Assignment - 1

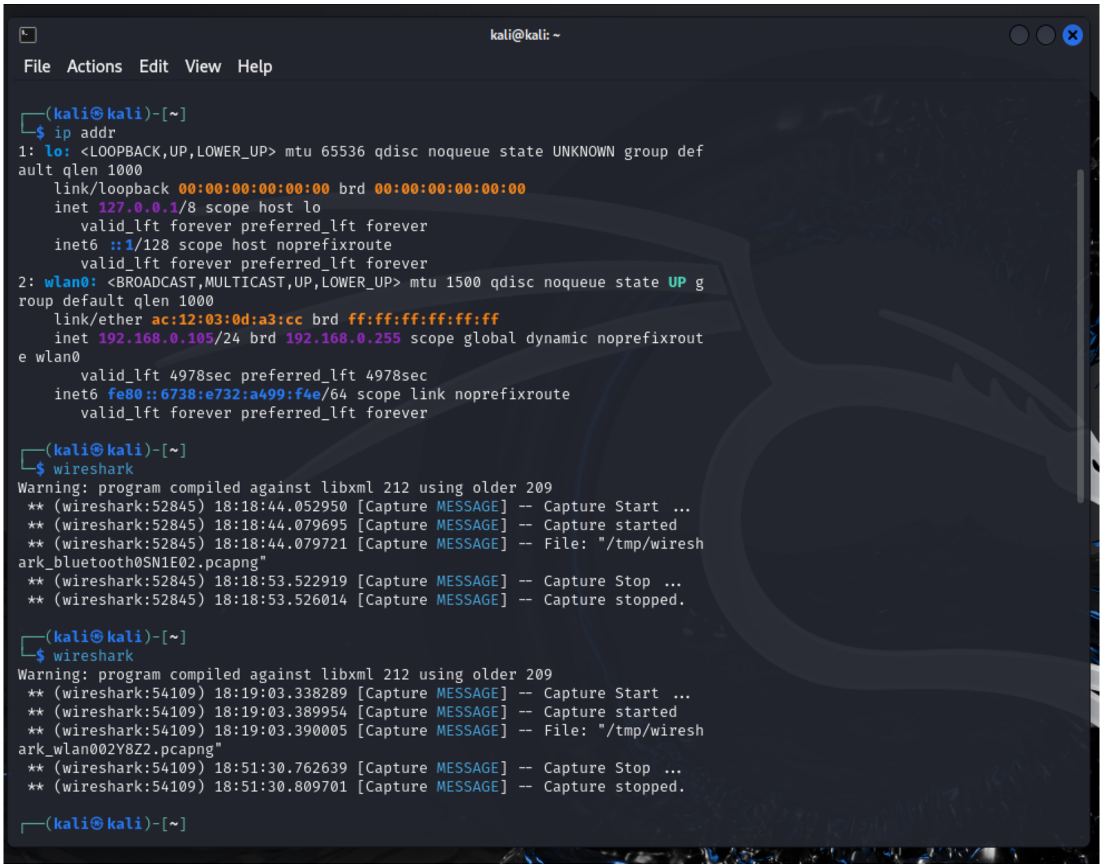
Part 1: Exploring Basic Networking Commands

Objective: This lab introduces students to essential networking commands used for diagnosing, monitoring, and troubleshooting networks. By completing this assignment, students will develop hands-on experience with commands in Windows, Linux, or macOS.

Title: Basic Networking Commands for Network Analysis

Identifying Network Configuration

1. **Objective:** Understand the network configuration of your system.
2. **Steps**
   I. Run the following commands to view network configuration details:
      A. **Windows:** `ipconfig`
      B. **Linux/macOS:** `ifconfig` or `ip addr`
   II. Note the following:
      A. IP Address
      B. Subnet Mask
      C. Default Gateway



```
┌──(kali㉿kali)-[~]
└─$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP g
roup default qlen 1000
    link/ether ac:12:03:0d:a3:cc brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.105/24 brd 192.168.0.255 scope global dynamic noprefixrout
e wlan0
       valid_lft 4978sec preferred_lft 4978sec
    inet6 fe80::6738:e732:a499:f4e/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ wireshark
Warning: program compiled against libxml 212 using older 209
 ** (wireshark:52845) 18:18:44.052950 [Capture MESSAGE] -- Capture Start ...
 ** (wireshark:52845) 18:18:44.079695 [Capture MESSAGE] -- Capture started
 ** (wireshark:52845) 18:18:44.079721 [Capture MESSAGE] -- File: "/tmp/wiresh
ark_bluetooth0SN1E02.pcapng"
 ** (wireshark:52845) 18:18:53.522919 [Capture MESSAGE] -- Capture Stop ...
 ** (wireshark:52845) 18:18:53.526014 [Capture MESSAGE] -- Capture stopped.

┌──(kali㉿kali)-[~]
└─$ wireshark
Warning: program compiled against libxml 212 using older 209
 ** (wireshark:54109) 18:19:03.338289 [Capture MESSAGE] -- Capture Start ...
 ** (wireshark:54109) 18:19:03.389954 [Capture MESSAGE] -- Capture started
 ** (wireshark:54109) 18:19:03.390005 [Capture MESSAGE] -- File: "/tmp/wiresh
ark_wlan002Y8Z2.pcapng"
 ** (wireshark:54109) 18:51:30.762639 [Capture MESSAGE] -- Capture Stop ...
 ** (wireshark:54109) 18:51:30.809701 [Capture MESSAGE] -- Capture stopped.

┌──(kali㉿kali)-[~]
```

Output:

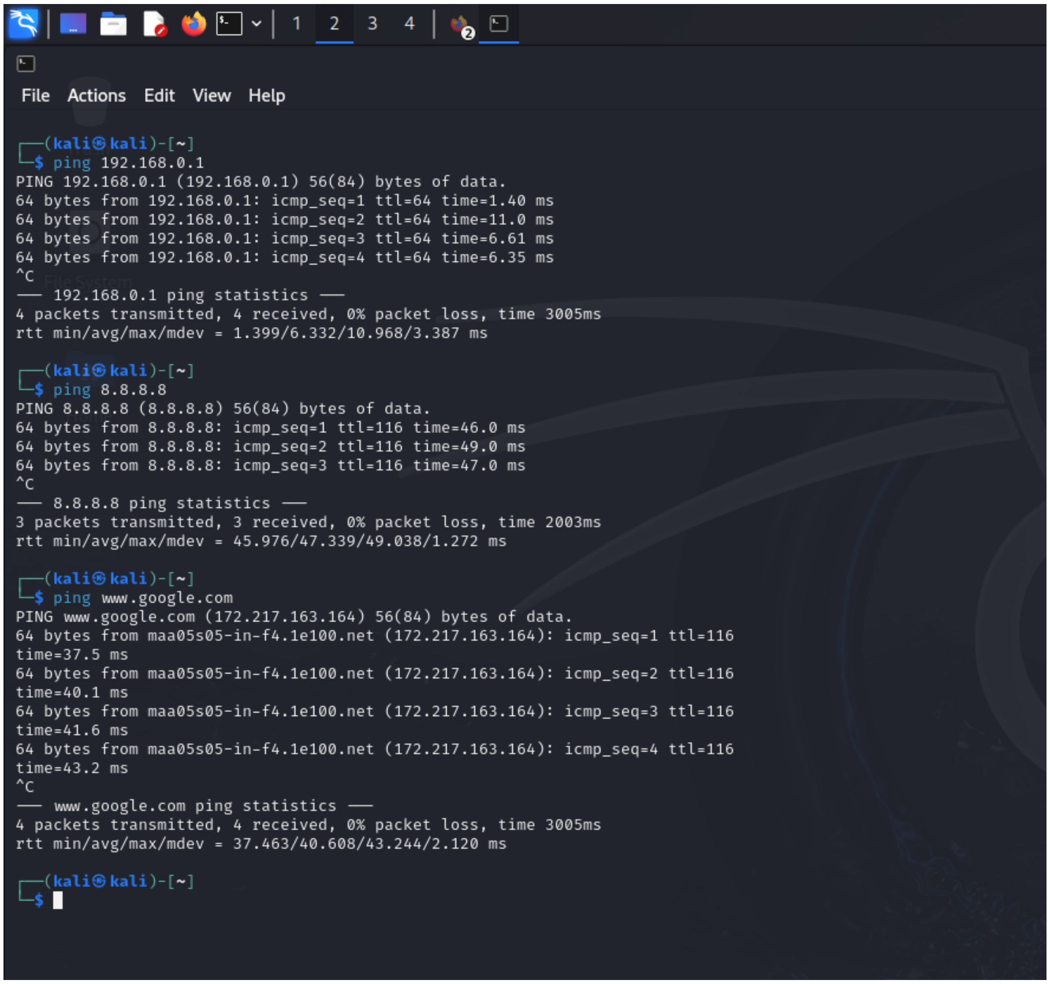
3. **Questions**
   I. What is your system's IP address?
      A. 192.168.0.105

   II. What is the role of the default gateway in your network?
      A. The default gateway connects your local network to external networks, forwarding traffic destined for devices outside your subnet.

