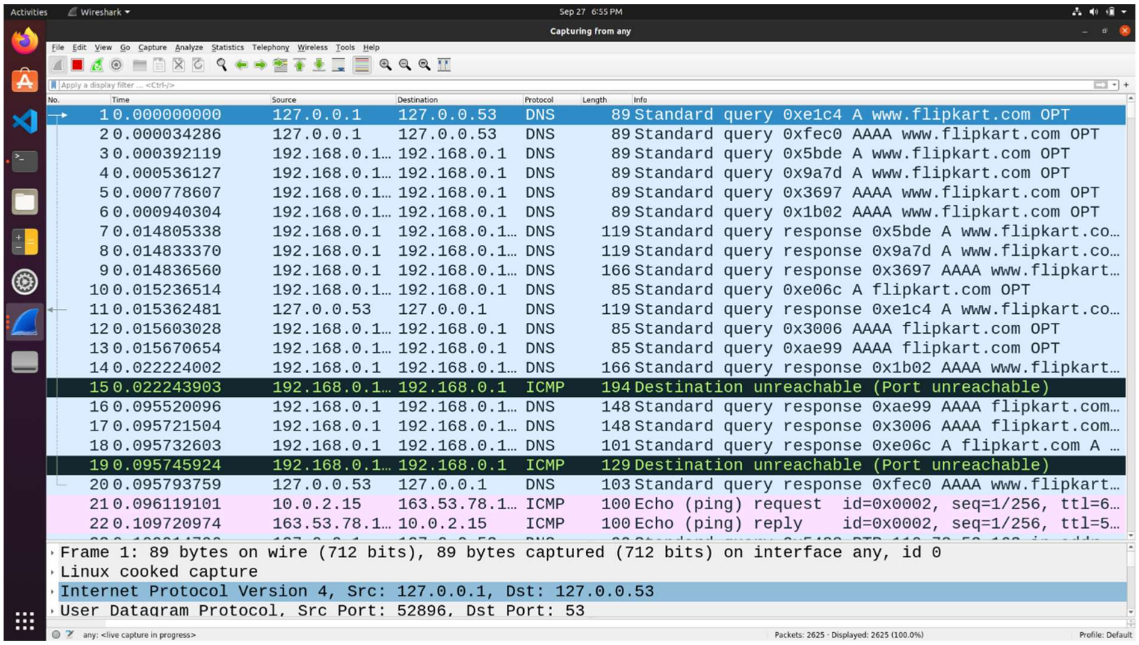
CN Lab Report – Week 4

PES1UG 21CS361

Nandan N

1. First Test – Pinging using default DNS

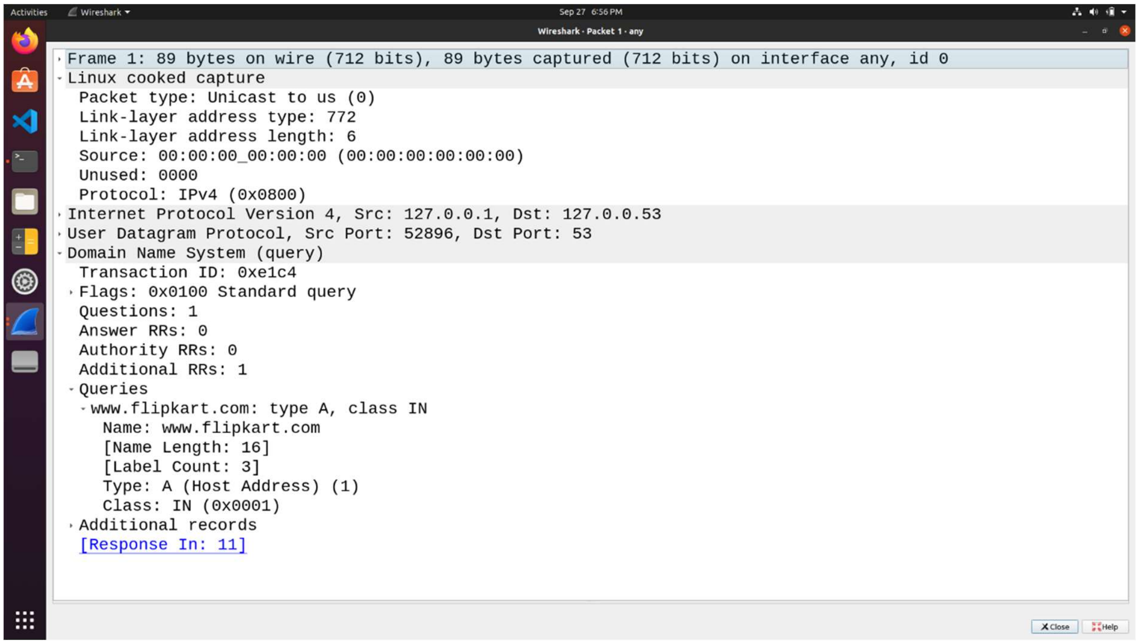
- Wireshark is used to capture the packets in the background while pinging **`www.flipkart.com`**
- The IP Address of the Local DNS server is observed to be **`127.0.0.53`**.
- The query is of type **`A`** which stands for authoritative. The answer contains the **`A`** type record along with the IP address of the website – **`163.53.78.110`**.
- The first query and authoritative response are shown below.


Activities
Wireshark
Sep 27 6:55 PM
Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
any: <live capture in progress>
Packets: 2625 · Displayed: 2625 (100.0%)
Profile: Default

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	127.0.0.1	127.0.0.53	DNS	89	Standard query 0xe1c4 A www.flipkart.com OPT
2	0.000034286	127.0.0.1	127.0.0.53	DNS	89	Standard query 0xfec0 AAAA www.flipkart.com OPT
3	0.000392119	192.168.0.1…	192.168.0.1	DNS	89	Standard query 0x5bde A www.flipkart.com OPT
4	0.000536127	192.168.0.1…	192.168.0.1	DNS	89	Standard query 0x9a7d A www.flipkart.com OPT
5	0.000778607	192.168.0.1…	192.168.0.1	DNS	89	Standard query 0x3697 AAAA www.flipkart.com OPT
6	0.000940304	192.168.0.1…	192.168.0.1	DNS	89	Standard query 0x1b02 AAAA www.flipkart.com OPT
7	0.014805338	192.168.0.1	192.168.0.1…	DNS	119	Standard query response 0x5bde A www.flipkart.co…
8	0.014833370	192.168.0.1	192.168.0.1…	DNS	119	Standard query response 0x9a7d A www.flipkart.co…
9	0.014836560	192.168.0.1	192.168.0.1…	DNS	166	Standard query response 0x3697 AAAA www.flipkart…
10	0.015236514	192.168.0.1…	192.168.0.1	DNS	85	Standard query 0xe06c A flipkart.com OPT
11	0.015362481	127.0.0.53	127.0.0.1	DNS	119	Standard query response 0xe1c4 A www.flipkart.co…
12	0.015603028	192.168.0.1…	192.168.0.1	DNS	85	Standard query 0x3006 AAAA flipkart.com OPT
13	0.015670654	192.168.0.1…	192.168.0.1	DNS	85	Standard query 0xae99 AAAA flipkart.com OPT
14	0.022224002	192.168.0.1	192.168.0.1…	DNS	166	Standard query response 0x1b02 AAAA www.flipkart…
15	0.022243903	192.168.0.1…	192.168.0.1	ICMP	194	Destination unreachable (Port unreachable)
16	0.095520096	192.168.0.1	192.168.0.1…	DNS	148	Standard query response 0xae99 AAAA flipkart.com…
17	0.095721504	192.168.0.1	192.168.0.1…	DNS	148	Standard query response 0x3006 AAAA flipkart.com…
18	0.095732603	192.168.0.1	192.168.0.1…	DNS	101	Standard query response 0xe06c A flipkart.com A …
19	0.095745924	192.168.0.1…	192.168.0.1	ICMP	129	Destination unreachable (Port unreachable)
20	0.095793759	127.0.0.53	127.0.0.1	DNS	103	Standard query response 0xfec0 AAAA www.flipkart…
21	0.096119101	10.0.2.15	163.53.78.1…	ICMP	100	Echo (ping) request id=0x0002, seq=1/256, ttl=6…
22	0.109720974	163.53.78.1…	10.0.2.15	ICMP	100	Echo (ping) reply id=0x0002, seq=1/256, ttl=5…

