**Name**: Khushei Meghana Meda

**SRN**: PES1201800416

**Week number**: 4

**Name of experiment**: Implementation of a Local DNS Server

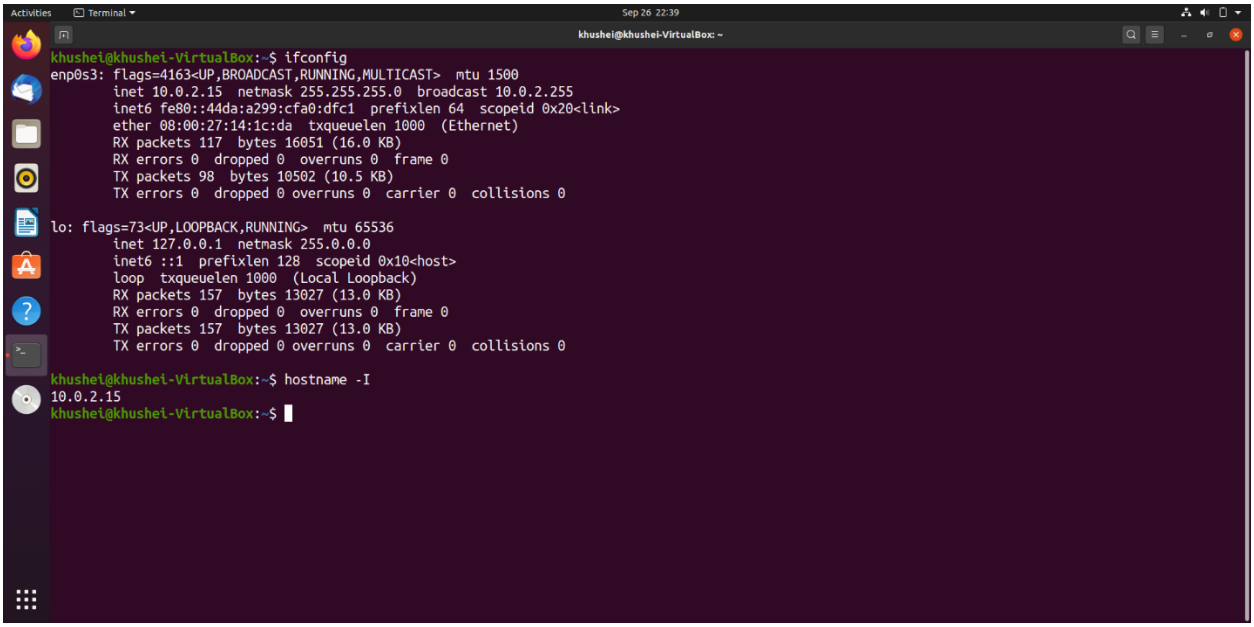
**Date**: 30-09-2020

**Objectives of the experiment**: The objectives of this lab are to understand:
- DNS and how it works
- Install and set up a DNS server
- Functionality and operations

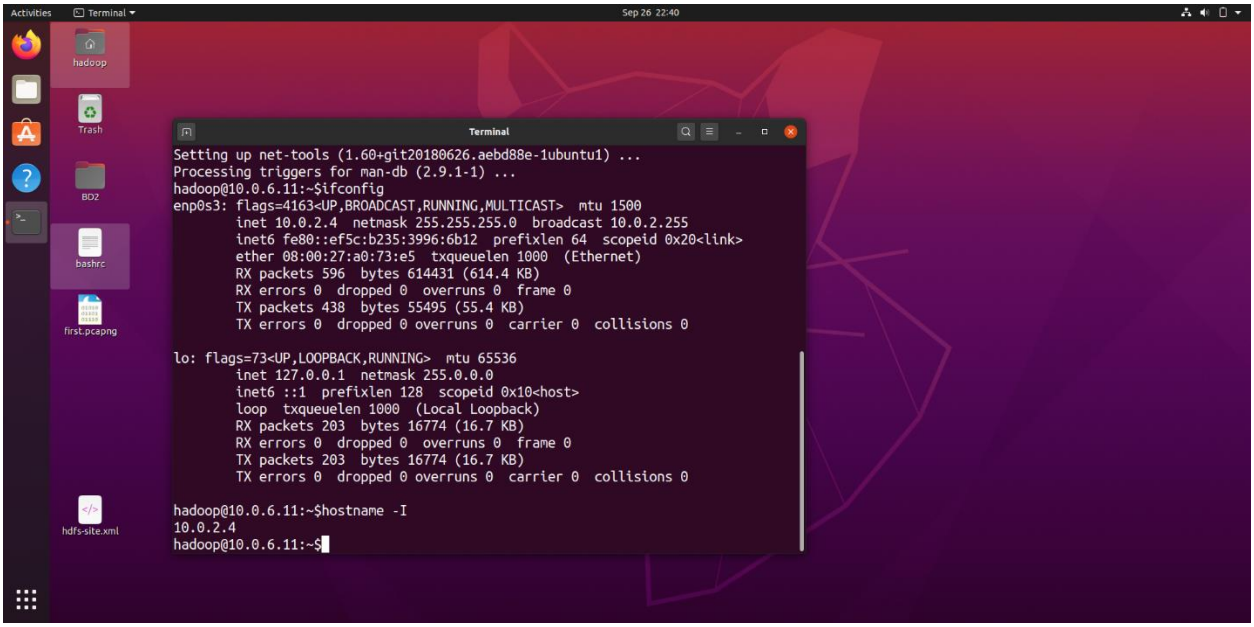
**Lab Setup**

DNS Server: 10.0.2.15 User/Client: 10.0.2.4

Server:

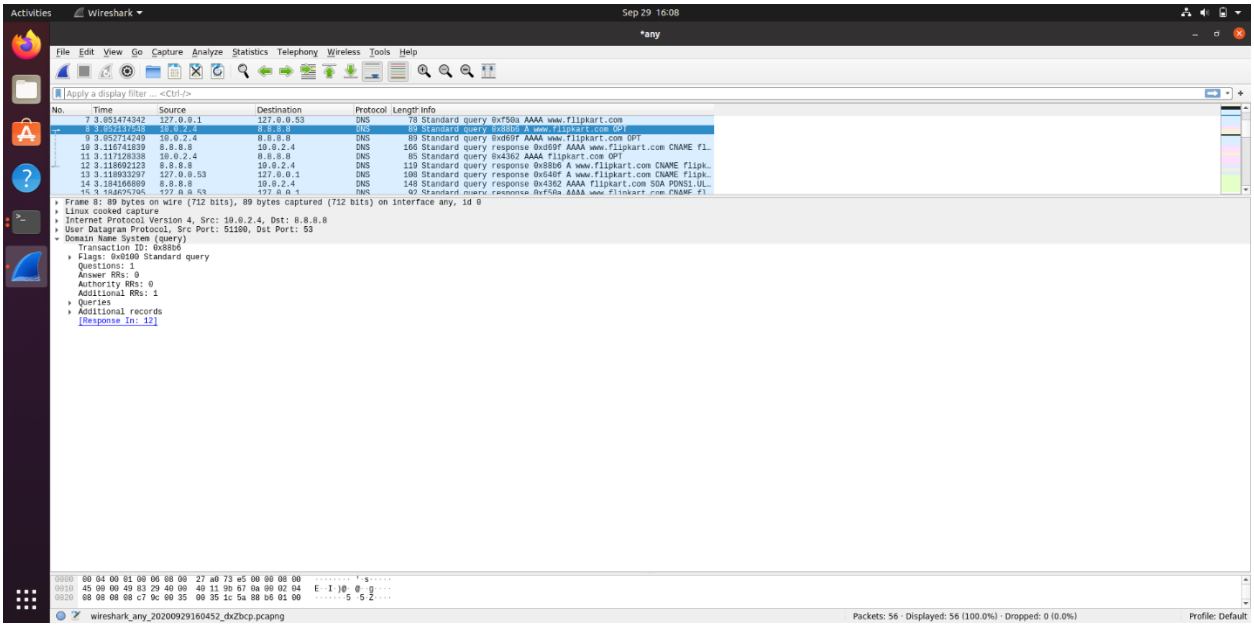


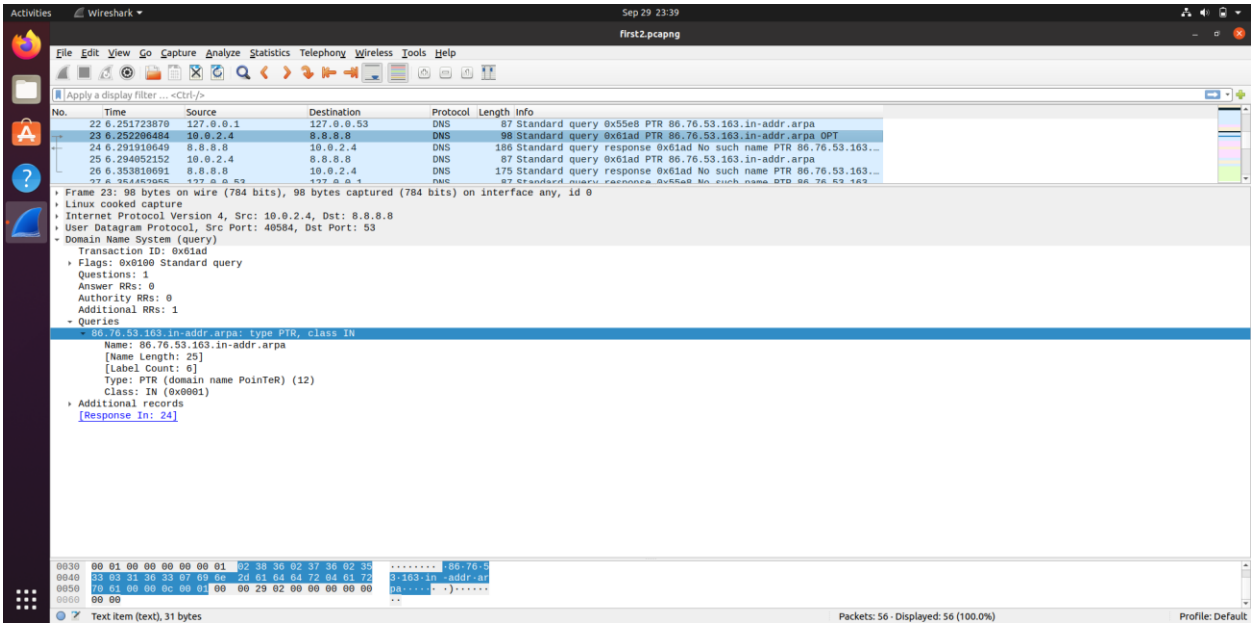

Client:



