

## SECTION: K

**Terminal**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-I>

No.	Time	Source	Destination	Protocol	Length	Info
16	0.709979875	10.1.10.42	224.0.0.251	TCP	122	Standard query response 0x0000 AAAA, cache flush fe80::c80c:f540:7d3:cab7 A, cache flush 10.1.10.42
17	0.931621525	fe80::a913:6c27:c1c0::	ff02::fb	MNMS	224	Standard query 0x0000 ANY d.8.d.6.c.1.c.7.2.c.6.3.1.9.a.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.f.ip6.arpa, "Q"
18	0.931695642	10.1.10.33	224.0.0.251	MNMS	204	Standard query 0x0000 ANY d.8.d.6.c.1.c.7.2.c.6.3.1.9.a.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.f.ip6.arpa, "Q"
19	0.931911907	fe80::7360:3162:43ef::	ff02::fb	MNMS	126	Standard query response 0x0000 AAAA, cache flush fe80::7360:3162:43ef:1918
20	0.932044246	10.1.10.39	224.0.0.251	MNMS	122	Standard query response 0x0000 AAAA, cache flush fe80::7360:3162:43ef:1918 A, cache flush 10.1.10.39
21	1.407788202	142.250.192.74	10.1.10.207	TLSv1.2	151	Application Data
22	1.451744432	10.1.10.207	142.250.192.74	TCP	66	36436 - 443 [ACK] Seq=1 Ack=86 Win=501 Len=0 TSval=2551205363 TSecr=682061614
23	1.457274844	fe80::11a:e76:c149::	ff02::fb	MNMS	225	Standard query 0x0000 PTR _ftp._tcp._tcp.local, "QM" question
24	1.457746124	10.1.10.154	224.0.0.251	MNMS	205	Standard query 0x0000 PTR _ftp._tcp.local, "QM" question TXT UBUNTU18.04._sbm._tcp.local, "QM" question
25	1.670259941	10.1.10.207	192.168.3.5	DNS	74	Standard query 0xee2e A www.google.com
26	1.670552748	192.168.3.5	10.1.10.207	DNS	90	Standard query response 0xee2e A www.google.com A 172.217.31.196
27	1.670842304	10.1.10.207	172.217.31.196	ICMP	98	Echo (ping) request id=0x7488, seq=1/256, ttl=64 (no response found!)
28	1.797844238	Elitigo.as:a5:a04	Elitigo.as:a5:a06	ARP	60	Who has 10.1.10.207 Tell 10.1.10.43
29	1.797867718	Elitigo.as:a5:a06	Elitigo.as:a5:a04	ARP	42	10.1.10.207 is at b8:ae:ed:a5:a0:96
30	2.445337150	HewlettPrt.39:96:b3	Spanning-tree(for-)S	SIP	64	RST, Root = 0/9/34/64:a9:59:78:40 Cost = 22020 Port = 0x8022 [ETHERNET FRAME CHECK SEQUENCE INCORREC
31	2.642876487	10.1.10.207	13.33.171.86	TLSv1.2	105	Application Data
32	2.642924557	10.1.10.207	34.98.75.36	TCP	105	Application Data
33	2.649024063	13.33.171.86	10.1.10.207	TCP	66	443 - 50088 [ACK] Seq=1 Ack=40 Win=135 Len=0 TSval=1908354855 TSecr=1599292974
34	2.649141898	13.33.171.86	10.1.10.207	TLSv1.2	105	Application Data
35	2.652045953	34.98.75.36	10.1.10.207	TCP	66	443 - 33170 [ACK] Seq=1 Ack=40 Win=269 Len=0 TSval=3373694695 TSecr=1165458913
36	2.652065300	34.98.75.36	10.1.10.207	TLSv1.2	105	Application Data
37	2.687779875	10.1.10.207	172.217.31.196	ICMP	98	Echo (ping) request id=0x7488, seq=2/512, ttl=64 (no response found!)
38	2.687779875	10.1.10.207	172.217.31.196	ICMP	98	Echo (ping) request id=0x7488, seq=2/512, ttl=64 (no response found!)