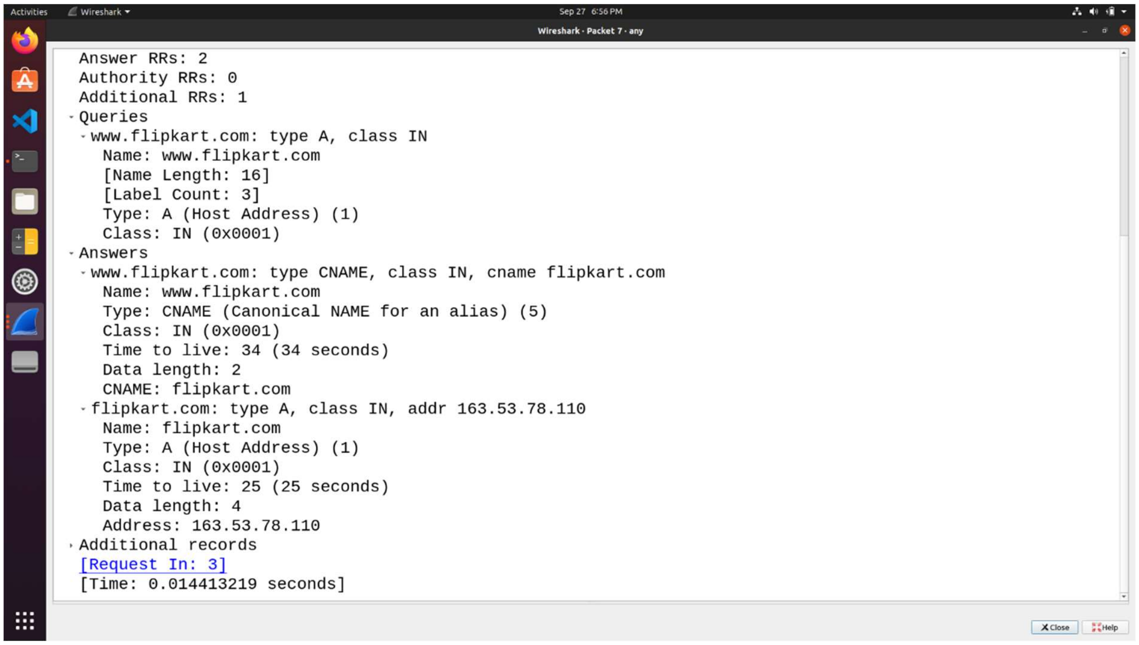
```
Frame 1: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.53
User Datagram Protocol, Src Port: 52896, Dst Port: 53
```

Wireshark Packet Capture



```
› Frame 1: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface any, id 0
⌄ Linux cooked capture
    Packet type: Unicast to us (0)
    Link-layer address type: 772
    Link-layer address length: 6
    Source: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Unused: 0000
    Protocol: IPv4 (0x0800)
› Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.53
› User Datagram Protocol, Src Port: 52896, Dst Port: 53
⌄ Domain Name System (query)
    Transaction ID: 0xe1c4
  › Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    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)
  › Additional records
    [Response In: 11]
```

DNS Query

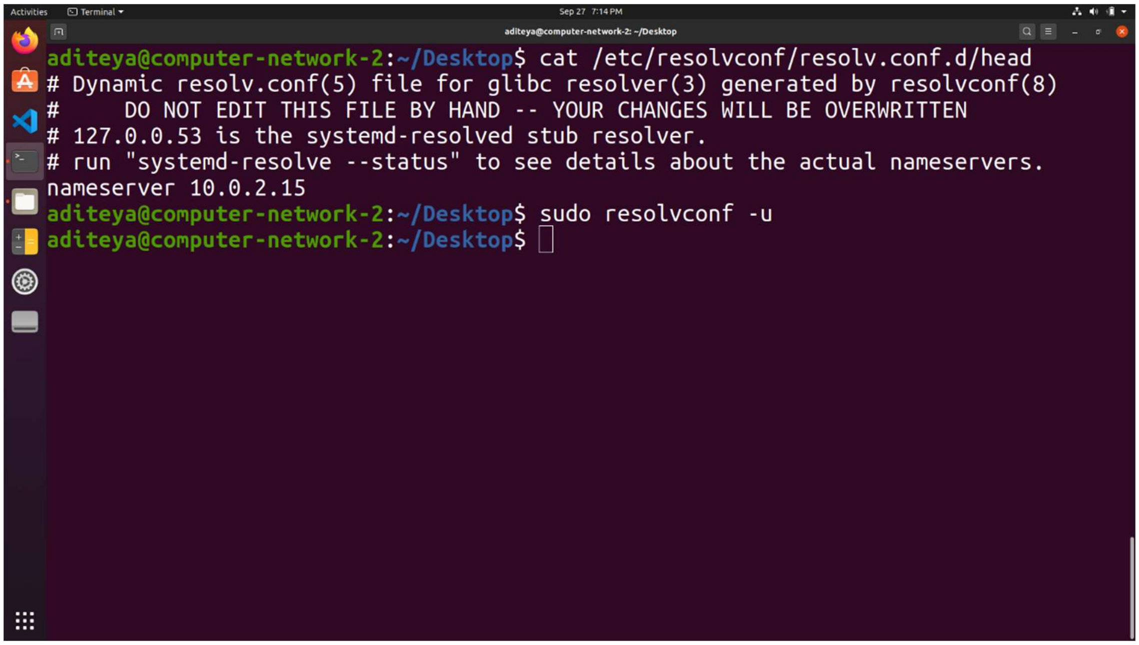


```
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 1
  ⌄ Queries
    ⌄ www.flipkart.com: type A, class IN
        Name: www.flipkart.com
        [Name Length: 16]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  ⌄ Answers
    ⌄ www.flipkart.com: type CNAME, class IN, cname flipkart.com
        Name: www.flipkart.com
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 34 (34 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: 25 (25 seconds)
        Data length: 4
        Address: 163.53.78.110
  › Additional records
    [Request In: 3]
    [Time: 0.014413219 seconds]
```

DNS Response

2. Task 1 – Configuring Client Machine

- The IP Address of the client machine is **`10.0.2.4`** and the IP Address of the server machine is **`10.0.2.15`**.
- We need to add the IP Address of the custom DNS server (**`10.0.2.15`**) to the client machine.
- This is done by adding the IP address of the server to the file **`/etc/resolvconf/resolv.conf.d/head`** which stores the order of DNS server resolution. This ensures that the custom DNS server will be used to resolve names.
- The IP Address of the custom DNS server is also added to the DNS menu under the IPv4 Network Settings.
- The changes are applied by using the command **`sudo resolvconf -u`**

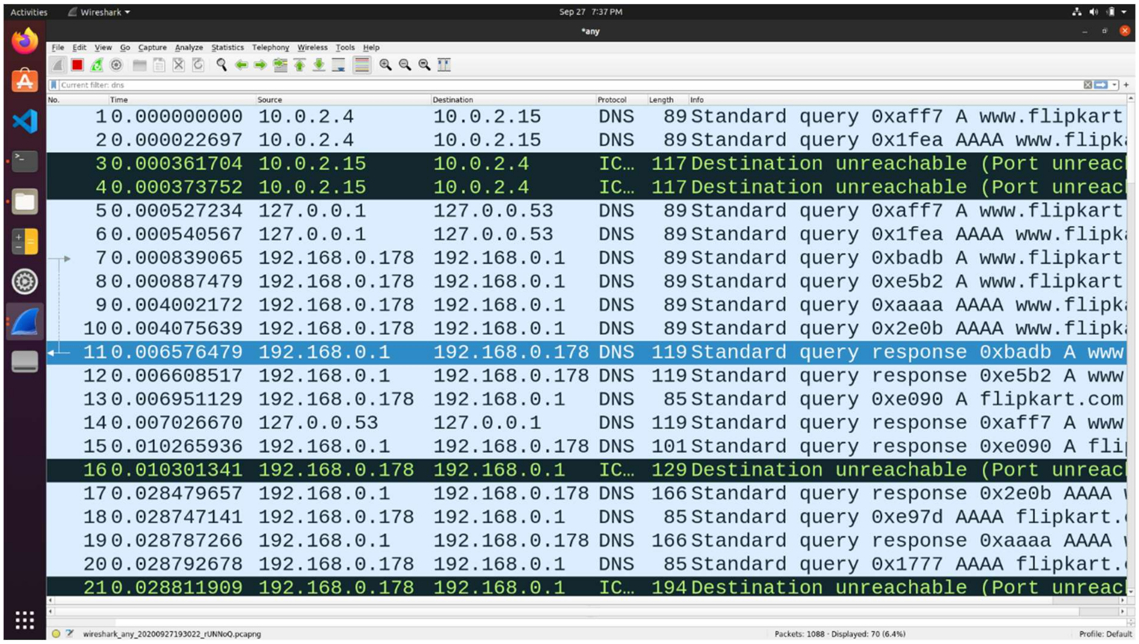


```
aditeya@computer-network-2:~/Desktop$ cat /etc/resolvconf/resolv.conf.d/head
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
# 127.0.0.53 is the systemd-resolved stub resolver.
# run "systemd-resolve --status" to see details about the actual nameservers.
nameserver 10.0.2.15
aditeya@computer-network-2:~/Desktop$ sudo resolvconf -u
aditeya@computer-network-2:~/Desktop$ 
```

