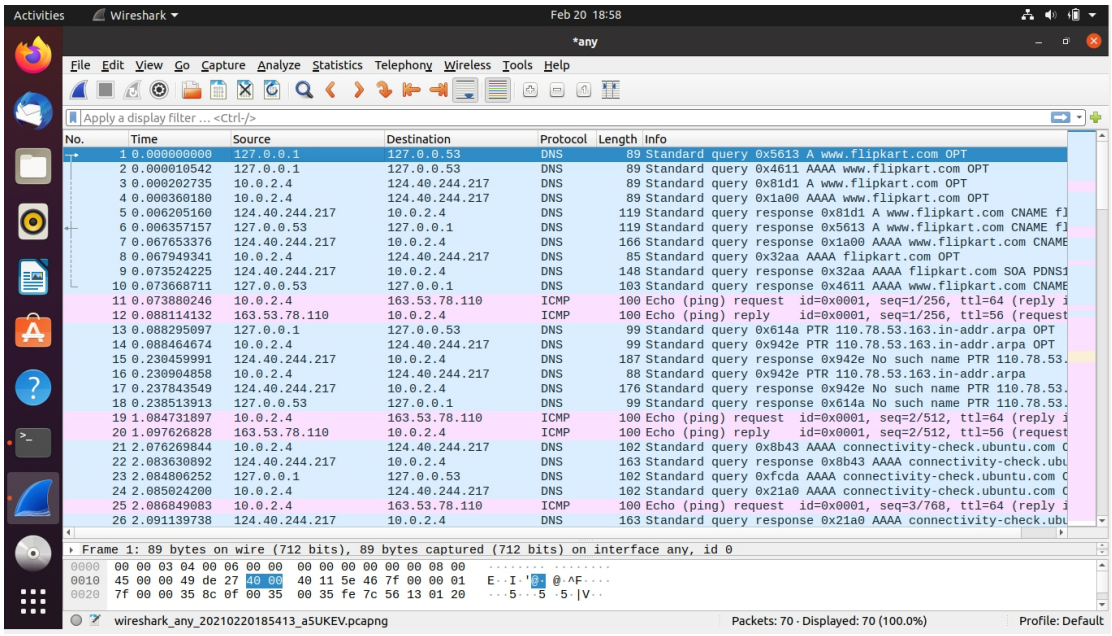
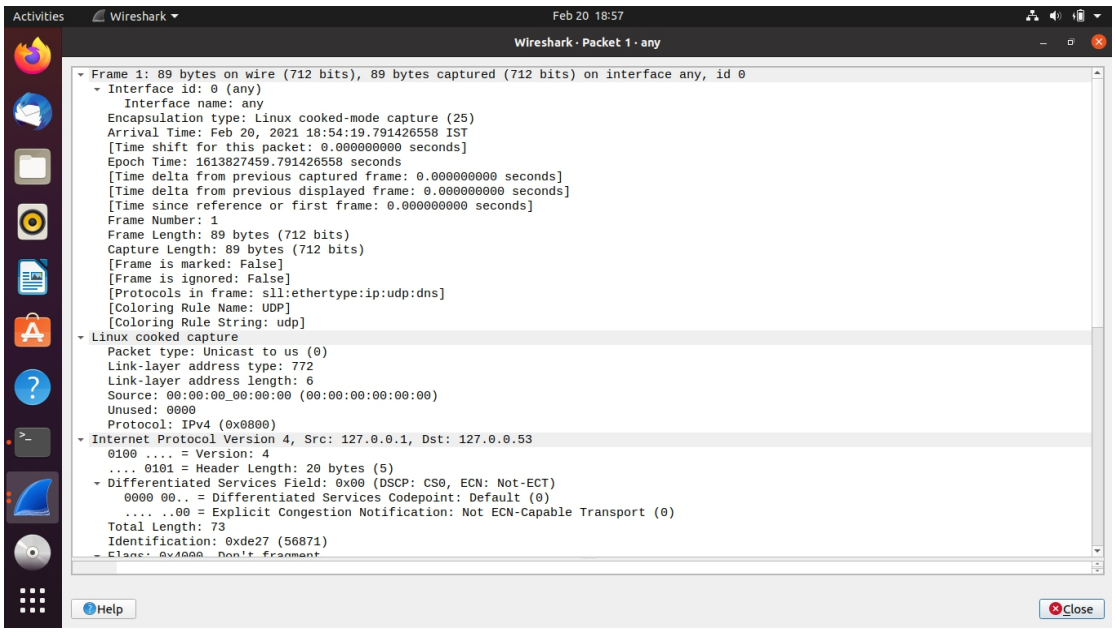
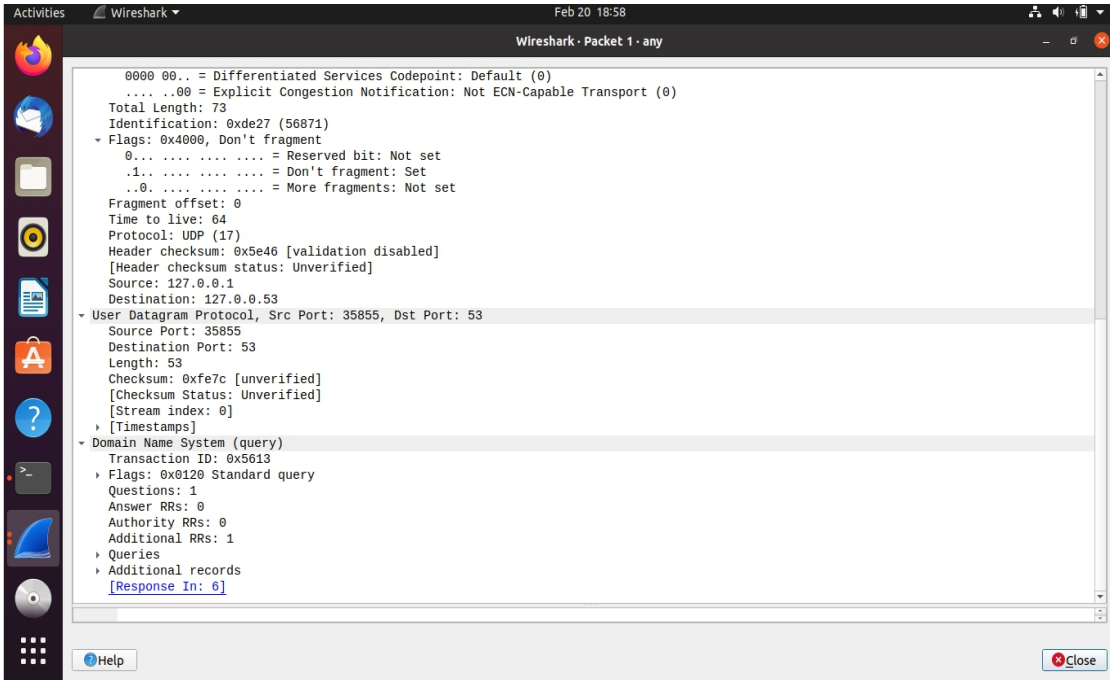
CN Lab Report – Week 4

NAME	SRN	SECTION
ANKITH J RAI	PES1UG19CS069	B

Observation 1:

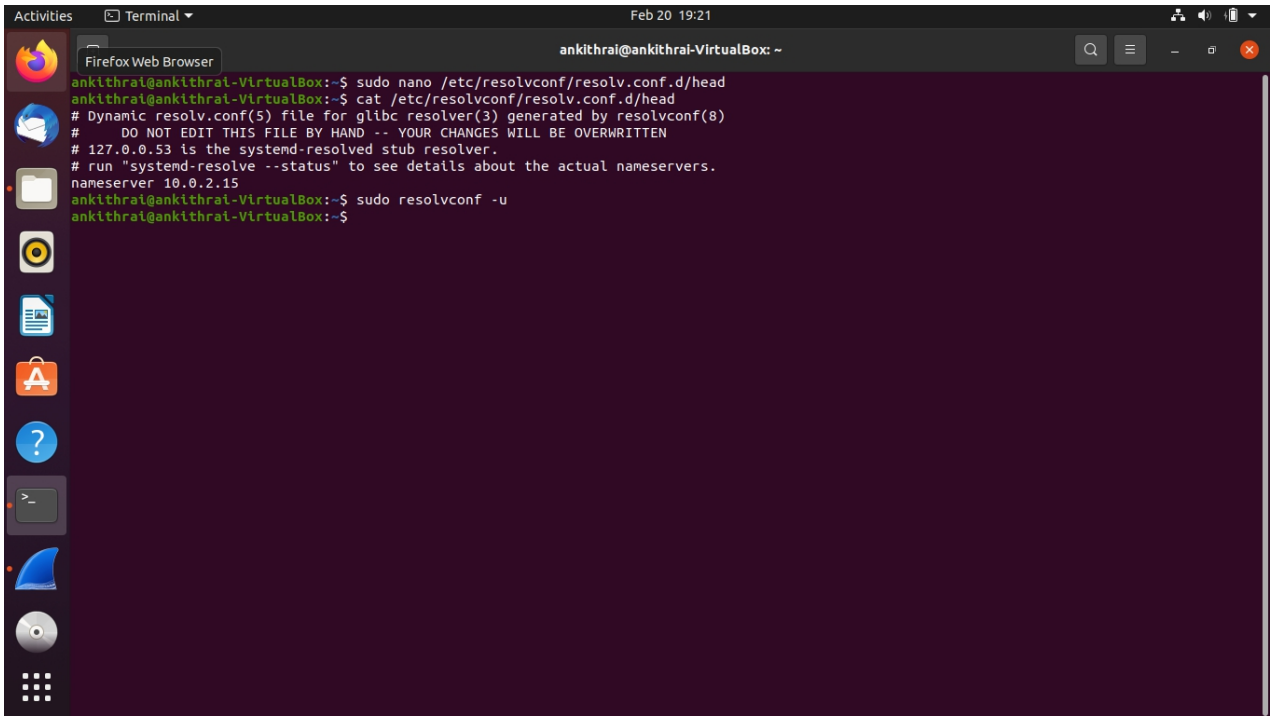






Part 1: Setting Up a Local DNS Server

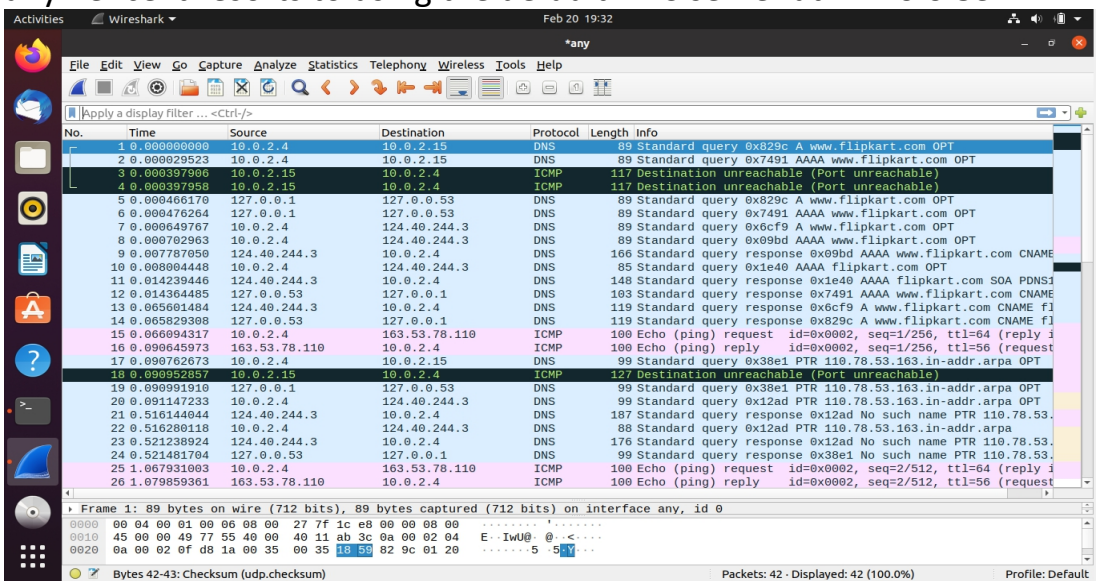
Task 1: Configure the User/Client Machine

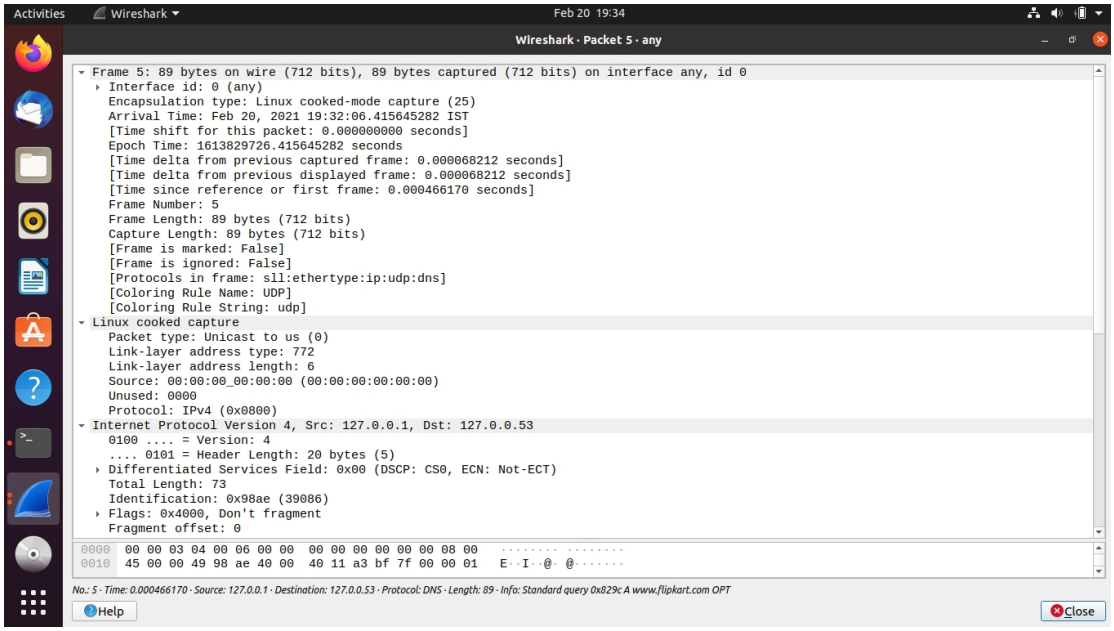


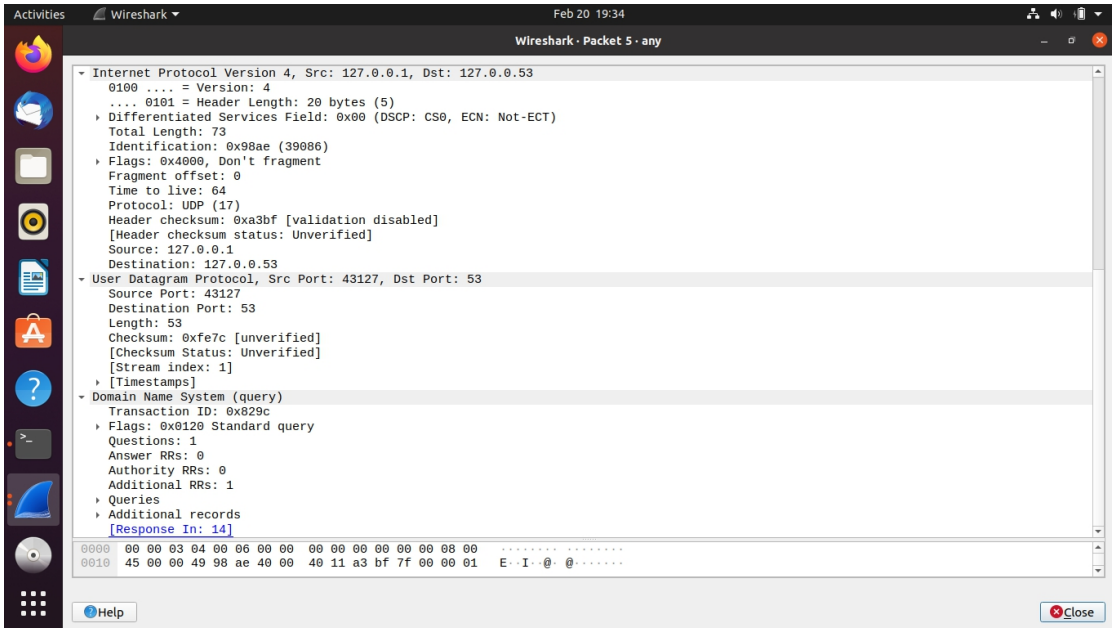
Observation 2:

We obtain a destination unreachable error in Wireshark as the server

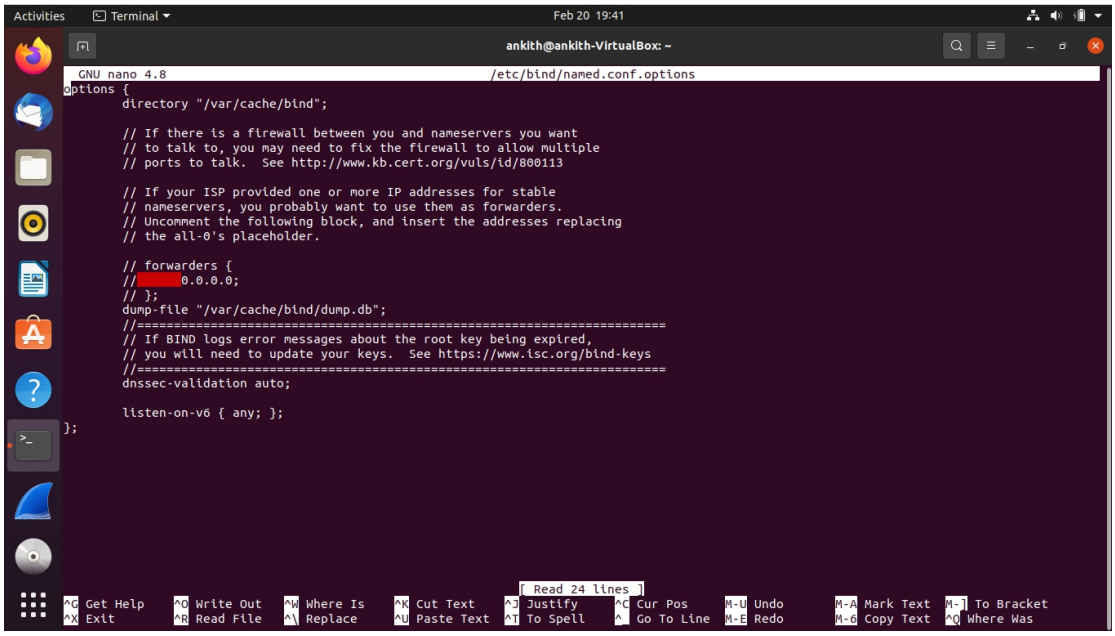
machine does not have a DNS server associated with it.The client tries to obtain the DNS record from **10.0.2.15** but it does not receive any hence it resorts to using the default DNS server at **127.0.0.53**.