Frame 25: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0  
Ethernet II, Src: Elitigo.as:a5:a06 (08:ae:ed:a5:a0:06), Dest: HewlettPdt:86:90 (08:00:0c:2c:62:02)  
Internet Protocol Version 4, Src: 10.1.10.207, Dst: 192.168.3.5  
User Datagram Protocol, Src Port: 47734, Dst Port: 53  
Domain Name System (query)

```

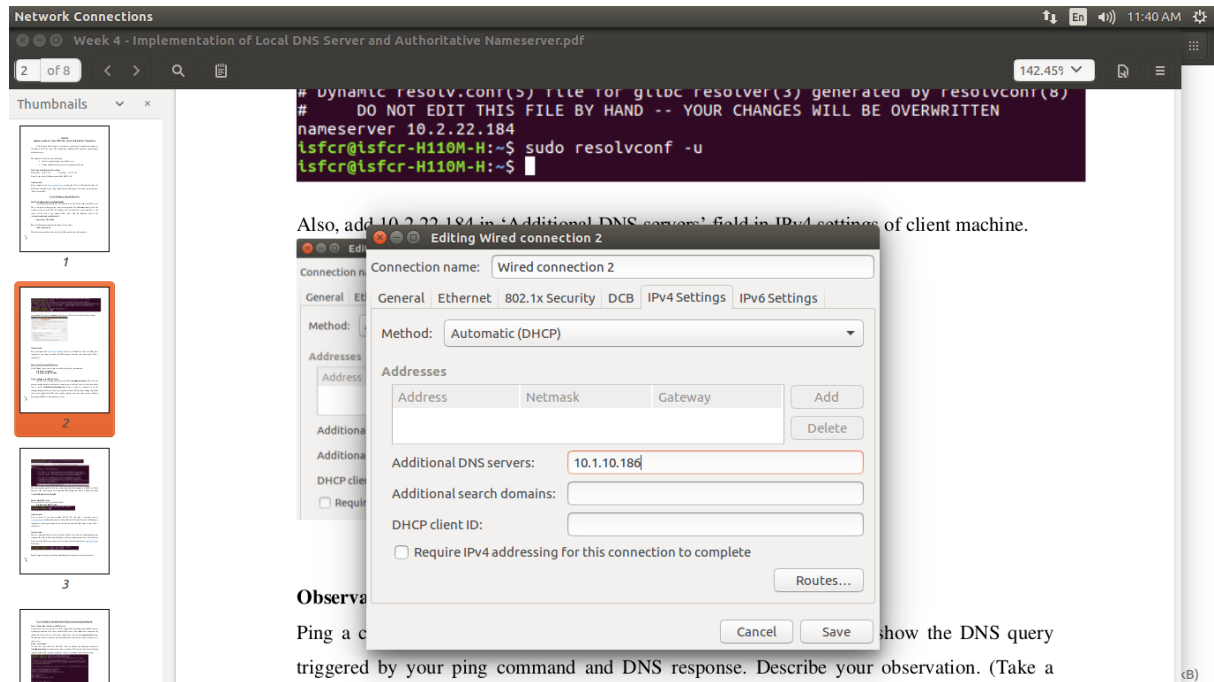
student@peassat196: ~/Desktop/621
student@peassat196:~/Desktop/621$ ping www.google.com
PING www.google.com (172.217.31.196) 56(84) bytes of data.
^C
^C
--- www.google.com ping statistics ---
26 packets transmitted, 0 received, 100% packet loss, time 25577ms

student@peassat196:~/Desktop/621$ ping www.google.com
PING www.google.com (172.217.31.196) 56(84) bytes of data.