Reconfiguring name server resolution order

3. Second Test

- The Flipkart website is pinged again, and Wireshark is used to capture packets.
- 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`**.



Activities
Wireshark
Sep 27 7:37 PM
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Current filter: dns

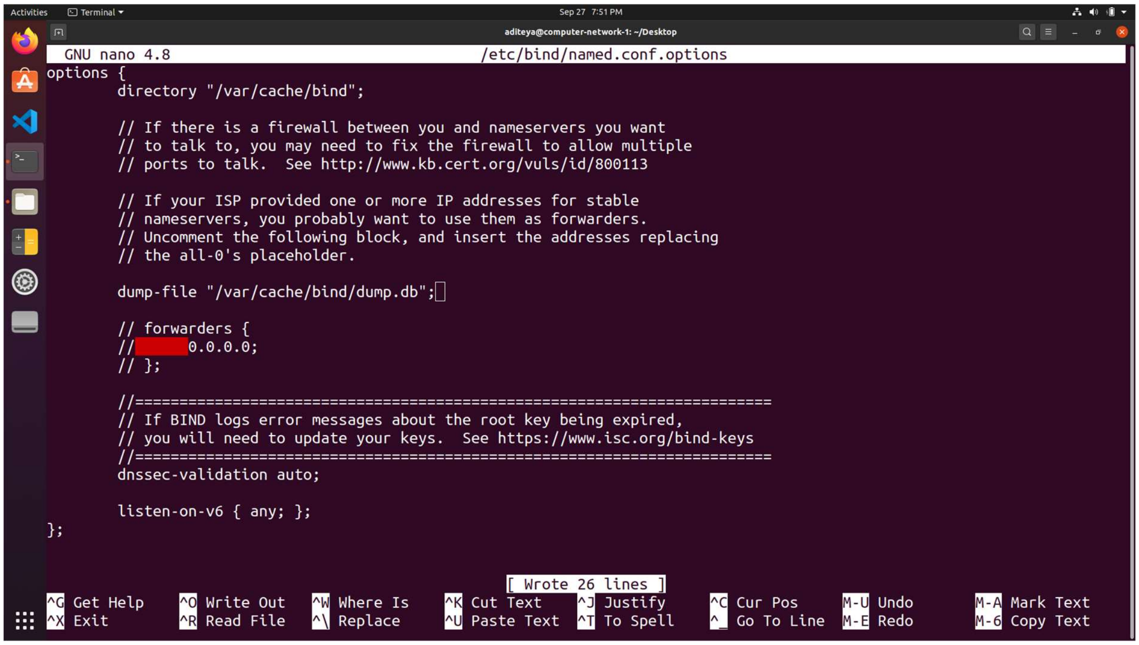
```
No. Time         Source        Destination   Protocol Length Info
  1 0.000000000  10.0.2.4      10.0.2.15     DNS       89 Standard query 0xaff7 A www.flipkart
  2 0.000022697  10.0.2.4      10.0.2.15     DNS       89 Standard query 0x1fea AAAA www.flipk
  3 0.000361704  10.0.2.15     10.0.2.4      IC…      117 Destination unreachable (Port unreac
  4 0.000373752  10.0.2.15     10.0.2.4      IC…      117 Destination unreachable (Port unreac
  5 0.000527234  127.0.0.1     127.0.0.53    DNS       89 Standard query 0xaff7 A www.flipkart
  6 0.000540567  127.0.0.1     127.0.0.53    DNS       89 Standard query 0x1fea AAAA www.flipk
  7 0.000839065  192.168.0.178 192.168.0.1   DNS       89 Standard query 0xbadb A www.flipkart
  8 0.000887479  192.168.0.178 192.168.0.1   DNS       89 Standard query 0xe5b2 A www.flipkart
  9 0.004002172  192.168.0.178 192.168.0.1   DNS       89 Standard query 0xaaaa AAAA www.flipk
 10 0.004075639  192.168.0.178 192.168.0.1   DNS       89 Standard query 0x2e0b AAAA www.flipk
 11 0.006576479  192.168.0.1   192.168.0.178 DNS      119 Standard query response 0xbadb A www
 12 0.006608517  192.168.0.1   192.168.0.178 DNS      119 Standard query response 0xe5b2 A www
 13 0.006951129  192.168.0.178 192.168.0.1   DNS       85 Standard query 0xe090 A flipkart.com
 14 0.007026670  127.0.0.53    127.0.0.1     DNS      119 Standard query response 0xaff7 A www
 15 0.010265936  192.168.0.1   192.168.0.178 DNS      101 Standard query response 0xe090 A fli
 16 0.010301341  192.168.0.178 192.168.0.1   IC…      129 Destination unreachable (Port unreac
 17 0.028479657  192.168.0.1   192.168.0.178 DNS      166 Standard query response 0x2e0b AAAA
 18 0.028747141  192.168.0.178 192.168.0.1   DNS       85 Standard query 0xe97d AAAA flipkart.
 19 0.028787266  192.168.0.1   192.168.0.178 DNS      166 Standard query response 0xaaaa AAAA
 20 0.028792678  192.168.0.178 192.168.0.1   DNS       85 Standard query 0x1777 AAAA flipkart.
 21 0.028811909  192.168.0.178 192.168.0.1   IC…      194 Destination unreachable (Port unreac
```

```
wireshark_any_20200927193022_rUNNoQ.pcapng          Packets: 1088 · Displayed: 70 (6.4%)          Profile: Default
```

