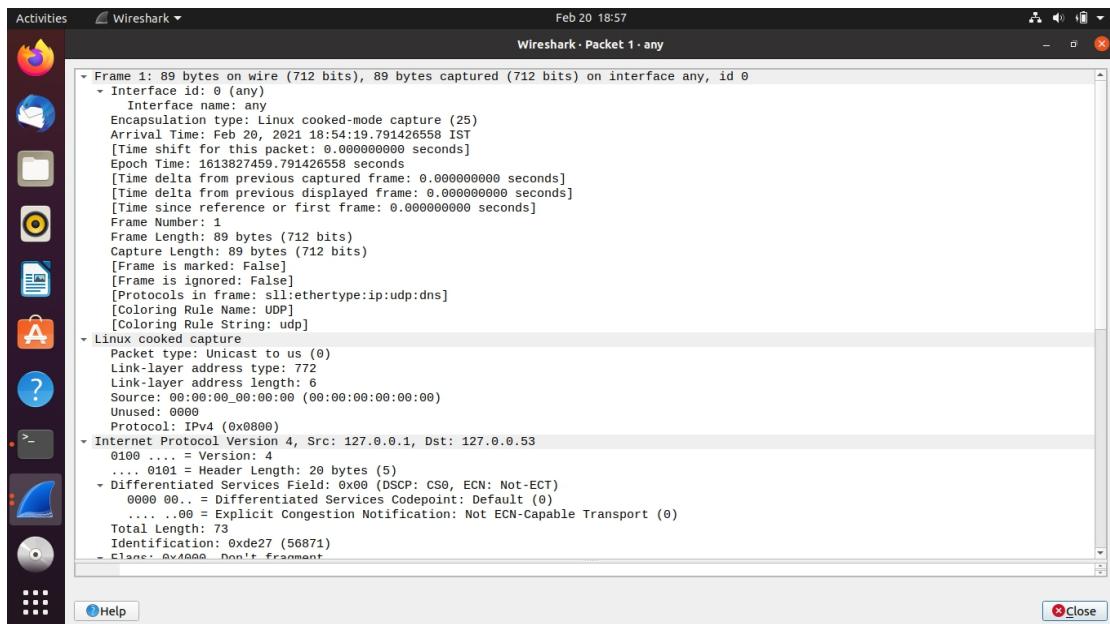
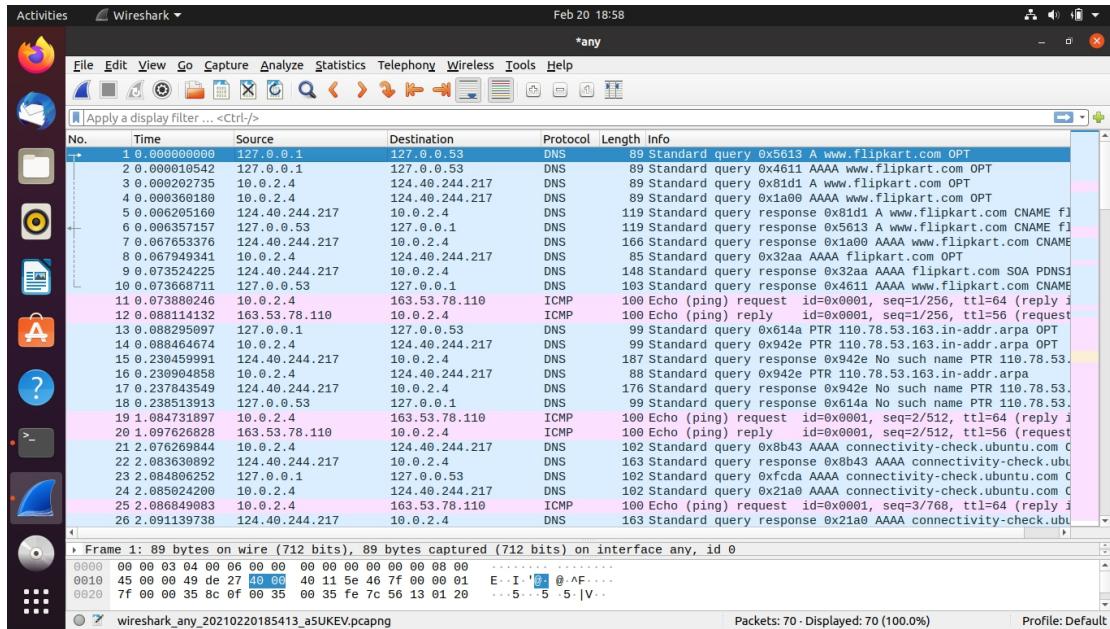
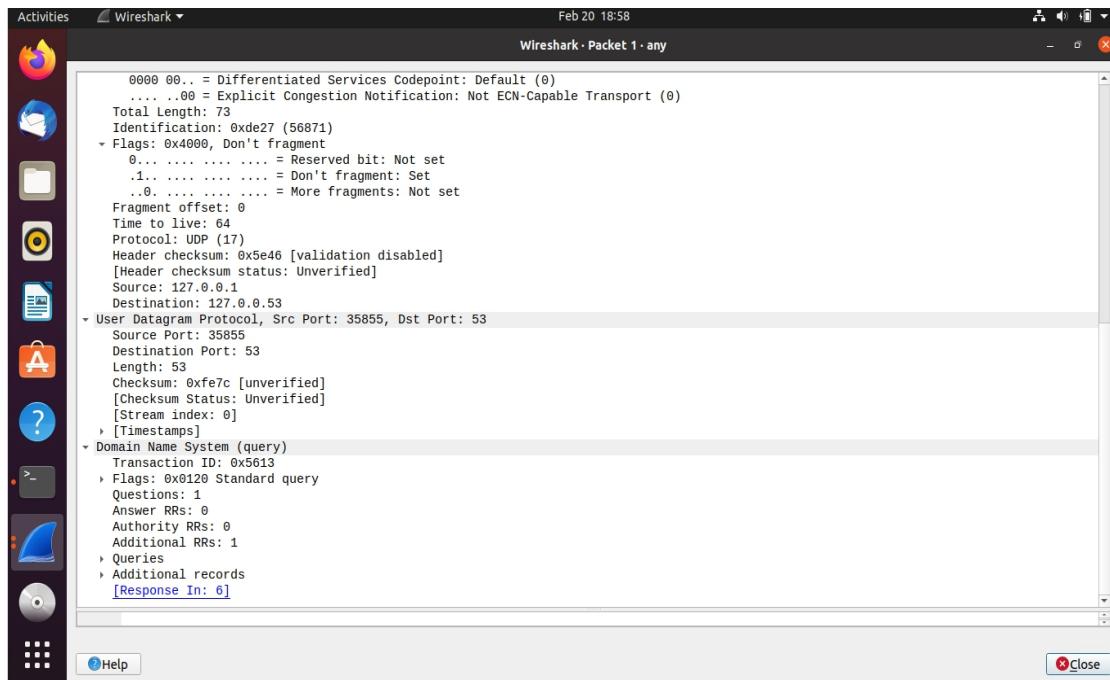


