END SEMESTER ASSESSMENT (ESA)

B.TECH. (CSE)

IV SEMESTER

UE20CS253-COMPUTER NETWORKS

INDUSTRY PROBLEM PROJECT REPORT

ON

WEB SERVER MONITORING TECNIQUES

SUBMITTED BY

NAME	SRN
AMISHA MATHEW	PES2UG20CS038
ANANYA ADIGA	PES2UG20CS043
APOORVA NARONIKAR	PES2UG20CS062

JANUARY – MAY 2022

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

PES University, Electronic City Campus,

Bengaluru – 560100, Karnataka, India

ABSTRACT OF THE PROJECT

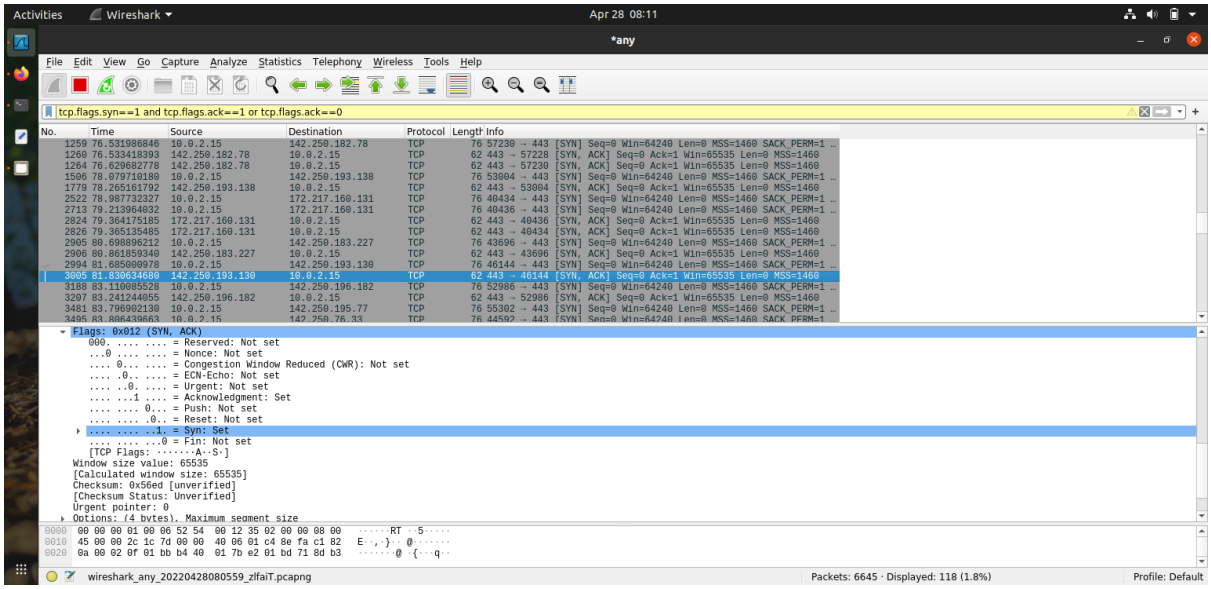
Monitoring helps track the popularity and growth of websites and web applications. Traffic and connection metrics offer direct insight into site activity, including the number of active users and the duration of each session. This data can help you develop plans for scaling your website, optimizing your application, or deploying other services to support the increased demand. monitoring will alert you to any errors or failures that could result in downtime.

Web servers monitoring techniques are used to monitor –

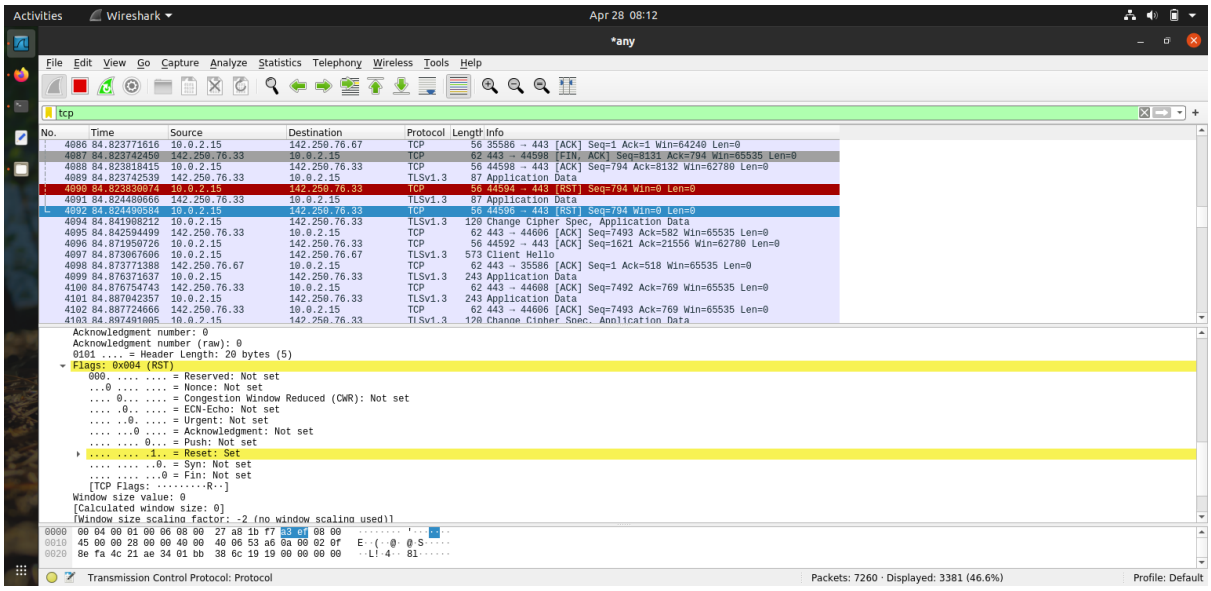
- **Connections** to clients and other servers on the network
- **Requests** for host resources such as CPU, RAM, and disk access
- **Traffic** being transferred to and from the server at any given time
- **Availability** of other web servers for proxying requests