```

wreshark epn250 20220303112818 pfVKILpcanqg

## Setting Up 10.1.10.186 (Server) as Additional DNS Server:

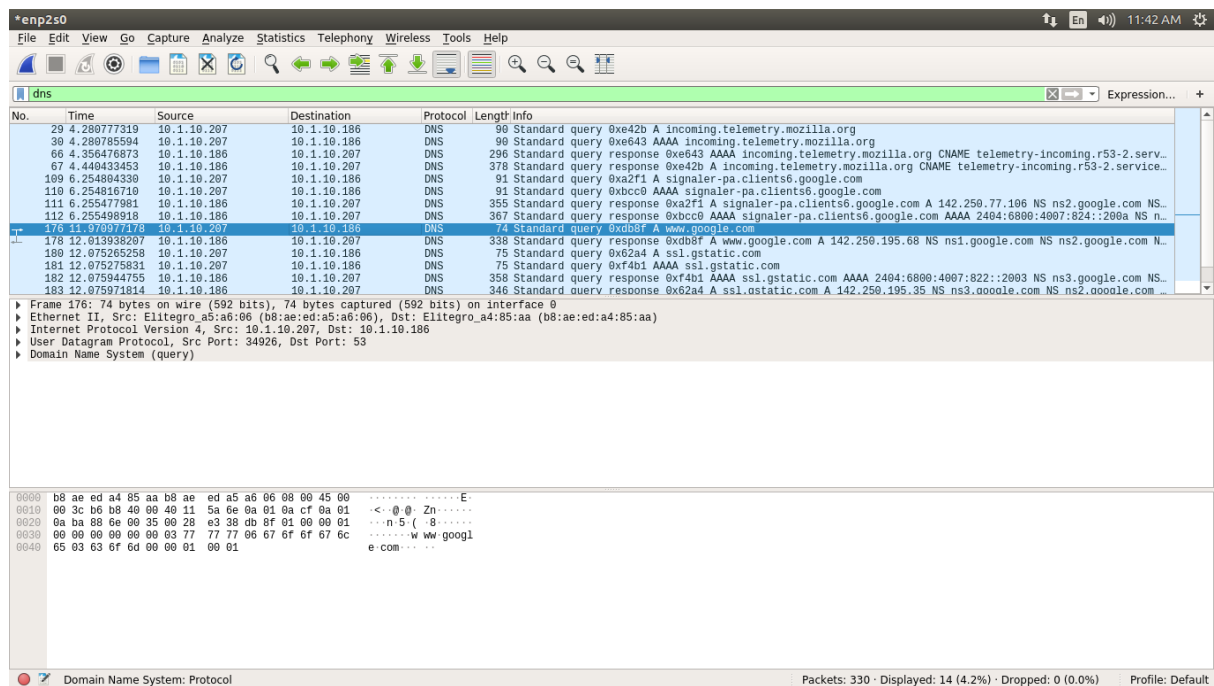


Also, add 10.1.10.186 in 'Additional DNS servers' field in IPv4 settings of client machine.

Observation 2:

Pinging a client machine (10.1.10.207) from the server (10.1.10.186) shows the DNS query triggered by your ping command and DNS response. Describe your observation. (Take a

## Observation 2:



No.	Time	Source	Destination	Protocol	Length	Info
29	4.280777319	10.1.10.207	10.1.10.186	DNS	90	Standard query 0xe42b A incoming.telemetry.mozilla.org
30	4.280785594	10.1.10.186	10.1.10.207	DNS	90	Standard query response 0xe42b A incoming.telemetry.mozilla.org
66	4.356476873	10.1.10.186	10.1.10.207	DNS	296	Standard query response 0xe42b A incoming.telemetry.mozilla.org CNAME telemetry-incoming.r53-2.serv...
67	4.440433453	10.1.10.186	10.1.10.207	DNS	378	Standard query response 0xe42b A incoming.telemetry.mozilla.org CNAME telemetry-incoming.r53-2.serv...
109	6.254894339	10.1.10.207	10.1.10.186	DNS	91	Standard query 0xa2f1 A signaler-pa.clients6.google.com
110	6.254816710	10.1.10.207	10.1.10.186	DNS	91	Standard query response 0xbcc0 AAAA signaler-pa.clients6.google.com
111	6.255477981	10.1.10.186	10.1.10.207	DNS	355	Standard query response 0xa2f1 A signaler-pa.clients6.google.com A 142.250.77.196 NS ns2.google.com NS...
112	6.255498918	10.1.10.186	10.1.10.207	DNS	367	Standard query response 0xbcc0 AAAA signaler-pa.clients6.google.com AAAA 2404:6800:4007:824::200a NS n...
176	11.970077178	10.1.10.207	10.1.10.186	DNS	74	Standard query 0xdb8f A www.google.com
178	12.013933297	10.1.10.186	10.1.10.207	DNS	338	Standard query response 0xdb8f A www.google.com A 142.250.195.68 NS ns1.google.com NS ns2.google.com N...
180	12.075285258	10.1.10.207	10.1.10.186	DNS	75	Standard query 0x62a4 A ssl.gstatic.com
181	12.075275831	10.1.10.207	10.1.10.186	DNS	75	Standard query 0xf4b1 AAAA ssl.gstatic.com
182	12.075944755	10.1.10.186	10.1.10.207	DNS	358	Standard query response 0xf4b1 AAAA ssl.gstatic.com AAAA 2404:6800:4007:822::2003 NS ns3.google.com NS...
183	12.075971814	10.1.10.186	10.1.10.207	DNS	346	Standard query response 0x62a4 A ssl.gstatic.com A 142.250.195.35 NS ns3.google.com NS ns2.google.com N...