Testing Network Connectivity

1. **Objective:** Use the `ping` command to test connectivity with other devices.
2. **Steps**
   I. Ping the following:
      A. Your default gateway.
      B. A public server (e.g., `8.8.8.8`).
      C. A domain name (e.g., `www.google.com`).
   II. Record the round-trip time (RTT) for each ping.

Output:



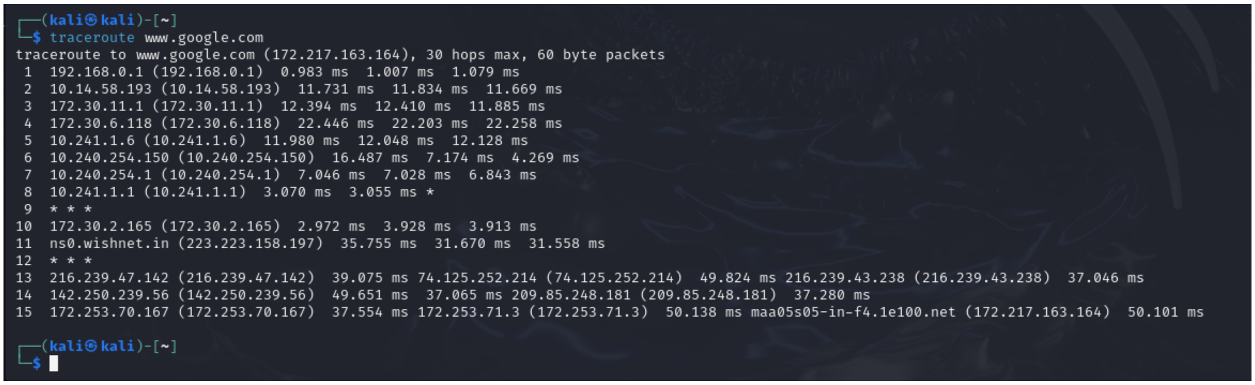
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=1.40 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=11.0 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=6.61 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=6.35 ms
^C
── 192.168.0.1 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.399/6.332/10.968/3.387 ms

┌──(kali㉿kali)-[~]
└─$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=46.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=49.0 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=47.0 ms
^C
── 8.8.8.8 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 45.976/47.339/49.038/1.272 ms

┌──(kali㉿kali)-[~]
└─$ ping www.google.com
PING www.google.com (172.217.163.164) 56(84) bytes of data.
64 bytes from maa05s05-in-f4.1e100.net (172.217.163.164): icmp_seq=1 ttl=116
time=37.5 ms
64 bytes from maa05s05-in-f4.1e100.net (172.217.163.164): icmp_seq=2 ttl=116
time=40.1 ms
64 bytes from maa05s05-in-f4.1e100.net (172.217.163.164): icmp_seq=3 ttl=116
time=41.6 ms
64 bytes from maa05s05-in-f4.1e100.net (172.217.163.164): icmp_seq=4 ttl=116
time=43.2 ms
^C
── www.google.com ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 37.463/40.608/43.244/2.120 ms

┌──(kali㉿kali)-[~]
└─$ 
```

3. **Questions**
   I. Was the ping to each target successful?
      A. Yes

   II. If a ping failed, what might be the reason?
      A. A ping may fail due to network congestion, routing issues, server unavailability, firewalls, or hardware/software constraints.

Tracing Routes

1. **Objective:** Use the traceroute command to map the path to a destination.
2. **Steps:**
   I. Run:
      A. **Windows:** `tracert www.google.com`
      B. **Linux/macOS:** `traceroute www.google.com`
   II. Observe the hops the packets take to reach the destination.



```
┌──(kali㉿kali)-[~]
└─$ traceroute www.google.com
traceroute to www.google.com (172.217.163.164), 30 hops max, 60 byte packets
 1  192.168.0.1 (192.168.0.1)  0.983 ms  1.007 ms  1.079 ms
 2  10.14.58.193 (10.14.58.193)  11.731 ms  11.834 ms  11.669 ms
 3  172.30.11.1 (172.30.11.1)  12.394 ms  12.410 ms  11.885 ms
 4  172.30.6.118 (172.30.6.118)  22.446 ms  22.203 ms  22.258 ms
 5  10.241.1.6 (10.241.1.6)  11.980 ms  12.048 ms  12.128 ms
 6  10.240.254.150 (10.240.254.150)  16.487 ms  7.174 ms  4.269 ms
 7  10.240.254.1 (10.240.254.1)  7.046 ms  7.028 ms  6.843 ms
 8  10.241.1.1 (10.241.1.1)  3.070 ms  3.055 ms *
 9  * * *
10  172.30.2.165 (172.30.2.165)  2.972 ms  3.928 ms  3.913 ms
11  ns0.wishnet.in (223.223.158.197)  35.755 ms  31.670 ms  31.558 ms
12  * * *
13  216.239.47.142 (216.239.47.142)  39.075 ms 74.125.252.214 (74.125.252.214)  49.824 ms 216.239.43.238 (216.239.43.238)  37.046 ms
14  142.250.239.56 (142.250.239.56)  49.651 ms  37.065 ms 209.85.248.181 (209.85.248.181)  37.280 ms
15  172.253.70.167 (172.253.70.167)  37.554 ms 172.253.71.3 (172.253.71.3)  50.138 ms maa05s05-in-f4.1e100.net (172.217.163.164)  50.101 ms

┌──(kali㉿kali)-[~]
└─$ █
```

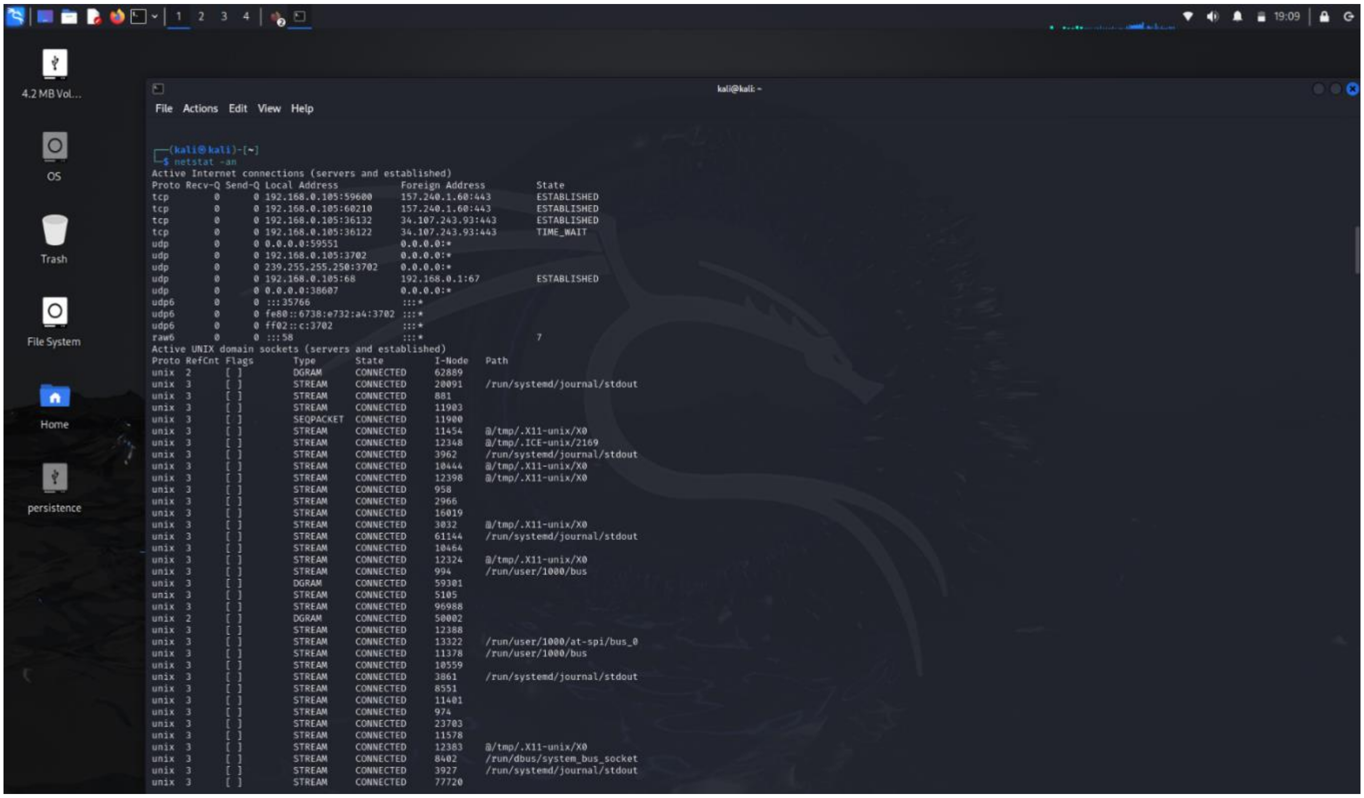
Output:

3. **Questions**
   I. How many hops did it take to reach `www.google.com`?
      A. 30 hops

   II. Did any hops time out? If so, what could cause this?
      A. Yes, Timeouts in traceroute occur due to firewalls, rate limiting, unresponsive devices, routing issues, or overloaded nodes.

Examining Active Connections

1. **Objective:** Identify active network connections using `netstat`.
2. **Steps:**
   I. Run:
      A. **Windows/Linux/macOS:** `netstat -an`
   II. Identify:
      A. Any established TCP connections.
      B. Any listening ports on your machine.