Tools like wireshark, netstat, nmap to be used for achieving the required output

1.Technique to monitor TCP SYN requests to the web server with wireshark output

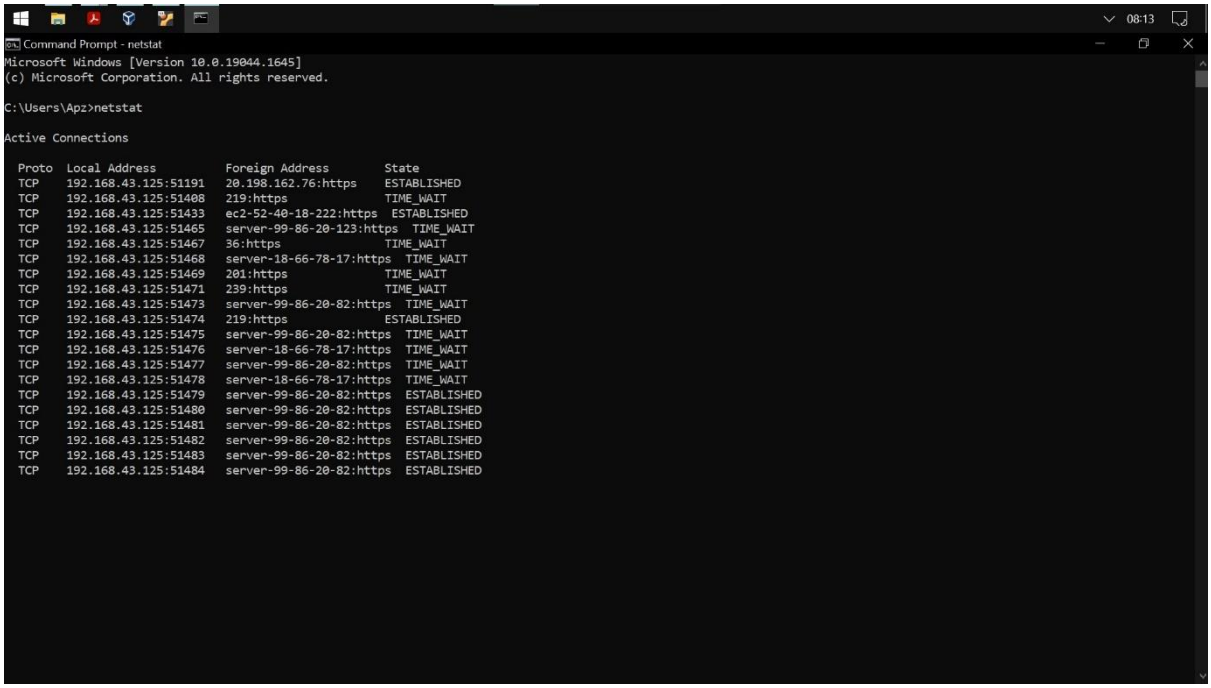


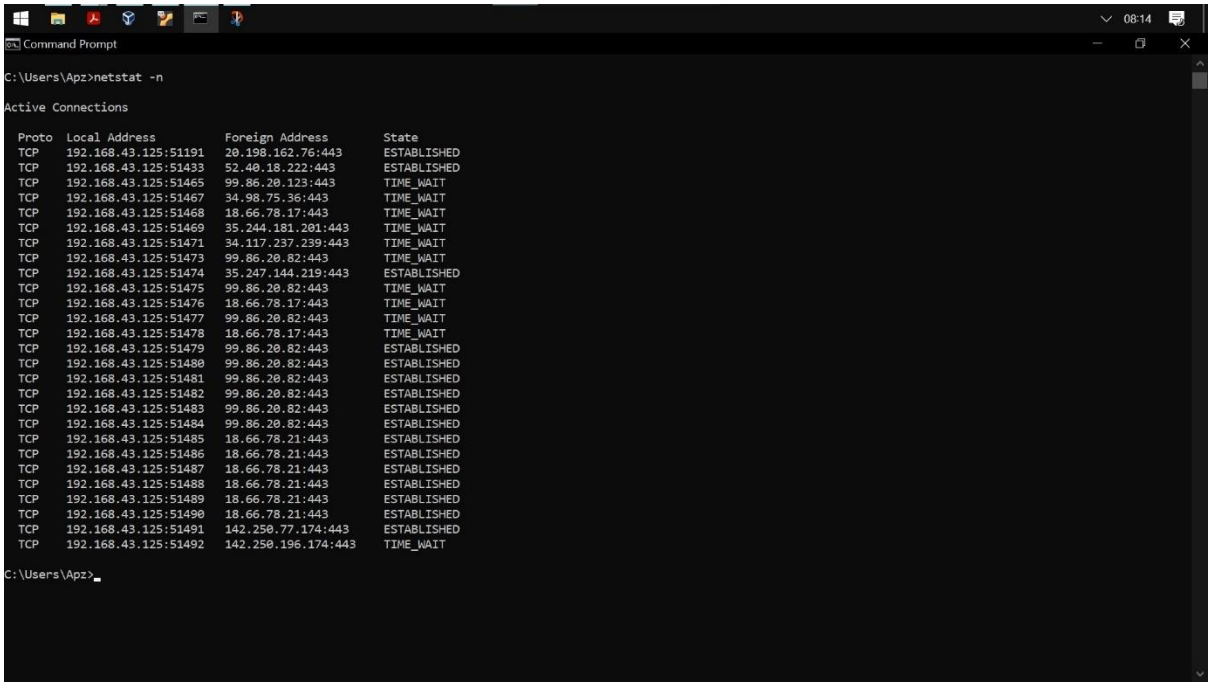
2.Technique to monitor TCP reset connections sent to and from the Web Server with wireshark output



3. Technique to monitor established open connections on a Web Server with netstat output

You use the netstat command to generate displays that show network status and protocol statistics. Netstat (Network Statistics) is a command-line tool available on most operating systems that will display the current status of TCP and UDP conversations