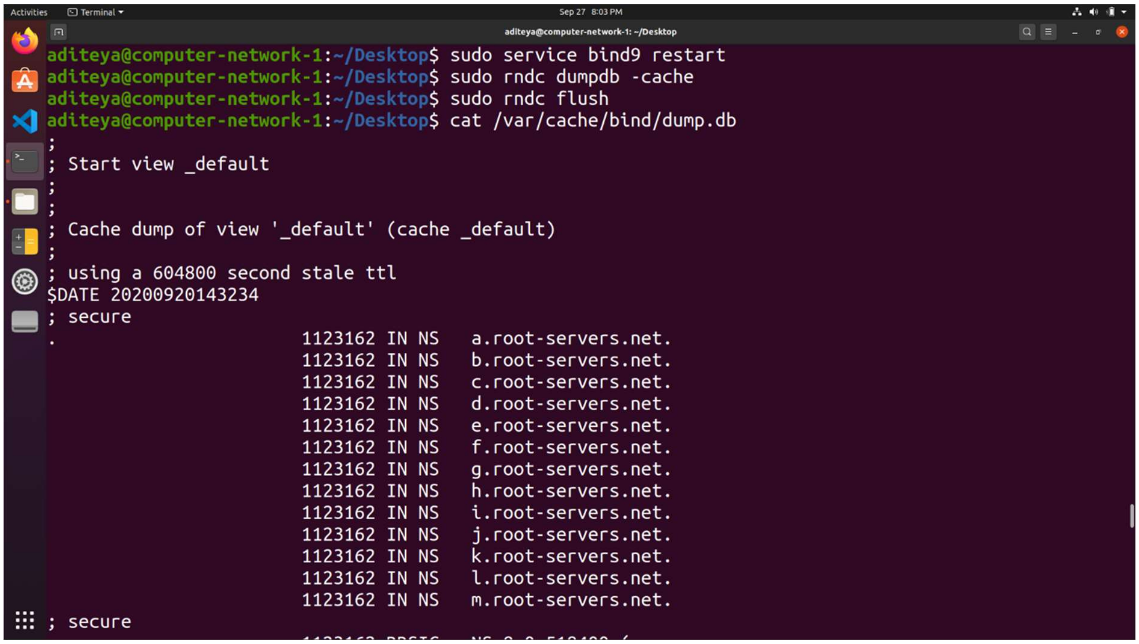
Wireshark Packet Capture

4. Task 2 – Setting Up Local DNS Server

- The **bind9** server is used as the DNS server on the server machine. It is installed using **sudo apt install bind9**.
- The configuration file for the server is **/etc/bind/named.conf.options**.
- An entry specifying the dump file for the DNS cache is added to the configuration file.
- The cache can be dumped into the file using **sudo rndc dumpdb -cache** and can be cleared or flushed out using **sudo rndc flush**.



```
  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.

        dump-file "/var/cache/bind/dump.db";

        // forwarders {
        //[redacted]0.0.0.0;
        // };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation auto;

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

                                   [ Wrote 26 lines ]
^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo       M-A Mark Text
^X Exit        ^R Read File   ^\ Replace     ^U Paste Text  ^T To Spell    ^_ Go To Line  M-E Redo       M-6 Copy Text
```

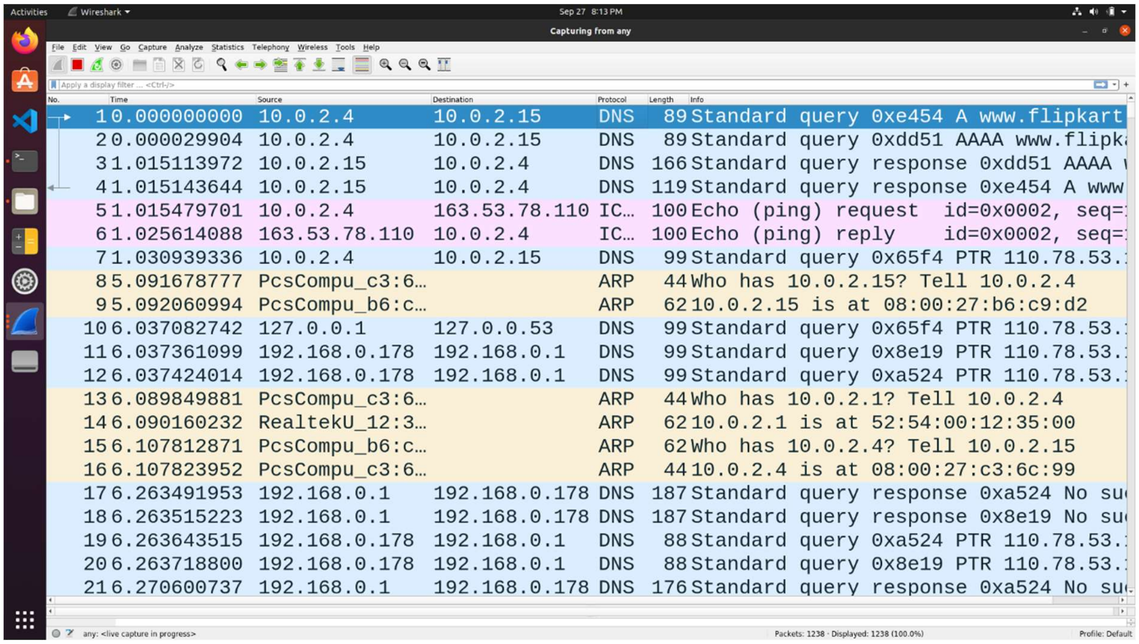


```
aditeya@computer-network-1:~/Desktop$ sudo service bind9 restart
aditeya@computer-network-1:~/Desktop$ sudo rndc dumpdb -cache
aditeya@computer-network-1:~/Desktop$ sudo rndc flush
aditeya@computer-network-1:~/Desktop$ cat /var/cache/bind/dump.db
;
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
; using a 604800 second stale ttl
$DATE 20200920143234
; secure
.                       1123162 IN NS   a.root-servers.net.
                        1123162 IN NS   b.root-servers.net.
                        1123162 IN NS   c.root-servers.net.
                        1123162 IN NS   d.root-servers.net.
                        1123162 IN NS   e.root-servers.net.
                        1123162 IN NS   f.root-servers.net.
                        1123162 IN NS   g.root-servers.net.
                        1123162 IN NS   h.root-servers.net.
                        1123162 IN NS   i.root-servers.net.
                        1123162 IN NS   j.root-servers.net.
                        1123162 IN NS   k.root-servers.net.
                        1123162 IN NS   l.root-servers.net.
                        1123162 IN NS   m.root-servers.net.
; secure
```

Viewing the cache dump file

5. Third Test

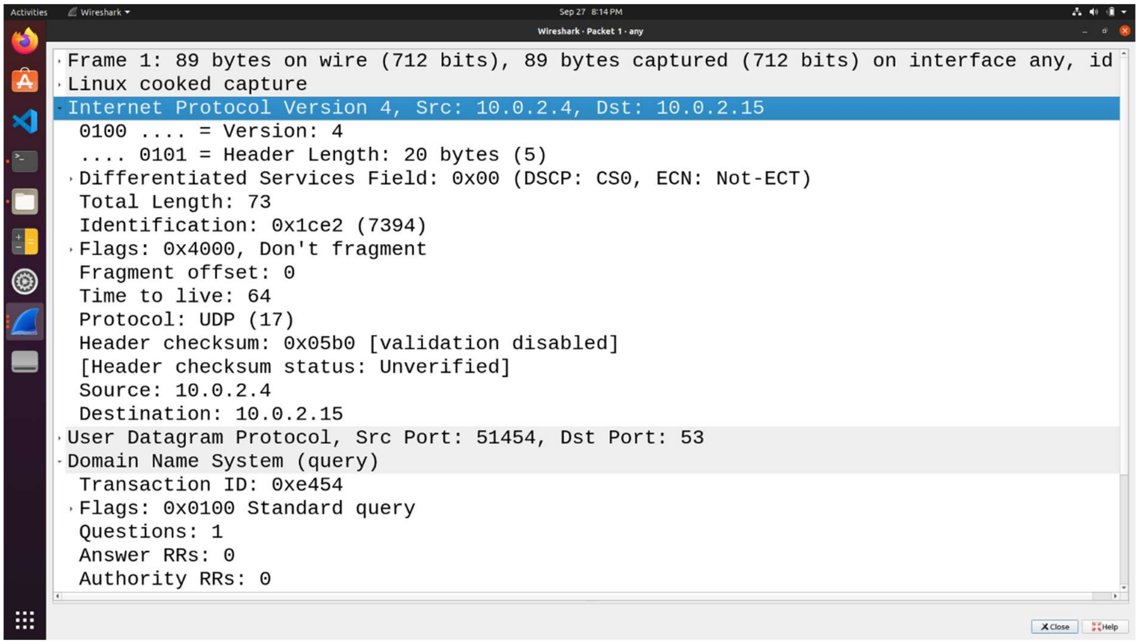
- The Flipkart website is pinged again with Wireshark running in the background.
- The IP Address of the local DNS server is clearly seen in the screenshots below.
- The cache is dumped into the `dumpfile` so it can be seen.
- The cache file also contains the canonical hostname and the **A** type records with the IP Address of the Flipkart website.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.4	10.0.2.15	DNS	89	Standard query 0xe454 A www.flipkart
2	0.000029904	10.0.2.4	10.0.2.15	DNS	89	Standard query 0xdd51 AAAA www.flipk
3	1.015113972	10.0.2.15	10.0.2.4	DNS	166	Standard query response 0xdd51 AAAA
4	1.015143644	10.0.2.15	10.0.2.4	DNS	119	Standard query response 0xe454 A www
5	1.015479701	10.0.2.4	163.53.78.110	IC…	100	Echo (ping) request id=0x0002, seq=
6	1.025614088	163.53.78.110	10.0.2.4	IC…	100	Echo (ping) reply id=0x0002, seq=
7	1.030939336	10.0.2.4	10.0.2.15	DNS	99	Standard query 0x65f4 PTR 110.78.53.
8	5.091678777	PcsCompu_c3:6…		ARP	44	Who has 10.0.2.15? Tell 10.0.2.4
9	5.092060994	PcsCompu_b6:c…		ARP	62	10.0.2.15 is at 08:00:27:b6:c9:d2
10	6.037082742	127.0.0.1	127.0.0.53	DNS	99	Standard query 0x65f4 PTR 110.78.53.
11	6.037361099	192.168.0.178	192.168.0.1	DNS	99	Standard query 0x8e19 PTR 110.78.53.
12	6.037424014	192.168.0.178	192.168.0.1	DNS	99	Standard query 0xa524 PTR 110.78.53.
13	6.089849881	PcsCompu_c3:6…		ARP	44	Who has 10.0.2.1? Tell 10.0.2.4
14	6.090160232	RealtekU_12:3…		ARP	62	10.0.2.1 is at 52:54:00:12:35:00
15	6.107812871	PcsCompu_b6:c…		ARP	62	Who has 10.0.2.4? Tell 10.0.2.15
16	6.107823952	PcsCompu_c3:6…		ARP	44	10.0.2.4 is at 08:00:27:c3:6c:99
17	6.263491953	192.168.0.1	192.168.0.178	DNS	187	Standard query response 0xa524 No su
18	6.263515223	192.168.0.1	192.168.0.178	DNS	187	Standard query response 0x8e19 No su
19	6.263643515	192.168.0.178	192.168.0.1	DNS	88	Standard query 0xa524 PTR 110.78.53.
20	6.263718800	192.168.0.178	192.168.0.1	DNS	88	Standard query 0x8e19 PTR 110.78.53.
21	6.270600737	192.168.0.1	192.168.0.178	DNS	176	Standard query response 0xa524 No su