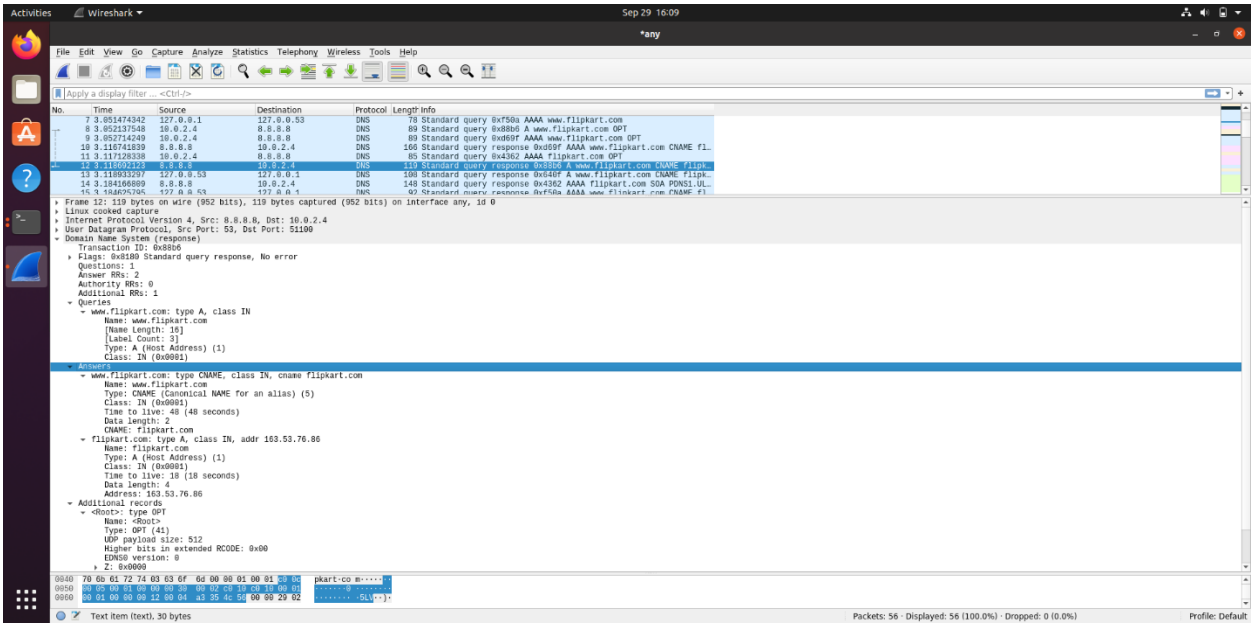

**First Test:**

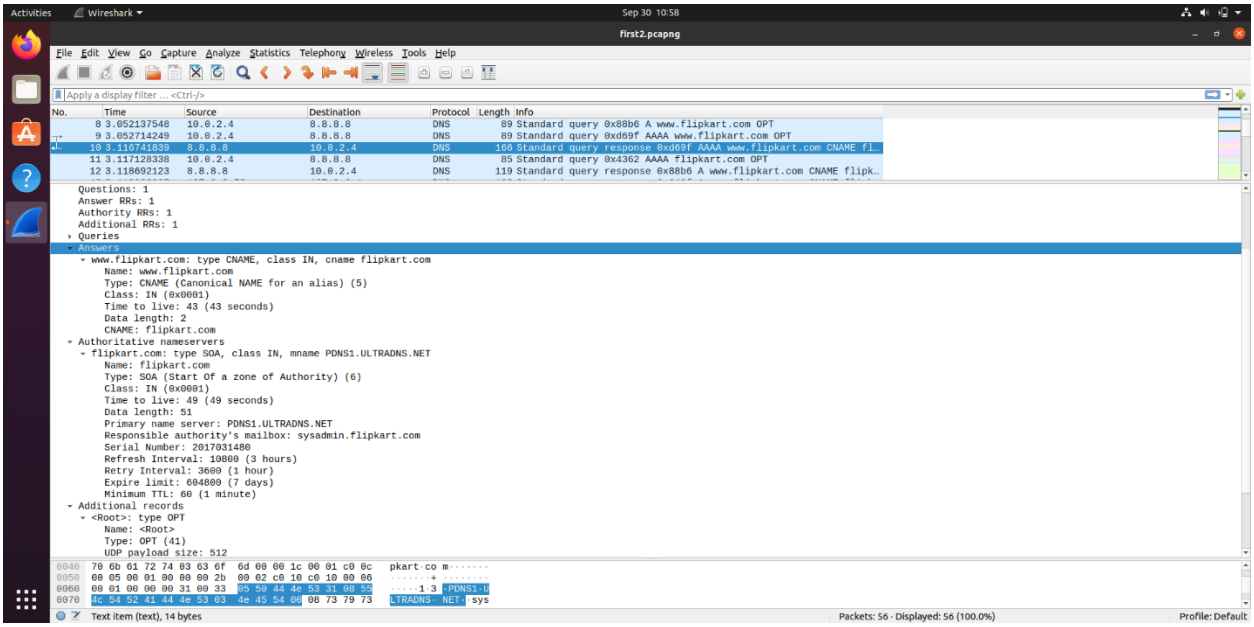
Queries-

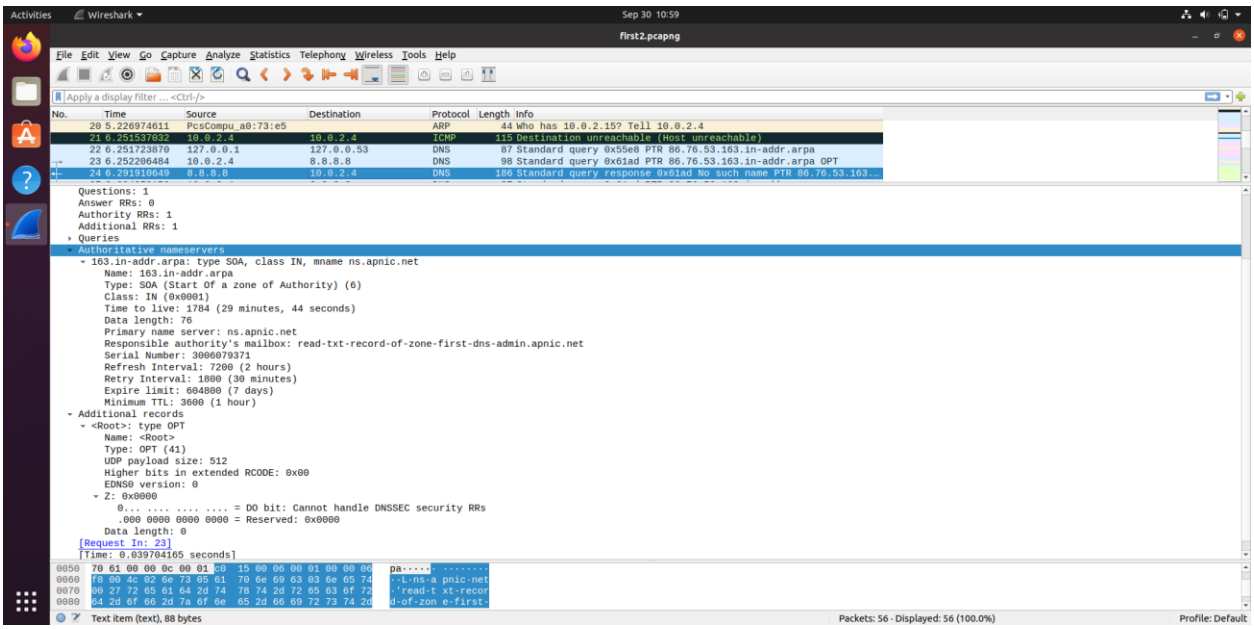



Activities
Wireshark
Sep 29 23:39
first2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
22 6.251723870 127.0.0.1 127.0.0.53 DNS 87 Standard query 0x55e8 PTR 86.76.53.163.in-addr.arpa
23 6.252296484 10.0.2.4 8.8.8.8 DNS 98 Standard query 0x61ad PTR 86.76.53.163.in-addr.arpa OPT
24 6.291910649 8.8.8.8 10.0.2.4 DNS 186 Standard query response 0x61ad No such name PTR 86.76.53.163...
25 6.294052152 10.0.2.4 8.8.8.8 DNS 87 Standard query 0x61ad PTR 86.76.53.163.in-addr.arpa
26 6.353810691 8.8.8.8 10.0.2.4 DNS 175 Standard query response 0x61ad No such name PTR 86.76.53.163...
Frame 23: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 40584, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x61ad
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
Queries
86.76.53.163.in-addr.arpa: type PTR, class IN
Name: 86.76.53.163.in-addr.arpa
[Name Length: 25]
[Label Count: 6]
Type: PTR (domain name PoinTeR) (12)
Class: IN (0x0001)
Additional records
[Response In: 24]
Text item (text), 31 bytes
Packets: 56 · Displayed: 56 (100.0%)
Profile: Default

Responses-


Activities
Wireshark
Sep 29 16:09
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
7 3.051474342 127.0.0.1 127.0.0.53 DNS 78 Standard query 0xf50a AAAA www.flipkart.com
8 3.052137548 10.0.2.4 8.8.8.8 DNS 89 Standard query 0x88b6 A www.flipkart.com OPT
9 3.052714249 10.0.2.4 8.8.8.8 DNS 89 Standard query 0xd69f AAAA www.flipkart.com OPT
10 3.116741839 8.8.8.8 10.0.2.4 DNS 166 Standard query response 0xd69f AAAA www.flipkart.com CNAME fl...
11 3.117128338 10.0.2.4 8.8.8.8 DNS 85 Standard query 0x4362 AAAA flipkart.com OPT
12 3.118602123 8.8.8.8 10.0.2.4 DNS 119 Standard query response 0x88b6 A www.flipkart.com CNAME flipk...
13 3.118703327 127.0.0.53 127.0.0.1 DNS 108 Standard query response 0x640f A www.flipkart.com CNAME flipk...
14 3.184166899 8.8.8.8 10.0.2.4 DNS 148 Standard query response 0x4362 AAAA flipkart.com SOA PDNS1.UL...
15 3.184925795 127.0.0.53 127.0.0.1 DNS 92 Standard query response 0xf50a AAAA www.flipkart.com CNAME fl...
Frame 12: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 10.0.2.4
User Datagram Protocol, Src Port: 53, Dst Port: 51100
Domain Name System (response)
Transaction ID: 0x88b6
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 1
Queries
www.flipkart.com: type A, class IN
Name: www.flipkart.com
[Name Length: 16]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
Answers
www.flipkart.com: type CNAME, class IN, cname flipkart.com
Name: www.flipkart.com
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 48 (48 seconds)
Data length: 2
CNAME: flipkart.com
flipkart.com: type A, class IN, addr 163.53.76.86
Name: flipkart.com
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 18 (18 seconds)
Data length: 4
Address: 163.53.76.86
Additional records
<Root>: type OPT
Name: <Root>
Type: OPT (41)
UDP payload size: 512
Higher bits in extended RCODE: 0x00
EDNS0 version: 0
Z: 0x0000
Text item (text), 30 bytes
Packets: 56 · Displayed: 56 (100.0%) · Dropped: 0 (0.0%)
Profile: Default




Observation: The ping request is resolved by first requesting the ISP; the DNS request created is A record, which requests TLD and that requests Authoritative Servers for the IP address.

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

They are sent over UDP.

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

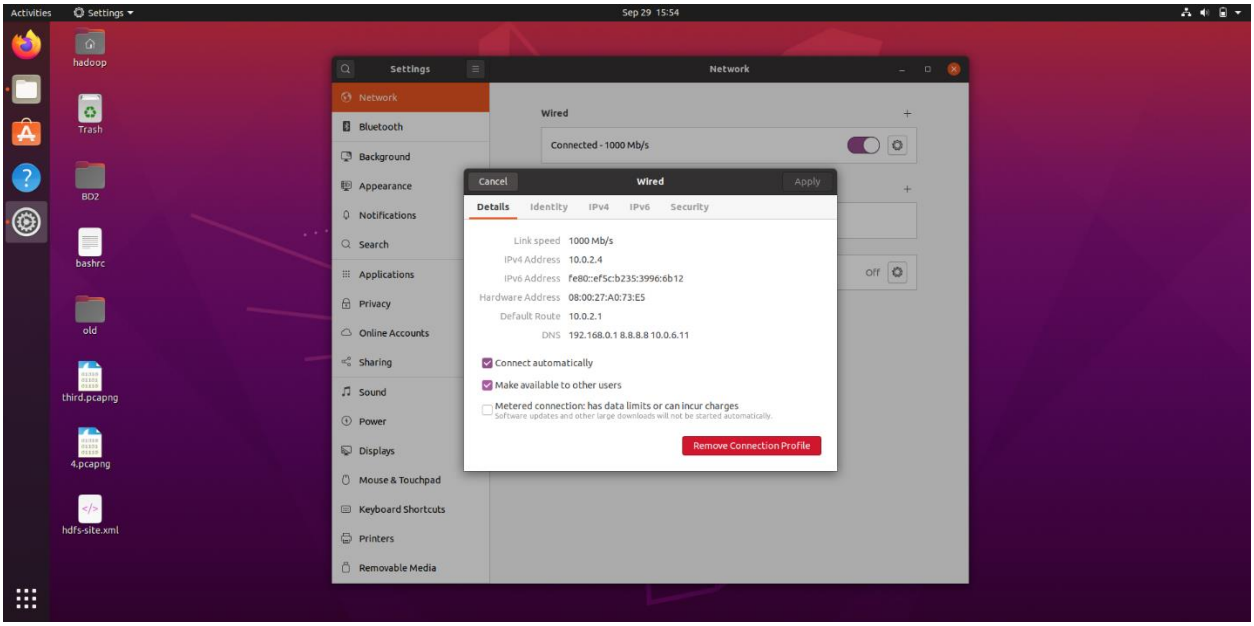
Destination Port for DNS query message: 53

Source Port for DNS response message: 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?