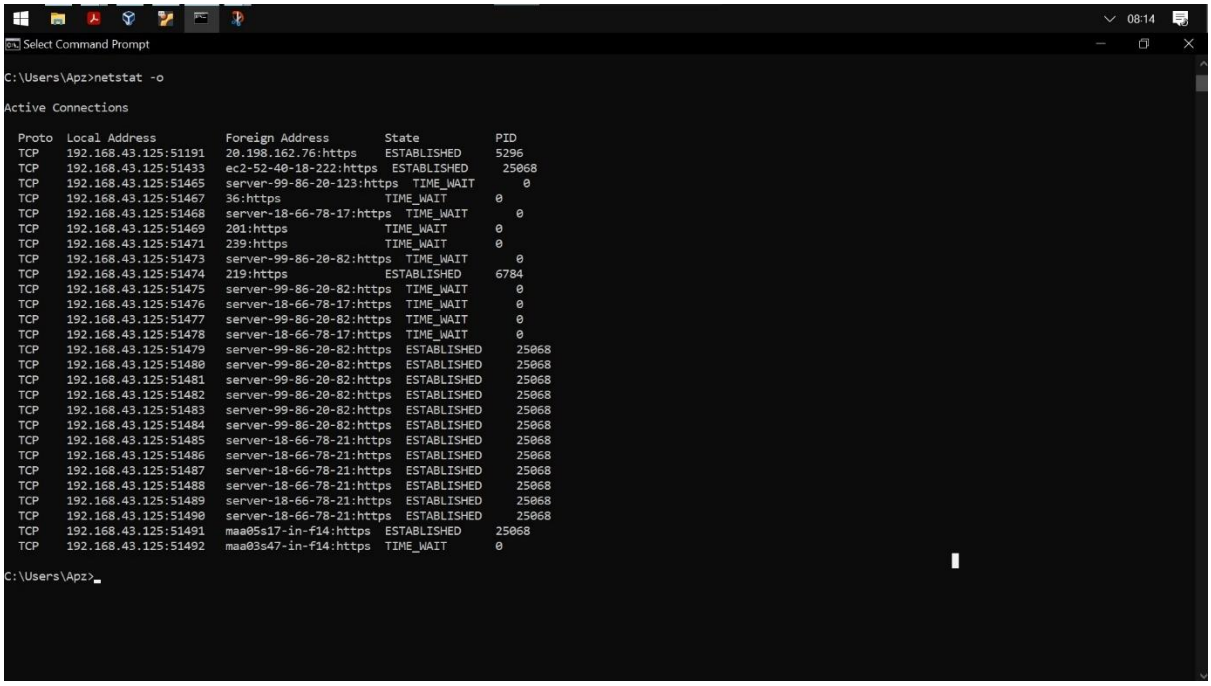




4. Technique to monitor TCP half open connections on the Web Server with netstat output

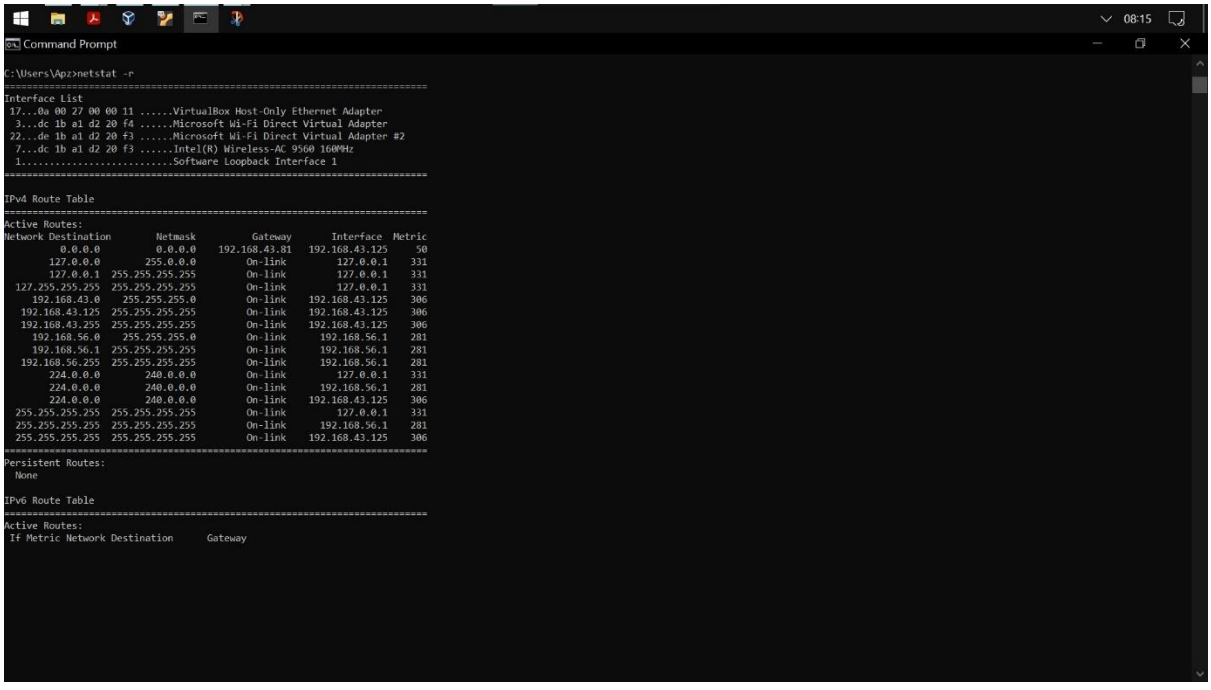
netstat- networking tool used for troubleshooting and configuration, that can also serve as a monitoring tool for connections over the network