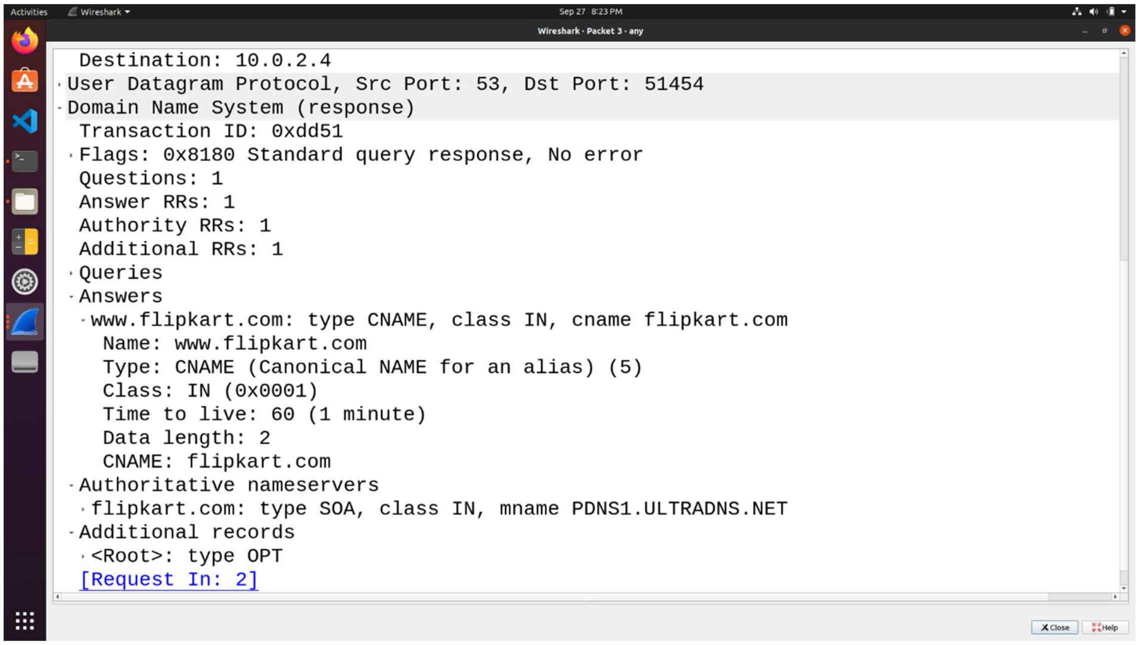
any: <live capture in progress>   Packets: 1238 · Displayed: 1238 (100.0%)   Profile: Default

Wireshark Packet Capture



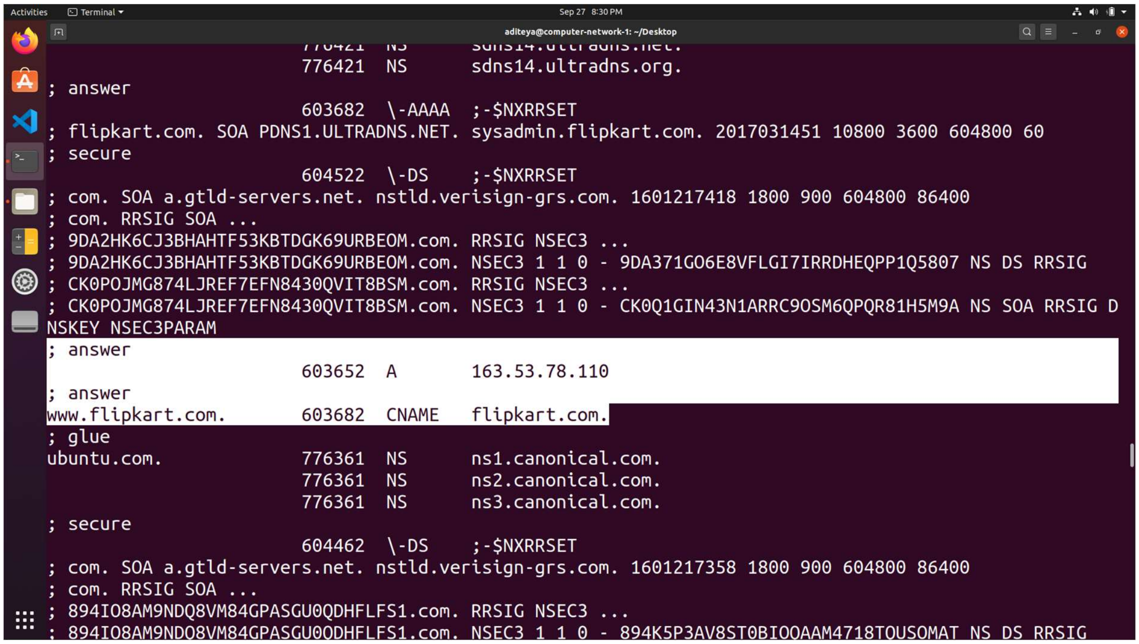
```
› Frame 1: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface any, id
› Linux cooked capture
⌄ Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 73
    Identification: 0x1ce2 (7394)
  › Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0x05b0 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.4
    Destination: 10.0.2.15
› User Datagram Protocol, Src Port: 51454, Dst Port: 53
⌄ Domain Name System (query)
    Transaction ID: 0xe454
  › Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
```

DNS Query Packet



```
    Destination: 10.0.2.4
› User Datagram Protocol, Src Port: 53, Dst Port: 51454
⌄ Domain Name System (response)
    Transaction ID: 0xdd51
  › Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 1
    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: 60 (1 minute)
        Data length: 2
        CNAME: flipkart.com
  ⌄ Authoritative nameservers
    › flipkart.com: type SOA, class IN, mname PDNS1.ULTRADNS.NET
  ⌄ Additional records
    › <Root>: type OPT
    [Request In: 2]
```