CN Lab Report – Week 4

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

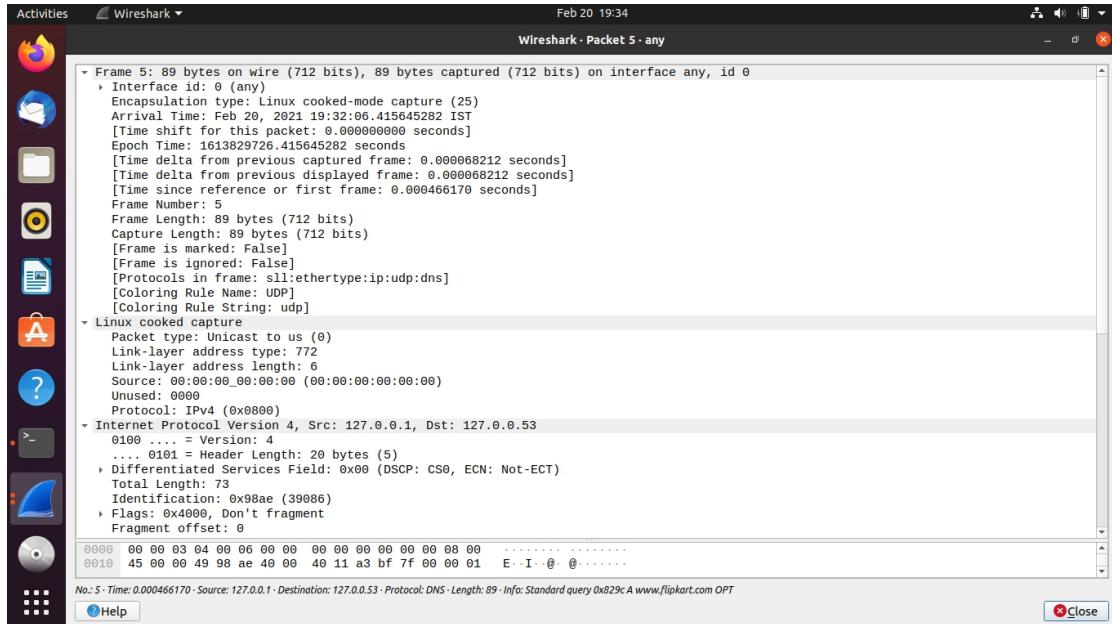
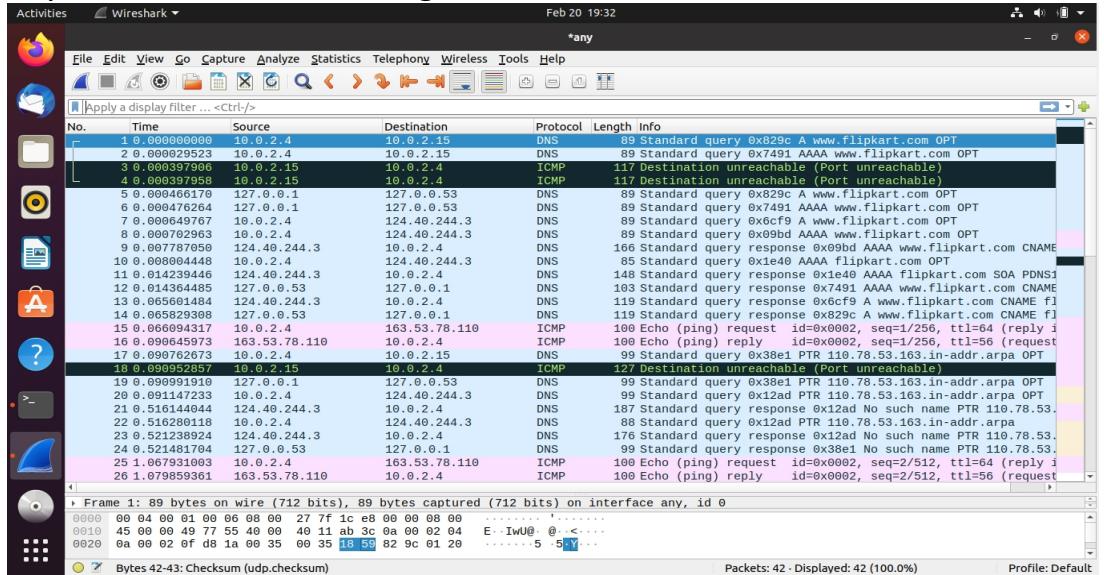
A screenshot of a terminal window titled "Terminal". The title bar shows "Activities Terminal" and the status bar indicates "Feb 20 19:21". The terminal window contains the following command-line session:

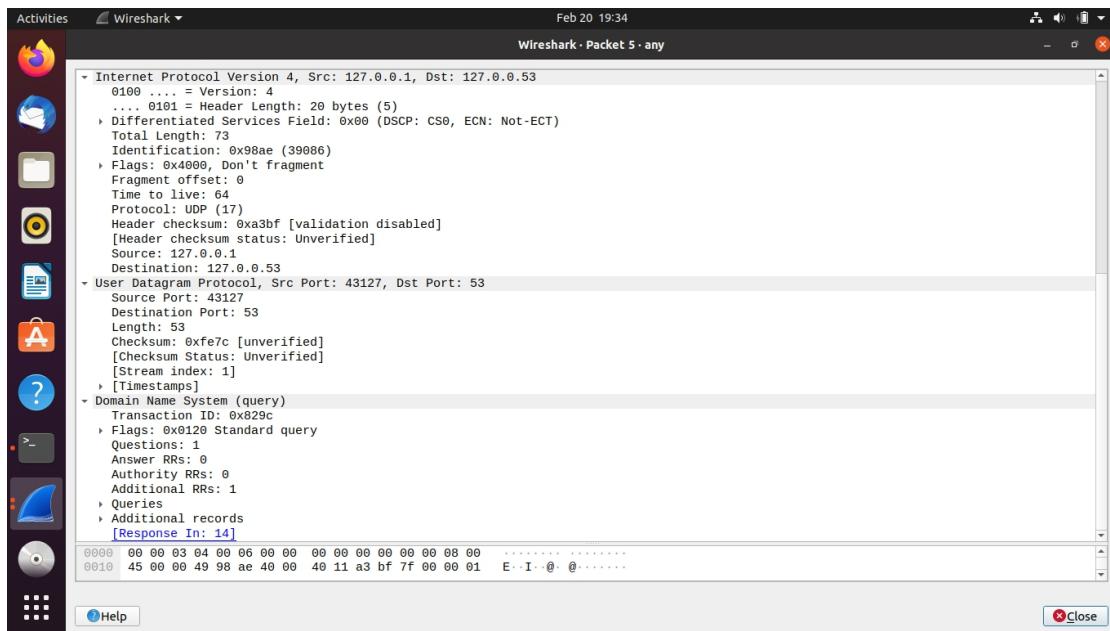
```
ankithrai@ankithrai-VirtualBox:~$ sudo nano /etc/resolvconf/resolv.conf.d/head
ankithrai@ankithrai-VirtualBox:~$ cat /etc/resolvconf/resolv.conf.d/head
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
# DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
# 127.0.0.53 is the systemd-resolved stub resolver.
# run "systemd-resolve --status" to see details about the actual nameservers.
nameserver 10.0.2.15
ankithrai@ankithrai-VirtualBox:~$ sudo resolvconf -u
ankithrai@ankithrai-VirtualBox:~$
```