netstat -o

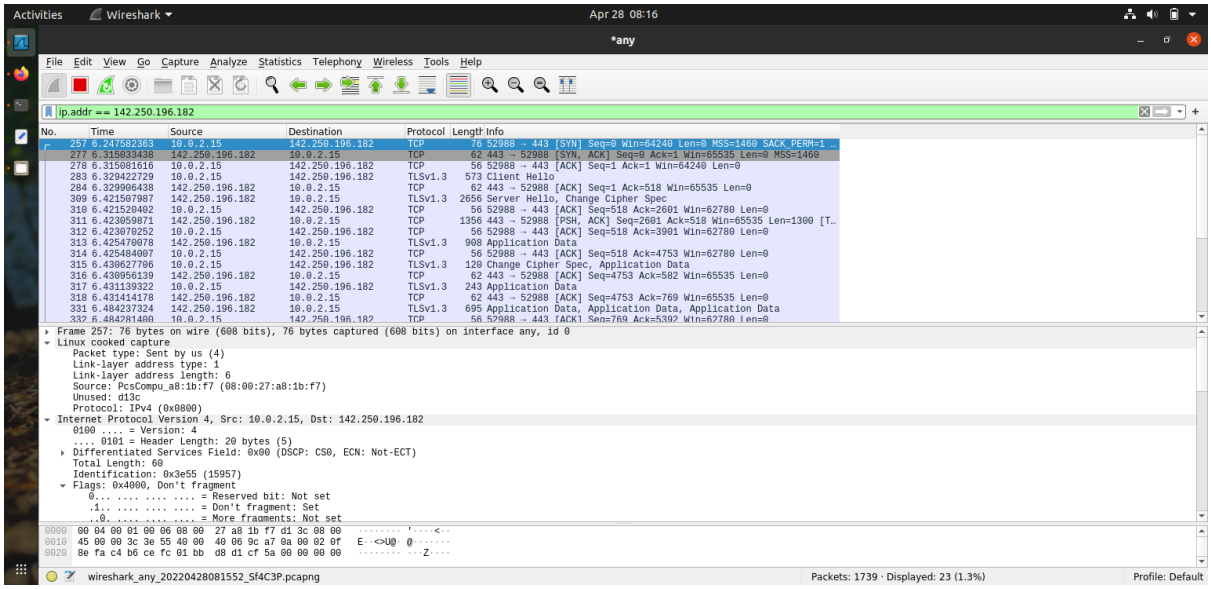


netstat -r : routing table for ipv4 and ipv6

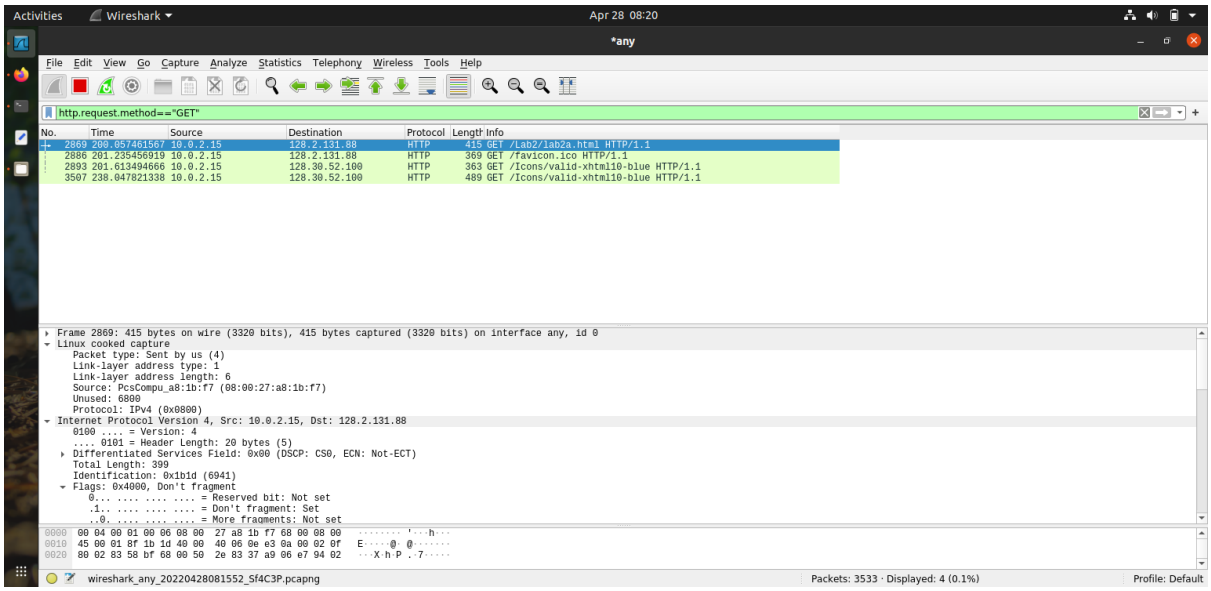
netstat lets you see which machines your machine is talking to over the network