DNS Response Packet



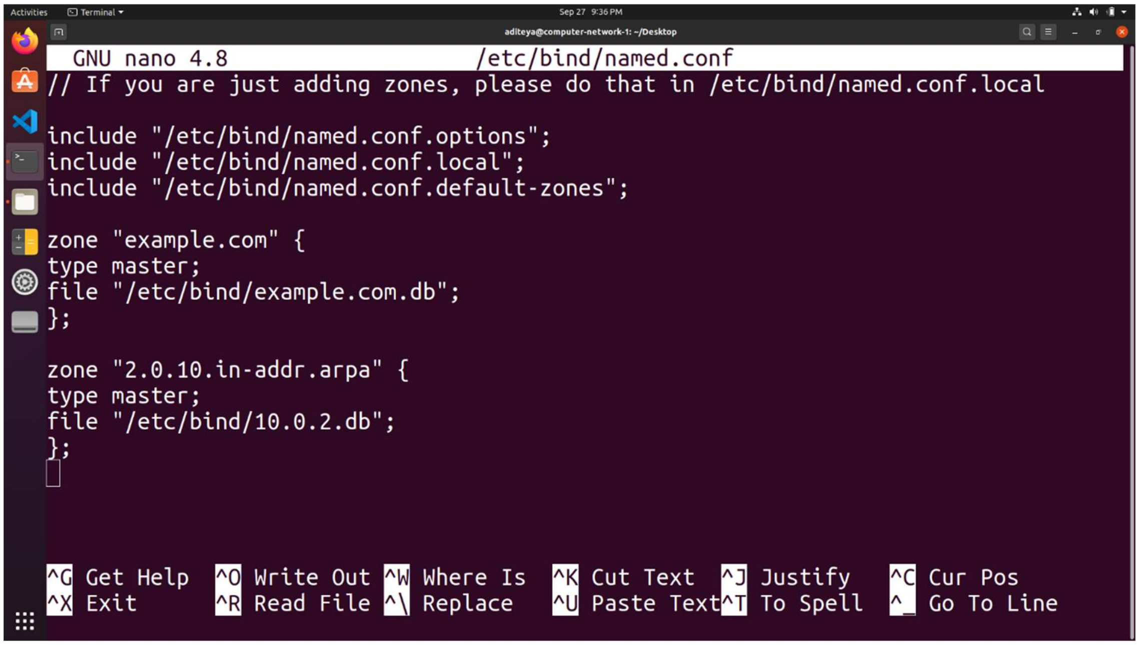
```
                        776421  NS      sdns14.ultradns.net.
                        776421  NS      sdns14.ultradns.org.
; answer
                        603682  \-AAAA  ;-$NXRRSET
; flipkart.com. SOA PDNS1.ULTRADNS.NET. sysadmin.flipkart.com. 2017031451 10800 3600 604800 60
; secure
                        604522  \-DS    ;-$NXRRSET
; com. SOA a.gtld-servers.net. nstld.verisign-grs.com. 1601217418 1800 900 604800 86400
; com. RRSIG SOA ...
; 9DA2HK6CJ3BHAHTF53KBTDGK69URBEOM.com. RRSIG NSEC3 ...
; 9DA2HK6CJ3BHAHTF53KBTDGK69URBEOM.com. NSEC3 1 1 0 - 9DA371GO6E8VFLGI7IRRDHEQPP1Q5807 NS DS RRSIG
; CK0POJMG874LJREF7EFN8430QVIT8BSM.com. RRSIG NSEC3 ...
; CK0POJMG874LJREF7EFN8430QVIT8BSM.com. NSEC3 1 1 0 - CK0Q1GIN43N1ARRC9OSM6QPQR81H5M9A NS SOA RRSIG D
NSKEY NSEC3PARAM
; answer
                        603652  A       163.53.78.110
; answer
www.flipkart.com.       603682  CNAME   flipkart.com.
; glue
ubuntu.com.             776361  NS      ns1.canonical.com.
                        776361  NS      ns2.canonical.com.
                        776361  NS      ns3.canonical.com.
; secure
                        604462  \-DS    ;-$NXRRSET
; com. SOA a.gtld-servers.net. nstld.verisign-grs.com. 1601217358 1800 900 604800 86400
; com. RRSIG SOA ...
; 894I08AM9NDQ8VM84GPASGU0QDHFLFS1.com. RRSIG NSEC3 ...
; 894I08AM9NDQ8VM84GPASGU0QDHFLFS1.com. NSEC3 1 1 0 - 894K5P3AV8ST0BIOQAM4718TQUSOMAT NS DS RRSIG
```

Cache Dumpfile

6. Task 3 – Hosting a Zone in the Local DNS Server

6.1 Zone Creation

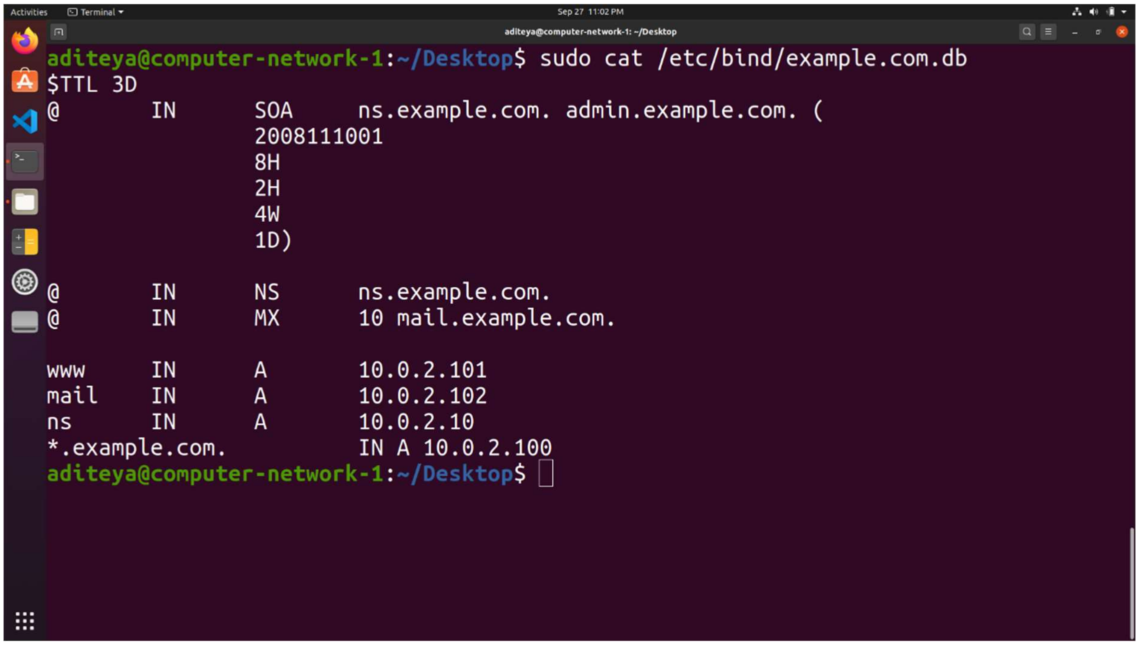
- The two zones corresponding to the domain **`www.example.com`** must be added to the **`/etc/bind/named.conf`** file in the server.
- The first zone corresponds to the forward lookup (translation from hostname to IP Address) and the second zone is for the reverse lookup (translation from IP Address to hostname).



```
  GNU nano 4.8                    /etc/bind/named.conf
// 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";
};




^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Paste Text^T To Spell  ^_ Go To Line
```

6.2 Forward and Reverse Lookup

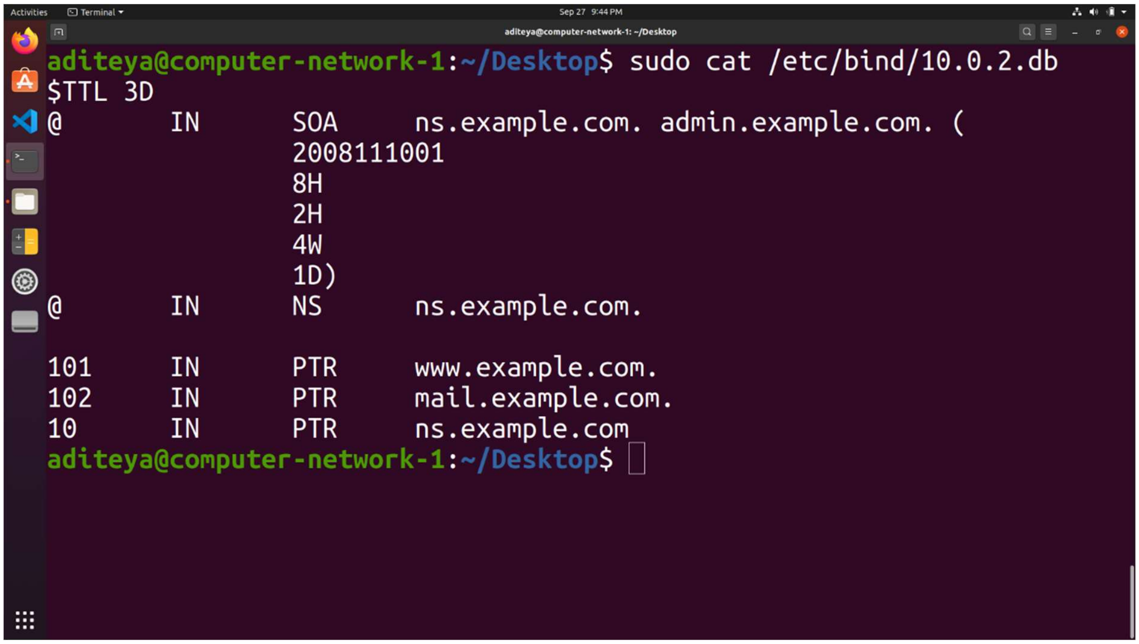
- The forward lookup file is located at **`/etc/bind/example.com.db`**
- The symbol `@` is used to indicate the origin specified, in this case **`www.example.com`**
- There are 7 records in the lookup file, an SOA record, a nameserver, a mailserver and 4 authoritative records.
- The `TTL` field tells the server how long this record should stay in the cache before being removed. In this case the local DNS server requests for a fresh entry from the name server.



```
aditeya@computer-network-1:~/Desktop$ 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
aditeya@computer-network-1:~/Desktop$ 
```