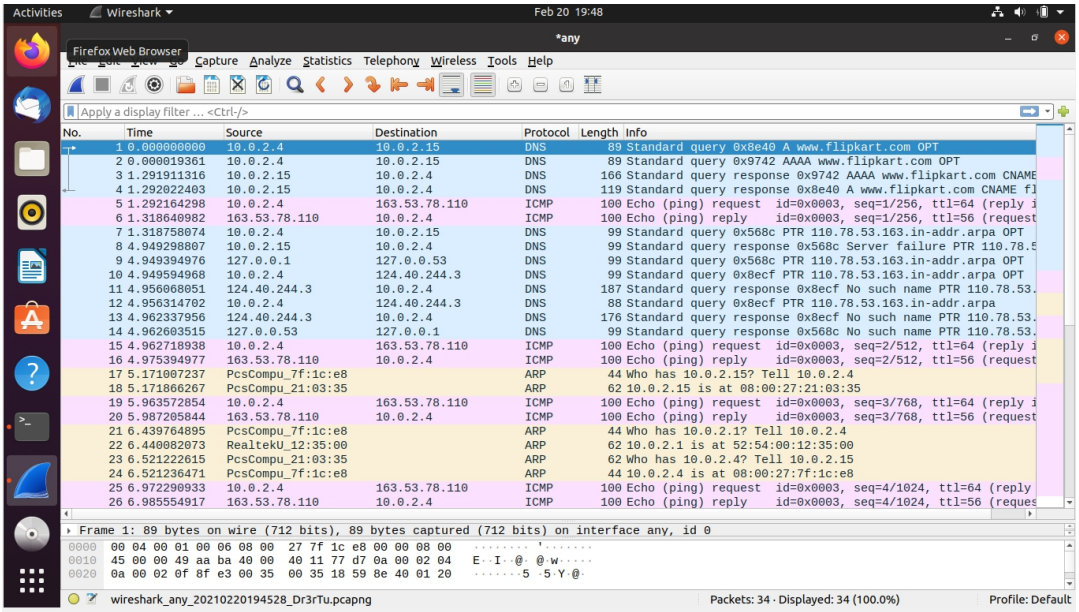


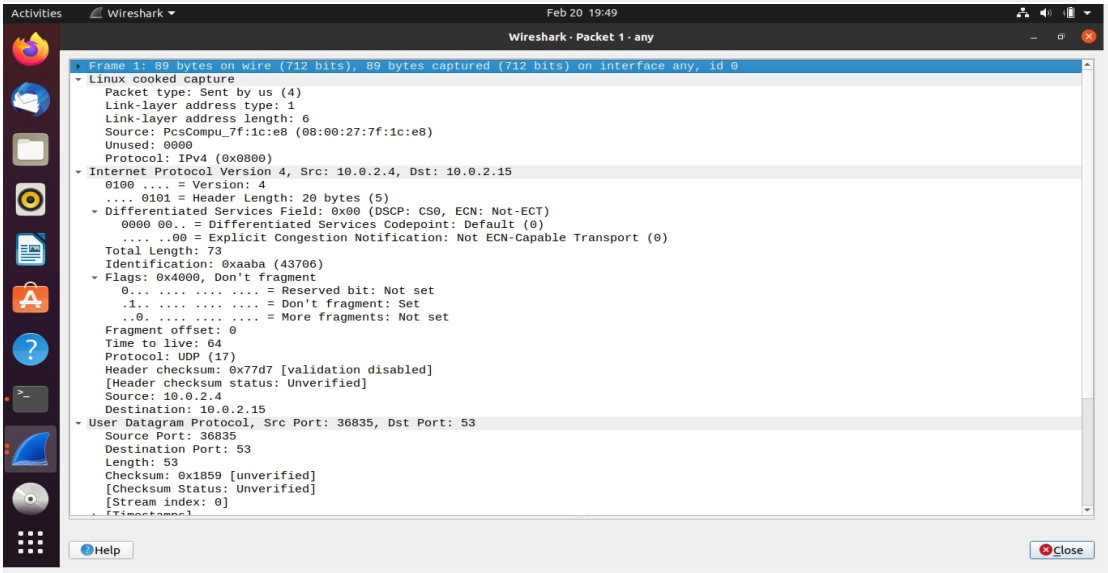


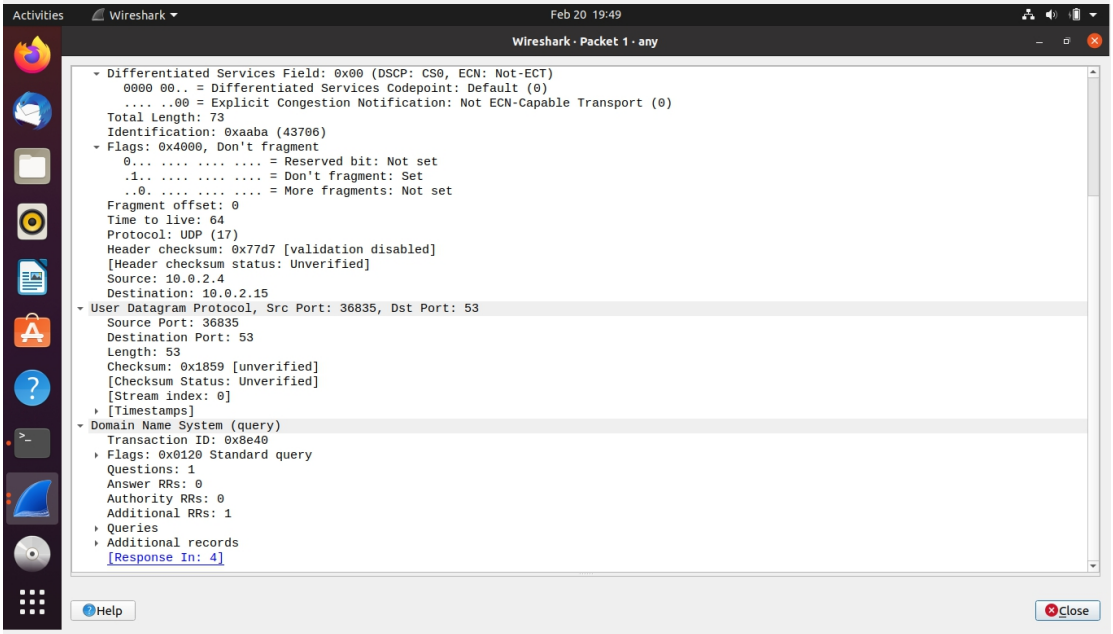
Task 2: Set Up a Local DNS Server



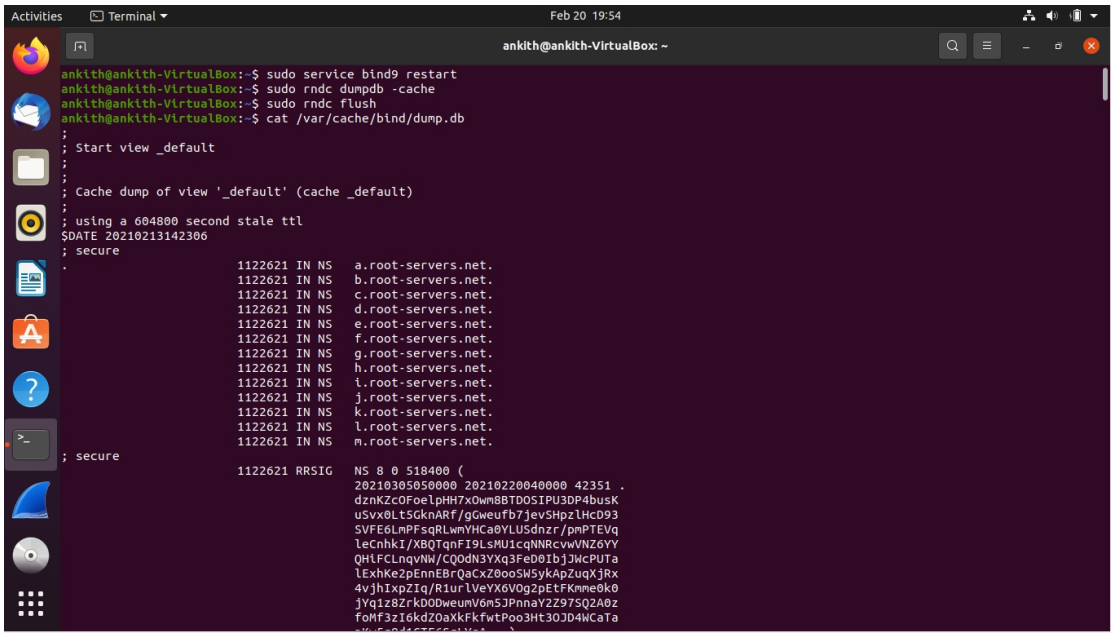
Observation 3:

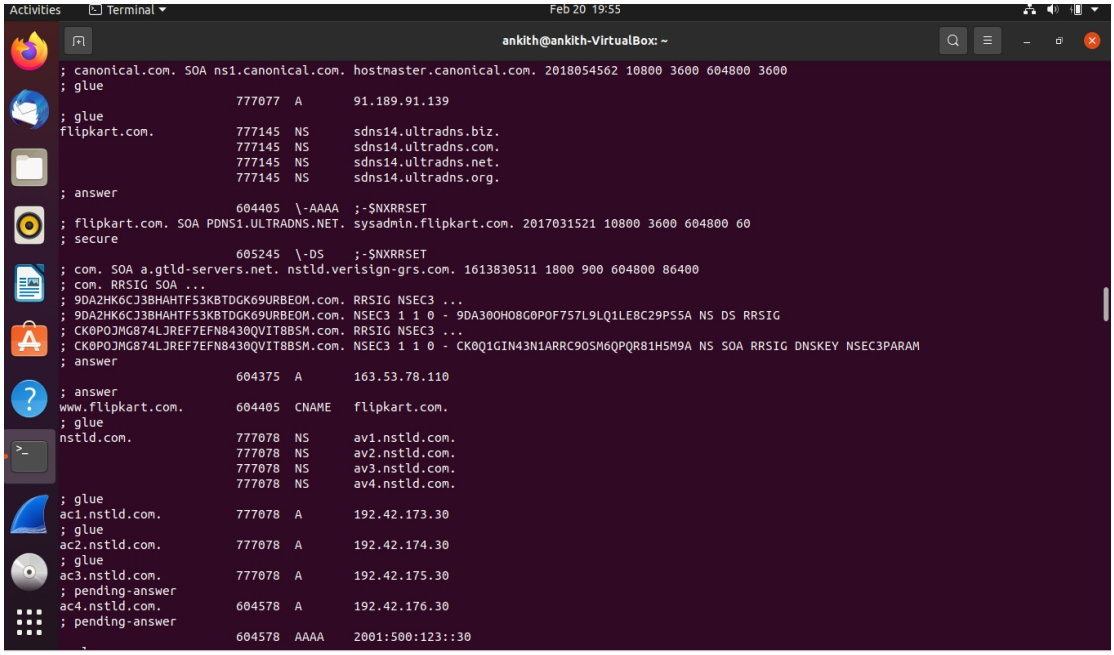

Activities
Wireshark
Feb 20 19:48
*any
Firefox Web Browser
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 10.0.2.4 10.0.2.15 DNS 89 Standard query 0x8e40 A www.flipkart.com OPT
2 0.000019361 10.0.2.4 10.0.2.15 DNS 89 Standard query 0x9742 AAAA www.flipkart.com OPT
3 1.291911316 10.0.2.15 10.0.2.4 DNS 166 Standard query response 0x9742 AAAA www.flipkart.com CNAME
4 1.292022403 10.0.2.15 10.0.2.4 DNS 119 Standard query response 0x8e40 A www.flipkart.com CNAME fl
5 1.292164298 10.0.2.4 163.53.78.110 ICMP 100 Echo (ping) request id=0x0003, seq=1/256, ttl=64 (reply i
6 1.318640982 163.53.78.110 10.0.2.4 ICMP 100 Echo (ping) reply id=0x0003, seq=1/256, ttl=56 (request
7 1.318758074 10.0.2.4 10.0.2.15 DNS 99 Standard query 0x568c PTR 110.78.53.163.in-addr.arpa OPT
8 4.949298807 10.0.2.15 10.0.2.4 DNS 99 Standard query response 0x568c Server failure PTR 110.78.5
9 4.949394976 127.0.0.1 127.0.0.53 DNS 99 Standard query 0x568c PTR 110.78.53.163.in-addr.arpa OPT
10 4.949594968 10.0.2.4 124.40.244.3 DNS 99 Standard query 0x8ecf PTR 110.78.53.163.in-addr.arpa OPT
11 4.956068051 124.40.244.3 10.0.2.4 DNS 187 Standard query response 0x8ecf No such name PTR 110.78.53.
12 4.956314702 10.0.2.4 124.40.244.3 DNS 88 Standard query 0x8ecf PTR 110.78.53.163.in-addr.arpa
13 4.962337956 124.40.244.3 10.0.2.4 DNS 176 Standard query response 0x8ecf No such name PTR 110.78.53.
14 4.962603515 127.0.0.53 127.0.0.1 DNS 99 Standard query response 0x568c No such name PTR 110.78.53.
15 4.962718938 10.0.2.4 163.53.78.110 ICMP 100 Echo (ping) request id=0x0003, seq=2/512, ttl=64 (reply i
16 4.975394977 163.53.78.110 10.0.2.4 ICMP 100 Echo (ping) reply id=0x0003, seq=2/512, ttl=56 (request
17 5.171007237 PcsCompu_7f:1c:e8 ARP 44 Who has 10.0.2.15? Tell 10.0.2.4
18 5.171866267 PcsCompu_21:03:35 ARP 62 10.0.2.15 is at 08:00:27:21:03:35
19 5.963572854 10.0.2.4 163.53.78.110 ICMP 100 Echo (ping) request id=0x0003, seq=3/768, ttl=64 (reply i
20 5.987205844 163.53.78.110 10.0.2.4 ICMP 100 Echo (ping) reply id=0x0003, seq=3/768, ttl=56 (request
21 6.439764895 PcsCompu_7f:1c:e8 ARP 44 Who has 10.0.2.1? Tell 10.0.2.4
22 6.440082073 RealtekU_12:35:00 ARP 62 10.0.2.1 is at 52:54:00:12:35:00
23 6.521222615 PcsCompu_21:03:35 ARP 62 Who has 10.0.2.4? Tell 10.0.2.15
24 6.521236471 PcsCompu_7f:1c:e8 ARP 44 10.0.2.4 is at 08:00:27:7f:1c:e8
25 6.972290933 10.0.2.4 163.53.78.110 ICMP 100 Echo (ping) request id=0x0003, seq=4/1024, ttl=64 (reply
26 6.985554917 163.53.78.110 10.0.2.4 ICMP 100 Echo (ping) reply id=0x0003, seq=4/1024, ttl=56 (reques
Frame 1: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface any, id 0
0000 00 04 00 01 00 06 08 00 27 7f 1c e8 00 00 08 00
0010 45 00 00 49 aa ba 40 00 40 11 77 d7 0a 00 02 04
0020 0a 00 02 0f 8f e3 00 35 00 35 18 59 8e 40 01 20
wireshark_any_20210220194528_Dr3rTu.pcapng
Packets: 34 · Displayed: 34 (100.0%)
Profile: Default