```
┌──(kali㉿kali)-[~]
└─$ netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.0.105:59600     157.240.1.60:443        ESTABLISHED
tcp        0      0 192.168.0.105:60210     157.240.1.60:443        ESTABLISHED
tcp        0      0 192.168.0.105:36132     34.107.243.93:443       ESTABLISHED
tcp        0      0 192.168.0.105:36122     34.107.243.93:443       TIME_WAIT
udp        0      0 0.0.0.0:59551           0.0.0.0:*
udp        0      0 192.168.0.105:3702      0.0.0.0:*
udp        0      0 239.255.255.250:3702    0.0.0.0:*
udp        0      0 192.168.0.105:68        192.168.0.1:67          ESTABLISHED
udp        0      0 0.0.0.0:38607           0.0.0.0:*
udp6       0      0 :::35766                :::*
udp6       0      0 fe80::6738:e732:a4:3702 :::*
udp6       0      0 ff02::c:3702            :::*
raw6       0      0 :::58                   :::*                    7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM      CONNECTED     62889
unix  3      [ ]         STREAM     CONNECTED     20091    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     881
unix  3      [ ]         STREAM     CONNECTED     11903
unix  3      [ ]         SEQPACKET  CONNECTED     11900
unix  3      [ ]         STREAM     CONNECTED     11454    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     12348    @/tmp/.ICE-unix/2169
unix  3      [ ]         STREAM     CONNECTED     3962     /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     10444    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     12398    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     958
unix  3      [ ]         STREAM     CONNECTED     2966
unix  3      [ ]         STREAM     CONNECTED     16019
unix  3      [ ]         STREAM     CONNECTED     3032     @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     61144    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     10464
unix  3      [ ]         STREAM     CONNECTED     12324    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     994      /run/user/1000/bus
unix  3      [ ]         DGRAM      CONNECTED     59301
unix  3      [ ]         STREAM     CONNECTED     5105
unix  3      [ ]         STREAM     CONNECTED     96988
unix  2      [ ]         DGRAM      CONNECTED     50002
unix  3      [ ]         STREAM     CONNECTED     12388
unix  3      [ ]         STREAM     CONNECTED     13322    /run/user/1000/at-spi/bus_0
unix  3      [ ]         STREAM     CONNECTED     11378    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     10559
unix  3      [ ]         STREAM     CONNECTED     3861     /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     8551
unix  3      [ ]         STREAM     CONNECTED     11401
unix  3      [ ]         STREAM     CONNECTED     974
unix  3      [ ]         STREAM     CONNECTED     23703
unix  3      [ ]         STREAM     CONNECTED     11578
unix  3      [ ]         STREAM     CONNECTED     12383    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     8402     /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     3927     /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     77720
```

Output:

3. **Questions**

   I. What are the most common protocols (e.g., TCP, UDP) used in the active connections?

      A. TCP and UDP

   II. Why might some ports be in a listening state?

      A. Ports are in a listening state to allow services or applications to await incoming connections from clients or other processes.

DNS and Name Resolution

1. **Objective:** Understand how DNS resolves domain names to IP addresses.
2. **Steps:**

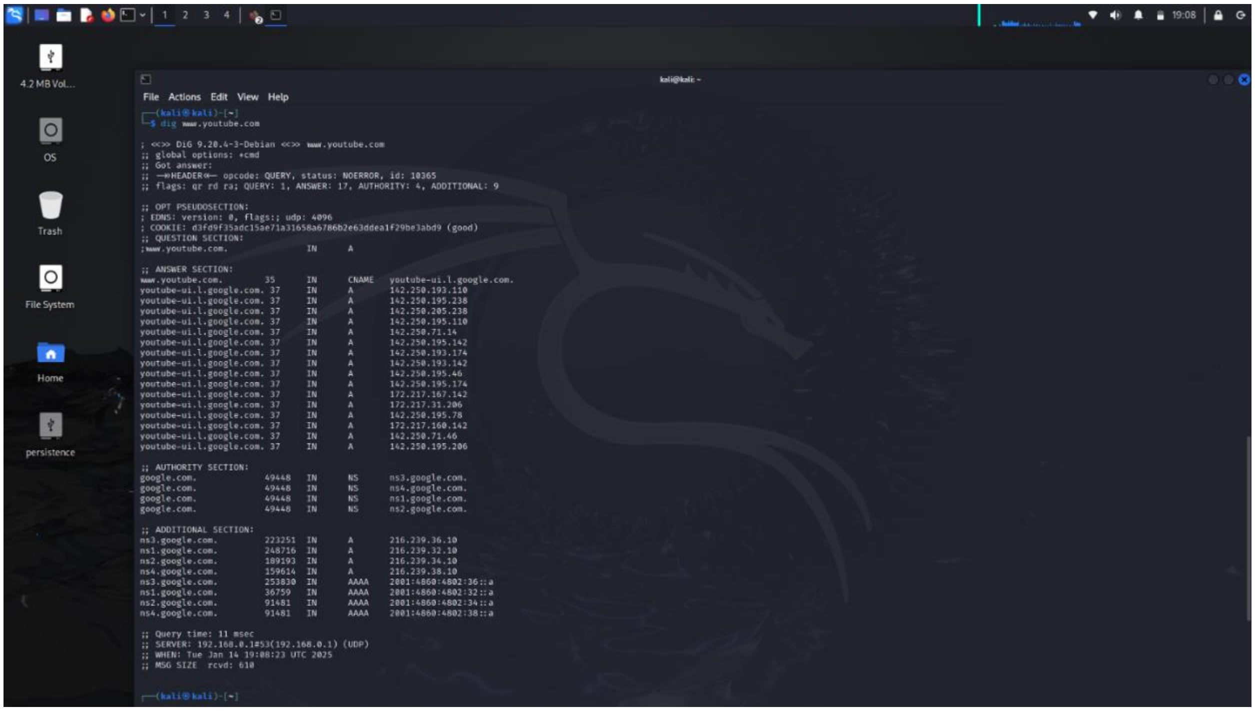
   I. Run:

      A. **Windows:** `nslookup www.example.com`

      B. **Linux/macOS:** `nslookup www.example.com` or `dig www.example.com`

   II. Note the resolved IP address.

Output:



```
┌──(kali㉿kali)-[~]
└─$ dig www.youtube.com

; <<>> DiG 9.20.4-3-Debian <<>> www.youtube.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10365
;; flags: qr rd ra; QUERY: 1, ANSWER: 17, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: d3fd9f35adc15ae71a31658a6786b2e63ddea1f29be3abd9 (good)
;; QUESTION SECTION:
;www.youtube.com.               IN      A