The DNS query message is sent to 8.8.8.8. As we can see in the screenshot below, the IP address is present in the list of IP addresses for my local DNS server.

8.8.8.8 comes by default in the list of DNS for every connection that is already created or I create on my own.




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

The query highlighted in the first screenshot is a Type A Standard Query which stores hostname and its corresponding IPv4 address.

Below that we can also see Type AAAA Standard Query which stores hostname and its corresponding IPv6 address.

In the second screenshot, we can also see one PTR query message that resolves an IP address to a domain or host name, unlike an A record which points a domain name to an IP address.

The query messages do not contain any answers.

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

2 answers are provided in the response message for the A type query. The answers contain name of the host, type of the address, class, TTL, data length. The first answer has CNAME (has the canonical name of www.flipkart.com as flipkart.com) in the end and the second answer has the IP address.

Answers

www.flipkart.com: type CNAME, class IN, cname flipkart.com

Name: www.flipkart.com

Type: CNAME (Canonical NAME for an alias) (5)

Class: IN (0x0001)

Time to live: 48 (48 seconds)

Data length: 2

CNAME: flipkart.com

flipkart.com: type A, class IN, addr 163.53.76.86

Name: flipkart.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 18 (18 seconds)

Data length: 4

Address: 163.53.76.86

1 answer is provided in the response message for the AAAA type query. It has a CNAME record.

Answers

www.flipkart.com: type CNAME, class IN, cname flipkart.com

Name: www.flipkart.com

Type: CNAME (Canonical NAME for an alias) (5)

Class: IN (0x0001)

Time to live: 43 (43 seconds)

Data length: 2

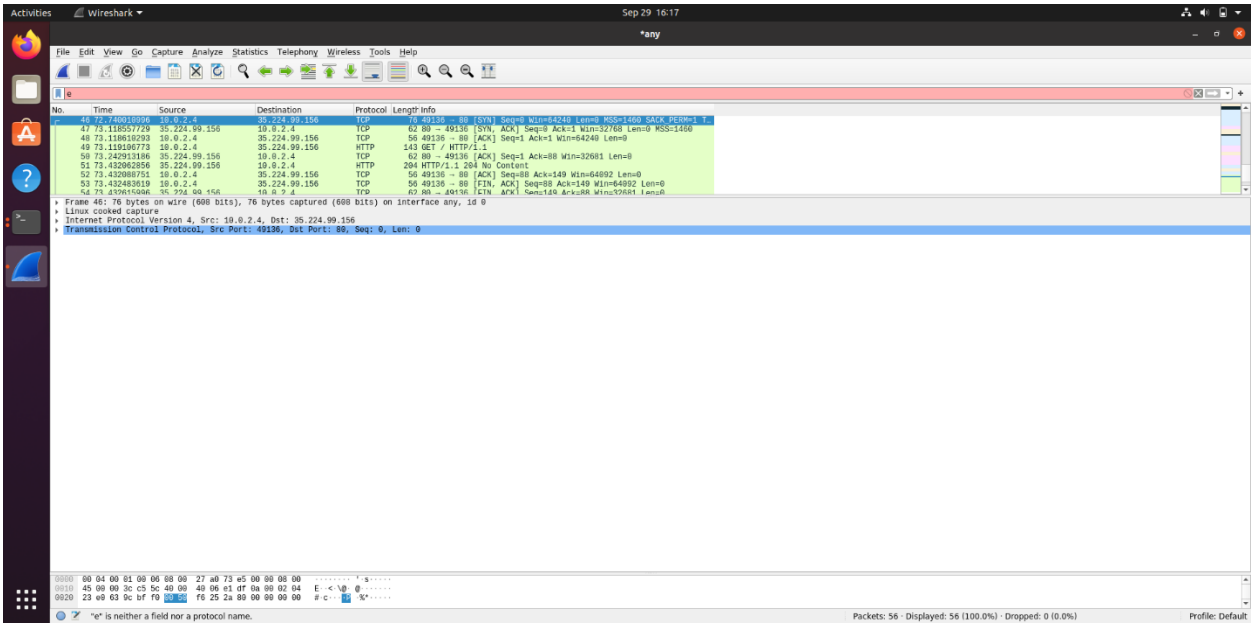
CNAME: flipkart.com

0 answers are provided for the PTR type query.

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?

No, the destination IP address of the SYN packet does not correspond to any of the IP addresses provided in the DNS response message. I get the IP address as 35.224.99.156 which is of Google Cloud.

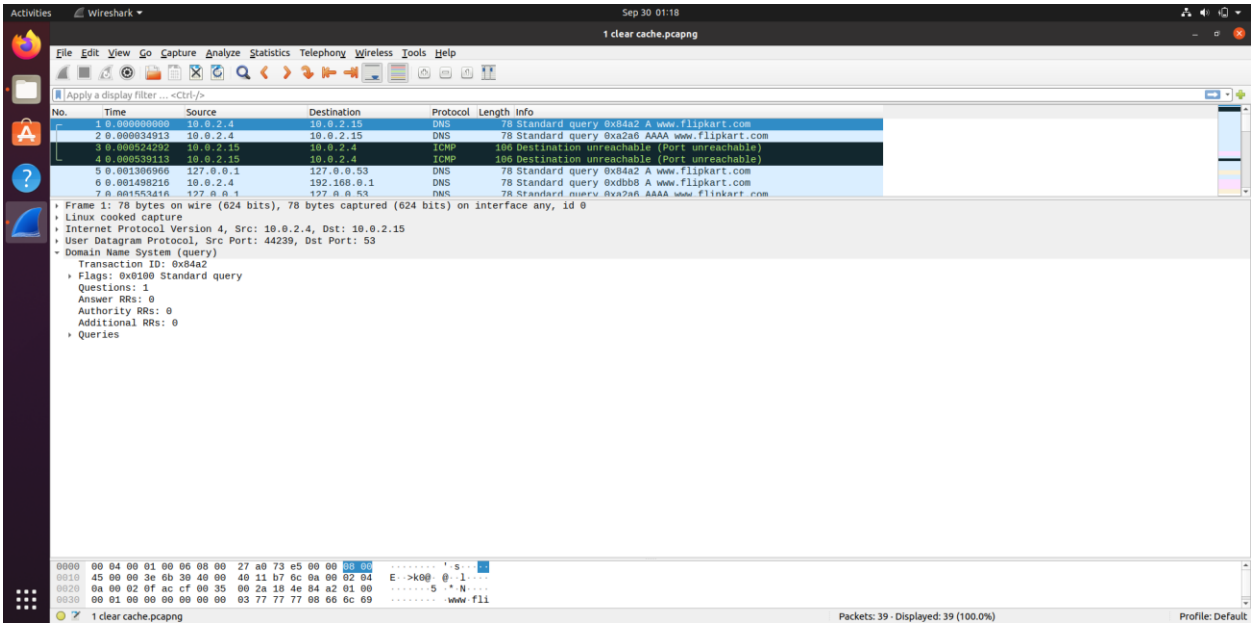
[Note: As I understand, I was supposed to get an IP address that was returned in the Answers section of the DNS response. However, despite trying three-four times this is what I got.]