Forward Lookup file

- The reverse lookup file is stored at **`/etc/bind/10.0.2.db`** and is used to translate IP Addresses to hostnames for the given domain, in this case example.com.
- For each IP Address defined in the forward lookup file, a corresponding hostname is referenced here.
- The record type here is PTR or DNS Pointer Record.

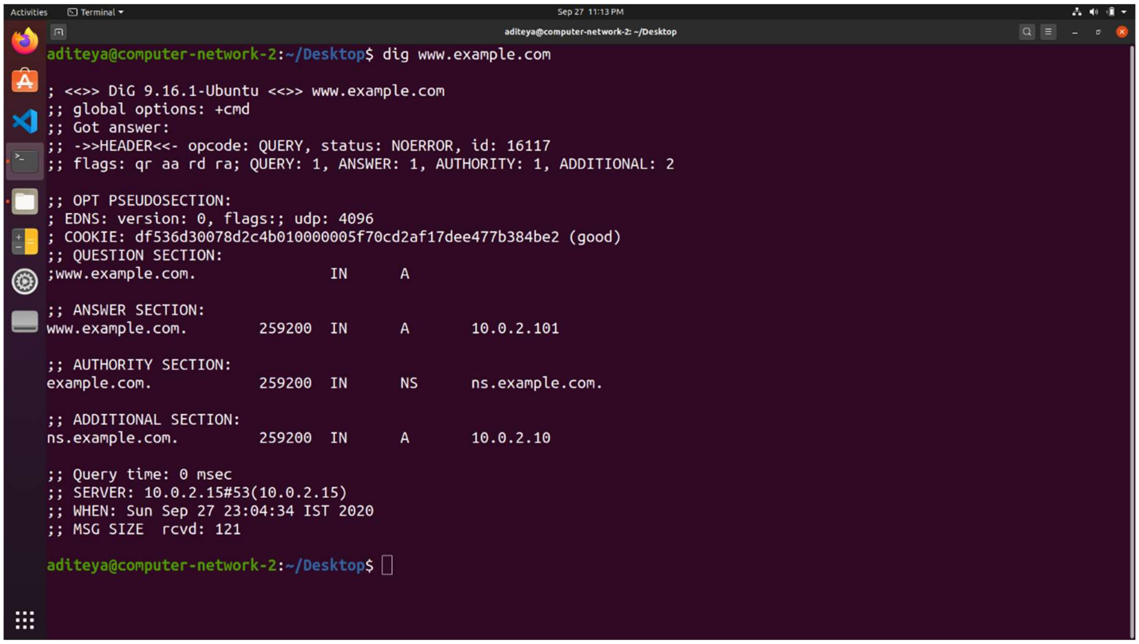


```
aditeya@computer-network-1:~/Desktop$ sudo cat /etc/bind/10.0.2.db
$TTL 3D
@       IN      SOA     ns.example.com. admin.example.com. (
                2008111001
                8H
                2H
                4W
                1D)
@       IN      NS      ns.example.com.

101     IN      PTR     www.example.com.
102     IN      PTR     mail.example.com.
10      IN      PTR     ns.example.com
aditeya@computer-network-1:~/Desktop$ 
```

Reverse Lookup file

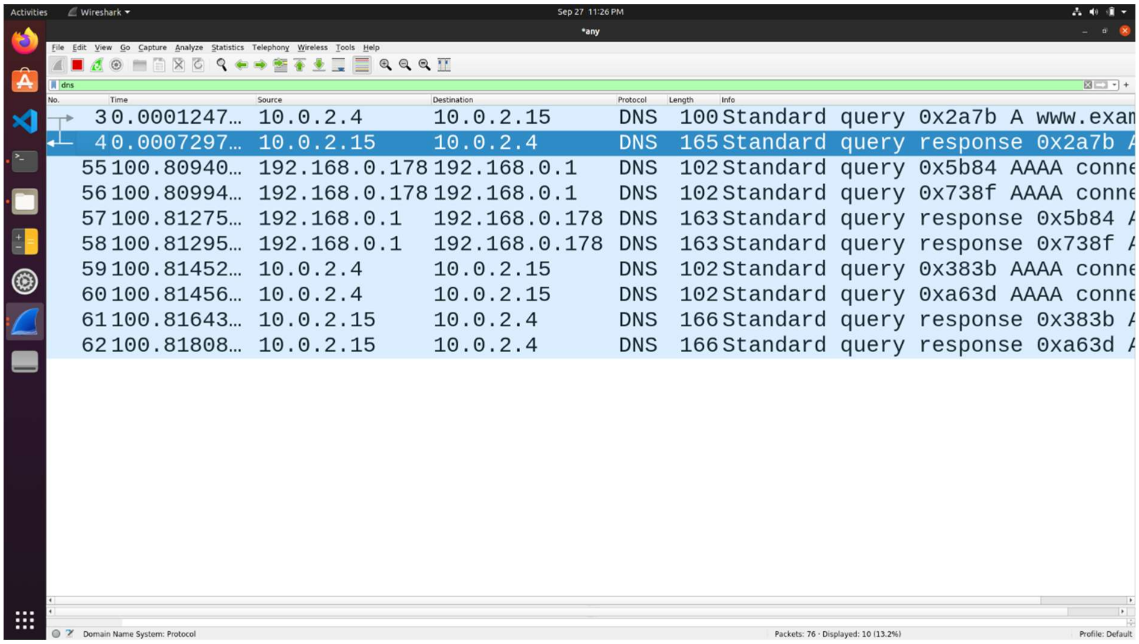
7. Fourth Test – Testing `www.example.com`

- The dig command is used to lookup name servers specified in the file **`/etc/resolv.conf`**
- Wireshark is used to capture the packets while running the command dig **`www.example.com`**
- The IP Address of the DNS Server and the returned IP Address of the domain set by us can be seen in the query and response packets.



```
aditeya@computer-network-2:~/Desktop$ dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16117
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: df536d30078d2c4b010000005f70cd2af17dee477b384be2 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       10.0.2.101

;; AUTHORITY SECTION:
example.com.            259200  IN      NS      ns.example.com.

;; ADDITIONAL SECTION:
ns.example.com.         259200  IN      A       10.0.2.10

;; Query time: 0 msec
;; SERVER: 10.0.2.15#53(10.0.2.15)
;; WHEN: Sun Sep 27 23:04:34 IST 2020
;; MSG SIZE  rcvd: 121

aditeya@computer-network-2:~/Desktop$ 
```