;; ANSWER SECTION:
www.youtube.com.        35      IN      CNAME   youtube-ui.l.google.com.
youtube-ui.l.google.com. 37     IN      A       142.250.193.110
youtube-ui.l.google.com. 37     IN      A       142.250.195.238
youtube-ui.l.google.com. 37     IN      A       142.250.205.238
youtube-ui.l.google.com. 37     IN      A       142.250.195.110
youtube-ui.l.google.com. 37     IN      A       142.250.71.14
youtube-ui.l.google.com. 37     IN      A       142.250.195.142
youtube-ui.l.google.com. 37     IN      A       142.250.193.174
youtube-ui.l.google.com. 37     IN      A       142.250.193.142
youtube-ui.l.google.com. 37     IN      A       142.250.195.46
youtube-ui.l.google.com. 37     IN      A       142.250.195.174
youtube-ui.l.google.com. 37     IN      A       172.217.167.142
youtube-ui.l.google.com. 37     IN      A       172.217.31.206
youtube-ui.l.google.com. 37     IN      A       142.250.195.78
youtube-ui.l.google.com. 37     IN      A       172.217.160.142
youtube-ui.l.google.com. 37     IN      A       142.250.71.46
youtube-ui.l.google.com. 37     IN      A       142.250.195.206

;; AUTHORITY SECTION:
google.com.             49448   IN      NS      ns3.google.com.
google.com.             49448   IN      NS      ns4.google.com.
google.com.             49448   IN      NS      ns1.google.com.
google.com.             49448   IN      NS      ns2.google.com.

;; ADDITIONAL SECTION:
ns3.google.com.         223251  IN      A       216.239.36.10
ns1.google.com.         248716  IN      A       216.239.32.10
ns2.google.com.         189193  IN      A       216.239.34.10
ns4.google.com.         159614  IN      A       216.239.38.10
ns3.google.com.         253830  IN      AAAA    2001:4860:4802:36::a
ns1.google.com.         36759   IN      AAAA    2001:4860:4802:32::a
ns2.google.com.         91481   IN      AAAA    2001:4860:4802:34::a
ns4.google.com.         91481   IN      AAAA    2001:4860:4802:38::a

;; Query time: 11 msec
;; SERVER: 192.168.0.1#53(192.168.0.1) (UDP)
;; WHEN: Tue Jan 14 19:08:23 UTC 2025
;; MSG SIZE  rcvd: 610

┌──(kali㉿kali)-[~]
```

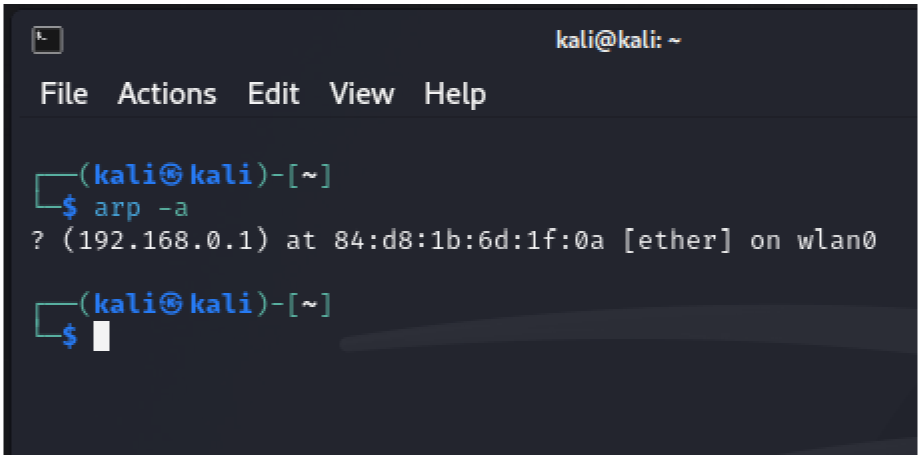
3. **Questions**
   I. What is the resolved IP address of `www.example.com`?
      A. 192.168.0.1

   II. What happens if you try to resolve a non-existent domain (e.g., `www.invalidexample.com`)?
      A. When you try to resolve a non-existent domain, the DNS query fails, returning an error like NXDOMAIN (Non-Existent Domain), indicating the domain does not exist in the DNS.

Exploring ARP Cache

1. **Objective:** View the ARP cache on your system.
2. **Steps:**
   I. Run:
      A. **Windows/Linux/macOS:** `arp -a`
   II. Identify:
      A. MAC addresses of devices in the cache.
      B. Corresponding IP addresses.

Output:



```
┌──(kali㉿kali)-[~]
└─$ arp -a
? (192.168.0.1) at 84:d8:1b:6d:1f:0a [ether] on wlan0

┌──(kali㉿kali)-[~]
└─$ 
```

3. **Questions**

I. What is the purpose of the ARP cache?

A. The ARP cache stores mappings of IP addresses to MAC addresses, enabling faster communication by avoiding repeated ARP requests for devices on the same local network.

II. How can outdated ARP entries affect network communication?

A. Outdated ARP entries can cause communication failures, increased latency, network congestion, and security vulnerabilities due to incorrect address mapping.

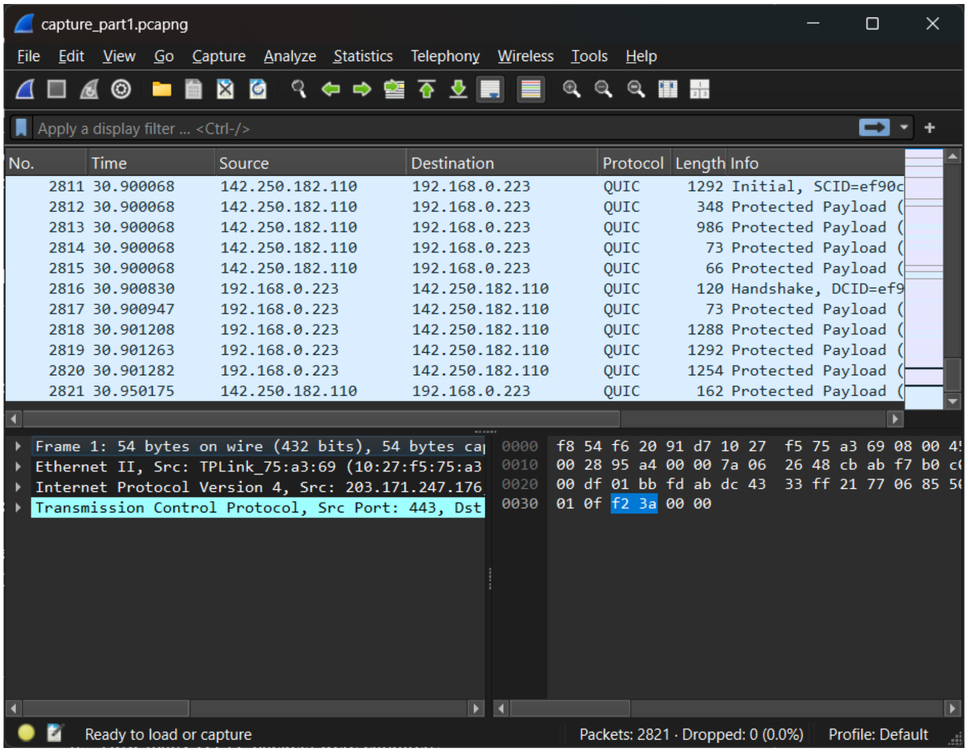
Part 2: Packet Capture and Analysis Using Wireshark

Objective: This lab introduces students to network packet analysis using Wireshark. By completing the assignment, students will learn how to capture, filter, and analyze network traffic effectively.

Getting Started with Wireshark

1. Objective: Familiarize students with the Wireshark interface and basic functionality.
2. Steps:
   I. Launch Wireshark and identify the available network interfaces.
   II. Start a packet capture on the primary interface (e.g., Wi-Fi or Ethernet).
   III. Browse a website (e.g., `www.example.com`) during the capture.
   IV. Stop the capture and save it as ***`capture_part1.pcap`*.**

Output:



No.	Time	Source	Destination	Protocol	Length	Info
2811	30.900068	142.250.182.110	192.168.0.223	QUIC	1292	Initial, SCID=ef90c
2812	30.900068	142.250.182.110	192.168.0.223	QUIC	348	Protected Payload (
2813	30.900068	142.250.182.110	192.168.0.223	QUIC	986	Protected Payload (
2814	30.900068	142.250.182.110	192.168.0.223	QUIC	73	Protected Payload (
2815	30.900068	142.250.182.110	192.168.0.223	QUIC	66	Protected Payload (
2816	30.900830	192.168.0.223	142.250.182.110	QUIC	120	Handshake, DCID=ef9
2817	30.900947	192.168.0.223	142.250.182.110	QUIC	73	Protected Payload (
2818	30.901208	192.168.0.223	142.250.182.110	QUIC	1288	Protected Payload (
2819	30.901263	192.168.0.223	142.250.182.110	QUIC	1292	Protected Payload (
2820	30.901282	192.168.0.223	142.250.182.110	QUIC	1254	Protected Payload (
2821	30.950175	142.250.182.110	192.168.0.223	QUIC	162	Protected Payload (