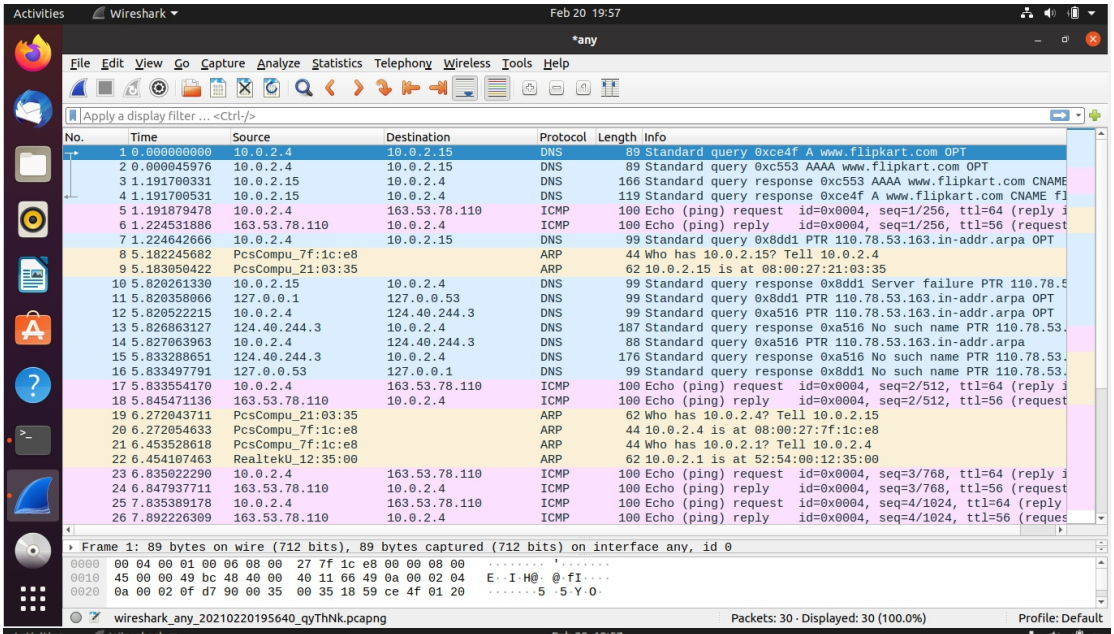

Activities
Wireshark
Feb 20 19:49
Wireshark · Packet 1 · any
Frame 1: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface any, id 0
Linux cooked capture
Packet type: Sent by us (4)
Link-layer address type: 1
Link-layer address length: 6
Source: PcsCompu_7f:1c:e8 (08:00:27:7f:1c:e8)
Unused: 0000
Protocol: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 73
Identification: 0xaaba (43706)
Flags: 0x4000, Don't fragment
0... .... = Reserved bit: Not set
.1.. .... = Don't fragment: Set
..0. .... = More fragments: Not set
Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0x77d7 [validation disabled]
[Header checksum status: Unverified]
Source: 10.0.2.4
Destination: 10.0.2.15
User Datagram Protocol, Src Port: 36835, Dst Port: 53
Source Port: 36835
Destination Port: 53
Length: 53
Checksum: 0x1859 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
Help
Close

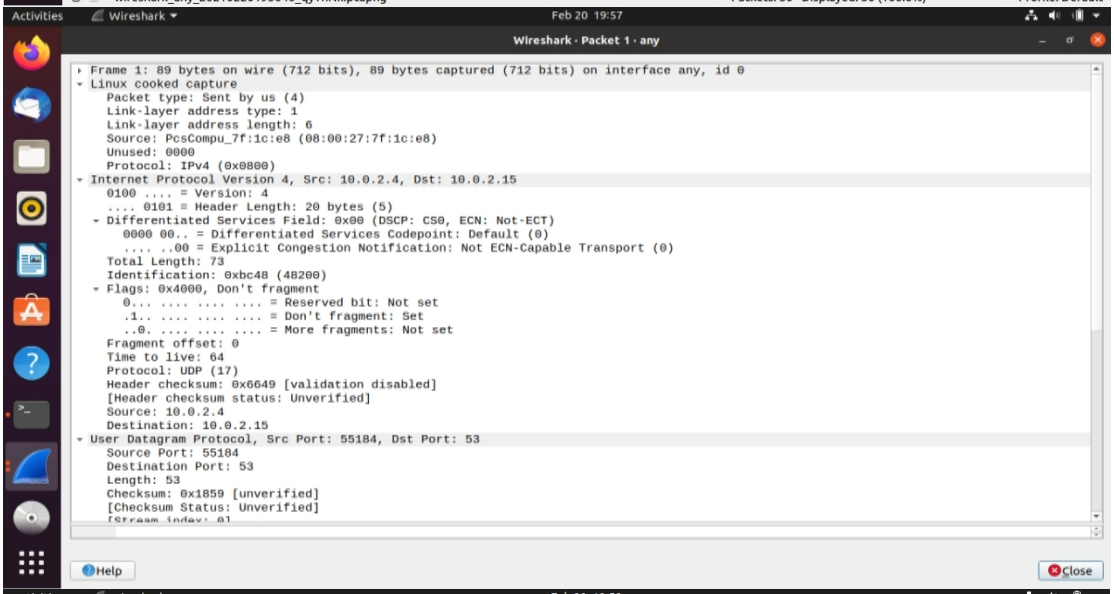

Activities
Wireshark
Feb 20 19:49
Wireshark · Packet 1 · any
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 73
Identification: 0xaaba (43706)
Flags: 0x4000, Don't fragment
0... .... = Reserved bit: Not set
.1.. .... = Don't fragment: Set
..0. .... = More fragments: Not set
Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0x77d7 [validation disabled]
[Header checksum status: Unverified]
Source: 10.0.2.4
Destination: 10.0.2.15
User Datagram Protocol, Src Port: 36835, Dst Port: 53
Source Port: 36835
Destination Port: 53
Length: 53
Checksum: 0x1859 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Timestamps]
Domain Name System (query)
Transaction ID: 0x8e40
Flags: 0x0120 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
Queries
Additional records
[Response In: 4]
Help
Close