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

```
Activities Terminal Feb 20 19:41
ankith@ankith-VirtualBox: ~
GNU nano 4.8 /etc/bind/named.conf.options

options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

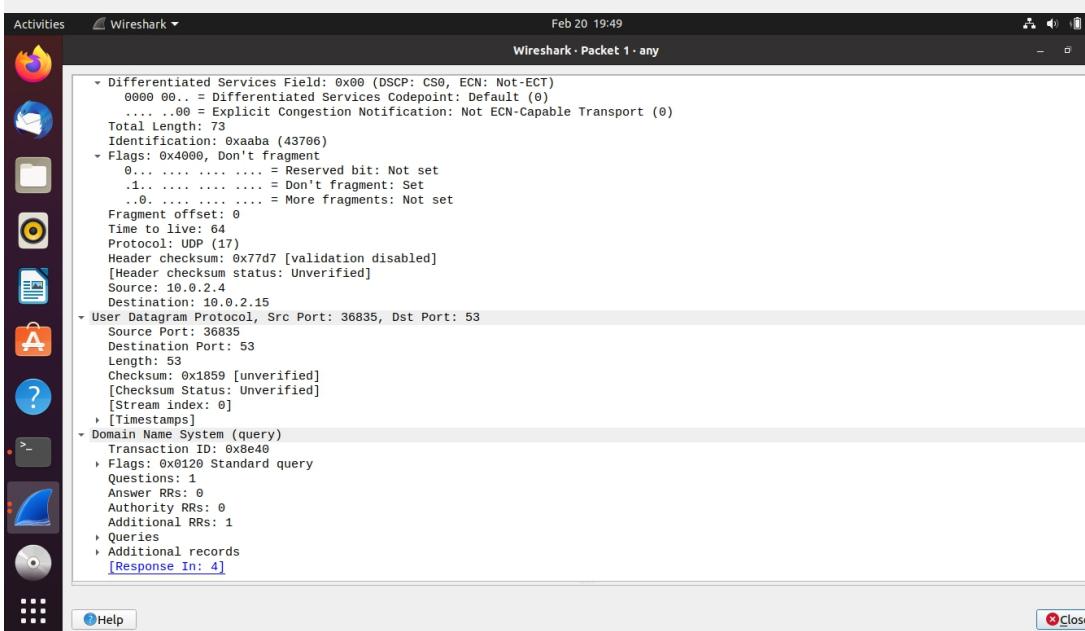
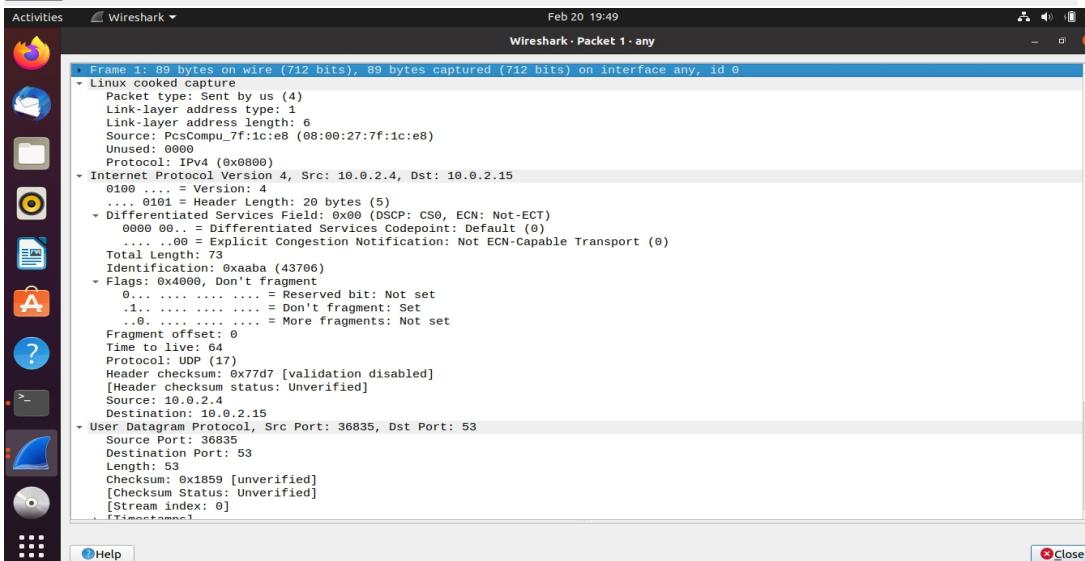
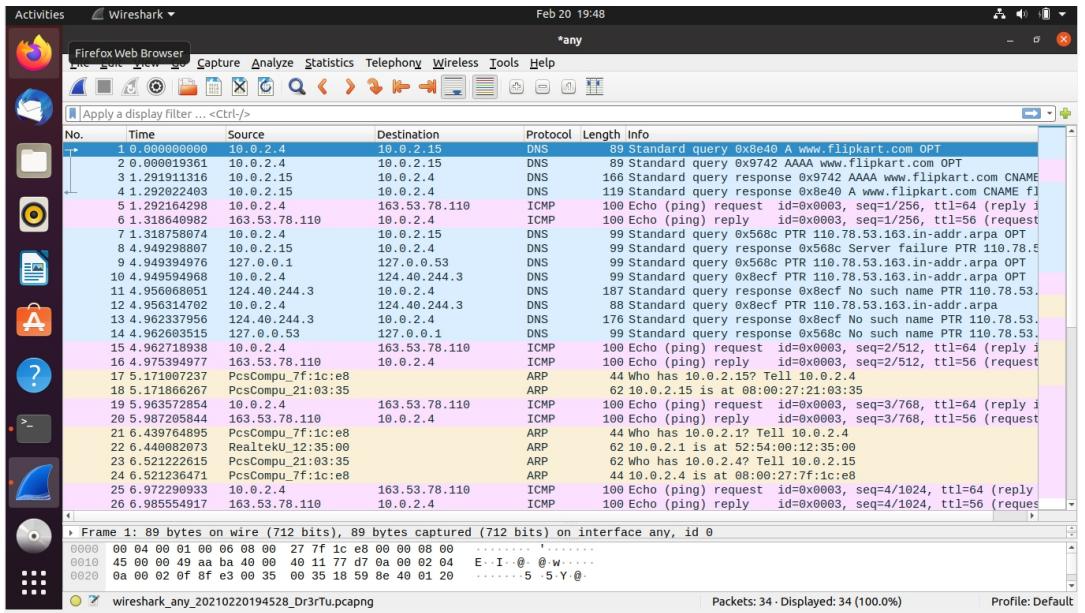
    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    // forwarders {
    //     0.0.0.0;
    // };
    dump-file "/var/cache/bind/dump.db";
    //================================================================
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys. See https://www.tsc.org/bind-keys
    //================================================================
    dnssec-validation auto;

    listen-on-v6 { any; };
};

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo
^X Exit ^R Read File ^Y Replace ^P Paste Text ^T To Spell ^G Go To Line M-E Redo
M-A Mark Text M-I To Bracket
M-G Copy Text ^Q Where Was
```