Domain Name System (query)

Domain Name System: Protocol

Packets: 330 · Displayed: 14 (4.2%) · Dropped: 0 (0.0%) · Profile: Default

## Observation 3:

The image displays two screenshots of the Wireshark network protocol analyzer. The top screenshot shows a capture of DNS traffic on interface eth0. The packet list pane on the left shows a series of DNS queries and responses. The packet details pane on the right shows the structure of a DNS query for 'www.google.com'. The packet bytes pane at the bottom shows the raw data of the query. A terminal window is overlaid on the right side of the top screenshot, showing a ping command being executed from a host named 'student@pessat196'. The ping command is 'ping www.google.com', and the output shows 'PING www.google.com (142.250.195.68) 56(84) bytes of data.' followed by '6 packets transmitted, 0 received, 100% packet loss, time 5099ms'. The bottom screenshot shows a capture of DNS traffic on interface eth0. The packet list pane on the left shows a series of DNS queries and responses. The packet details pane on the right shows the structure of a DNS query for 'www.example.com'. The packet bytes pane at the bottom shows the raw data of the query. A terminal window is overlaid on the right side of the bottom screenshot, showing a ping command being executed from a host named 'student@pessat196'. The ping command is 'ping www.example.com', and the output shows 'PING www.example.com (192.168.0.101) 56(84) bytes of data.' followed by '6 packets transmitted, 0 received, 100% packet loss, time 5099ms'.

**Terminal Output (Top Screenshot):**

```
student@pessat196:~$ ping www.google.com
PING www.google.com (142.250.195.68) 56(84) bytes of data.
6 packets transmitted, 0 received, 100% packet loss, time 5099ms
student@pessat196:~$
```

**Wireshark Packet List (Top Screenshot):**

No.	Time	Source	Destination	Protocol	Length	Info
9	0.551834418	10.1.10.186	10.1.10.207	DNS	358	Standard query response 0xb7d A safebrowsing.googleapis.com A 142.250.192.74 NS ns3.google.com NS ns1.google.com
10	0.951876315	10.1.10.186	10.1.10.207	DNS	370	Standard query response 0xe391 A safebrowsing.googleapis.com A 142.250.192.74 NS ns4.google.com NS ns3.google.com
11	0.951889634	10.1.10.186	10.1.10.207	DNS	74	Standard query 0x8b5e A www.google.com
37	1.233214835	10.1.10.207	10.1.10.186	DNS	338	Standard query response 0x8b5e A www.google.com A 142.250.195.68 NS ns4.google.com NS ns2.google.com NS ns...
41	2.278789641	10.1.10.186	10.1.10.207	DNS	84	Standard query 0xe406 A detectportal.firefox.com
46	3.744282188	10.1.10.207	192.168.3.5	DNS	84	Standard query 0xe406 A detectportal.firefox.com
47	3.744295991	10.1.10.207	4.2.2.2	DNS	84	Standard query 0xe406 A detectportal.firefox.com
48	3.744301761	10.1.10.207	202.138.96.2	DNS	84	Standard query 0xe406 A detectportal.firefox.com
49	3.744307206	10.1.10.207	202.138.103.100	DNS	84	Standard query 0xe406 A detectportal.firefox.com
50	3.744313929	10.1.10.207	19.1.10.186	DNS	84	Standard query 0xe406 A detectportal.firefox.com
51	3.744325555	10.1.10.207	202.138.96.2	DNS	84	Standard query 0xf2d1 AAAA detectportal.firefox.com
52	3.744694066	192.168.3.5	10.1.10.207	DNS	195	Standard query response 0xe406 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME prod.de...
53	3.747728166	10.1.10.207	192.168.3.5	DNS	84	Standard query 0x34cf A detectportal.firefox.com
54	3.748984859	192.168.3.5	10.1.10.207	DNS	195	Standard query response 0x34cf A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME prod.de...