5. Technique to monitor requests to a specific application on the Web server with wireshark output

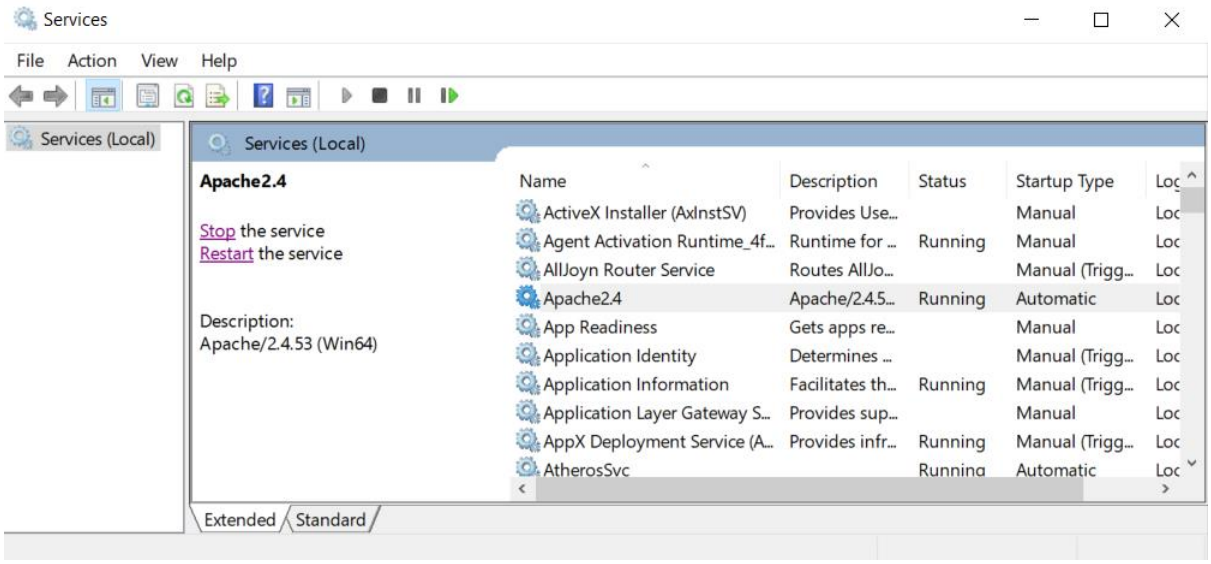


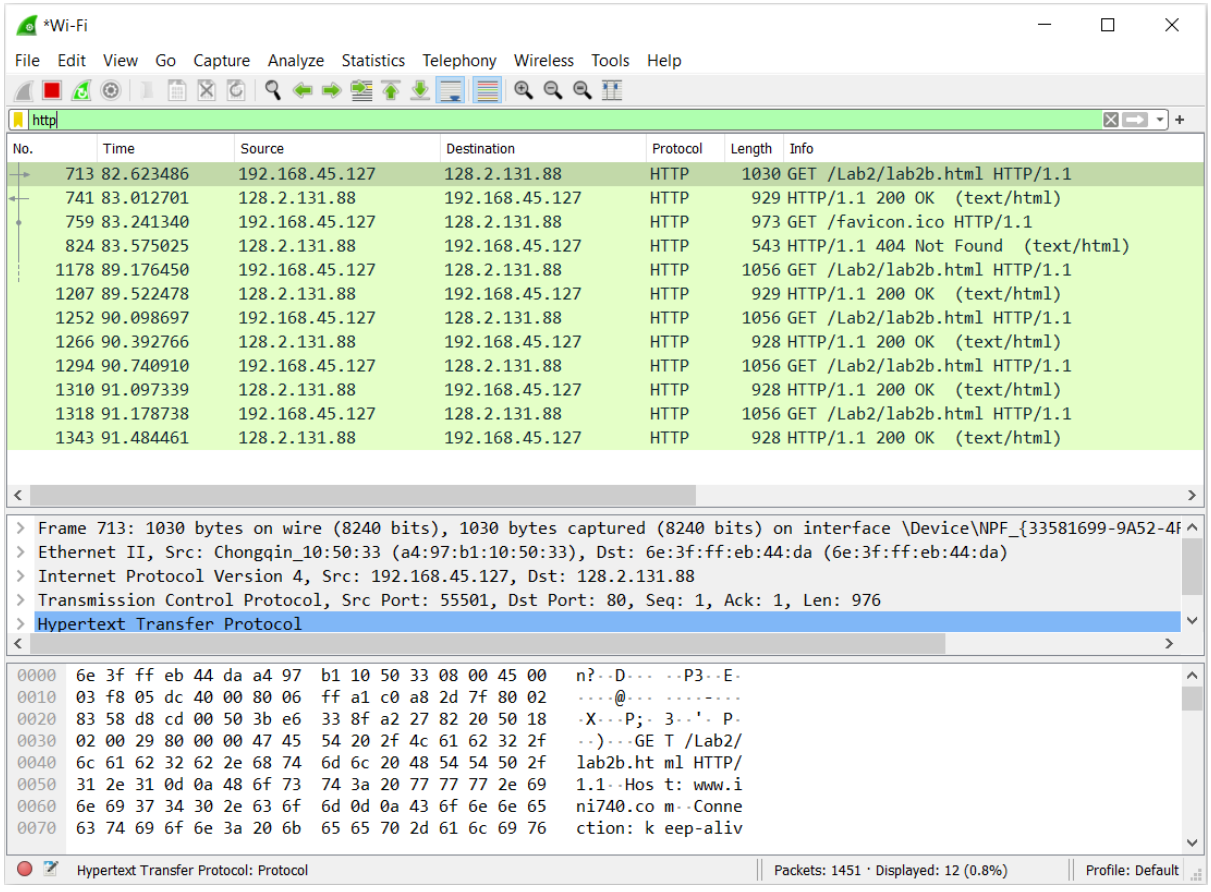
6. Technique to monitor HTTP GET requests to the web server with wireshark output



(i)Apache server

Free and open-source cross platform web service software. It is responsible for accepting directory requests from users and sending them their information