```
Frame 1: 54 bytes on wire (432 bits), 54 bytes ca
Ethernet II, Src: TPLink_75:a3:69 (10:27:f5:75:a3
Internet Protocol Version 4, Src: 203.171.247.176
Transmission Control Protocol, Src Port: 443, Dst
```

```
0000  f8 54 f6 20 91 d7 10 27  f5 75 a3 69 08 00 4
0010  00 28 95 a4 00 00 7a 06  26 48 cb ab f7 b0 c
0020  00 df 01 bb fd ab dc 43  33 ff 21 77 06 85 5
0030  01 0f f2 3a 00 00
```

3. **Questions**
   I. Which network interface did you use, and why?
      A. I chose the Wi-Fi interface because it provides a convenient and flexible connection, allowing mobility and access to the network without the need for physical cables.

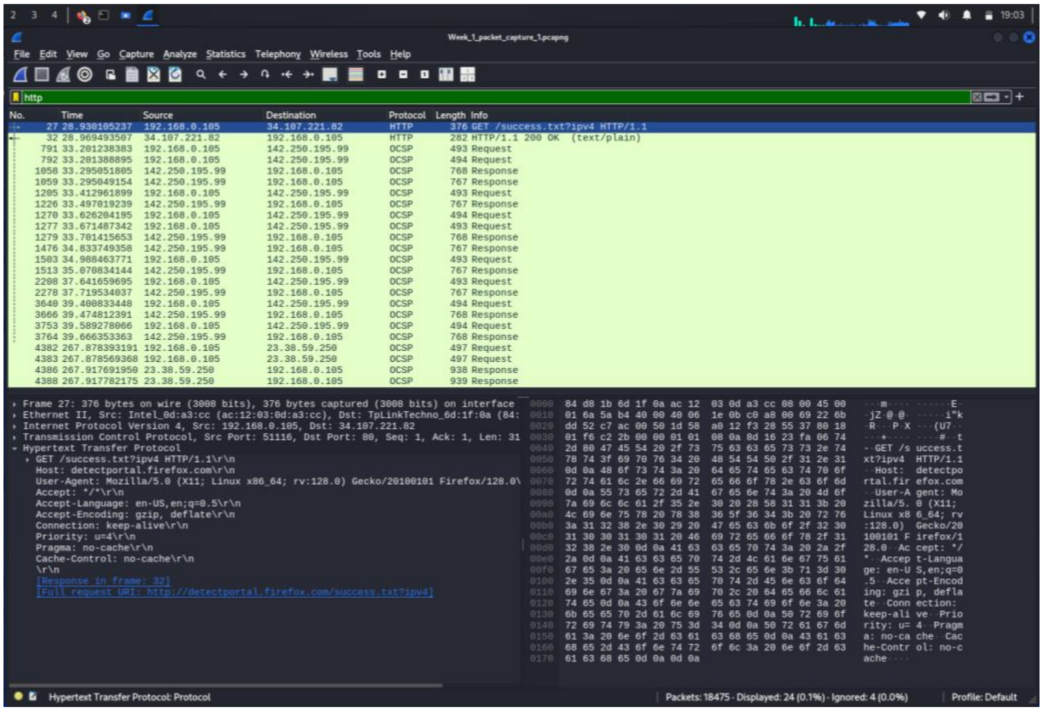
   II. How many packets were captured in total?
      A. 2821

Applying Filters

1. **Objective:** Learn to apply display filters to narrow down relevant packets.
2. **Tasks:**
   I. Use the capture from Part 1.
   II. Apply the following filters and note the results:
      - `http` (Display HTTP packets)
      - `dns` (Display DNS packets)
      - `ip.addr == <your IP>` (Display packets related to your IP address)
   III. Identify the DNS query and response for `www.example.com`.

Output:

http


2 3 4
19:03
Week_1_packet_capture_1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

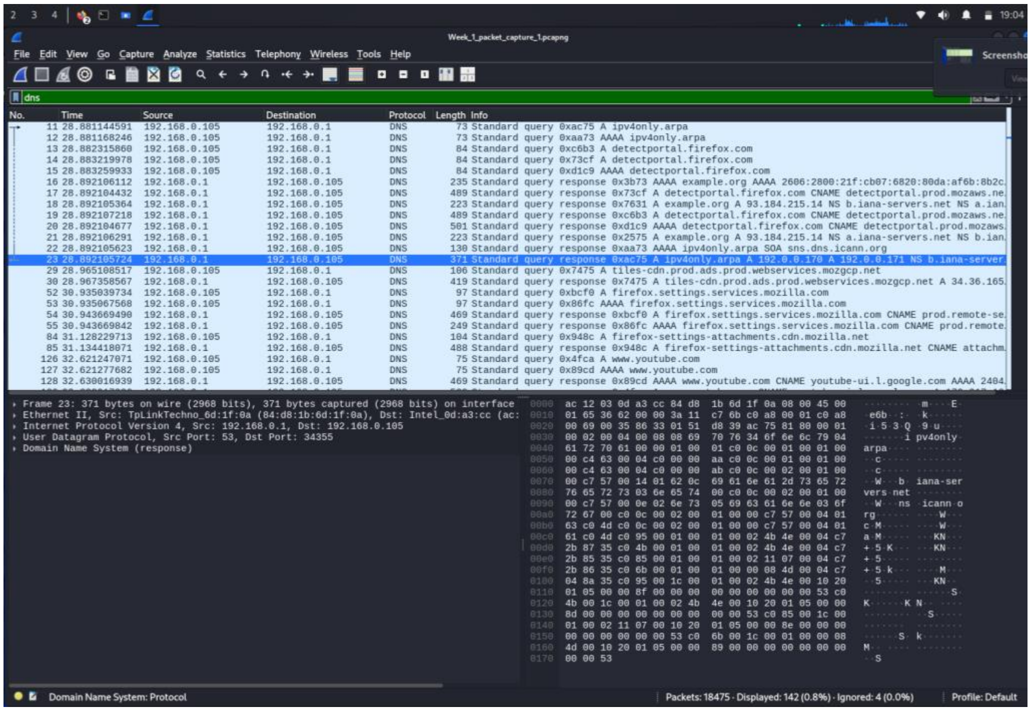
http

```
No.     Time           Source           Destination      Protocol  Length Info
     27 28.930105237   192.168.0.105    34.107.221.82    HTTP      376 GET /success.txt?ipv4 HTTP/1.1
     32 28.969493507   34.107.221.82    192.168.0.105    HTTP      282 HTTP/1.1 200 OK  (text/plain)
    791 33.201238383   192.168.0.105    142.250.195.99   OCSP      493 Request
    792 33.201388895   192.168.0.105    142.250.195.99   OCSP      494 Request
   1058 33.295051805   142.250.195.99   192.168.0.105    OCSP      768 Response
   1059 33.295049154   142.250.195.99   192.168.0.105    OCSP      767 Response
   1205 33.412961899   192.168.0.105    142.250.195.99   OCSP      493 Request
   1226 33.497019239   142.250.195.99   192.168.0.105    OCSP      767 Response
   1270 33.626204195   192.168.0.105    142.250.195.99   OCSP      494 Request
   1277 33.671487342   192.168.0.105    142.250.195.99   OCSP      493 Request
   1279 33.701415653   142.250.195.99   192.168.0.105    OCSP      768 Response
   1476 34.833749358   142.250.195.99   192.168.0.105    OCSP      767 Response
   1503 34.988463771   192.168.0.105    142.250.195.99   OCSP      493 Request
   1513 35.070834144   142.250.195.99   192.168.0.105    OCSP      767 Response
   2208 37.641659695   192.168.0.105    142.250.195.99   OCSP      493 Request
   2278 37.719534037   142.250.195.99   192.168.0.105    OCSP      767 Response
   3640 39.400833448   192.168.0.105    142.250.195.99   OCSP      494 Request
   3666 39.474812391   142.250.195.99   192.168.0.105    OCSP      768 Response
   3753 39.589278066   192.168.0.105    142.250.195.99   OCSP      494 Request
   3764 39.666353363   142.250.195.99   192.168.0.105    OCSP      768 Response
   4382 267.878393191  192.168.0.105    23.38.59.250     OCSP      497 Request
   4383 267.878569368  192.168.0.105    23.38.59.250     OCSP      497 Request
   4386 267.917691950  23.38.59.250     192.168.0.105    OCSP      938 Response
   4388 267.917782175  23.38.59.250     192.168.0.105    OCSP      939 Response
```