Observation 3:



Observation 4:

```
Activities Terminal ▾ Feb 20 19:54
ankith@ankith-VirtualBox:~$ sudo service bind9 restart
ankith@ankith-VirtualBox:~$ sudo rndc dumpdb -cache
ankith@ankith-VirtualBox:~$ sudo rndc flush
ankith@ankith-VirtualBox:~$ cat /var/cache/bind/dump.db
;
; Start view _default
;
; Cache dump of view '_default' (cache _default)
;
; using a 604800 second stale ttl
;DATE 20210213142306
; secure
.
1122621 IN NS a.root-servers.net.
1122621 IN NS b.root-servers.net.
1122621 IN NS c.root-servers.net.
1122621 IN NS d.root-servers.net.
1122621 IN NS e.root-servers.net.
1122621 IN NS f.root-servers.net.
1122621 IN NS g.root-servers.net.
1122621 IN NS h.root-servers.net.
1122621 IN NS i.root-servers.net.
1122621 IN NS j.root-servers.net.
1122621 IN NS k.root-servers.net.
1122621 IN NS l.root-servers.net.
1122621 IN NS m.root-servers.net.
;
; secure
1122621 RRSIG NS 8 0 518400 (
20210305050000 20210220040000 42351 .
dznKz0Foe1phHTx0wn8BT0D5TlPU3DP4busK
uSvx0L5cknArF/gQweufb7jevShp2lhcD93
SVFe6LmPfsRlwmYHca0YLUSdnzr/pmPTEvq
leCnhkI/xBQTonFI9LSwU1cqNNRcvwVNZ6YY
QHfFCLnqvNW/CQodn3YXq3Fe0BbjWcPUTa
lExhke2pennEBrqaCxZoooSW5ykapZugXjRx
4vh1xpZ1q/RiurlVeyX6vOgZpEtFkmneok0
jYq1z8ZrkD0WeumVn5JPnna2297SG2Qa0z
foMf3z16kd2oXFKfwtPoo3Ht30JD4WCaTa
=Y_E_04167555-LMaA
;
; glue
;
; glue
777077 A 91.189.91.139
;
; glue
flipkart.com. 777145 NS sdns14.ultradns.biz.
777145 NS sdns14.ultradns.com.
777145 NS sdns14.ultradns.net.
777145 NS sdns14.ultradns.org.
;
; answer
604405 \-AAAA ;-$NXRRSET
;
; flipkart.com. SOA PDNS1.ULTRADNS.NET. sysadmin.flipkart.com. 2017031521 10800 3600 604800 60
; secure
605245 \-DS ;-$NXRRSET
;
; com. SOA SOA.RRSIG.SOA...
9DA2HK6CJ3BHHTF53KBTDGK69URBEOM.com. RRSIG NSEC3 ...
; 9DA2HK6CJ3BHHTF53KBTDGK69URBEOM.com. NSEC3 1 0 - 9DA30HOH8G0P0F757L9LQ1LE8C29PSSA NS DS RRSIG
; CK0POJMG874LJREF7EFNB430QVIT8BSM.com. RRSIG NSEC3 ...
; CK0POJMG874LJREF7EFNB430QVIT8BSM.com. NSEC3 1 0 - CK0Q1GIN3N1ARRC90SM6QPQR81HSM9A NS SOA RRSIG DNSKEY NSEC3PARAM
; answer
604375 A 163.53.78.110
;
; answer
www.flipkart.com. 604405 CNAME flipkart.com.
; glue
nstld.com. 777078 NS av1.nstld.com.
777078 NS av2.nstld.com.
777078 NS av3.nstld.com.
777078 NS av4.nstld.com.
;
; glue
ac1.nstld.com. 777078 A 192.42.173.30
;
; glue
ac2.nstld.com. 777078 A 192.42.174.30
;
; glue
ac3.nstld.com. 777078 A 192.42.175.30
;
; pending-answer
ac4.nstld.com. 604578 A 192.42.176.30
;
; pending-answer
604578 AAAA 2001:500:123::30
```

```
Activities Terminal ▾ Feb 20 19:55
ankith@ankith-VirtualBox:~$ sudo service bind9 restart
