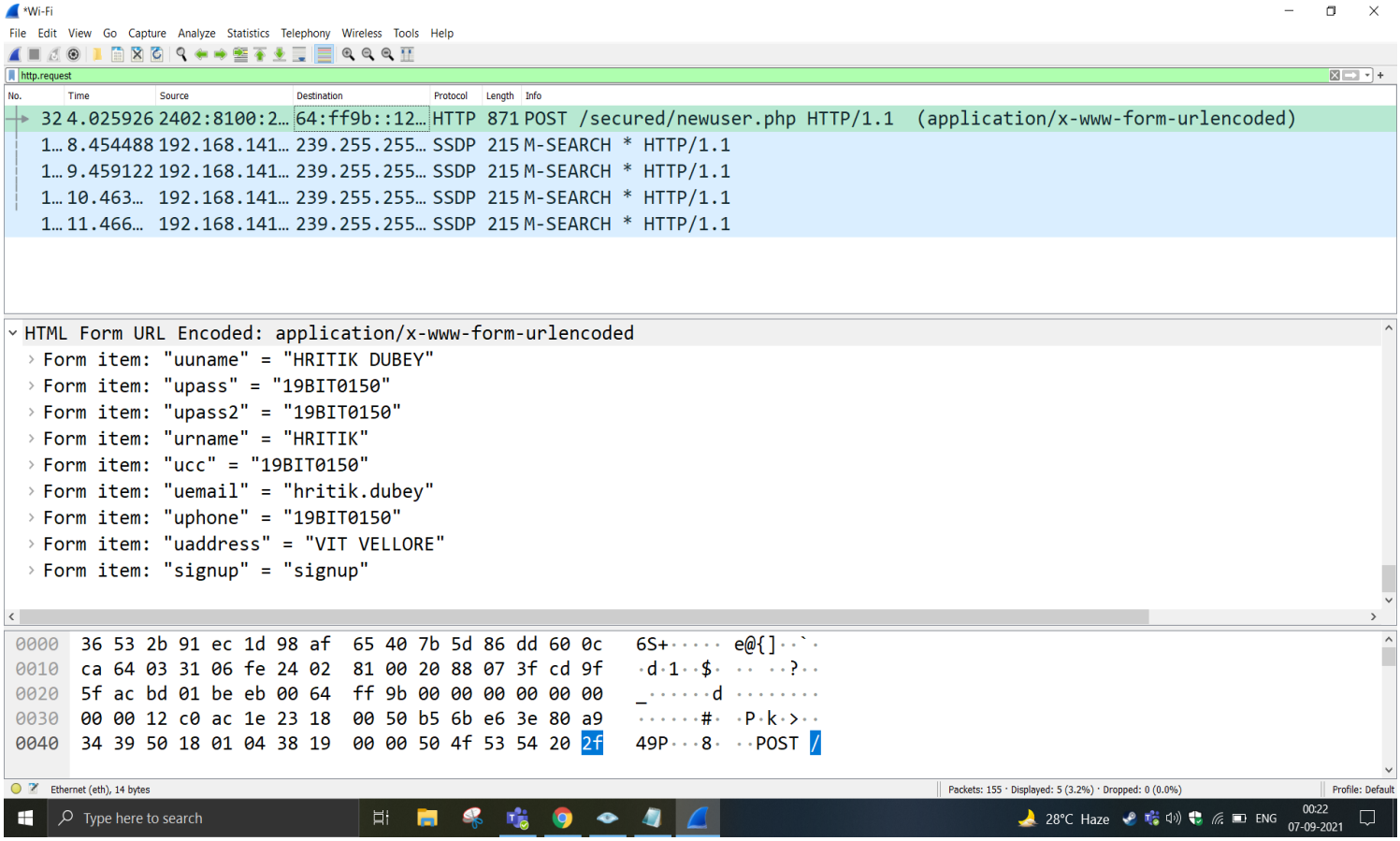
First we will create a sign up form on http://testphp.vulnweb.com/signup.php. The Http protocol used here is using POST form method with less security hence it can be extracted in packet.



Now we will apply a filter on Wireshark to find http.request packet.



Now we will find the form data, in the HTML form URL Encoded section.



As we can see that the form data which we will fill can now be seen in Packet analysis through wire shark.