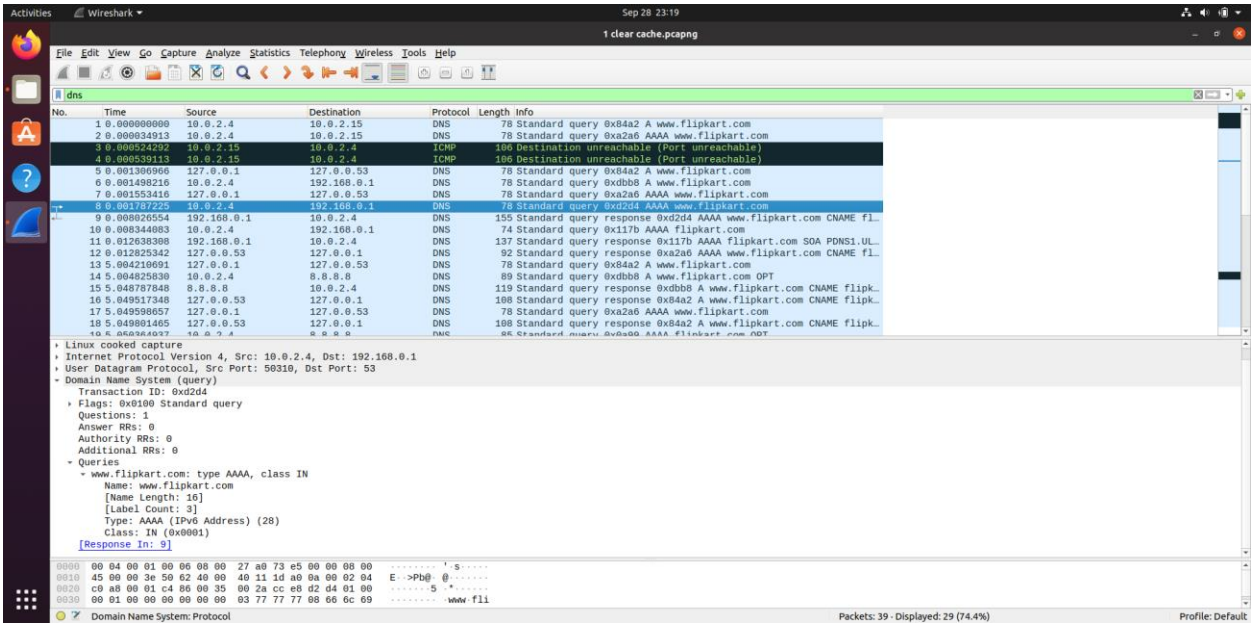


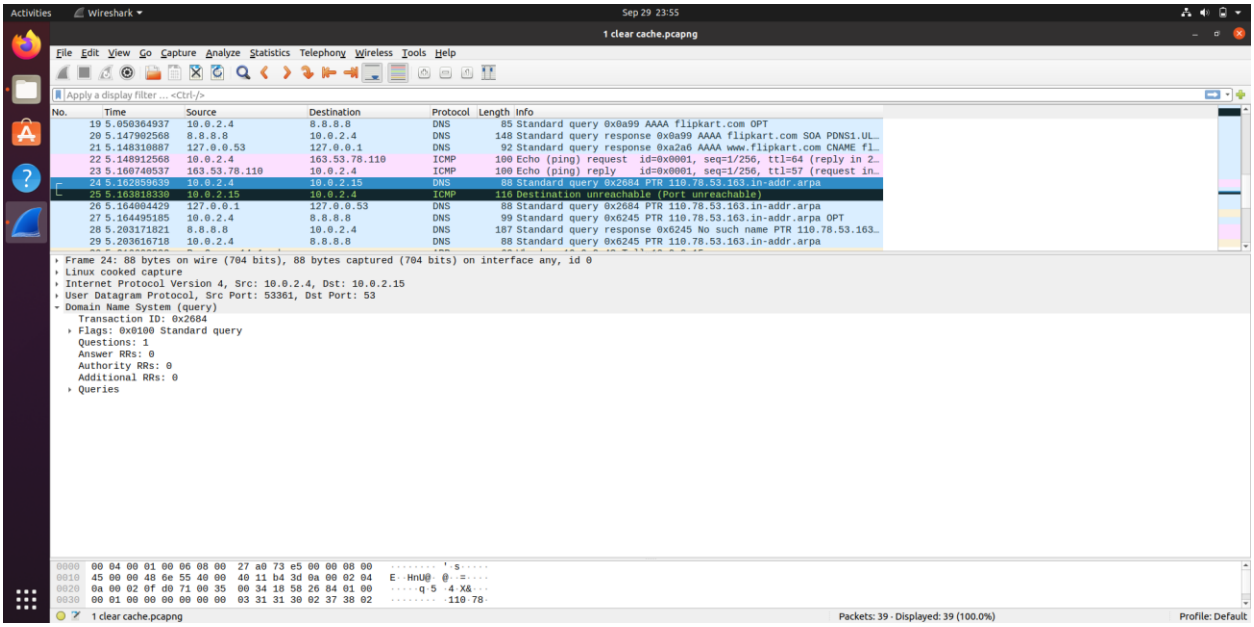
## Task 1: Configure the User Machine

## Second Test:

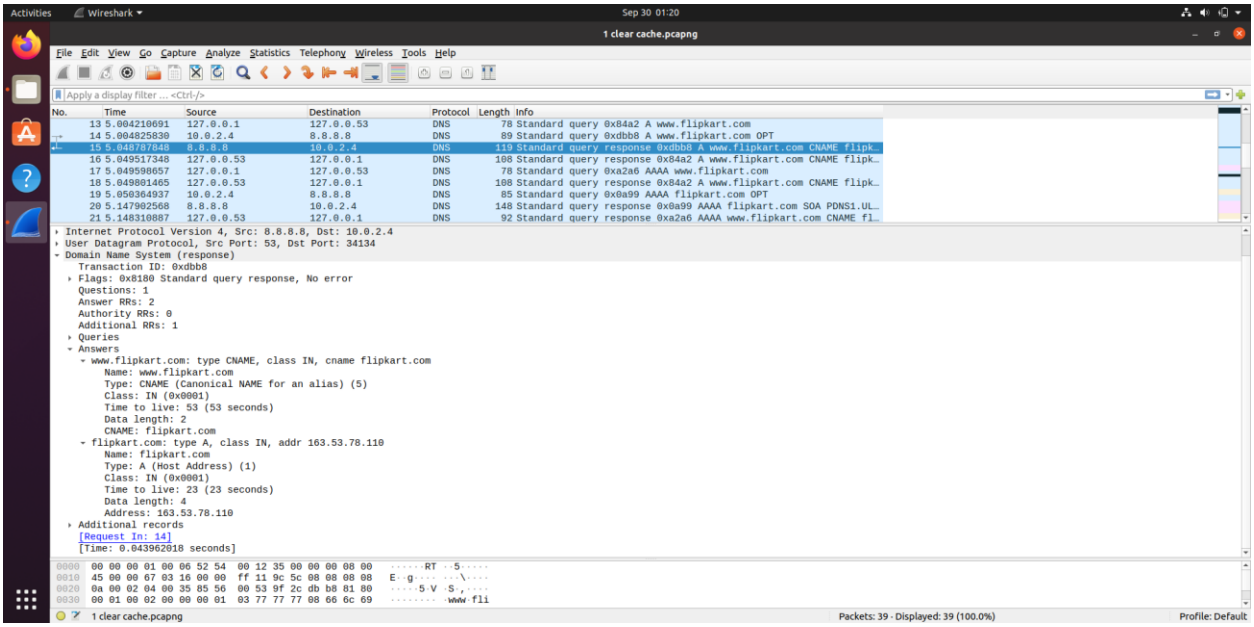
Queries-

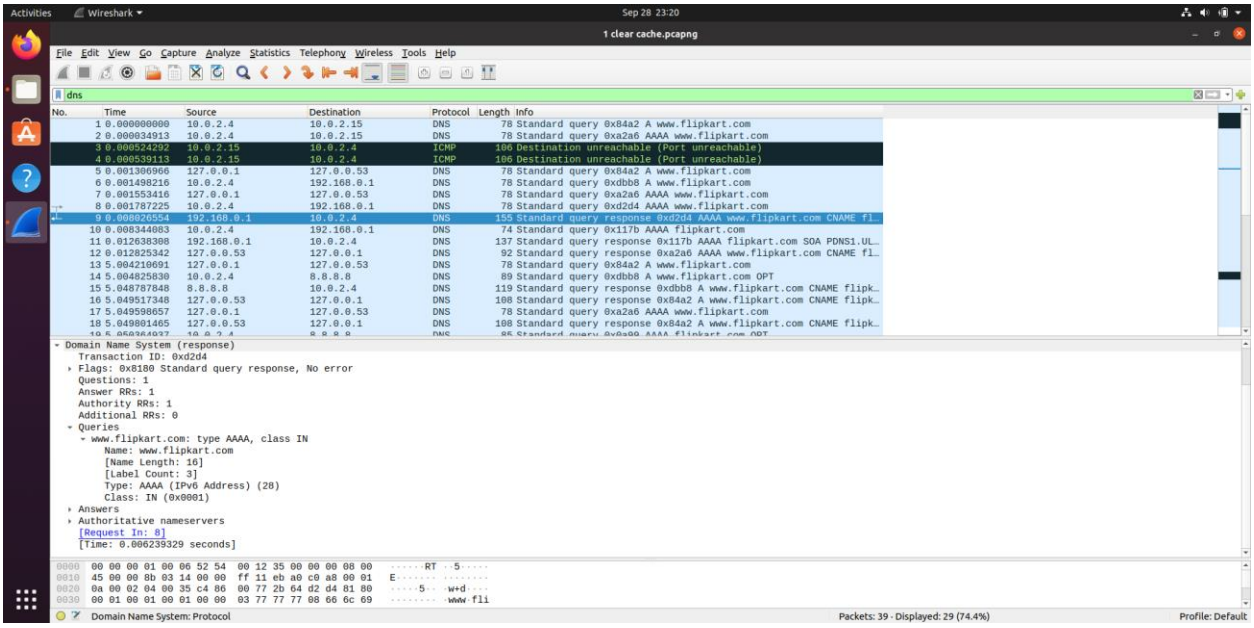


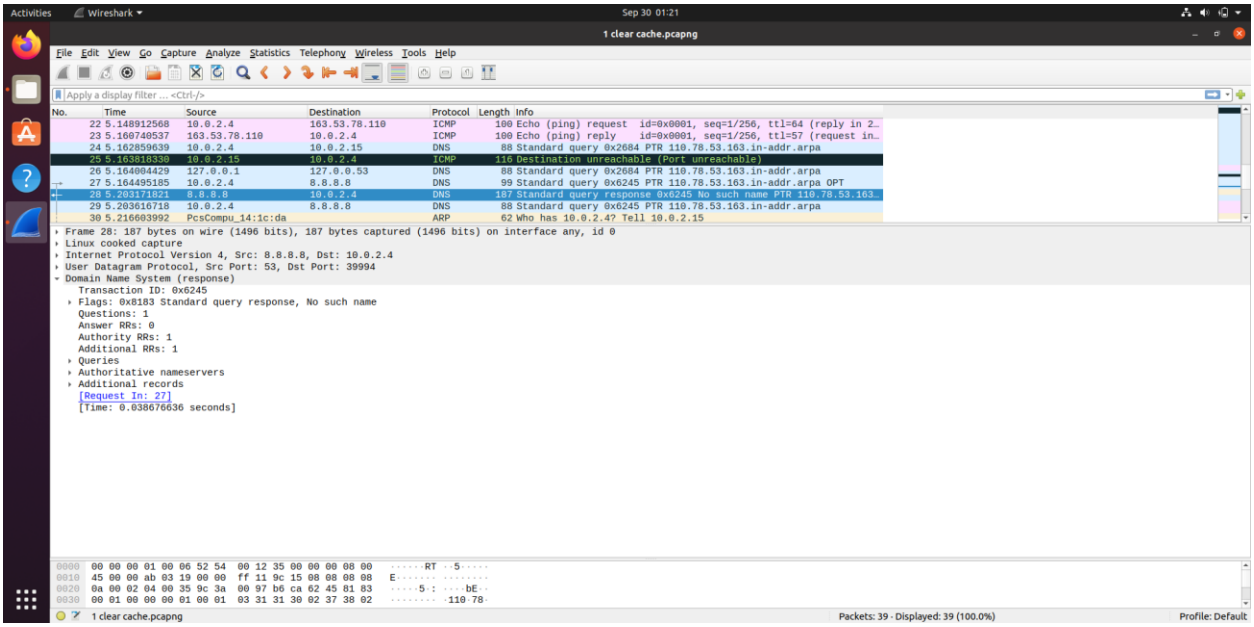




Activities
Wireshark
Sep 29 23:55
1 clear cache.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
19 5.050364937 10.0.2.4 8.8.8.8 DNS 85 Standard query 0x0a99 AAAA flipkart.com OPT
20 5.147902568 8.8.8.8 10.0.2.4 DNS 148 Standard query response 0x0a99 AAAA flipkart.com SOA PDNS1.UL…
21 5.148310887 127.0.0.53 127.0.0.1 DNS 92 Standard query response 0xa2a6 AAAA www.flipkart.com CNAME fl…
22 5.148912568 10.0.2.4 163.53.78.110 ICMP 100 Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 2…
23 5.160740537 163.53.78.110 10.0.2.4 ICMP 100 Echo (ping) reply id=0x0001, seq=1/256, ttl=57 (request in…
24 5.162859639 10.0.2.4 10.0.2.15 DNS 88 Standard query 0x2684 PTR 110.78.53.163.in-addr.arpa
25 5.163818330 10.0.2.15 10.0.2.4 ICMP 116 Destination unreachable (Port unreachable)
26 5.164004429 127.0.0.1 127.0.0.53 DNS 88 Standard query 0x2684 PTR 110.78.53.163.in-addr.arpa
27 5.164495185 10.0.2.4 8.8.8.8 DNS 99 Standard query 0x6245 PTR 110.78.53.163.in-addr.arpa OPT
28 5.203171821 8.8.8.8 10.0.2.4 DNS 187 Standard query response 0x6245 No such name PTR 110.78.53.163…
29 5.203616718 10.0.2.4 8.8.8.8 DNS 88 Standard query 0x6245 PTR 110.78.53.163.in-addr.arpa
Frame 24: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15
User Datagram Protocol, Src Port: 53361, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x2684
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
1 clear cache.pcapng
Packets: 39 · Displayed: 39 (100.0%)
Profile: Default

Responses-


Activities
Wireshark
Sep 30 01:20
1 clear cache.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
13 5.004210691 127.0.0.1 127.0.0.53 DNS 78 Standard query 0x84a2 A www.flipkart.com
14 5.004825830 10.0.2.4 8.8.8.8 DNS 89 Standard query 0xdbb8 A www.flipkart.com OPT
15 5.048787848 8.8.8.8 10.0.2.4 DNS 119 Standard query response 0xdbb8 A www.flipkart.com CNAME flipk…
16 5.049517348 127.0.0.53 127.0.0.1 DNS 108 Standard query response 0x84a2 A www.flipkart.com CNAME flipk…
17 5.049598657 127.0.0.1 127.0.0.53 DNS 78 Standard query 0xa2a6 AAAA www.flipkart.com
18 5.049801465 127.0.0.53 127.0.0.1 DNS 108 Standard query response 0x84a2 A www.flipkart.com CNAME flipk…
19 5.050364937 10.0.2.4 8.8.8.8 DNS 85 Standard query 0x0a99 AAAA flipkart.com OPT
20 5.147902568 8.8.8.8 10.0.2.4 DNS 148 Standard query response 0x0a99 AAAA flipkart.com SOA PDNS1.UL…
21 5.148310887 127.0.0.53 127.0.0.1 DNS 92 Standard query response 0xa2a6 AAAA www.flipkart.com CNAME fl…
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 10.0.2.4
User Datagram Protocol, Src Port: 53, Dst Port: 34134
Domain Name System (response)
Transaction ID: 0xdbb8
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 1
Queries
Answers
www.flipkart.com: type CNAME, class IN, cname flipkart.com
Name: www.flipkart.com
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 53 (53 seconds)
Data length: 2
CNAME: flipkart.com
flipkart.com: type A, class IN, addr 163.53.78.110
Name: flipkart.com
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 23 (23 seconds)
Data length: 4
Address: 163.53.78.110
Additional records
[Request In: 14]
[Time: 0.043962018 seconds]
1 clear cache.pcapng
Packets: 39 · Displayed: 39 (100.0%)
Profile: Default




Observations: In this test, the request is sent to the local DNS (the IP address we set: 10.0.2.15) instead of the ISP. Since the server VM is not yet configured we get an ICMP error message saying that the port is unreachable. The request is then sent by the client VM to ISP for domain name resolution.