ankith@ankith-VirtualBox:~$ sudo rndc dumpdb -cache
ankith@ankith-VirtualBox:~$ sudo rndc flush
ankith@ankith-VirtualBox:~$ cat /var/cache/bind/dump.db
;
; Start view _default
;
; Cache dump of view '_default' (cache _default)
;
; using a 604800 second stale ttl
;DATE 20210213142306
; secure
.
; canonical.com. SOA ns1.canonical.com. hostmaster.canonical.com. 2018054562 10800 3600 604800 3600
; glue
777077 A 91.189.91.139
;
; glue
flipkart.com. 777145 NS sdns14.ultradns.biz.
777145 NS sdns14.ultradns.com.
777145 NS sdns14.ultradns.net.
777145 NS sdns14.ultradns.org.
;
; answer
604405 \-AAAA ;-$NXRRSET
;
; flipkart.com. SOA PDNS1.ULTRADNS.NET. sysadmin.flipkart.com. 2017031521 10800 3600 604800 60
; secure
605245 \-DS ;-$NXRRSET
;
; com. SOA SOA.RRSIG.SOA...
9DA2HK6CJ3BHHTF53KBTDGK69URBEOM.com. RRSIG NSEC3 ...
; 9DA2HK6CJ3BHHTF53KBTDGK69URBEOM.com. NSEC3 1 0 - 9DA30HOH8G0P0F757L9LQ1LE8C29PSSA NS DS RRSIG
; CK0POJMG874LJREF7EFNB430QVIT8BSM.com. RRSIG NSEC3 ...
; CK0POJMG874LJREF7EFNB430QVIT8BSM.com. NSEC3 1 0 - CK0Q1GIN3N1ARRC90SM6QPQR81HSM9A NS SOA RRSIG DNSKEY NSEC3PARAM
; answer
604375 A 163.53.78.110
;
; answer
www.flipkart.com. 604405 CNAME flipkart.com.
; glue
nstld.com. 777078 NS av1.nstld.com.
777078 NS av2.nstld.com.
777078 NS av3.nstld.com.
777078 NS av4.nstld.com.
;
; glue
ac1.nstld.com. 777078 A 192.42.173.30
;
; glue
ac2.nstld.com. 777078 A 192.42.174.30
;
; glue
ac3.nstld.com. 777078 A 192.42.175.30
;
; pending-answer
ac4.nstld.com. 604578 A 192.42.176.30
;
; pending-answer
604578 AAAA 2001:500:123::30
```

Activities Wireshark ▾ Feb 20 19:57

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 0xc04f A www.flipkart.com OPT
2	0.000045976	10.0.2.4	10.0.2.15	DNS	89	Standard query 0xc0533 AAAA www.flipkart.com CNAME
3	1.1917090331	10.0.2.15	10.0.2.4	DNS	166	Standard query response 0xc0533 AAAA www.flipkart.com CNAME
4	1.1917090331	10.0.2.15	10.0.2.4	DNS	119	Standard query response 0xc04f 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_7f:1c:e8		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	5.820358666	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_7f:1c:e8		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 08:00:27:2f:1c:e8
21	6.453528618	PcsCompu_7f:1c:e8		ARP	44	Who has 10.0.2.1? Tell 10.0.2.4
22	6.454167463	RouterKU_12:35:00		ARP	62	10.0.2.1 is at 52:54:00:12:35:00
23	6.8350622290	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 (request

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 00 40 11 66 49 0a 00 02 04 E I H@ 0 fI