```
› Frame 27: 376 bytes on wire (3008 bits), 376 bytes captured (3008 bits) on interface
› Ethernet II, Src: Intel_0d:a3:cc (ac:12:03:0d:a3:cc), Dst: TpLinkTechno_6d:1f:0a (84:
› Internet Protocol Version 4, Src: 192.168.0.105, Dst: 34.107.221.82
› Transmission Control Protocol, Src Port: 51116, Dst Port: 80, Seq: 1, Ack: 1, Len: 31
˅ Hypertext Transfer Protocol
  › GET /success.txt?ipv4 HTTP/1.1\r\n
    Host: detectportal.firefox.com\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0\
    Accept: */*\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Priority: u=4\r\n
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Response in frame: 32]
    [Full request URI: http://detectportal.firefox.com/success.txt?ipv4]
```

```
0000  84 d8 1b 6d 1f 0a ac 12  03 0d a3 cc 08 00 45 00   ···m···· ······E·
0010  01 6a 5a b4 40 00 40 06  1e 0b c0 a8 00 69 22 6b   ·jZ·@·@· ·····i"k
0020  dd 52 c7 ac 00 50 1d 58  a0 12 f3 28 55 37 80 18   ·R···P·X ···(U7··
0030  01 f6 c2 2b 00 00 01 01  08 0a 8d 16 23 fa 06 74   ···+···· ····#··t
0040  2d 80 47 45 54 20 2f 73  75 63 63 65 73 73 2e 74   -·GET /s uccess.t
0050  78 74 3f 69 70 76 34 20  48 54 54 50 2f 31 2e 31   xt?ipv4  HTTP/1.1
0060  0d 0a 48 6f 73 74 3a 20  64 65 74 65 63 74 70 6f   ··Host:  detectpo
0070  72 74 61 6c 2e 66 69 72  65 66 6f 78 2e 63 6f 6d   rtal.fir efox.com
0080  0d 0a 55 73 65 72 2d 41  67 65 6e 74 3a 20 4d 6f   ··User-A gent: Mo
0090  7a 69 6c 6c 61 2f 35 2e  30 20 28 58 31 31 3b 20   zilla/5. 0 (X11;
00a0  4c 69 6e 75 78 20 78 38  36 5f 36 34 3b 20 72 76   Linux x8 6_64; rv
00b0  3a 31 32 38 2e 30 29 20  47 65 63 6b 6f 2f 32 30   :128.0)  Gecko/20
00c0  31 30 30 31 30 31 20 46  69 72 65 66 6f 78 2f 31   100101 F irefox/1
00d0  32 38 2e 30 0d 0a 41 63  63 65 70 74 3a 20 2a 2f   28.0··Ac cept: */
00e0  2a 0d 0a 41 63 63 65 70  74 2d 4c 61 6e 67 75 61   *··Accep t-Langua
00f0  67 65 3a 20 65 6e 2d 55  53 2c 65 6e 3b 71 3d 30   ge: en-U S,en;q=0
0100  2e 35 0d 0a 41 63 63 65  70 74 2d 45 6e 63 6f 64   .5··Acce pt-Encod
0110  69 6e 67 3a 20 67 7a 69  70 2c 20 64 65 66 6c 61   ing: gzi p, defla
0120  74 65 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   te··Conn ection:
0130  6b 65 65 70 2d 61 6c 69  76 65 0d 0a 50 72 69 6f   keep-ali ve··Prio
0140  72 69 74 79 3a 20 75 3d  34 0d 0a 50 72 61 67 6d   rity: u= 4··Pragm
0150  61 3a 20 6e 6f 2d 63 61  63 68 65 0d 0a 43 61 63   a: no-ca che··Cac
0160  68 65 2d 43 6f 6e 74 72  6f 6c 3a 20 6e 6f 2d 63   he-Contr ol: no-c
0170  61 63 68 65 0d 0a 0d 0a                            ache····
```

Hypertext Transfer Protocol: Protocol | Packets: 18475 · Displayed: 24 (0.1%) · Ignored: 4 (0.0%) | Profile: Default dns



Week_1_packet_capture_1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
19:04

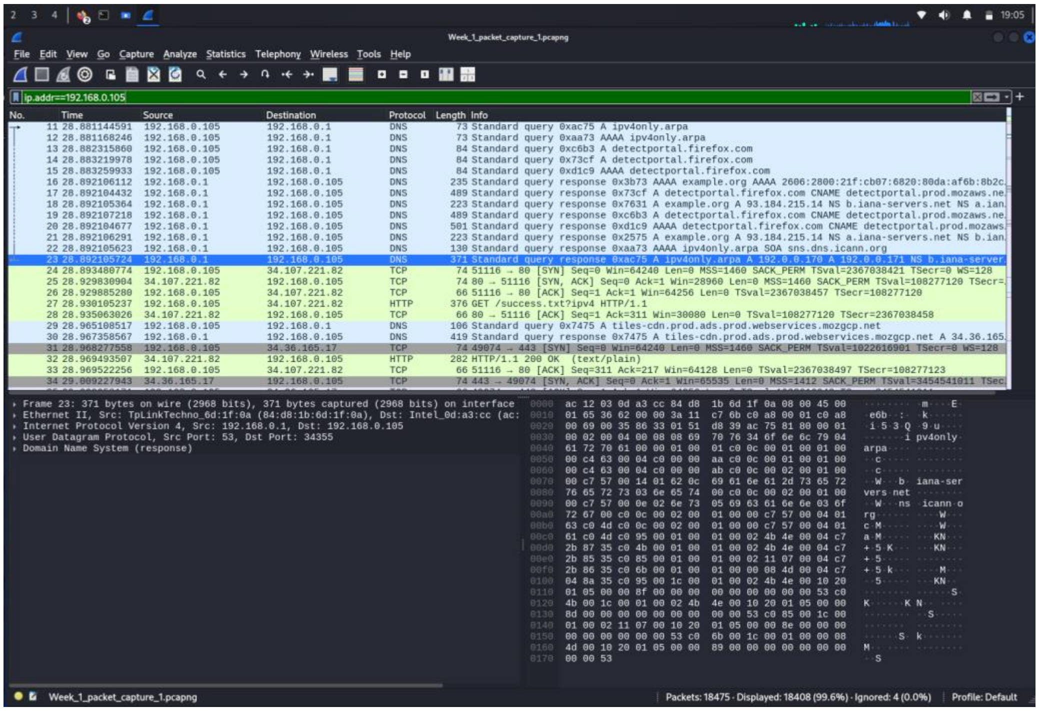
Filter: dns