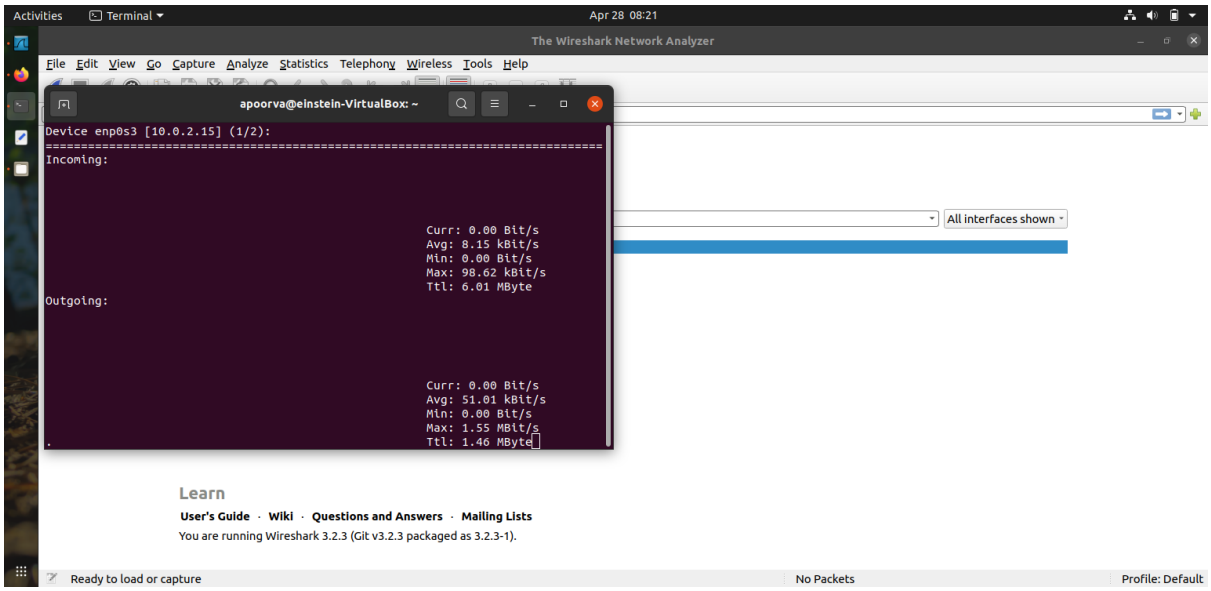


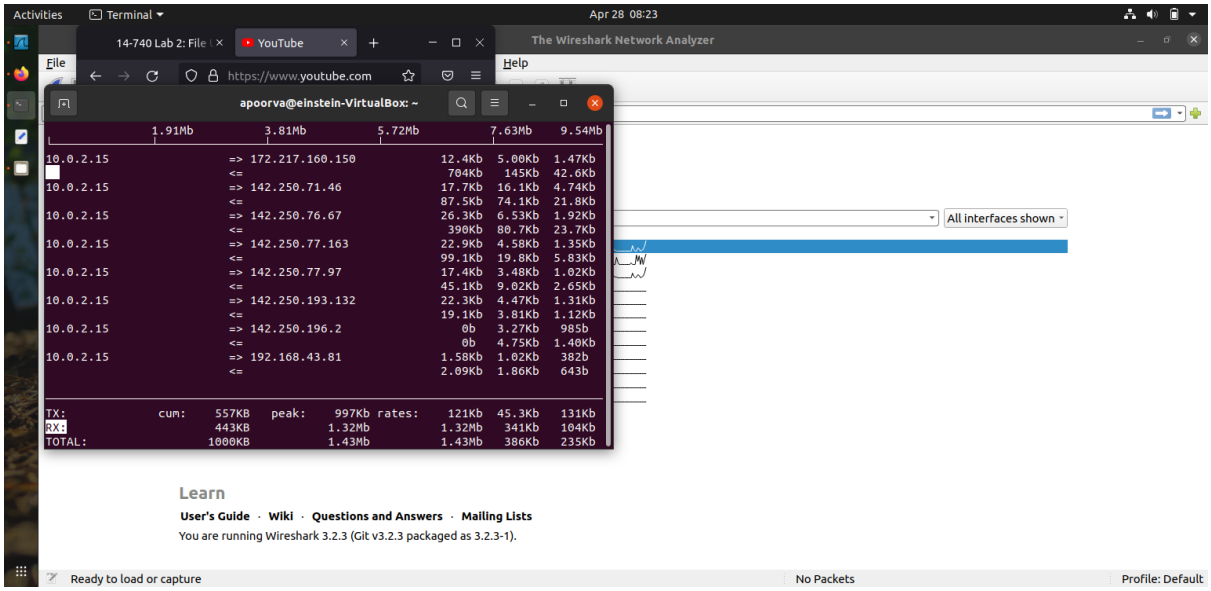
7. Technique to monitor server bandwidth with netstat output

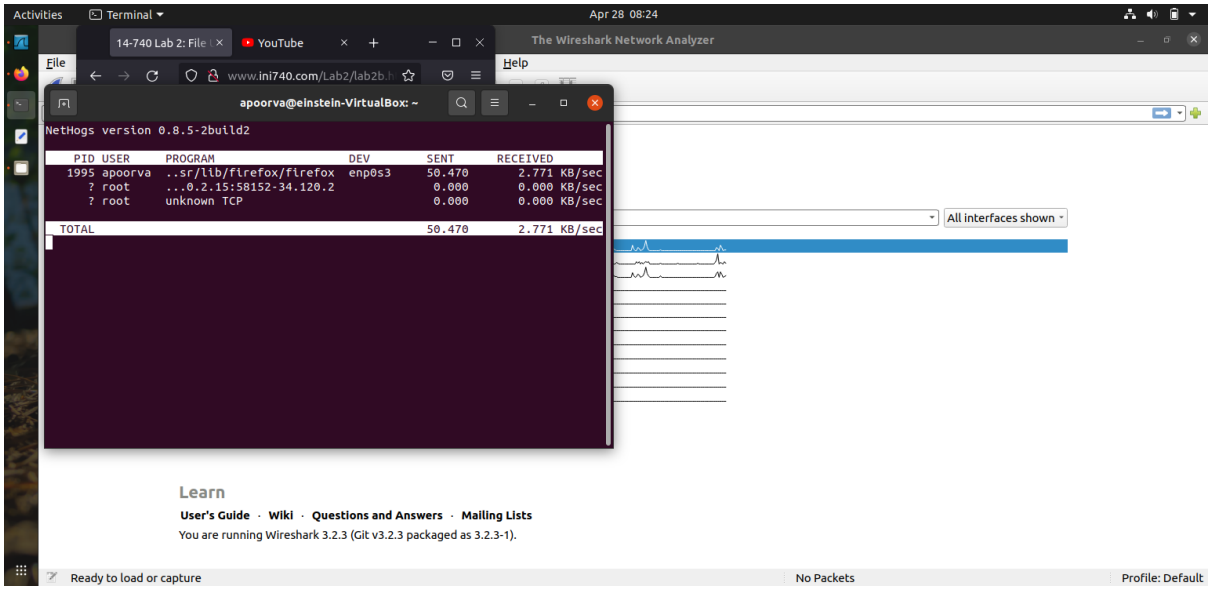
nload: allows users to monitor the incoming and outgoing traffic separately

iftop: measures data flowing through individual socket connections

nethogs: shows the bandwidth used by individual processes and sorts the lists by putting the most intensive processes on top