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

They are sent over UDP.

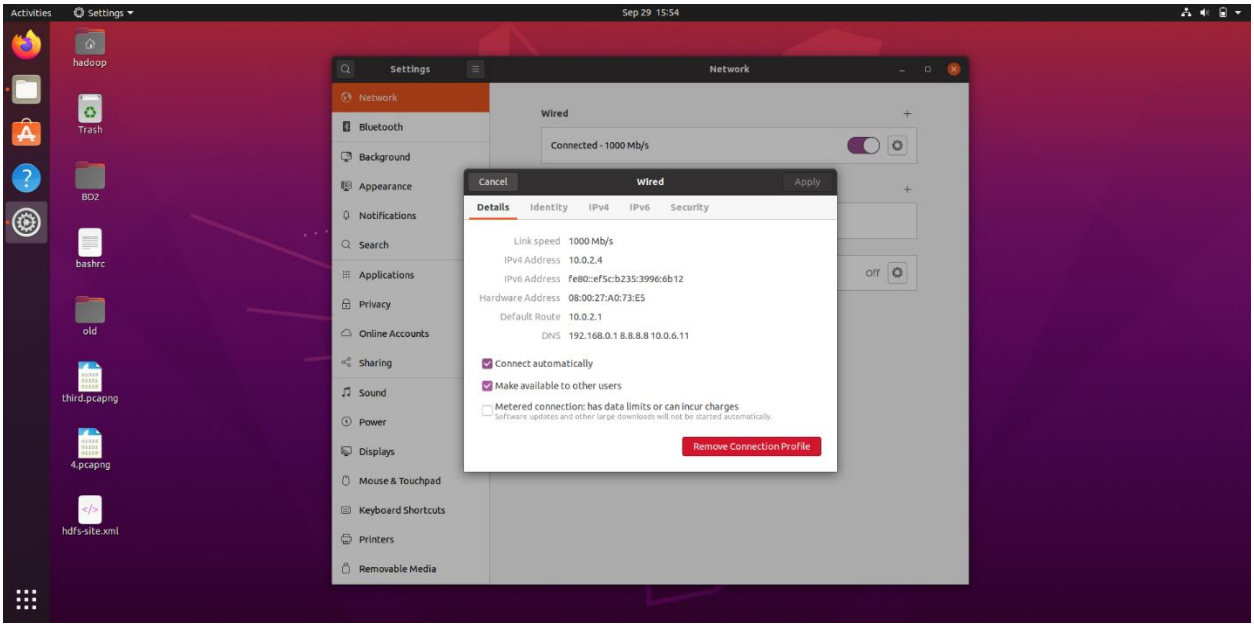
2) What is the destination port for the DNS query message? What is the source port of DNS response message?

Destination Port for DNS query message: 53

Source Port for DNS response message: 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?

The query message is sent to 10.0.2.15. Because the port was unreachable, it was sent from 10.0.2.4 to 192.168.0.1 which is the client's local DNS.




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

The query highlighted in the first screenshot is a Type A Standard Query which stores hostname and its corresponding IPv4 address.

The query highlighted in the second screenshot shows Type AAAA Standard Query which stores hostname and its corresponding IPv6 address.

In the third query screenshot, we can also see one PTR query message that resolves an IP address to a domain or host name, unlike an A record which points a domain name to an IP address.

The query messages do not contain any answers.

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

2 answers are provided in the response message for the A type query. 1 answer is provided for type AAAA and none for the PTR type. The format is the same as in the first test.

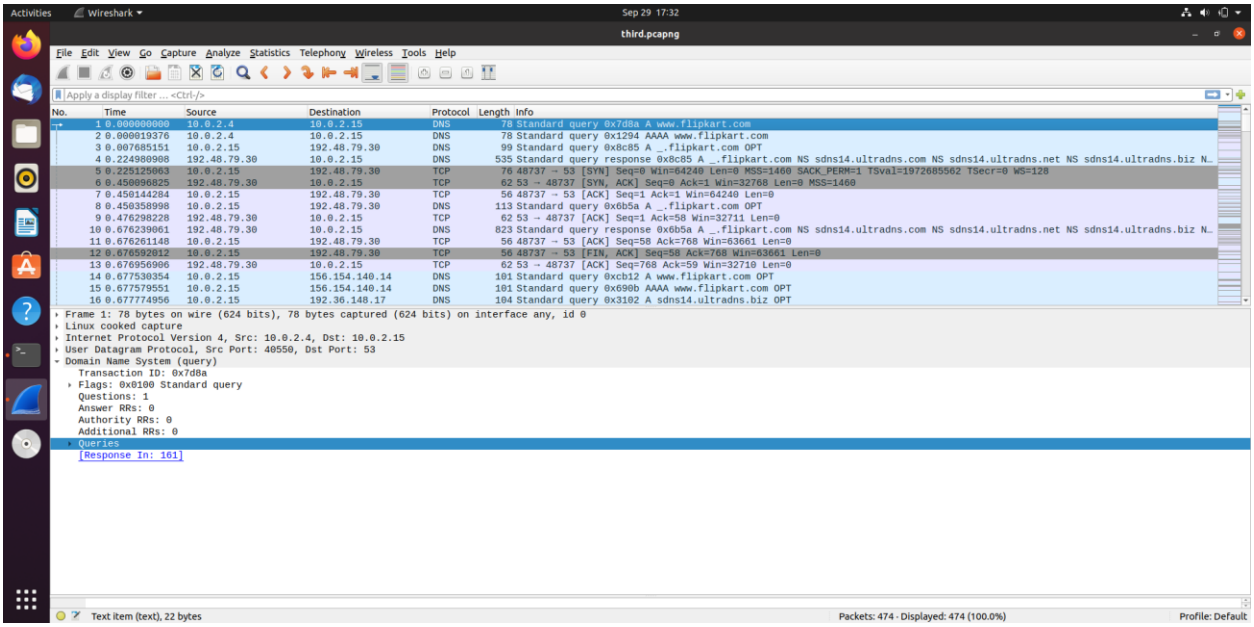
6) Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

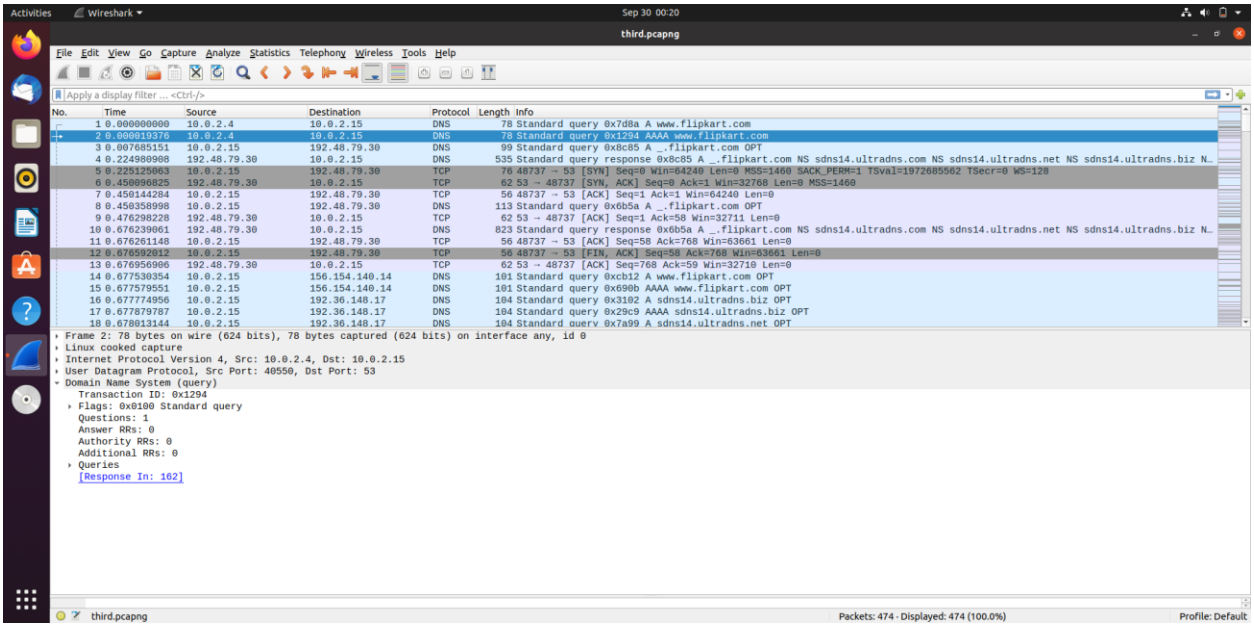
Output similar to that of first test.