```
No.   Time          Source          Destination     Protocol Length Info
   11 28.881144591  192.168.0.105   192.168.0.1     DNS       73 Standard query 0xac75 A ipv4only.arpa
   12 28.881168246  192.168.0.105   192.168.0.1     DNS       73 Standard query 0xaa73 AAAA ipv4only.arpa
   13 28.882315860  192.168.0.105   192.168.0.1     DNS       84 Standard query 0xc6b3 A detectportal.firefox.com
   14 28.883219978  192.168.0.105   192.168.0.1     DNS       84 Standard query 0x73cf A detectportal.firefox.com
   15 28.883259933  192.168.0.105   192.168.0.1     DNS       84 Standard query 0xd1c9 AAAA detectportal.firefox.com
   16 28.892106112  192.168.0.1     192.168.0.105   DNS      235 Standard query response 0x3b73 AAAA example.org AAAA 2606:2800:21f:cb07:6820:80da:af6b:8b2c
   17 28.892104432  192.168.0.1     192.168.0.105   DNS      489 Standard query response 0x73cf A detectportal.firefox.com CNAME detectportal.prod.mozaws.ne
   18 28.892105364  192.168.0.1     192.168.0.105   DNS      223 Standard query response 0x7631 A example.org A 93.184.215.14 NS b.iana-servers.net NS a.ian
   19 28.892107218  192.168.0.1     192.168.0.105   DNS      489 Standard query response 0xc6b3 A detectportal.firefox.com CNAME detectportal.prod.mozaws.ne
   20 28.892104677  192.168.0.1     192.168.0.105   DNS      501 Standard query response 0xd1c9 AAAA detectportal.firefox.com CNAME detectportal.prod.mozaws
   21 28.892106291  192.168.0.1     192.168.0.105   DNS      223 Standard query response 0x2575 A example.org A 93.184.215.14 NS a.iana-servers.net NS b.ian
   22 28.892105623  192.168.0.1     192.168.0.105   DNS      130 Standard query response 0xaa73 AAAA ipv4only.arpa SOA sns.dns.icann.org
   23 28.892105724  192.168.0.1     192.168.0.105   DNS      371 Standard query response 0xac75 A ipv4only.arpa A 192.0.0.170 A 192.0.0.171 NS b.iana-server
   29 28.965108517  192.168.0.105   192.168.0.1     DNS      106 Standard query 0x7475 A tiles-cdn.prod.ads.prod.webservices.mozgcp.net
   30 28.967358567  192.168.0.1     192.168.0.105   DNS      419 Standard query response 0x7475 A tiles-cdn.prod.ads.prod.webservices.mozgcp.net A 34.36.165
   52 30.935039734  192.168.0.105   192.168.0.1     DNS       97 Standard query 0xbcf0 A firefox.settings.services.mozilla.com
   53 30.935067568  192.168.0.105   192.168.0.1     DNS       97 Standard query 0x86fc AAAA firefox.settings.services.mozilla.com
   54 30.943669490  192.168.0.1     192.168.0.105   DNS      469 Standard query response 0xbcf0 A firefox.settings.services.mozilla.com CNAME prod.remote-se
   55 30.943669842  192.168.0.1     192.168.0.105   DNS      249 Standard query response 0x86fc AAAA firefox.settings.services.mozilla.com CNAME prod.remote
   84 31.128229713  192.168.0.105   192.168.0.1     DNS      104 Standard query 0x948c A firefox-settings-attachments.cdn.mozilla.net
   85 31.134418071  192.168.0.1     192.168.0.105   DNS      488 Standard query response 0x948c A firefox-settings-attachments.cdn.mozilla.net CNAME attachm
  126 32.621247071  192.168.0.105   192.168.0.1     DNS       75 Standard query 0x4fca A www.youtube.com
  127 32.621277682  192.168.0.105   192.168.0.1     DNS       75 Standard query 0x89cd AAAA www.youtube.com
  128 32.630016939  192.168.0.1     192.168.0.105   DNS      469 Standard query response 0x89cd AAAA www.youtube.com CNAME youtube-ui.l.google.com AAAA 2404
```

```
› Frame 23: 371 bytes on wire (2968 bits), 371 bytes captured (2968 bits) on interface
› Ethernet II, Src: TpLinkTechno_6d:1f:0a (84:d8:1b:6d:1f:0a), Dst: Intel_0d:a3:cc (ac:
› Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.105
› User Datagram Protocol, Src Port: 53, Dst Port: 34355
› Domain Name System (response)
```

```
0000  ac 12 03 0d a3 cc 84 d8  1b 6d 1f 0a 08 00 45 00   ·········m····E·
0010  01 65 36 62 00 00 3a 11  c7 6b c0 a8 00 01 c0 a8   ·e6b··:··k······
0020  00 69 00 35 86 33 01 51  d8 39 ac 75 81 80 00 01   ·i·5·3·Q·9·u····
0030  00 02 00 04 00 08 08 69  70 76 34 6f 6e 6c 79 04   ·······i pv4only·
0040  61 72 70 61 00 00 01 00  01 c0 0c 00 01 00 01 00   arpa············
0050  00 c4 63 00 04 c0 00 00  aa c0 0c 00 01 00 01 00   ··c·············
0060  00 c4 63 00 04 c0 00 00  ab c0 0c 00 02 00 01 00   ··c·············
0070  00 c7 57 00 14 01 62 0c  69 61 6e 61 2d 73 65 72   ··W···b· iana-ser
0080  76 65 72 73 03 6e 65 74  00 c0 0c 00 02 00 01 00   vers·net········
0090  00 c7 57 00 0e 02 6e 73  05 69 63 61 6e 6e 03 6f   ··W···ns ·icann·o
00a0  72 67 00 c0 0c 00 02 00  01 00 00 c7 57 00 04 01   rg··········W···
00b0  63 c0 4d c0 0c 00 02 00  01 00 00 c7 57 00 04 01   c·M·········W···
00c0  61 c0 4d c0 95 00 01 00  01 00 02 4b 4e 00 04 c7   a·M········KN···
00d0  2b 87 35 c0 4b 00 01 00  01 00 02 4b 4e 00 04 c7   +·5·K······KN···
00e0  2b 85 35 c0 85 00 01 00  01 00 02 11 07 00 04 c7   +·5·············
00f0  2b 86 35 c0 6b 00 01 00  01 00 00 08 4d 00 04 c7   +·5·k·······M···
0100  04 8a 35 c0 95 00 1c 00  01 00 02 4b 4e 00 10 20   ··5········KN··
0110  01 05 00 00 8f 00 00 00  00 00 00 00 00 00 53 c0   ··············S·
0120  4b 00 1c 00 01 00 02 4b  4e 00 10 20 01 05 00 00   K······K N······
0130  8d 00 00 00 00 00 00 00  00 00 53 c0 85 00 1c 00   ··········S·····
0140  01 00 02 11 07 00 10 20  01 05 00 00 8e 00 00 00   ················
0150  00 00 00 00 00 00 53 c0  6b 00 1c 00 01 00 00 08   ······S· k·······
0160  4d 00 10 20 01 05 00 00  89 00 00 00 00 00 00 00   M···············
0170  00 00 53                                           ··S
```

Domain Name System: Protocol | Packets: 18475 · Displayed: 142 (0.8%) · Ignored: 4 (0.0%) | Profile: Default



Week_1_packet_capture_1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
19:05

Filter: ip.addr==192.168.0.105

```
No.   Time          Source          Destination     Protocol Length Info
   11 28.881144591  192.168.0.105   192.168.0.1     DNS       73 Standard query 0xac75 A ipv4only.arpa
   12 28.881168246  192.168.0.105   192.168.0.1     DNS       73 Standard query 0xaa73 AAAA ipv4only.arpa
   13 28.882315860  192.168.0.105   192.168.0.1     DNS       84 Standard query 0xc6b3 A detectportal.firefox.com
   14 28.883219978  192.168.0.105   192.168.0.1     DNS       84 Standard query 0x73cf A detectportal.firefox.com
   15 28.883259933  192.168.0.105   192.168.0.1     DNS       84 Standard query 0xd1c9 AAAA detectportal.firefox.com
   16 28.892106112  192.168.0.1     192.168.0.105   DNS      235 Standard query response 0x3b73 AAAA example.org AAAA 2606:2800:21f:cb07:6820:80da:af6b:8b2c
   17 28.892104432  192.168.0.1     192.168.0.105   DNS      489 Standard query response 0x73cf A detectportal.firefox.com CNAME detectportal.prod.mozaws.ne
   18 28.892105364  192.168.0.1     192.168.0.105   DNS      223 Standard query response 0x7631 A example.org A 93.184.215.14 NS b.iana-servers.net NS a.ian
   19 28.892107218  192.168.0.1     192.168.0.105   DNS      489 Standard query response 0xc6b3 A detectportal.firefox.com CNAME detectportal.prod.mozaws.ne
   20 28.892104677  192.168.0.1     192.168.0.105   DNS      501 Standard query response 0xd1c9 AAAA detectportal.firefox.com CNAME detectportal.prod.mozaws
   21 28.892106291  192.168.0.1     192.168.0.105   DNS      223 Standard query response 0x2575 A example.org A 93.184.215.14 NS a.iana-servers.net NS b.ian
   22 28.892105623  192.168.0.1     192.168.0.105   DNS      130 Standard query response 0xaa73 AAAA ipv4only.arpa SOA sns.dns.icann.org
   23 28.892105724  192.168.0.1     192.168.0.105   DNS      371 Standard query response 0xac75 A ipv4only.arpa A 192.0.0.170 A 192.0.0.171 NS b.iana-server
   24 28.893480774  192.168.0.105   34.107.221.82   TCP       74 51116 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2367038421 TSecr=0 WS=128
   25 28.929830904  34.107.221.82   192.168.0.105   TCP       74 80 → 51116 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=108277120 TSecr=
   26 28.929885280  192.168.0.105   34.107.221.82   TCP       66 51116 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2367038457 TSecr=108277120
   27 28.930105237  192.168.0.105   34.107.221.82   HTTP     376 GET /success.txt?ipv4 HTTP/1.1
   28 28.935063026  34.107.221.82   192.168.0.105   TCP       66 80 → 51116 [ACK] Seq=1 Ack=311 Win=30080 Len=0 TSval=108277120 TSecr=2367038458
   29 28.965108517  192.168.0.105   192.168.0.1     DNS      106 Standard query 0x7475 A tiles-cdn.prod.ads.prod.webservices.mozgcp.net
   30 28.967358567  192.168.0.1     192.168.0.105   DNS      419 Standard query response 0x7475 A tiles-cdn.prod.ads.prod.webservices.mozgcp.net A 34.36.165
   31 28.968277558  192.168.0.105   34.36.165.17    TCP       74 49074 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1022616901 TSecr=0 WS=128
   32 28.969493507  34.107.221.82   192.168.0.105   HTTP     282 HTTP/1.1 200 OK  (text/plain)
   33 28.969522256  192.168.0.105   34.107.221.82   TCP       66 51116 → 80 [ACK] Seq=311 Ack=217 Win=64128 Len=0 TSval=2367038497 TSecr=108277123
   34 29.009227943  34.36.165.17    192.168.0.105   TCP       74 443 → 49074 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM TSval=345454101 TSec
```