Activities
Terminal
Apr 28 08:21
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
apoorva@einstein-VirtualBox: ~
Device enp0s3 [10.0.2.15] (1/2):
Incoming:
Curr: 0.00 Bit/s
Avg: 8.15 kBit/s
Min: 0.00 Bit/s
Max: 98.62 kBit/s
Ttl: 6.01 MByte
Outgoing:
Curr: 0.00 Bit/s
Avg: 51.01 kBit/s
Min: 0.00 Bit/s
Max: 1.55 MBit/s
Ttl: 1.46 MByte
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.2.3 (Git v3.2.3 packaged as 3.2.3-1).
Ready to load or capture
No Packets
Profile: Default

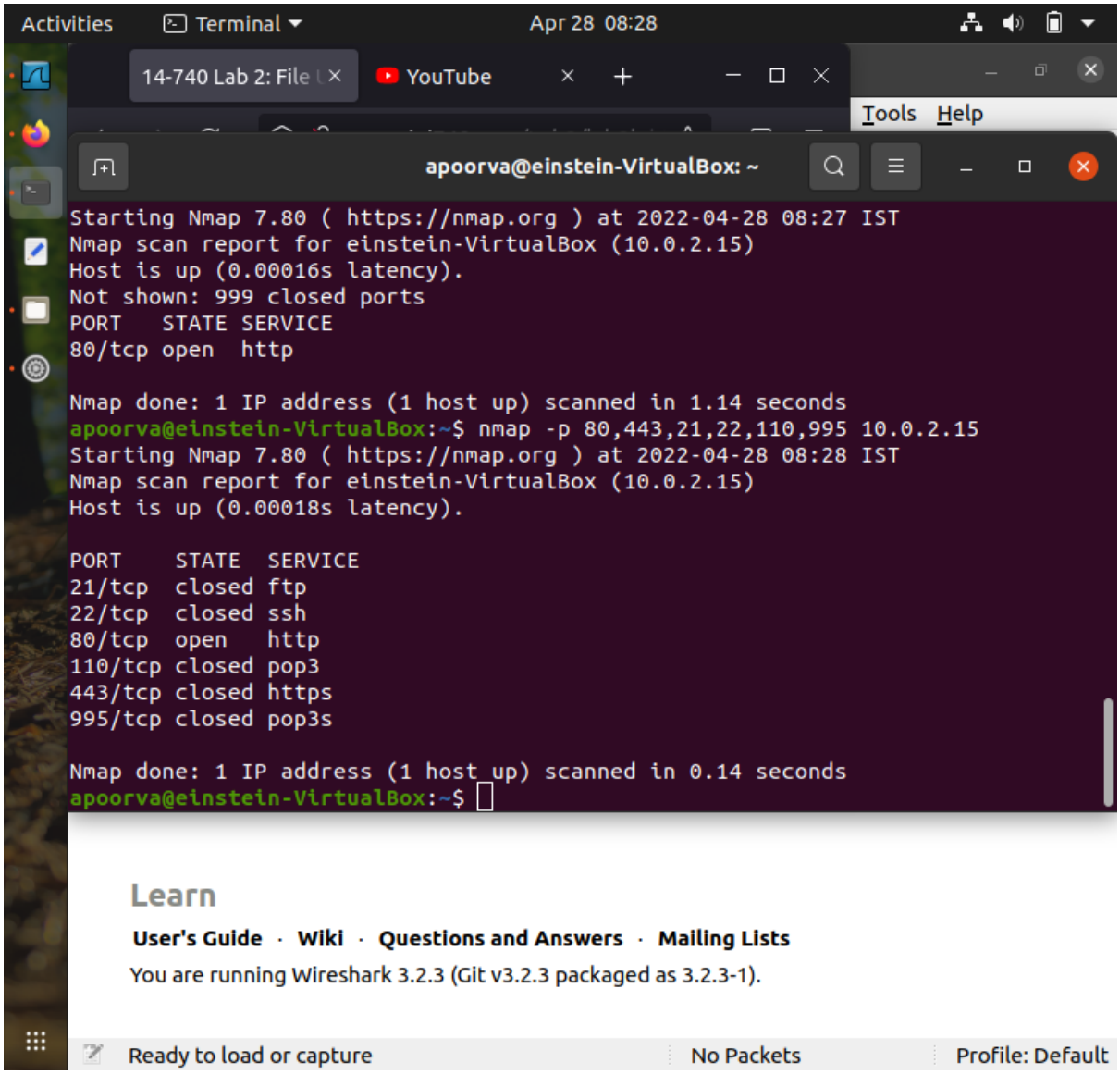

Activities
Terminal
Apr 28 08:23
14-740 Lab 2: File
YouTube
https://www.youtube.com
The Wireshark Network Analyzer
File
Help
apoorva@einstein-VirtualBox: ~
1.91Mb 3.81Mb 5.72Mb 7.63Mb 9.54Mb
10.0.2.15 => 172.217.160.150 12.4Kb 5.00Kb 1.47Kb
<= 704Kb 145Kb 42.6Kb
10.0.2.15 => 142.250.71.46 17.7Kb 16.1Kb 4.74Kb
<= 87.5Kb 74.1Kb 21.8Kb
10.0.2.15 => 142.250.76.67 26.3Kb 6.53Kb 1.92Kb
<= 390Kb 80.7Kb 23.7Kb
10.0.2.15 => 142.250.77.163 22.9Kb 4.58Kb 1.35Kb
<= 99.1Kb 19.8Kb 5.83Kb
10.0.2.15 => 142.250.77.97 17.4Kb 3.48Kb 1.02Kb
<= 45.1Kb 9.02Kb 2.65Kb
10.0.2.15 => 142.250.193.132 22.3Kb 4.47Kb 1.31Kb
<= 19.1Kb 3.81Kb 1.12Kb
10.0.2.15 => 142.250.196.2 0b 3.27Kb 985b
<= 0b 4.75Kb 1.40Kb
10.0.2.15 => 192.168.43.81 1.58Kb 1.02Kb 382b
<= 2.09Kb 1.86Kb 643b
TX: cum: 557KB peak: 997Kb rates: 121Kb 45.3Kb 131Kb
RX: 443KB 1.32Mb 1.32Mb 341Kb 104Kb
TOTAL: 1000KB 1.43Mb 1.43Mb 386Kb 235Kb
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.2.3 (Git v3.2.3 packaged as 3.2.3-1).
Ready to load or capture
No Packets
Profile: Default