0020 0a 00 02 0f d7 90 00 35 00 35 18 59 ca 4f 01 20 5 5 Y O

wireshark_any_20210220195640_qyThNk.pcapng Packets: 30 · Displayed: 30 (100.0%) Profile: Default

Activities Wireshark ▾ Wireshark · Packet 1 · any Feb 20 19:57

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 (08:00:27:2f: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 (DSCHP: 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

.... 0000 ..0000 = Reserved bit: Not set

.... 1000 ..0000 = Don't Fragment: Set

.... 0000 ..0000 = 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]

[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

.... 0000 ..0000 = Response: Message is a query

.... 0000 00.. = Opcode: Standard query (0)

.... ..00 ..00 = Truncated: Message is not truncated

.... ..10 ..00 = Recursion desired: Do query recursively

.... ..00 ..00 = Z: reserved (0)

.... ..00 ..10 = AD bit: Set

.... ..00 ..00 = 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

Activities Wireshark ▾ Wireshark · Packet 1 · any Feb 20 19:58

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

.... 0000 ..0000 = Response: Message is a query

.... 0000 00.. = Opcode: Standard query (0)

.... ..00 ..00 = Truncated: Message is not truncated

.... ..10 ..00 = Recursion desired: Do query recursively

.... ..00 ..00 = Z: reserved (0)

.... ..00 ..10 = AD bit: Set

.... ..00 ..00 = 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.

The image shows three vertically stacked terminal windows from a Linux desktop environment. The top window displays the /etc/bind/named.conf file, which includes configurations for the example.com zone and the 2.0.10.in-addr.arpa zone. The middle window shows the contents of the /etc/bind/10.0.2.db file, which contains the zone's SOA record and PTR records for hosts www, mail, and ns. The bottom window shows the contents of the /etc/bind/example.com.db file, which contains the zone's SOA record and MX record for mail, along with A records for www and *.

```
GNU nano 4.8 /etc/bind/named.conf
// This is the primary configuration file for the BIND DNS server named.
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local
include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
zone "example.com" {
    type master;
    file "/etc/bind/example.com.db";
};
zone "2.0.10.in-addr.arpa" {
    type master;
    file "/etc/bind/10.0.2.db";
};■

Activities Terminal Feb 20 20:14
ankith@ankith-VirtualBox:~ Modified

Activities Terminal Feb 20 21:16
ankith@ankith-VirtualBox:~ [sudo] password for ankith:
$TTL 3D
@ IN SOA ns.example.com. admin.example.com. (
    2008111001
    8H
    2H
    4W
    1D)
@ IN NS ns.example.com.
101 IN PTR www.example.com.
102 IN PTR mail.example.com.
10 IN PTR ns.example.com.
ankith@ankith-VirtualBox:~ ■

Activities Terminal Feb 20 21:17
Firefox Web Browser
ankith@ankith-VirtualBox:~ $ sudo cat /etc/bind/example.com.db
$TTL 3D
@ IN SOA ns.example.com. admin.example.com. (
    2008111001
    8H
    2H
    4W
    1D)
@ IN NS ns.example.com.
@ IN MX 10 mail.example.com.
www IN A 10.0.2.101
mail IN A 10.0.2.102
ns IN A 10.0.2.10
*.example.com. IN A 10.0.2.100
ankith@ankith-VirtualBox:~ $
```

Task 4: Restart the BIND server and test

The screenshot shows a Linux desktop environment with two terminal windows and a Wireshark network traffic capture window.