```
› Frame 23: 371 bytes on wire (2968 bits), 371 bytes captured (2968 bits) on interface
› Ethernet II, Src: TpLinkTechno_6d:1f:0a (84:d8:1b:6d:1f:0a), Dst: Intel_0d:a3:cc (ac:
› Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.105
› User Datagram Protocol, Src Port: 53, Dst Port: 34355
› Domain Name System (response)
```

```
0000  ac 12 03 0d a3 cc 84 d8  1b 6d 1f 0a 08 00 45 00   ·········m····E·
0010  01 65 36 62 00 00 3a 11  c7 6b c0 a8 00 01 c0 a8   ·e6b··:··k······
0020  00 69 00 35 86 33 01 51  d8 39 ac 75 81 80 00 01   ·i·5·3·Q·9·u····
0030  00 02 00 04 00 08 08 69  70 76 34 6f 6e 6c 79 04   ·······i pv4only·
0040  61 72 70 61 00 00 01 00  01 c0 0c 00 01 00 01 00   arpa············
0050  00 c4 63 00 04 c0 00 00  aa c0 0c 00 01 00 01 00   ··c·············
0060  00 c4 63 00 04 c0 00 00  ab c0 0c 00 02 00 01 00   ··c·············
0070  00 c7 57 00 14 01 62 0c  69 61 6e 61 2d 73 65 72   ··W···b· iana-ser
0080  76 65 72 73 03 6e 65 74  00 c0 0c 00 02 00 01 00   vers·net········
0090  00 c7 57 00 0e 02 6e 73  05 69 63 61 6e 6e 03 6f   ··W···ns ·icann·o
00a0  72 67 00 c0 0c 00 02 00  01 00 00 c7 57 00 04 01   rg··········W···
00b0  63 c0 4d c0 0c 00 02 00  01 00 00 c7 57 00 04 01   c·M·········W···
00c0  61 c0 4d c0 95 00 01 00  01 00 02 4b 4e 00 04 c7   a·M········KN···
00d0  2b 87 35 c0 4b 00 01 00  01 00 02 4b 4e 00 04 c7   +·5·K······KN···
00e0  2b 85 35 c0 85 00 01 00  01 00 02 11 07 00 04 c7   +·5·············
00f0  2b 86 35 c0 6b 00 01 00  01 00 00 08 4d 00 04 c7   +·5·k·······M···
0100  04 8a 35 c0 95 00 1c 00  01 00 02 4b 4e 00 10 20   ··5········KN··
0110  01 05 00 00 8f 00 00 00  00 00 00 00 00 00 53 c0   ··············S·
0120  4b 00 1c 00 01 00 02 4b  4e 00 10 20 01 05 00 00   K······K N······
0130  8d 00 00 00 00 00 00 00  00 00 53 c0 85 00 1c 00   ··········S·····
0140  01 00 02 11 07 00 10 20  01 05 00 00 8e 00 00 00   ················
0150  00 00 00 00 00 00 53 c0  6b 00 1c 00 01 00 00 08   ······S· k·······
0160  4d 00 10 20 01 05 00 00  89 00 00 00 00 00 00 00   M···············
0170  00 00 53                                           ··S
```

Week_1_packet_capture_1.pcapng | Packets: 18475 · Displayed: 18408 (99.6%) · Ignored: 4 (0.0%) | Profile: Default

ip.addr == 192.168.0.105

3. **Questions**
    I. What is the IP address resolved for `www.example.com`?
        A. 192.168.0.1

    II. How many HTTP packets were captured?
        A. 15

Analyzing Protocols

1. **Objective:** Dive deeper into protocol details and packet structure.
2. **Steps:**
    I. Select a single HTTP GET request packet.
    II. Expand the protocol layers (Ethernet, IP, TCP, HTTP) in the packet details pane.
    III. Note the source IP, destination IP, and the requested URL.
3. **Questions**
    I. What is the source and destination IP of the HTTP packet?
        A. Source: 192.168.0.105, Destination: 34.107.221.82

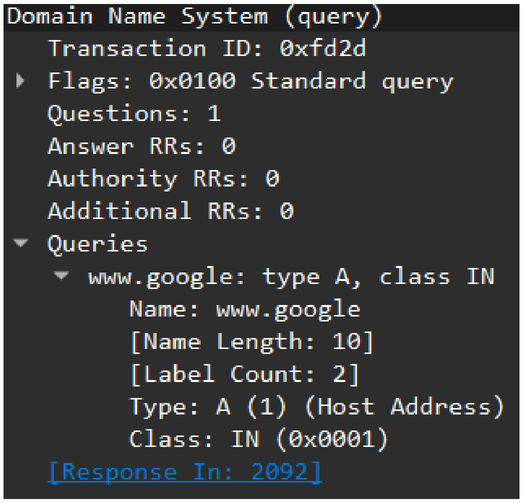
    II. What is the URL requested in the GET packet?
        A. firefox.com

Capturing Specific Traffic

1. **Objective:** Use capture filters to focus on specific traffic.
2. **Tasks:**
    I. Restart Wireshark and apply the following capture filter: `port 53` (DNS traffic).
    II. Initiate a new DNS query by visiting a new website (e.g., `www.google.com`).
    III. Stop the capture and save it as `capture_part4.pcap`.

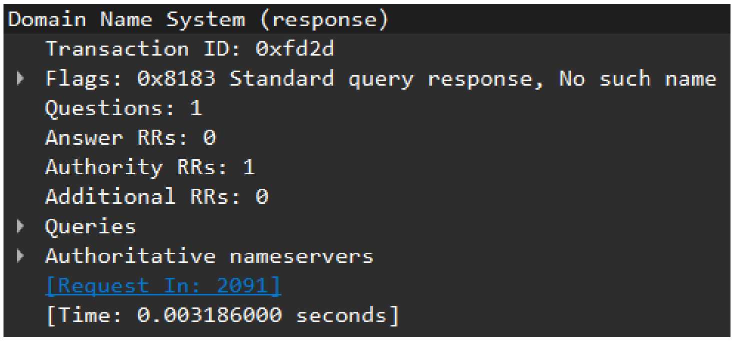
3. **Questions**

I. What is the DNS query sent for `www.google.com`?



```
Domain Name System (query)
    Transaction ID: 0xfd2d
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
      ▾ www.google: type A, class IN
            Name: www.google
            [Name Length: 10]
            [Label Count: 2]
            Type: A (1) (Host Address)
            Class: IN (0x0001)
    [Response In: 2092]
```

II. What was the response from the DNS server?



```
Domain Name System (response)
    Transaction ID: 0xfd2d
  ▸ Flags: 0x8183 Standard query response, No such name
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
  ▸ Queries
  ▸ Authoritative nameservers
    [Request In: 2091]
    [Time: 0.003186000 seconds]
```