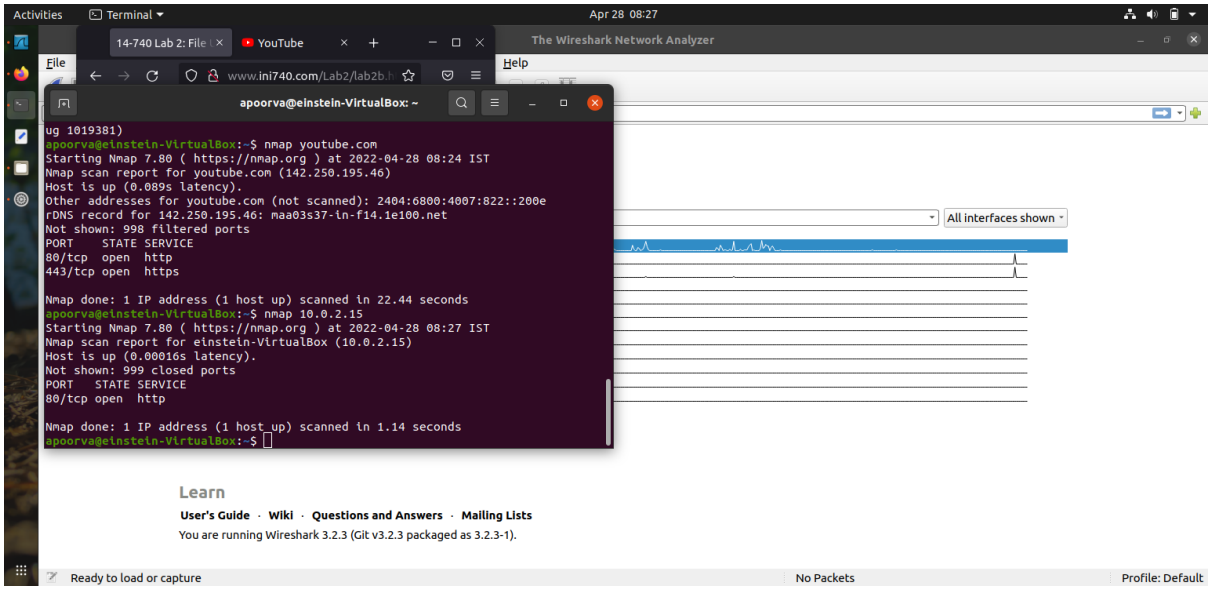


8. Technique to monitor the port status of a Web Server with nmap output

nmap- to map their networks

Nmap provides utilities to determine what hosts are available on the network, what ports are available on those hosts, what OS and firewalls are in use and much more. It has the capability to scan whole subnets and TCP port ranges, allowing engineers to spot problem devices and open sockets.


Activities
Terminal
Apr 28 08:28
14-740 Lab 2: File
YouTube
Tools Help
apoorva@einstein-VirtualBox: ~
Starting Nmap 7.80 (https://nmap.org) at 2022-04-28 08:27 IST
Nmap scan report for einstein-VirtualBox (10.0.2.15)
Host is up (0.00016s latency).
Not shown: 999 closed ports
PORT STATE SERVICE
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 1.14 seconds
apoorva@einstein-VirtualBox:~$ nmap -p 80,443,21,22,110,995 10.0.2.15
Starting Nmap 7.80 (https://nmap.org) at 2022-04-28 08:28 IST
Nmap scan report for einstein-VirtualBox (10.0.2.15)
Host is up (0.00018s latency).
PORT STATE SERVICE
21/tcp closed ftp
22/tcp closed ssh
80/tcp open http
110/tcp closed pop3
443/tcp closed https
995/tcp closed pop3s
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
apoorva@einstein-VirtualBox:~$
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.2.3 (Git v3.2.3 packaged as 3.2.3-1).
Ready to load or capture
No Packets
Profile: Default


Activities
Terminal
Apr 28 08:27
14-740 Lab 2: File
YouTube
The Wireshark Network Analyzer
File
Help
www.ini740.com/Lab2/lab2b.h
apoorva@einstein-VirtualBox: ~
ug 1019381)
apoorva@einstein-VirtualBox:~$ nmap youtube.com
Starting Nmap 7.80 (https://nmap.org) at 2022-04-28 08:24 IST
Nmap scan report for youtube.com (142.250.195.46)
Host is up (0.089s latency).
Other addresses for youtube.com (not scanned): 2404:6800:4007:822::200e
rDNS record for 142.250.195.46: maa03s37-in-f14.1e100.net
Not shown: 998 filtered ports
PORT STATE SERVICE
80/tcp open http
443/tcp open https
Nmap done: 1 IP address (1 host up) scanned in 22.44 seconds
apoorva@einstein-VirtualBox:~$ nmap 10.0.2.15
Starting Nmap 7.80 (https://nmap.org) at 2022-04-28 08:27 IST
Nmap scan report for einstein-VirtualBox (10.0.2.15)
Host is up (0.00016s latency).
Not shown: 999 closed ports
PORT STATE SERVICE
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 1.14 seconds
apoorva@einstein-VirtualBox:~$
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.2.3 (Git v3.2.3 packaged as 3.2.3-1).
Ready to load or capture
No Packets
Profile: Default