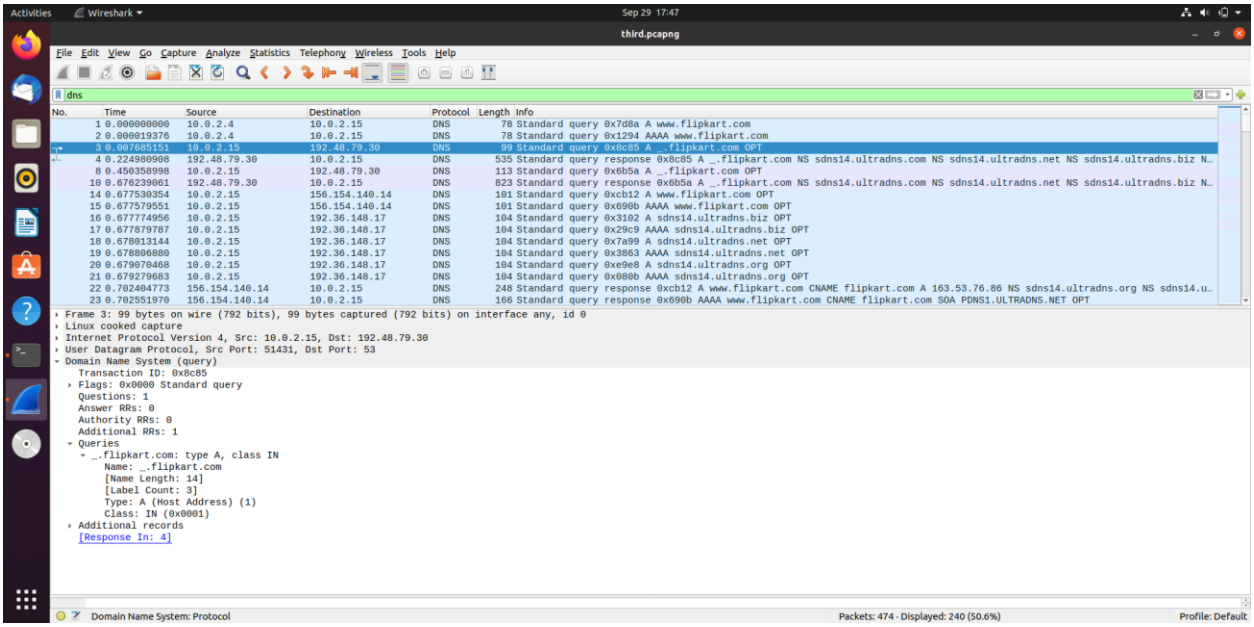
**Task 2: Set Up a Local DNS Server**

**Third Test:**

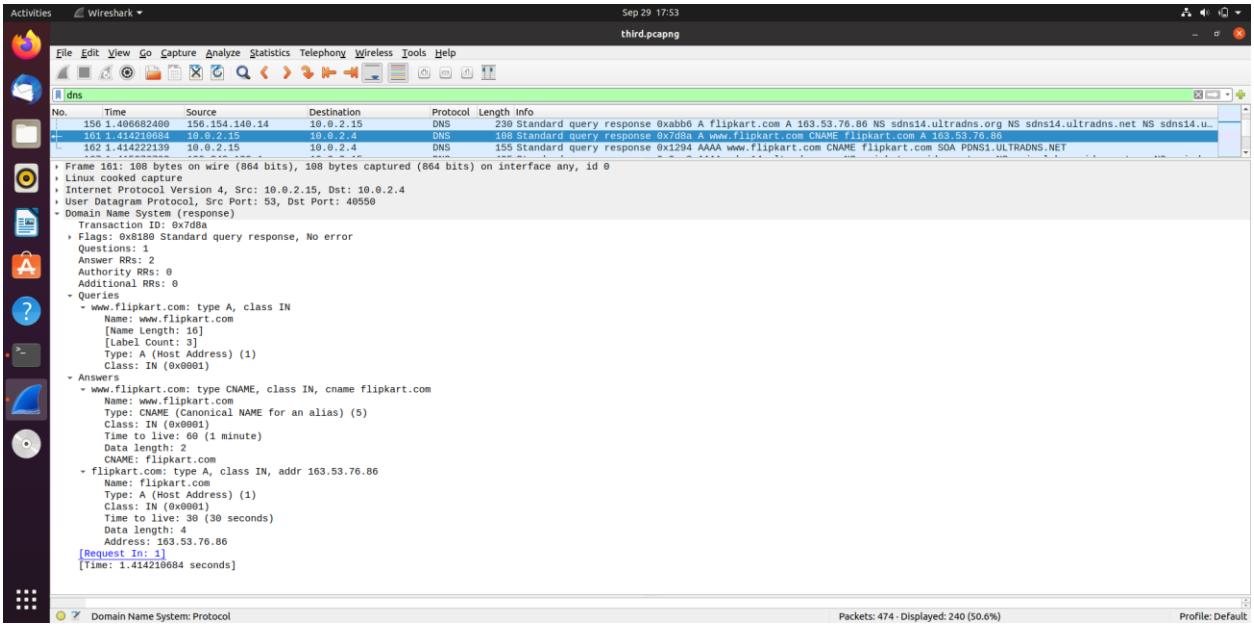
Queries-

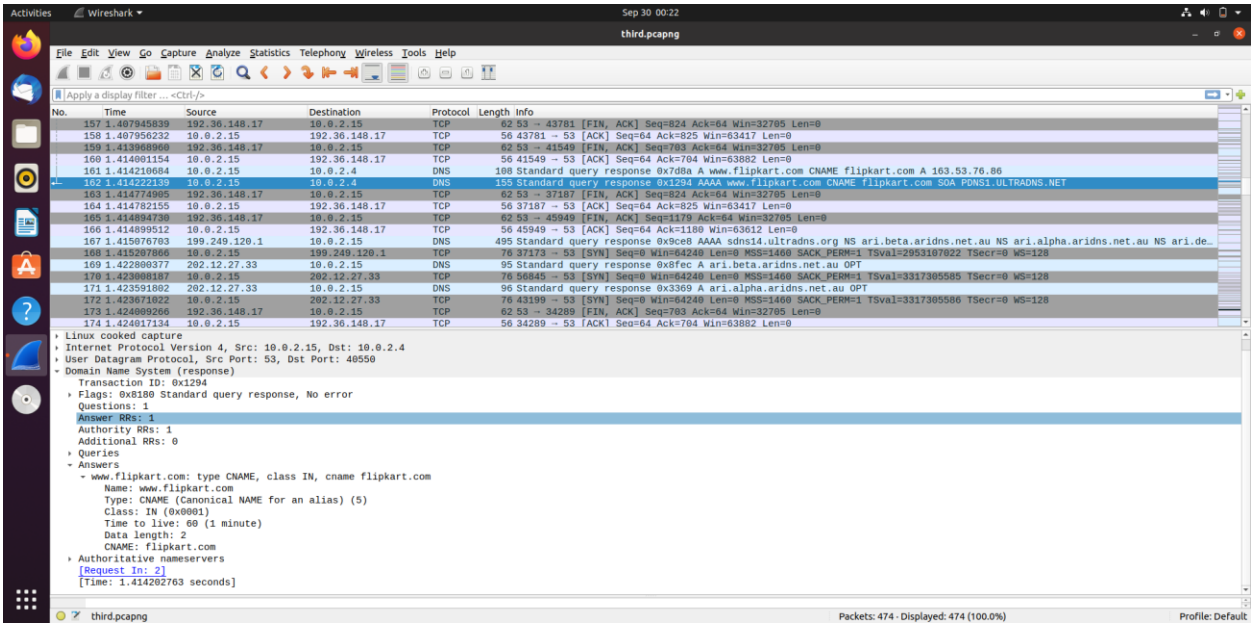


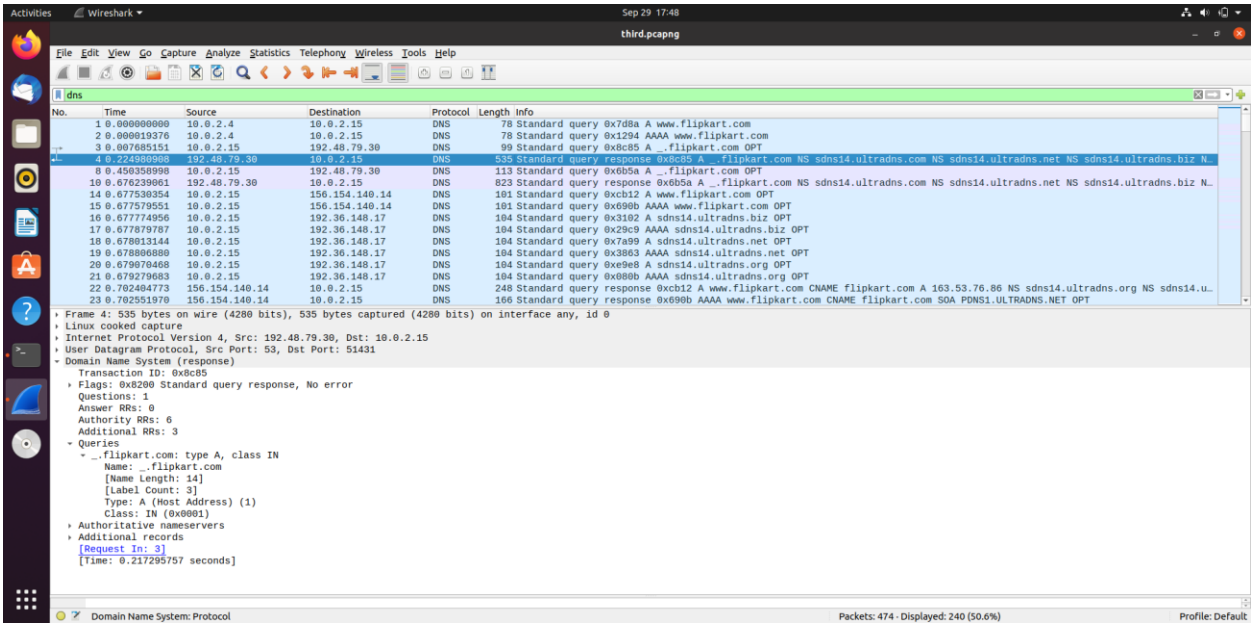




Activities
Wireshark
Sep 29 17:47
third.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
1 0.000000000 10.0.2.4 10.0.2.15 DNS 78 Standard query 0x7d8a A www.flipkart.com
2 0.000019376 10.0.2.4 10.0.2.15 DNS 78 Standard query 0x1294 AAAA www.flipkart.com
3 0.007685151 10.0.2.15 192.48.79.30 DNS 99 Standard query 0x8c85 A _.flipkart.com OPT
4 0.224980908 192.48.79.30 10.0.2.15 DNS 535 Standard query response 0x8c85 A _.flipkart.com NS sdns14.ultradns.com NS sdns14.ultradns.net NS sdns14.ultradns.biz N…
8 0.450358998 10.0.2.15 192.48.79.30 DNS 113 Standard query 0x6b5a A _.flipkart.com OPT
10 0.676239061 192.48.79.30 10.0.2.15 DNS 823 Standard query response 0x6b5a A _.flipkart.com NS sdns14.ultradns.com NS sdns14.ultradns.net NS sdns14.ultradns.biz N…
14 0.677530354 10.0.2.15 156.154.140.14 DNS 101 Standard query 0xcb12 A www.flipkart.com OPT
15 0.677579551 10.0.2.15 156.154.140.14 DNS 101 Standard query 0x690b AAAA www.flipkart.com OPT
16 0.677774956 10.0.2.15 192.36.148.17 DNS 104 Standard query 0x3102 A sdns14.ultradns.biz OPT
17 0.677879787 10.0.2.15 192.36.148.17 DNS 104 Standard query 0x29c9 AAAA sdns14.ultradns.biz OPT
18 0.678013144 10.0.2.15 192.36.148.17 DNS 104 Standard query 0x7a99 A sdns14.ultradns.net OPT
19 0.678806880 10.0.2.15 192.36.148.17 DNS 104 Standard query 0x3863 AAAA sdns14.ultradns.net OPT
20 0.679070468 10.0.2.15 192.36.148.17 DNS 104 Standard query 0xe9e8 A sdns14.ultradns.org OPT
21 0.679279683 10.0.2.15 192.36.148.17 DNS 104 Standard query 0x080b AAAA sdns14.ultradns.org OPT
22 0.702404773 156.154.140.14 10.0.2.15 DNS 248 Standard query response 0xcb12 A www.flipkart.com CNAME flipkart.com A 163.53.76.86 NS sdns14.ultradns.org NS sdns14.u…
23 0.702551970 156.154.140.14 10.0.2.15 DNS 166 Standard query response 0x690b AAAA www.flipkart.com CNAME flipkart.com SOA PDNS1.ULTRADNS.NET OPT
Frame 3: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.48.79.30
User Datagram Protocol, Src Port: 51431, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x8c85
Flags: 0x0000 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
Queries
_.flipkart.com: type A, class IN
Name: _.flipkart.com
[Name Length: 14]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
Additional records
[Response In: 4]
Domain Name System: Protocol
Packets: 474 · Displayed: 240 (50.6%)
Profile: Default