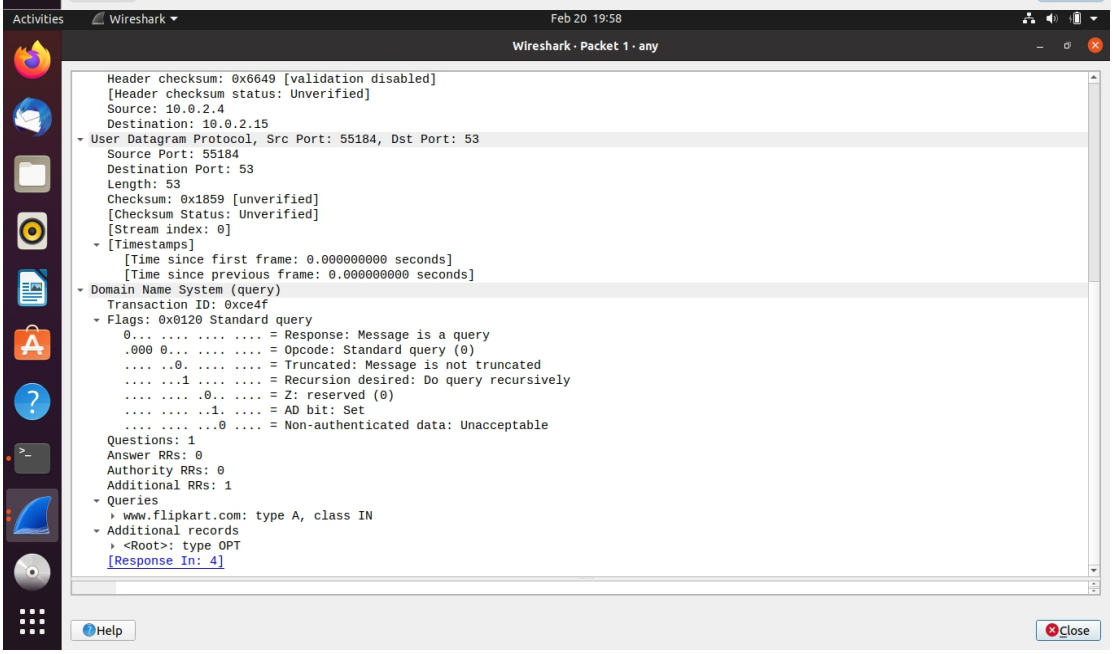
Observation 4:





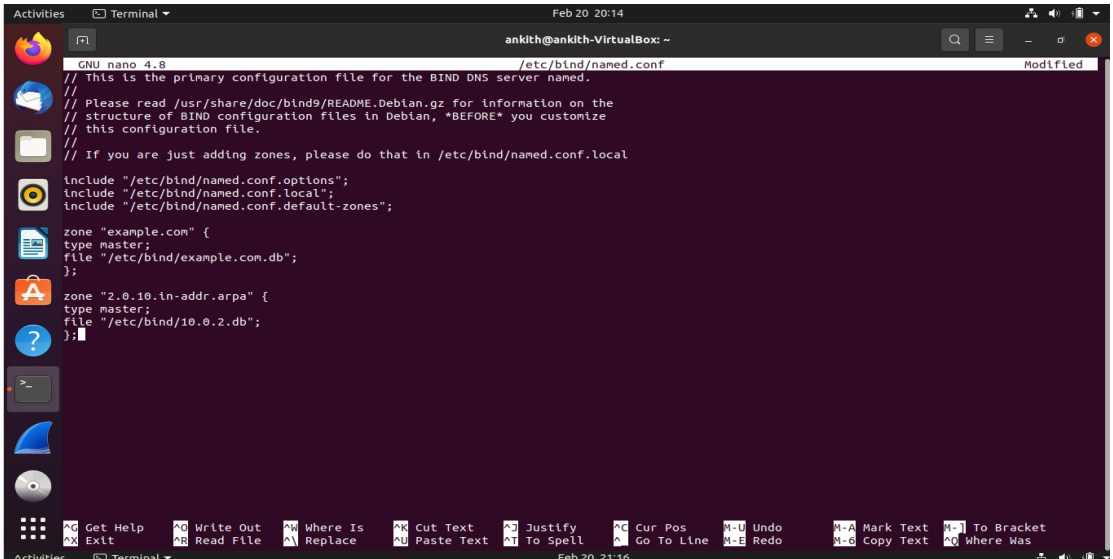

Activities
Wireshark
Feb 20 19:57
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 10.0.2.4 10.0.2.15 DNS 89 Standard query 0xce4f A www.flipkart.com OPT
2 0.000045976 10.0.2.4 10.0.2.15 DNS 89 Standard query 0xc553 AAAA www.flipkart.com OPT
3 1.191700331 10.0.2.15 10.0.2.4 DNS 166 Standard query response 0xc553 AAAA www.flipkart.com CNAME
4 1.191700531 10.0.2.15 10.0.2.4 DNS 119 Standard query response 0xce4f A www.flipkart.com CNAME fl
5 1.191879478 10.0.2.4 163.53.78.110 ICMP 100 Echo (ping) request id=0x0004, seq=1/256, ttl=64 (reply i
6 1.224531886 163.53.78.110 10.0.2.4 ICMP 100 Echo (ping) reply id=0x0004, seq=1/256, ttl=56 (request
7 1.224642666 10.0.2.4 10.0.2.15 DNS 99 Standard query 0x8dd1 PTR 110.78.53.163.in-addr.arpa OPT
8 5.182245682 PcsCompu_7f:1c:e8 ARP 44 Who has 10.0.2.15? Tell 10.0.2.4
9 5.183050422 PcsCompu_21:03:35 ARP 62 10.0.2.15 is at 08:00:27:21:03:35
10 5.820261330 10.0.2.15 10.0.2.4 DNS 99 Standard query response 0x8dd1 Server failure PTR 110.78.5
11 5.820358066 127.0.0.1 127.0.0.53 DNS 99 Standard query 0x8dd1 PTR 110.78.53.163.in-addr.arpa OPT
12 5.820522215 10.0.2.4 124.40.244.3 DNS 99 Standard query 0xa516 PTR 110.78.53.163.in-addr.arpa OPT
13 5.826863127 124.40.244.3 10.0.2.4 DNS 187 Standard query response 0xa516 No such name PTR 110.78.53.
14 5.827063963 10.0.2.4 124.40.244.3 DNS 88 Standard query 0xa516 PTR 110.78.53.163.in-addr.arpa
15 5.833288651 124.40.244.3 10.0.2.4 DNS 176 Standard query response 0xa516 No such name PTR 110.78.53.
16 5.833497791 127.0.0.53 127.0.0.1 DNS 99 Standard query response 0x8dd1 No such name PTR 110.78.53.
17 5.833554170 10.0.2.4 163.53.78.110 ICMP 100 Echo (ping) request id=0x0004, seq=2/512, ttl=64 (reply i
18 5.845471136 163.53.78.110 10.0.2.4 ICMP 100 Echo (ping) reply id=0x0004, seq=2/512, ttl=56 (request
19 6.272043711 PcsCompu_21:03:35 ARP 62 Who has 10.0.2.4? Tell 10.0.2.15
20 6.272054633 PcsCompu_7f:1c:e8 ARP 44 10.0.2.4 is at 08:00:27:7f:1c:e8
21 6.453528618 PcsCompu_7f:1c:e8 ARP 44 Who has 10.0.2.1? Tell 10.0.2.4
22 6.454107463 RealtekU_12:35:00 ARP 62 10.0.2.1 is at 52:54:00:12:35:00
23 6.835022290 10.0.2.4 163.53.78.110 ICMP 100 Echo (ping) request id=0x0004, seq=3/768, ttl=64 (reply i
24 6.847937711 163.53.78.110 10.0.2.4 ICMP 100 Echo (ping) reply id=0x0004, seq=3/768, ttl=56 (request
25 7.835389178 10.0.2.4 163.53.78.110 ICMP 100 Echo (ping) request id=0x0004, seq=4/1024, ttl=64 (reply
26 7.892226309 163.53.78.110 10.0.2.4 ICMP 100 Echo (ping) reply id=0x0004, seq=4/1024, ttl=56 (reques
Frame 1: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface any, id 0
0000 00 04 00 01 00 06 08 00 27 7f 1c e8 00 00 08 00
0010 45 00 00 49 bc 48 40 00 40 11 66 49 0a 00 02 04
0020 0a 00 02 0f d7 90 00 35 00 35 18 59 ce 4f 01 20
wireshark_any_20210220195640_qyThNk.pcapng
Packets: 30 · Displayed: 30 (100.0%)
Profile: Default