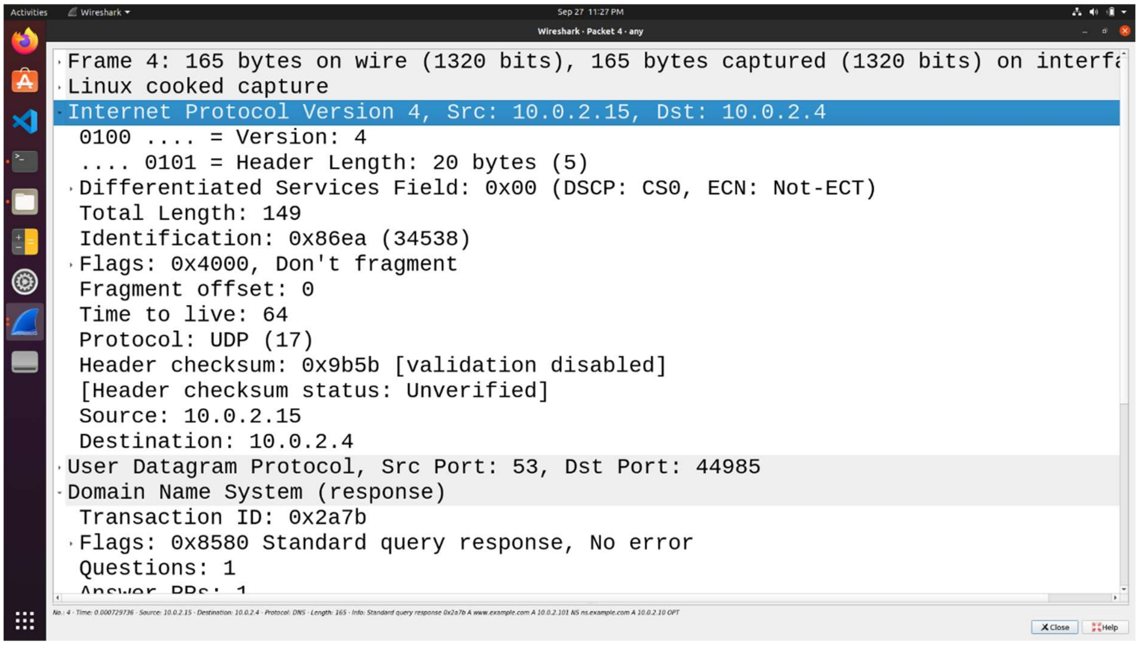
`dig www.example.com`


Activities
Wireshark
Sep 27 11:26 PM
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Profile: Default

```
No.  Time           Source         Destination    Protocol Length Info
  3 0.0001247…    10.0.2.4       10.0.2.15       DNS      100 Standard query 0x2a7b A www.exam
  4 0.0007297…    10.0.2.15      10.0.2.4        DNS      165 Standard query response 0x2a7b A
 55 100.80940…    192.168.0.178  192.168.0.1     DNS      102 Standard query 0x5b84 AAAA conne
 56 100.80994…    192.168.0.178  192.168.0.1     DNS      102 Standard query 0x738f AAAA conne
 57 100.81275…    192.168.0.1    192.168.0.178   DNS      163 Standard query response 0x5b84 A
 58 100.81295…    192.168.0.1    192.168.0.178   DNS      163 Standard query response 0x738f A
 59 100.81452…    10.0.2.4       10.0.2.15       DNS      102 Standard query 0x383b AAAA conne
 60 100.81456…    10.0.2.4       10.0.2.15       DNS      102 Standard query 0xa63d AAAA conne
 61 100.81643…    10.0.2.15      10.0.2.4        DNS      166 Standard query response 0x383b A
 62 100.81808…    10.0.2.15      10.0.2.4        DNS      166 Standard query response 0xa63d A
```

```
Domain Name System: Protocol                    Packets: 76 · Displayed: 10 (13.2%)
```

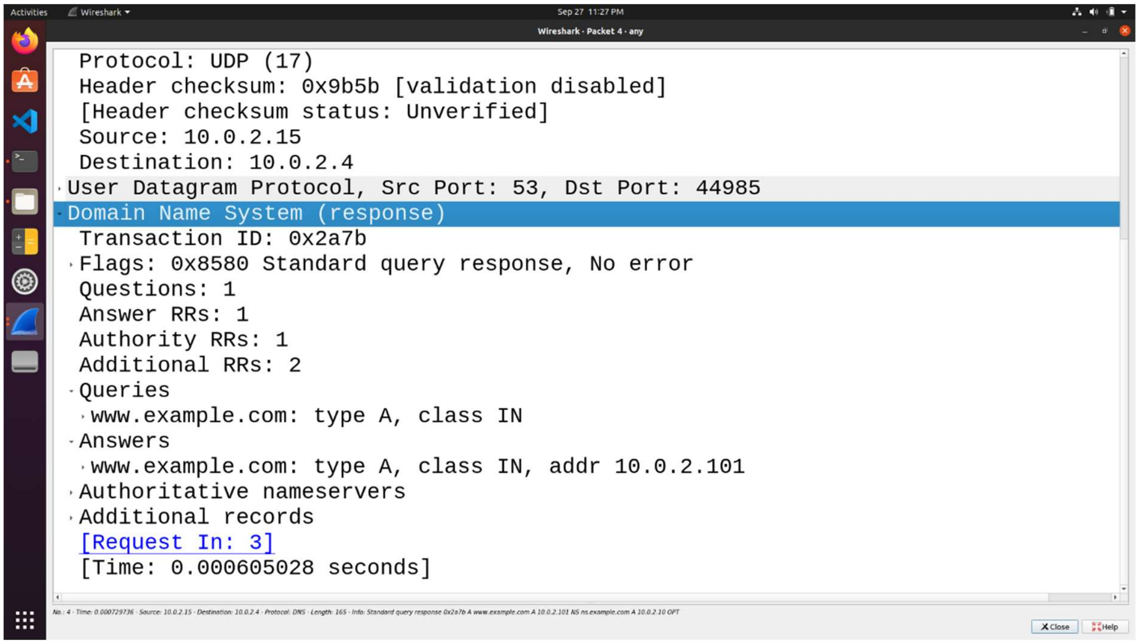
Wireshark Packet Capture



```
Frame 4: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interfa
Linux cooked capture
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.4
 0100 .... = Version: 4
 .... 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 149
 Identification: 0x86ea (34538)
 Flags: 0x4000, Don't fragment
 Fragment offset: 0
 Time to live: 64
 Protocol: UDP (17)
 Header checksum: 0x9b5b [validation disabled]
 [Header checksum status: Unverified]
 Source: 10.0.2.15
 Destination: 10.0.2.4
User Datagram Protocol, Src Port: 53, Dst Port: 44985
Domain Name System (response)
 Transaction ID: 0x2a7b
 Flags: 0x8580 Standard query response, No error
 Questions: 1
 Answer RRs: 1
```

```
No.: 4 · Time: 0.000729736 · Source: 10.0.2.15 · Destination: 10.0.2.4 · Protocol: DNS · Length: 165 · Info: Standard query response 0x2a7b A www.example.com A 10.0.2.101 NS ns.example.com A 10.0.2.10 OPT
```

DNS Response Packet



```
  Protocol: UDP (17)
  Header checksum: 0x9b5b [validation disabled]
  [Header checksum status: Unverified]
  Source: 10.0.2.15
  Destination: 10.0.2.4
User Datagram Protocol, Src Port: 53, Dst Port: 44985
Domain Name System (response)
  Transaction ID: 0x2a7b
  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 10.0.2.101
  Authoritative nameservers
  Additional records
  [Request In: 3]
  [Time: 0.000605028 seconds]

No.: 4 · Time: 0.000729736 · Source: 10.0.2.15 · Destination: 10.0.2.4 · Protocol: DNS · Length: 165 · Info: Standard query response 0x2a7b A www.example.com A 10.0.2.101 NS ns.example.com A 10.0.2.10 OPT
```

DNS Response Packet

8. Questions

Q1. *Locate the DNS query and response messages. Are then sent over UDP or TCP?*
Answer - The DNS Query and Response messages are visible in the screenshots. They are sent over UDP.

Q2. *What is the destination port for the DNS query message? What is the source port of DNS response message?*
Answer – The destination and source ports of the DNS query and response messages are the same. The port number for DNS protocol is **53**.

Q3. *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?*

Answer – The DNS query is made to server at the IP Address 10.0.2.15. This is the same as the local DNS server configured.

Q4. *Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?*

Answer – The DNS Query is of type **A** since it requests for an authoritative record. The answer section is empty since it does not have any answer.

Q5. *Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?*
Answer – 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.

Q6. *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?*
Answer – The destination IP Address of the SYN packet corresponds to the IP Address of hostname (`www.flipkart.com`) retrieved from the response message.