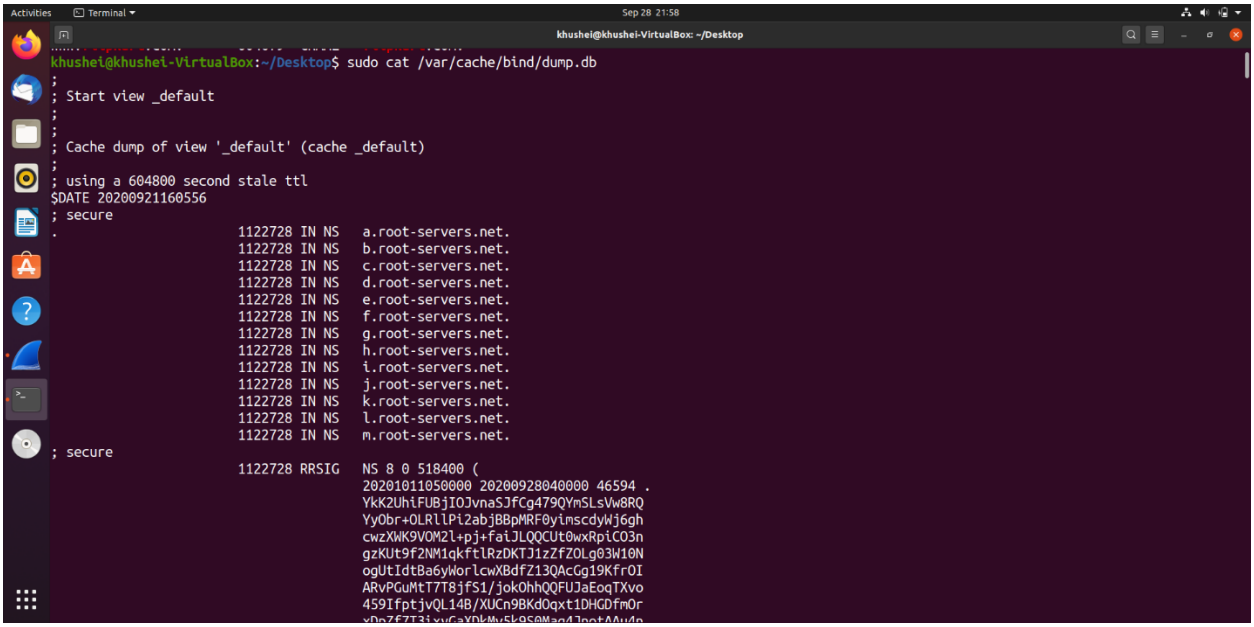
Responses-

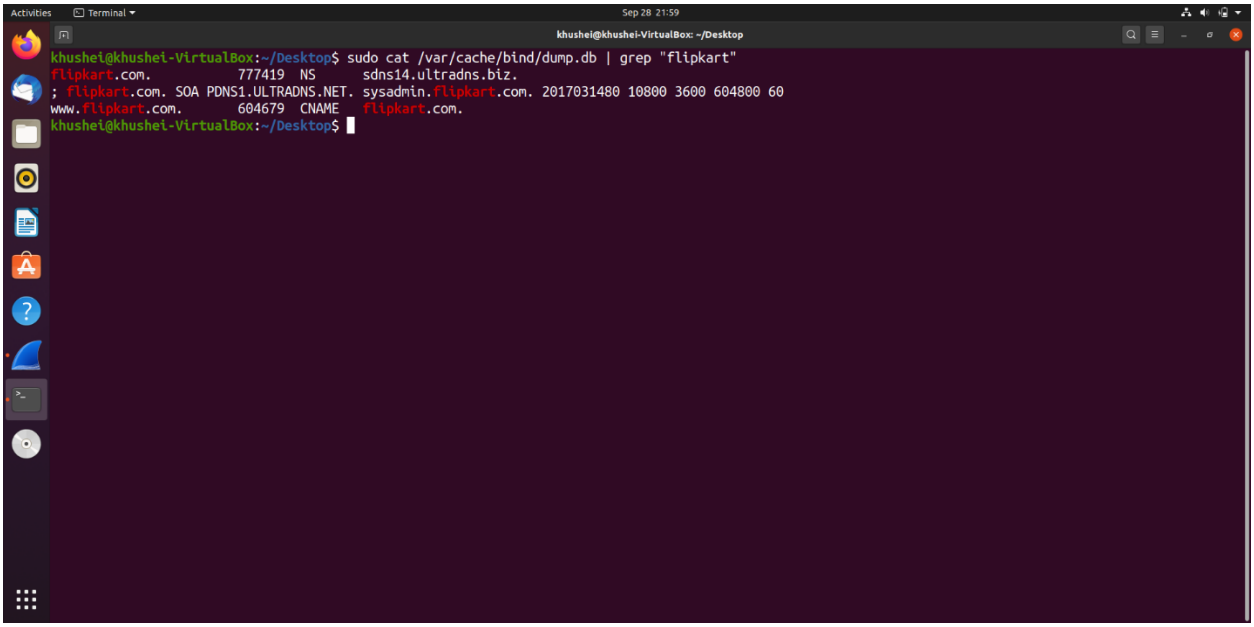

Activities
Wireshark
Sep 29 17:53
third.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
156 1.406682400 156.154.140.14 10.0.2.15 DNS 230 Standard query response 0xabb6 A flipkart.com A 163.53.76.86 NS sdns14.ultradns.org NS sdns14.ultradns.net NS sdns14.u…
161 1.414210684 10.0.2.15 10.0.2.4 DNS 108 Standard query response 0x7d8a A www.flipkart.com CNAME flipkart.com A 163.53.76.86
162 1.414222139 10.0.2.15 10.0.2.4 DNS 155 Standard query response 0x1294 AAAA www.flipkart.com CNAME flipkart.com SOA PDNS1.ULTRADNS.NET
Frame 161: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.4
User Datagram Protocol, Src Port: 53, Dst Port: 40550
Domain Name System (response)
Transaction ID: 0x7d8a
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
Queries
www.flipkart.com: type A, class IN
Name: www.flipkart.com
[Name Length: 16]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
Answers
www.flipkart.com: type CNAME, class IN, cname flipkart.com
Name: www.flipkart.com
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 60 (1 minute)
Data length: 2
CNAME: flipkart.com
flipkart.com: type A, class IN, addr 163.53.76.86
Name: flipkart.com
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 30 (30 seconds)
Data length: 4
Address: 163.53.76.86
[Request In: 1]
[Time: 1.414210684 seconds]
Domain Name System: Protocol
Packets: 474 · Displayed: 240 (50.6%)
Profile: Default


Activities
Wireshark
Sep 30 00:22
third.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
157 1.407945839 192.36.148.17 10.0.2.15 TCP 62 53 → 43781 [FIN, ACK] Seq=824 Ack=64 Win=32705 Len=0
158 1.407956232 10.0.2.15 192.36.148.17 TCP 56 43781 → 53 [ACK] Seq=64 Ack=825 Win=63417 Len=0
159 1.413960960 192.36.148.17 10.0.2.15 TCP 62 53 → 41549 [FIN, ACK] Seq=703 Ack=64 Win=32705 Len=0
160 1.414001154 10.0.2.15 192.36.148.17 TCP 56 41549 → 53 [ACK] Seq=64 Ack=704 Win=63882 Len=0
161 1.414210684 10.0.2.15 10.0.2.4 DNS 108 Standard query response 0x7d8a A www.flipkart.com CNAME flipkart.com A 163.53.76.86
162 1.414222139 10.0.2.15 10.0.2.4 DNS 155 Standard query response 0x1294 AAAA www.flipkart.com CNAME flipkart.com SOA PDNS1.ULTRADNS.NET
163 1.414774905 192.36.148.17 10.0.2.15 TCP 62 53 → 37187 [FIN, ACK] Seq=824 Ack=64 Win=32705 Len=0
164 1.414782155 10.0.2.15 192.36.148.17 TCP 56 37187 → 53 [ACK] Seq=64 Ack=825 Win=63417 Len=0
165 1.414894730 192.36.148.17 10.0.2.15 TCP 62 53 → 45949 [FIN, ACK] Seq=1179 Ack=64 Win=32705 Len=0
166 1.414899512 10.0.2.15 192.36.148.17 TCP 56 45949 → 53 [ACK] Seq=64 Ack=1180 Win=63612 Len=0
167 1.415076703 199.249.120.1 10.0.2.15 DNS 495 Standard query response 0x9ce8 AAAA sdns14.ultradns.org NS ari.beta.aridns.net.au NS ari.alpha.aridns.net.au NS ari.de…
168 1.415207866 10.0.2.15 199.249.120.1 TCP 76 37173 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2953107022 TSecr=0 WS=128
169 1.422800377 202.12.27.33 10.0.2.15 DNS 95 Standard query response 0x8fec A ari.beta.aridns.net.au OPT
170 1.423000187 10.0.2.15 202.12.27.33 TCP 76 56845 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3317305585 TSecr=0 WS=128
171 1.423591802 202.12.27.33 10.0.2.15 DNS 96 Standard query response 0x3369 A ari.alpha.aridns.net.au OPT
172 1.423671022 10.0.2.15 202.12.27.33 TCP 76 43199 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3317305586 TSecr=0 WS=128
173 1.424009266 192.36.148.17 10.0.2.15 TCP 62 53 → 34289 [FIN, ACK] Seq=703 Ack=64 Win=32705 Len=0
174 1.424017134 10.0.2.15 192.36.148.17 TCP 56 34289 → 53 [ACK] Seq=64 Ack=704 Win=63882 Len=0
Linux cooked capture
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.4
User Datagram Protocol, Src Port: 53, Dst Port: 40550
Domain Name System (response)
Transaction ID: 0x1294
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 1
Additional RRs: 0
Queries
Answers
www.flipkart.com: type CNAME, class IN, cname flipkart.com
Name: www.flipkart.com
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 60 (1 minute)
Data length: 2
CNAME: flipkart.com
Authoritative nameservers
[Request In: 2]
[Time: 1.414202763 seconds]
third.pcapng
Packets: 474 · Displayed: 474 (100.0%)
Profile: Default


Activities
Wireshark
Sep 29 17:48
third.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
1 0.000000000 10.0.2.4 10.0.2.15 DNS 78 Standard query 0x7d8a A www.flipkart.com
2 0.000019376 10.0.2.4 10.0.2.15 DNS 78 Standard query 0x1294 AAAA www.flipkart.com
3 0.007685151 10.0.2.15 192.48.79.30 DNS 99 Standard query 0x8c85 A _.flipkart.com OPT
4 0.224980908 192.48.79.30 10.0.2.15 DNS 535 Standard query response 0x8c85 A _.flipkart.com NS sdns14.ultradns.com NS sdns14.ultradns.net NS sdns14.ultradns.biz N…
8 0.450358998 10.0.2.15 192.48.79.30 DNS 113 Standard query 0x6b5a A _.flipkart.com OPT
10 0.676239061 192.48.79.30 10.0.2.15 DNS 823 Standard query response 0x6b5a A _.flipkart.com NS sdns14.ultradns.com NS sdns14.ultradns.net NS sdns14.ultradns.biz N…
14 0.677530354 10.0.2.15 156.154.140.14 DNS 101 Standard query 0xcb12 A www.flipkart.com OPT
15 0.677579551 10.0.2.15 156.154.140.14 DNS 101 Standard query 0x690b AAAA www.flipkart.com OPT
16 0.677774956 10.0.2.15 192.36.148.17 DNS 104 Standard query 0x3102 A sdns14.ultradns.biz OPT
17 0.677879787 10.0.2.15 192.36.148.17 DNS 104 Standard query 0x29c9 AAAA sdns14.ultradns.biz OPT
18 0.678013144 10.0.2.15 192.36.148.17 DNS 104 Standard query 0x7a99 A sdns14.ultradns.net OPT
19 0.678806880 10.0.2.15 192.36.148.17 DNS 104 Standard query 0x3863 AAAA sdns14.ultradns.net OPT
20 0.679070468 10.0.2.15 192.36.148.17 DNS 104 Standard query 0xe9e8 A sdns14.ultradns.org OPT
21 0.679279683 10.0.2.15 192.36.148.17 DNS 104 Standard query 0x080b AAAA sdns14.ultradns.org OPT
22 0.702404773 156.154.140.14 10.0.2.15 DNS 248 Standard query response 0xcb12 A www.flipkart.com CNAME flipkart.com A 163.53.76.86 NS sdns14.ultradns.org NS sdns14.u…
23 0.702551970 156.154.140.14 10.0.2.15 DNS 166 Standard query response 0x690b AAAA www.flipkart.com CNAME flipkart.com SOA PDNS1.ULTRADNS.NET OPT
Frame 4: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 192.48.79.30, Dst: 10.0.2.15
User Datagram Protocol, Src Port: 53, Dst Port: 51431
Domain Name System (response)
Transaction ID: 0x8c85
Flags: 0x8200 Standard query response, No error
Questions: 1
Answer RRs: 0
Authority RRs: 6
Additional RRs: 3
Queries
_.flipkart.com: type A, class IN
Name: _.flipkart.com
[Name Length: 14]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
Authoritative nameservers
Additional records
[Request In: 3]
[Time: 0.217295757 seconds]
Domain Name System: Protocol
Packets: 474 · Displayed: 240 (50.6%)
Profile: Default

Cache-




Observations: Since the local DNS with IP address 10.0.2.15 is set up and configured, the IP address of www.flipkart.com is fetched from the local DNS itself. When the cache is cleared on server and we ping from the client, the first wireshark capture has the entire trace which is being cached, as shown above.

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

They are sent over UDP.