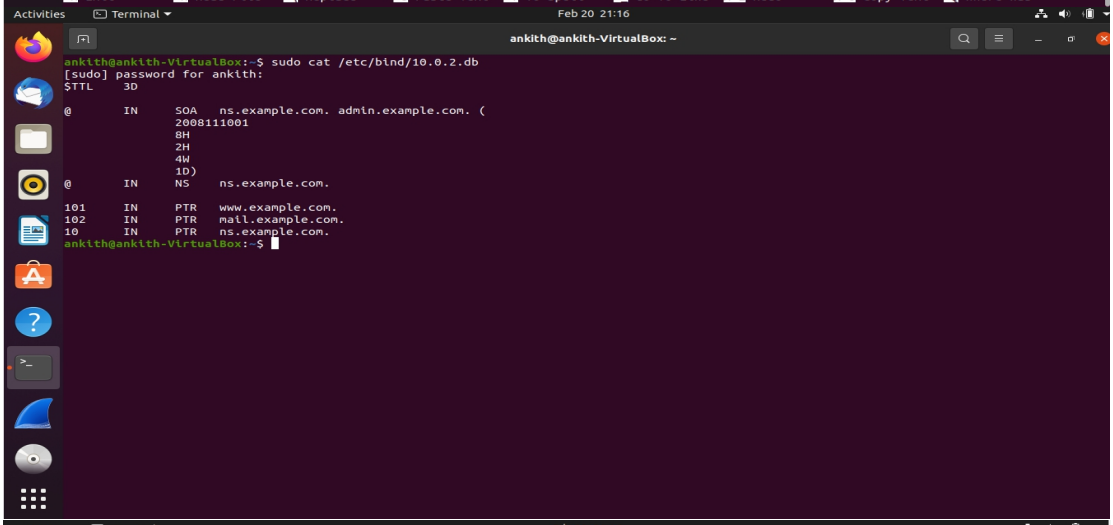

Activities
Wireshark
Feb 20 19:57
Wireshark · Packet 1 · any
Frame 1: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface any, id 0
Linux cooked capture
Packet type: Sent by us (4)
Link-layer address type: 1
Link-layer address length: 6
Source: PcsCompu_7f:1c:e8 (08:00:27:7f:1c:e8)
Unused: 0000
Protocol: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 73
Identification: 0xbc48 (48200)
Flags: 0x4000, Don't fragment
0... .... = Reserved bit: Not set
.1.. .... = Don't fragment: Set
..0. .... = More fragments: Not set
Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0x6649 [validation disabled]
[Header checksum status: Unverified]
Source: 10.0.2.4
Destination: 10.0.2.15
User Datagram Protocol, Src Port: 55184, Dst Port: 53
Source Port: 55184
Destination Port: 53
Length: 53
Checksum: 0x1859 [unverified]
[Checksum Status: Unverified]
Help
Close

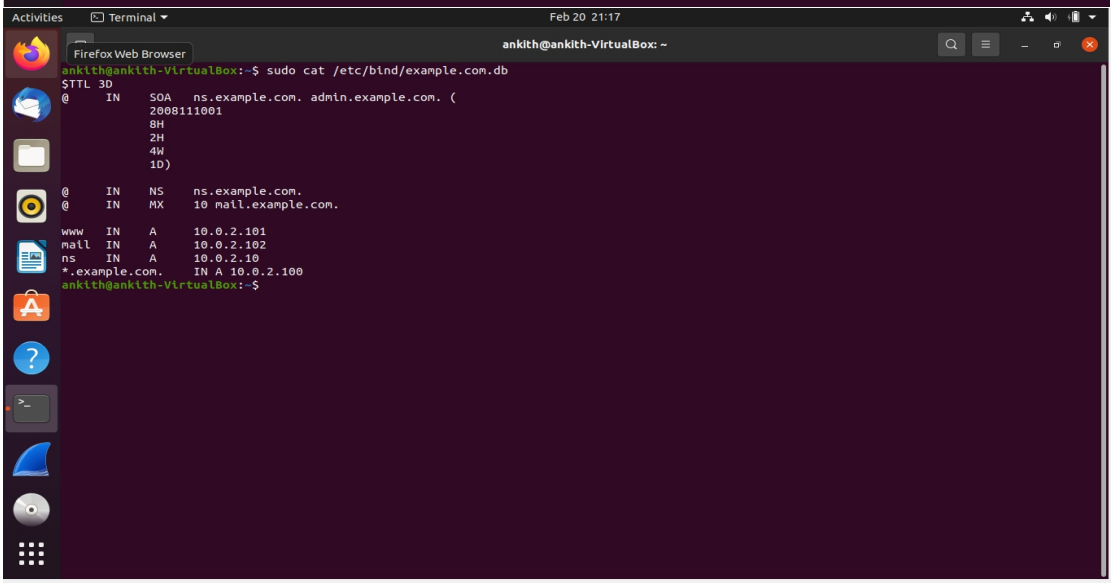

Activities
Wireshark
Feb 20 19:58
Wireshark · Packet 1 · any
Header checksum: 0x6649 [validation disabled]
[Header checksum status: Unverified]
Source: 10.0.2.4
Destination: 10.0.2.15
User Datagram Protocol, Src Port: 55184, Dst Port: 53
Source Port: 55184
Destination Port: 53
Length: 53
Checksum: 0x1859 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Timestamps]
[Time since first frame: 0.000000000 seconds]
[Time since previous frame: 0.000000000 seconds]
Domain Name System (query)
Transaction ID: 0xce4f
Flags: 0x0120 Standard query
0... .... = Response: Message is a query
.000 0... .... = Opcode: Standard query (0)
.... ..0. .... = Truncated: Message is not truncated
....1 .... = Recursion desired: Do query recursively
.... .0.. .... = Z: reserved (0)
....1. .... = AD bit: Set
....0 .... = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
Queries
www.flipkart.com: type A, class IN
Additional records
<Root>: type OPT
[Response In: 4]
Help
Close

Part 2: Setting Up an Authoritative Nameserver for example.com domain

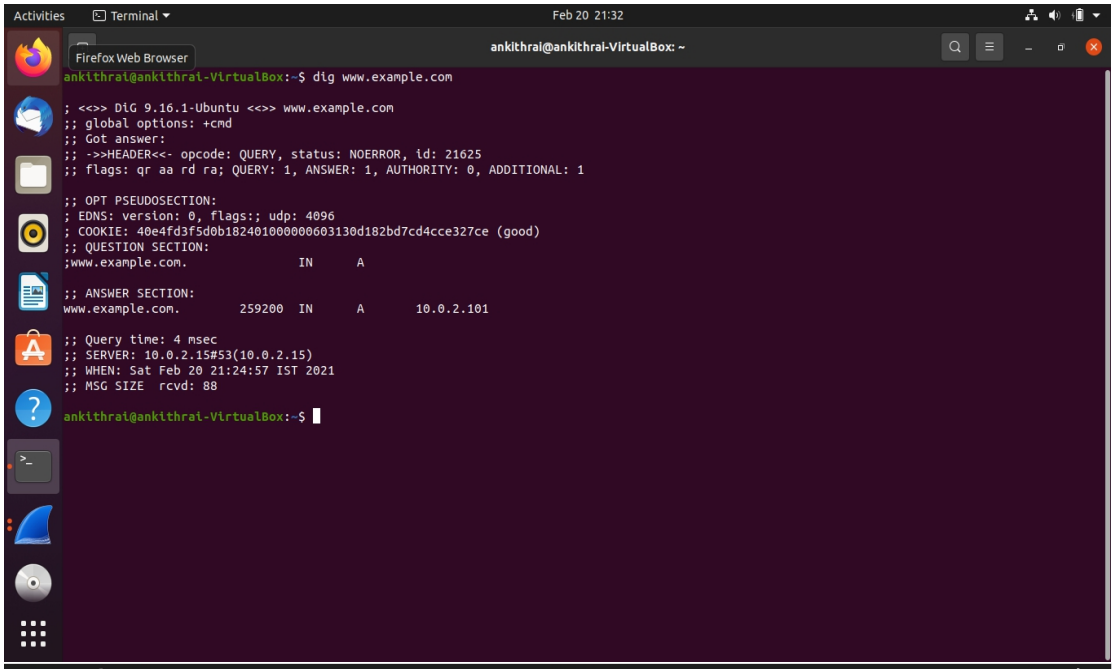
Task 3: Host a Zone in the Local DNS server.