**Wireshark Packet List (Bottom Screenshot):**

No.	Time	Source	Destination	Protocol	Length	Info
5	2.955893068	10.1.10.207	10.1.10.186	DNS	86	Standard query 0x7ab9 A www.example.com OPT
6	2.955893068	10.1.10.186	10.1.10.207	DNS	165	Standard query response 0x7ab9 A www.example.com A 192.168.0.101 NS ns.example.com A 192.168.0.10 OPT
7	3.914291637	10.1.10.207	10.1.10.186	DNS	84	Standard query 0x4c3c A detectportal.firefox.com
8	3.914311188	10.1.10.207	10.1.10.186	DNS	84	Standard query 0xf3f9 AAAA detectportal.firefox.com
10	3.915078822	10.1.10.186	10.1.10.207	DNS	313	Standard query response 0x4c3c A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME pro...
14	3.935406011	10.1.10.207	10.1.10.186	DNS	71	Standard query 0x4e5b A example.org
15	3.935414834	10.1.10.207	10.1.10.186	DNS	71	Standard query 0x0433 AAAA example.org
16	3.935456897	10.1.10.207	10.1.10.186	DNS	71	Standard query 0xa0c6 A example.org
17	3.935487691	10.1.10.207	10.1.10.186	DNS	73	Standard query 0x2e6d A ipv4only.arpa
18	3.935491799	10.1.10.207	10.1.10.186	DNS	73	Standard query 0xa265 AAAA ipv4only.arpa
21	3.936444235	10.1.10.207	10.1.10.186	DNS	84	Standard query 0x552d A detectportal.firefox.com
22	3.936449549	10.1.10.207	10.1.10.186	DNS	84	Standard query 0xc17d AAAA detectportal.firefox.com
25	3.988982373	10.1.10.186	10.1.10.207	DNS	371	Standard query response 0x2e6d A ipv4only.arpa A 192.0.0.170 A 192.0.0.171 NS c.iana-servers.net NS ns...
26	3.988165000	10.1.10.186	10.1.10.207	DNS	130	Standard query response 0xa265 AAAA ipv4only.arpa SOA sns.dns.icann.org

# Dig www.example.com

Terminal

Week 4 - Implementation of Local DNS Server and Authoritative Nameserver.pdf

7 of 8

142.459

12:32 PM

Thumbnails

5

6

7

8

80%

We can see that the ANSWER SECTION contains the DNS mapping. We can see that the IP address of [www.example.com](http://www.example.com) is now 192.168.0.101, which is what we have setup in the DNS server.

student@pessat196:~\$ dig www.example.com

```
;; MSG SIZE rcvd: 93
student@pessat196:~$ dig www.example.com
;<<<> Dig 9.10.3-P4-Ubuntu <<<> www.example.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 31417
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;; www.example.com.                IN      A
;; ANSWER SECTION:
;; www.example.com.                259200  IN      A      192.168.0.101
;; AUTHORITY SECTION:
;; example.com.                    259200  IN      NS      ns.example.com.
;; ADDITIONAL SECTION:
;; ns.example.com.                 259200  IN      A      192.168.0.10
Step 3: Observe the results
```