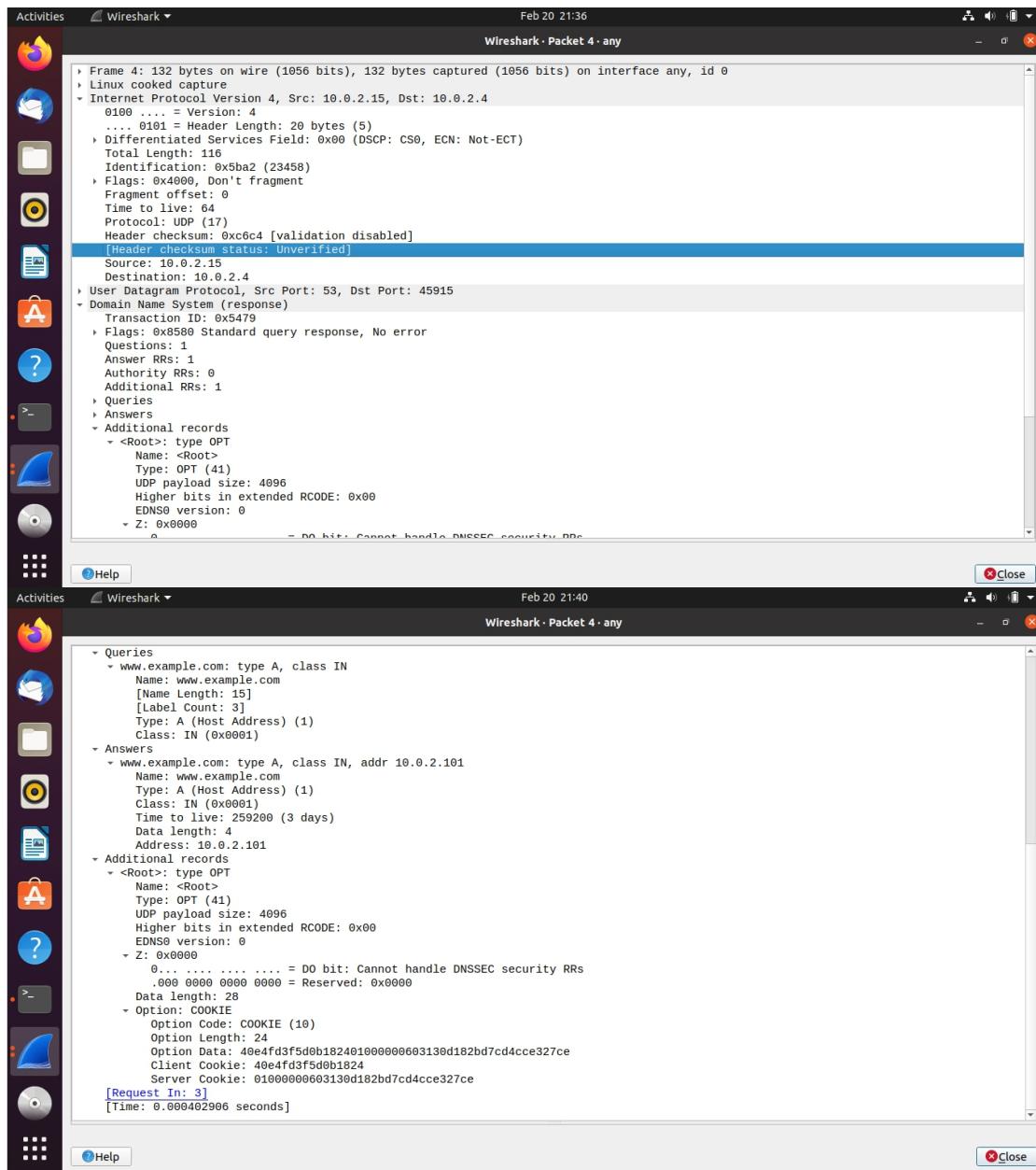
Terminal Window 1: Shows the command `dig www.example.com` being run in a Firefox terminal window. The output shows a successful DNS query to 10.0.2.15, returning the IP address 10.0.2.101 for www.example.com.

```
ankithrai@ankithrai-VirtualBox: ~
$ dig www.example.com
; <>> DiG 9.16.1-Ubuntu <>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 21625
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: 40e4fd3f5d0b182401000000603130d182bd7cd4cce327ce (good)
;; QUESTION SECTION:
;www.example.com.           IN      A
;; ANSWER SECTION:
www.example.com.    259200  IN      A      10.0.2.101
;; Query time: 4 msec
;; SERVER: 10.0.2.15#53(10.0.2.15)
;; WHEN: Sat Feb 20 21:24:57 IST 2021
;; MSG SIZE  rcvd: 88
ankithrai@ankithrai-VirtualBox: ~
```

Terminal Window 2: Shows the command `wireshark` being run in another terminal window.

Wireshark Window: Displays a network capture titled "any". It shows several frames, with frame 4 selected. Frame 4 is a DNS query from 10.0.2.15 to 10.0.2.4. The details pane shows the transaction ID is 0x5479, and the query is for the IP address of www.example.com. The bytes pane shows the raw hex and ASCII data of the DNS query frame.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	127.0.0.1	127.0.0.1	UDP	45	38875 → 38875 Len=1
2	0.000026682	::1	::1	UDP	65	43201 → 43201 Len=1
3	0.000054727	10.0.2.4	10.0.2.15	DNS	100	Standard query 0x5479 A www.example.com OPT
4	0.0000457633	10.0.2.15	10.0.2.4	DNS	132	Standard query response 0x5479 A www.example.com A 10.0.2.101
5	0.046231666	PcsCompu_21:03:35		ARP	62	Who has 10.0.2.4? Tell 10.0.2.15
6	0.046248198	PcsCompu_7f:1c:e8		ARP	44	10.0.2.4 is at 08:00:27:7f:1c:e8
7	0.228239962	PcsCompu_7f:1c:e8		ARP	44	Who has 10.0.2.15? Tell 10.0.2.4
8	0.228675896	PcsCompu_21:03:35		ARP	62	10.0.2.15 is at 08:00:27:21:03:35
9	52.712463727	fe80::ff97:db75:ba7... ff02::fb		MDNS	109	Standard query 0x0000 PTR _ipp.s._tcp.local, "QM" question



Observation Notebook Requirements/QUESTIONS:

1) Locate the DNS query and response messages. Are they 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 the 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.