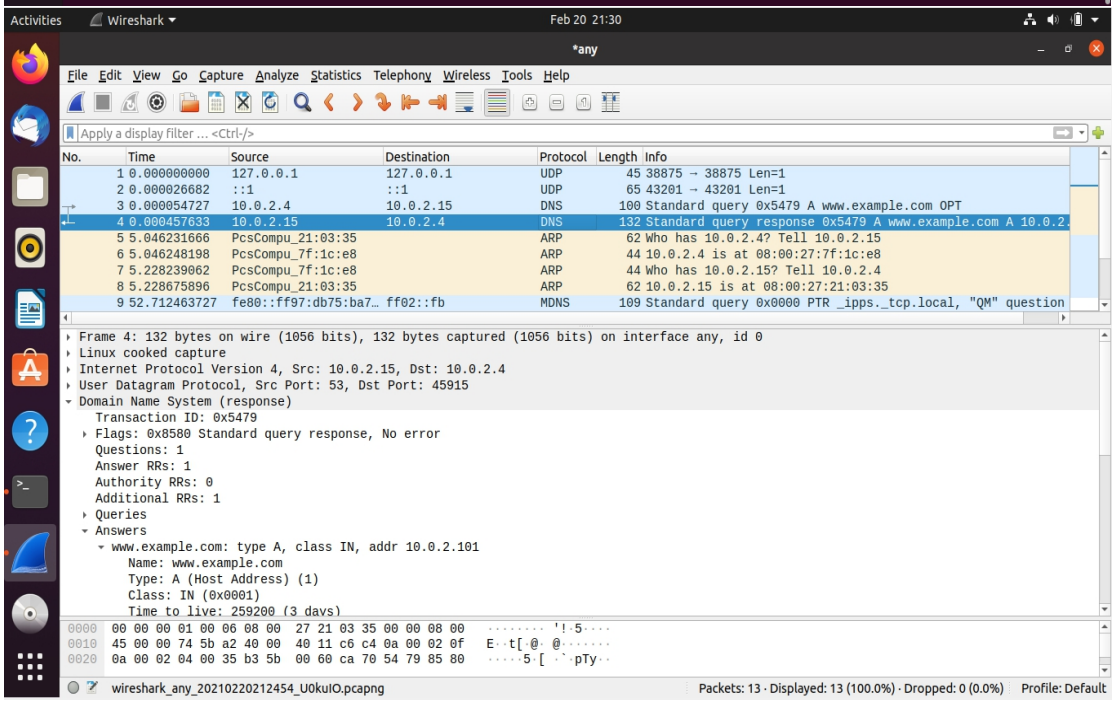


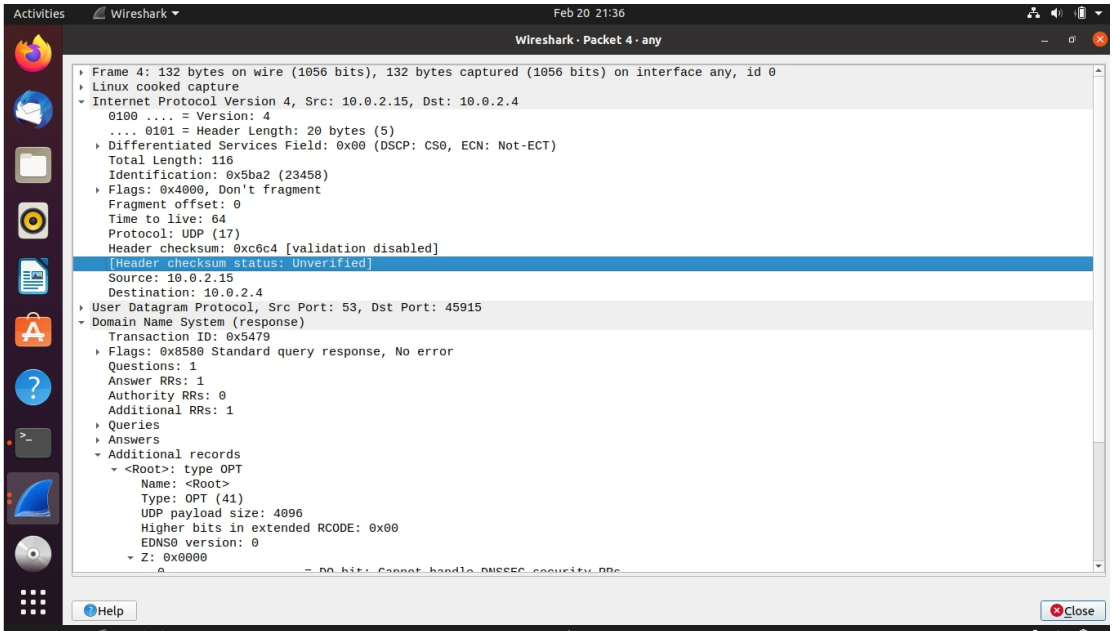


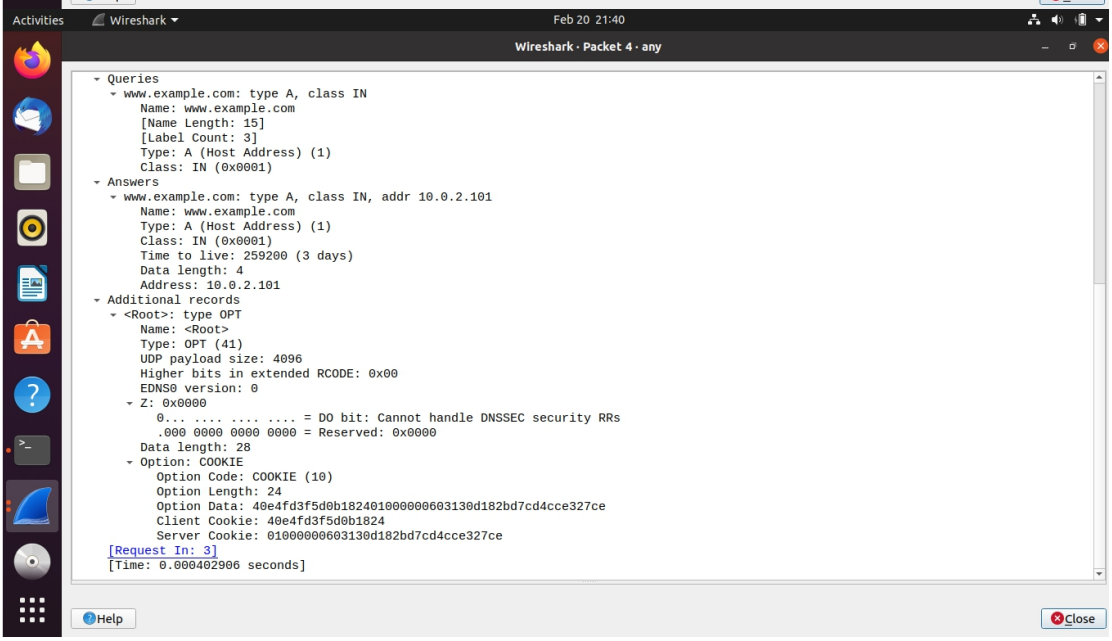


Task 4: Restart the BIND server and test









Observation Notebook Requirements/QUESTIONS:

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

Ans)The DNS query and response messages are visible in the screenshots.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?

Ans)The destination and source ports of the DNS query and response messages are the same.The port number is 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)The DNS query is made to server at IP Address 10.0.2.15. This is the same as the local DNS server configured.

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

Ans)The DNS query is of type A since it requests for an authoritative record. The answer section is empty.

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

Ans)The answer section of the DNS response message contains two Resource Records.

***CNAME RR*: This determines that the hostname flipkart.com refers to the canonical hostname www.flipkart.com.**

***A type RR*: This 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)The destination IP Address of the SYN packet corresponds to the IP Address of hostname (www.flipkart.com) retrieved from the response message.