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

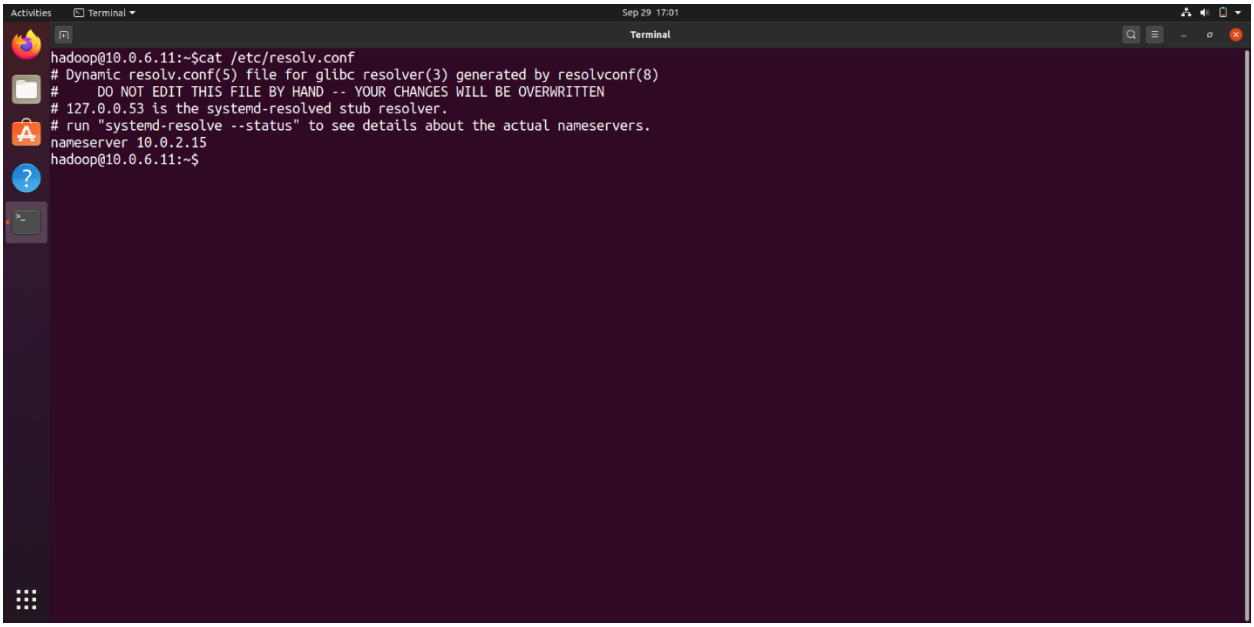
Destination Port for DNS query message: 53

Source Port for DNS response message: 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?

The query message is sent to 10.0.2.15.

From the server machine, again a query is made to 156.154.140.14 which is flipkart.com's name server.




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

The query highlighted in the first screenshot is a Type A Standard.

The next screenshot shows Type AAAA Standard Query.

The query messages do not contain any answers.

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

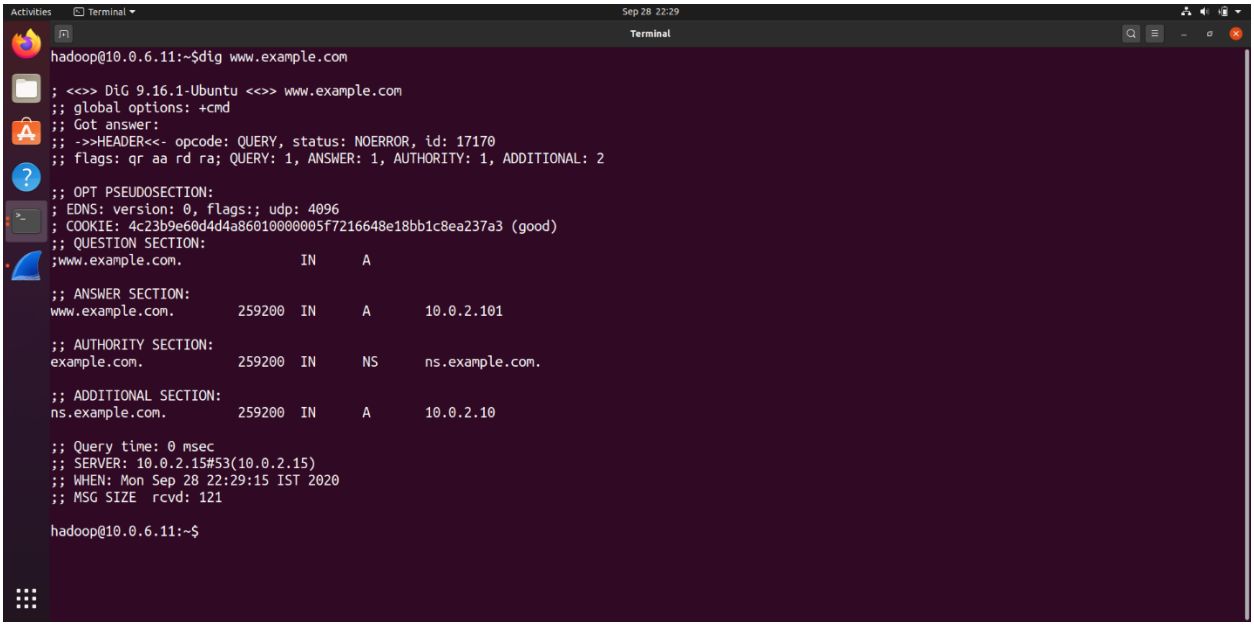
2 answers are provided in the response message for the A type query. 1 answer is provided in the response message for the AAAA type query. The format is same as that of the first test.

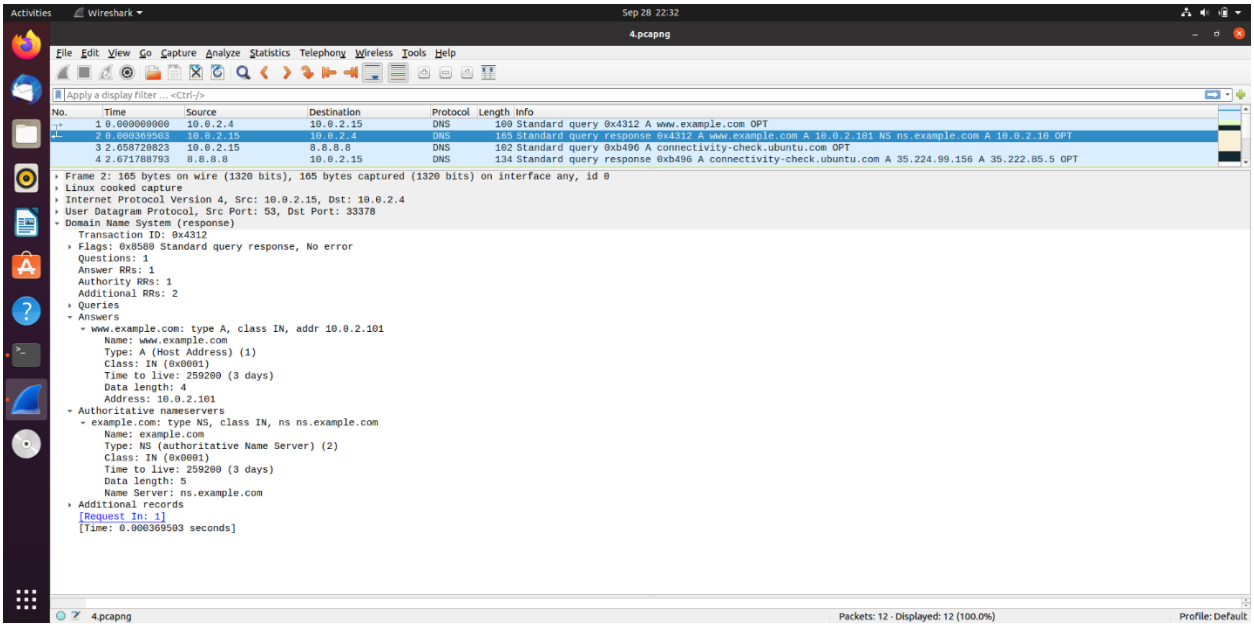
6) Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

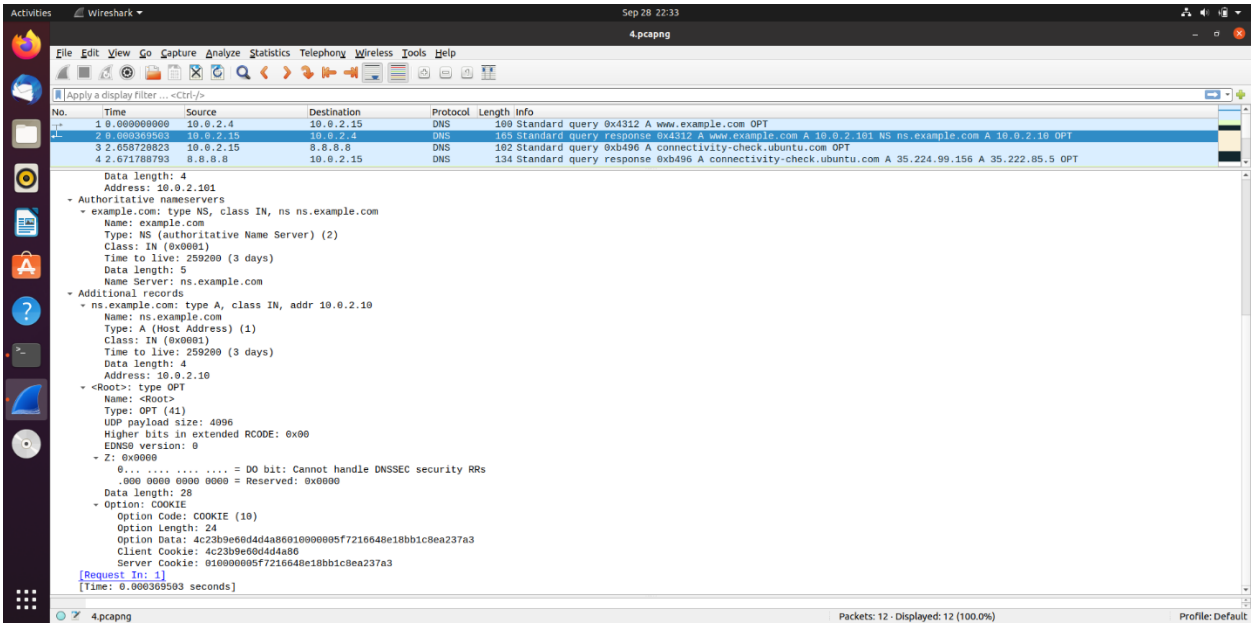
The destination IP address is shown as 192.48.79.30.

No, the destination IP address does not correspond to any of the IP addressed provided in the DNS response message.

## Task 4: Restart the BIND server and test




Activities
Wireshark
Sep 28 22:33
4.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 10.0.2.4 10.0.2.15 DNS 100 Standard query 0x4312 A www.example.com OPT
2 0.000369503 10.0.2.15 10.0.2.4 DNS 165 Standard query response 0x4312 A www.example.com A 10.0.2.101 NS ns.example.com A 10.0.2.10 OPT
3 2.658720823 10.0.2.15 8.8.8.8 DNS 102 Standard query 0xb496 A connectivity-check.ubuntu.com OPT
4 2.671788793 8.8.8.8 10.0.2.15 DNS 134 Standard query response 0xb496 A connectivity-check.ubuntu.com A 35.224.99.156 A 35.222.85.5 OPT
Data length: 4
Address: 10.0.2.101
Authoritative nameservers
example.com: type NS, class IN, ns ns.example.com
Name: example.com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 259200 (3 days)
Data length: 5
Name Server: ns.example.com
Additional records
ns.example.com: type A, class IN, addr 10.0.2.10
Name: ns.example.com
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 259200 (3 days)
Data length: 4
Address: 10.0.2.10
<Root>: type OPT
Name: <Root>
Type: OPT (41)
UDP payload size: 4096
Higher bits in extended RCODE: 0x00
EDNS0 version: 0
Z: 0x0000
0... .... .... .... = DO bit: Cannot handle DNSSEC security RRs
.000 0000 0000 0000 = Reserved: 0x0000
Data length: 28
Option: COOKIE
Option Code: COOKIE (10)
Option Length: 24
Option Data: 4c23b9e60d4d4a8601000005f7216648e18bb1c8ea237a3
Client Cookie: 4c23b9e60d4d4a86
Server Cookie: 01000005f7216648e18bb1c8ea237a3
[Request In: 1]
[Time: 0.000369503 seconds]
4.pcapng
Packets: 12 · Displayed: 12 (100.0%)
Profile: Default