\*nmap2s0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
5	2.955893068	10.1.10.207	10.1.10.186	DNS	86	Standard query 0x7ab9 A www.example.com OPT
6	2.955893068	10.1.10.186	10.1.10.207	DNS	185	Standard query response 0x7ab9 A www.example.com A 192.168.0.101 NS ns.example.com A 192.168.0.10 OPT
7	3.914291637	10.1.10.207	10.1.10.186	DNS	84	Standard query 0x4c3c A detectportal.firefox.com
8	3.914311188	10.1.10.207	10.1.10.186	DNS	84	Standard query 0x3f39 AAAA detectportal.firefox.com
9	3.915078822	10.1.10.186	10.1.10.207	DNS	313	Standard query response 0x4c3c A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME pro...
14	3.935496011	10.1.10.207	10.1.10.186	DNS	71	Standard query 0x4e5b A example.org
15	3.935414834	10.1.10.207	10.1.10.186	DNS	71	Standard query 0x0433 AAAA example.org
16	3.935456897	10.1.10.207	10.1.10.186	DNS	71	Standard query 0xa0c6 A example.org
17	3.935487691	10.1.10.207	10.1.10.186	DNS	73	Standard query 0x2e6d A ipv4only.arpa
18	3.935491799	10.1.10.207	10.1.10.186	DNS	73	Standard query 0xa265 AAAA ipv4only.arpa
21	3.936444235	10.1.10.207	10.1.10.186	DNS	84	Standard query 0x552d A detectportal.firefox.com
22	3.936449549	10.1.10.207	10.1.10.186	DNS	84	Standard query 0xc17d AAAA detectportal.firefox.com
25	3.988982373	10.1.10.186	10.1.10.207	DNS	371	Standard query response 0x2e6d A ipv4only.arpa A 192.0.0.170 A 192.0.0.171 NS c.iana-servers.net NS...
26	3.988165000	10.1.10.186	10.1.10.207	DNS	130	Standard query response 0xa265 AAAA ipv4only.arpa SOA sns.dns.icann.org

Frame 6: 135 bytes on wire (1080 bits), 135 bytes captured (1080 bits) on interface 0

Ethernet II, Src: Elitrogo\_a4:85:aa (b8:ae:ed:a4:85:aa), Dst: Elitrogo\_a5:a6:06 (b8:ae:ed:a5:a6:06)

Internet Protocol Version 4, Src: 10.1.10.186, Dst: 10.1.10.207

User Datagram Protocol, Src Port: 53, Dst Port: 44883

Domain Name System (response)

Transaction ID: 0x7ab9

Flags: 0x8580 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 1

Additional RRs: 2

Queries

www.example.com: type A, class IN

Answers

www.example.com: type A, class IN, addr 192.168.0.101

Name: www.example.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 259200

Data length: 4

Address: 192.168.0.101

Authoritative nameservers

example.com: type NS, class IN, ns ns.example.com

Additional records

[Request In: 5]

[Time: 0.000564322 seconds]

0000 b8 ae ed a5 a6 06 b8 ae ed a4 85 aa 08 00 45 00 .....E-

0010 00 79 06 f5 00 00 40 11 49 f5 0a 01 0a ba 0a 01 y...@.I.....

wireshark\_nmap2s0\_20220303123158\_3nLXzp.cpng

Packets: 45 · Displayed: 24 (53.3%) · Dropped: 0 (0.0%) Profile: Default

## 2. Server Side

IP address is 10.1.10.186

```
Terminal
student@pessat196:~
Preparing to unpack .../bind9_1:9.10.3.dfsg.P4-8ubuntu1.19_amd64.deb ...
Unpacking bind9 (1:9.10.3.dfsg.P4-8ubuntu1.19) ...
Processing triggers for libc-bin (2.23-0ubuntu11.3) ...
Processing triggers for man-db (2.7.5-1) ...
Processing triggers for ufw (0.35-0ubuntu2) ...
Processing triggers for ureadahead (0.100.0-19.1) ...
ureadahead will be reprofiled on next reboot
Processing triggers for systemd (229-4ubuntu21.31) ...
Setting up libirs141:amd64 (1:9.10.3.dfsg.P4-8ubuntu1.19) ...
Setting up bind9utils (1:9.10.3.dfsg.P4-8ubuntu1.19) ...
Setting up bind9 (1:9.10.3.dfsg.P4-8ubuntu1.19) ...
Adding group 'bind' (GID 132) ...
Done.
Adding system user 'bind' (UID 123) ...
Adding new user 'bind' (UID 123) with group 'bind' ...
Not creating home directory '/var/cache/bind'.
wrote key file '/etc/bind/rndc.key'
#
Processing triggers for libc-bin (2.23-0ubuntu11.3) ...
Processing triggers for ureadahead (0.100.0-19.1) ...
Processing triggers for systemd (229-4ubuntu21.31) ...
Processing triggers for ufw (0.35-0ubuntu2) ...
student@pessat196:~$ ifconfig
enp2s0    Link encap:Ethernet  HWaddr b8:ae:ed:a4:85:aa
          inet addr:10.1.10.186  Bcast:10.1.10.255  Mask:255.255.255.0
          inet6 addr: fe80::ca55:48a0:338e:3f0c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:328115 errors:0 dropped:0 overruns:0 frame:0
          TX packets:242383 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:110992248 (110.9 MB)  TX bytes:26364708 (26.3 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:128186 errors:0 dropped:0 overruns:0 frame:0
          TX packets:128186 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:18727582 (18.7 MB)  TX bytes:18727582 (18.7 MB)

student@pessat196:~$
```

## Dump.db

```
Terminal File Edit View Search Terminal Help
214 NS ns-cloud-d2.googledomains.com.
214 NS ns-cloud-d3.googledomains.com.
214 NS ns-cloud-d4.googledomains.com.
; ns-cloud-c3.googledomains.com [v4 TTL 1714] [v6 TTL 1714] [v4 success] [v6 success]
; ns-cloud-a4.googledomains.com [v4 TTL 1714] [v6 TTL 1714] [v4 success] [v6 success]
; ns-cloud-a1.googledomains.com [v4 TTL 1714] [v6 TTL 1714] [v4 success] [v6 success]
; ns-cloud-d3.googledomains.com [v4 TTL 1714] [v6 TTL 1714] [v4 success] [v6 success]
; ns-cloud-e3.googledomains.com [v4 TTL 1714] [v6 TTL 1714] [v4 success] [v6 success]
; ns-cloud-c4.googledomains.com [v4 TTL 1714] [v6 TTL 1714] [v4 success] [v6 success]
; ns-cloud-cl.googledomains.com [v4 TTL 1714] [v6 TTL 1714] [v4 success] [v6 success]
; ns-cloud-a2.googledomains.com [v4 TTL 1714] [v6 TTL 1714] [v4 success] [v6 success]
; ns-cloud-d4.googledomains.com [v4 TTL 1714] [v6 TTL 1714] [v4 success] [v6 success]
; ns-cloud-d1.googledomains.com [v4 TTL 1714] [v6 TTL 1714] [v4 success] [v6 success]
; ns-cloud-e4.googledomains.com [v4 TTL 1714] [v6 TTL 1714] [v4 success] [v6 success]
; ns-cloud-c2.googledomains.com [v4 TTL 1714] [v6 TTL 1714] [v4 success] [v6 success]
; ns-cloud-a3.googledomains.com [v4 TTL 1714] [v6 TTL 1714] [v4 success] [v6 success]
; ns-cloud-d2.googledomains.com [v4 TTL 1714] [v6 TTL 1714] [v4 success] [v6 success]
; ns-cloud-e2.googledomains.com [v4 TTL 1714] [v6 TTL 1714] [v4 success] [v6 success]
student@pessat196:~$ grep google.com /var/cache/bind/named_dump.db
google.com. 172702 NS ns1.google.com.
172702 NS ns2.google.com.
172702 NS ns3.google.com.
172702 NS ns4.google.com.
signaler-pa.clients6.google.com. 227 A 142.250.196.42
ns1.google.com. 172700 A 216.239.32.10
ns2.google.com. 172700 A 216.239.34.10
ns3.google.com. 172700 A 216.239.36.10
ns4.google.com. 172700 A 216.239.38.10
www.google.com. 202 A 142.250.195.68
googleapis.com. 172700 NS ns1.google.com.
172700 NS ns2.google.com.
172700 NS ns3.google.com.
172700 NS ns4.google.com.
gstatic.com. 172753 NS ns1.google.com.
172753 NS ns2.google.com.
172753 NS ns3.google.com.
172753 NS ns4.google.com.
student@pessat196:~$
```

## Observation Notebook Requirements:

1) Locate the DNS query and response messages. Are they sent over UDP or TCP?

Ans: UDP

2) What is the destination port for the DNS query message? What is the source port of DNS response messages?

Ans: 53

3) To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

Ans: 10.1.10.186

4) Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

Ans: Type A as it requests for an authoritative record. No answer

5) Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

Ans:

CNAME RR: Tells that the hostname flipkart.com refers to the canonical hostname www.flipkart.com.

A type RR: Provides the IP Address of the canonical hostname.

6) Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

Ans: Destination IP Address corresponds to the IP address of flipkart.com