

# CN Lab Report – Week 4

PES1UG19CS582

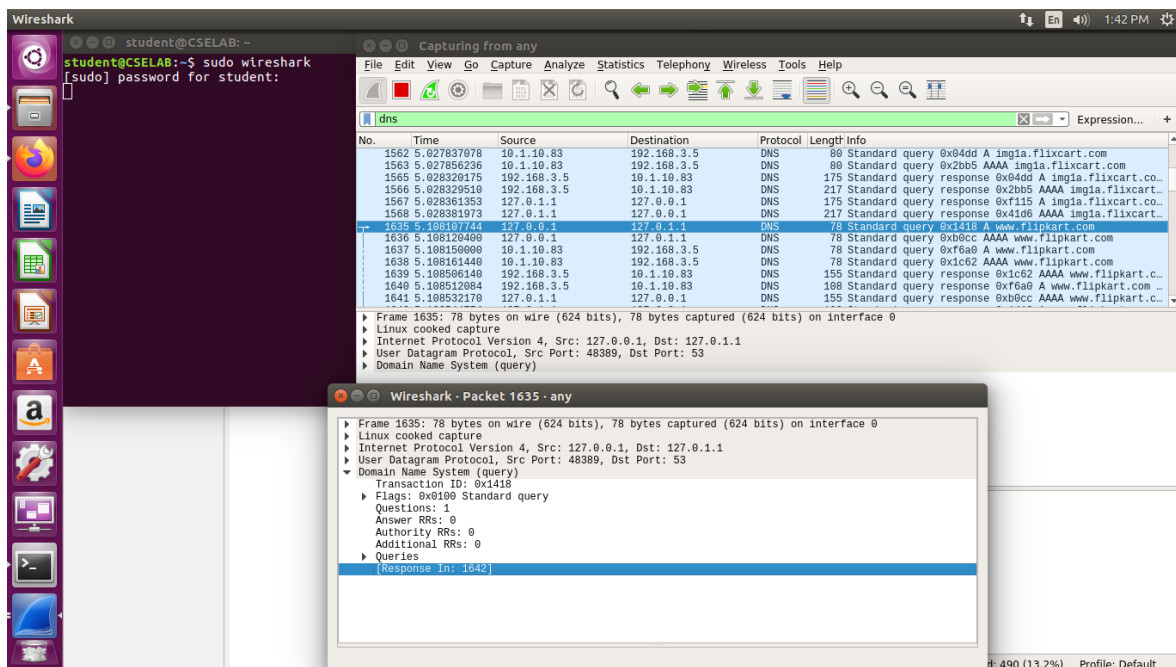
Vridhi Goyal

PES1UG19CS592

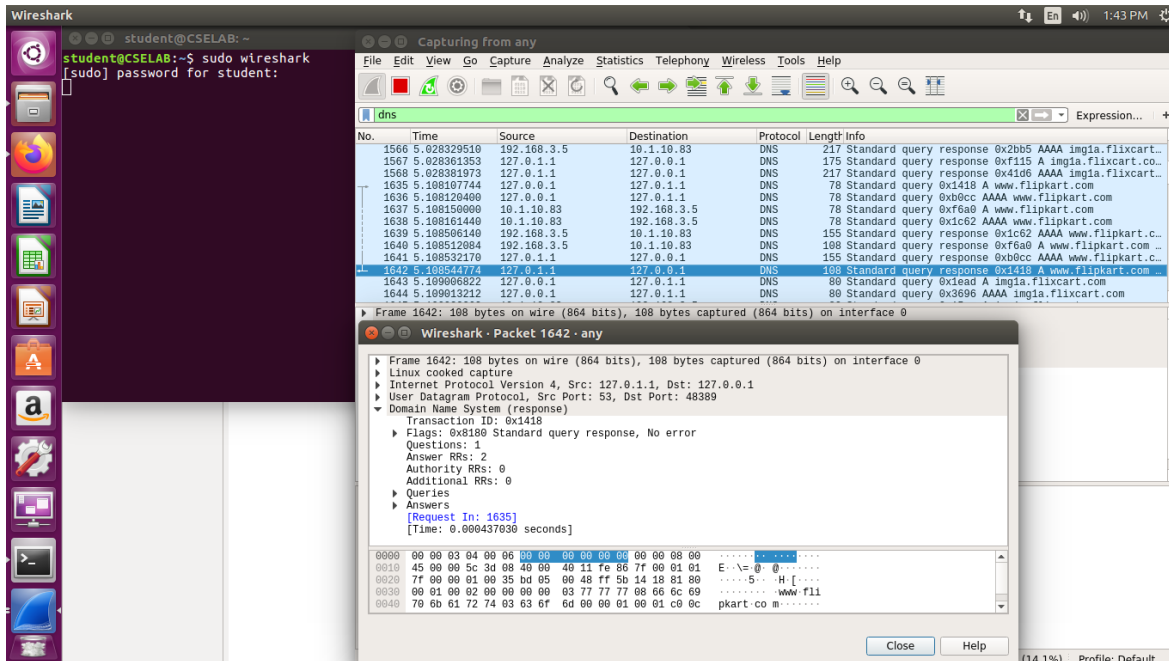
Yashi Chawla

## 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 **127.0.1.1**.
- 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 – **192.168.3.5**.
- The first query and authoritative response are shown below.



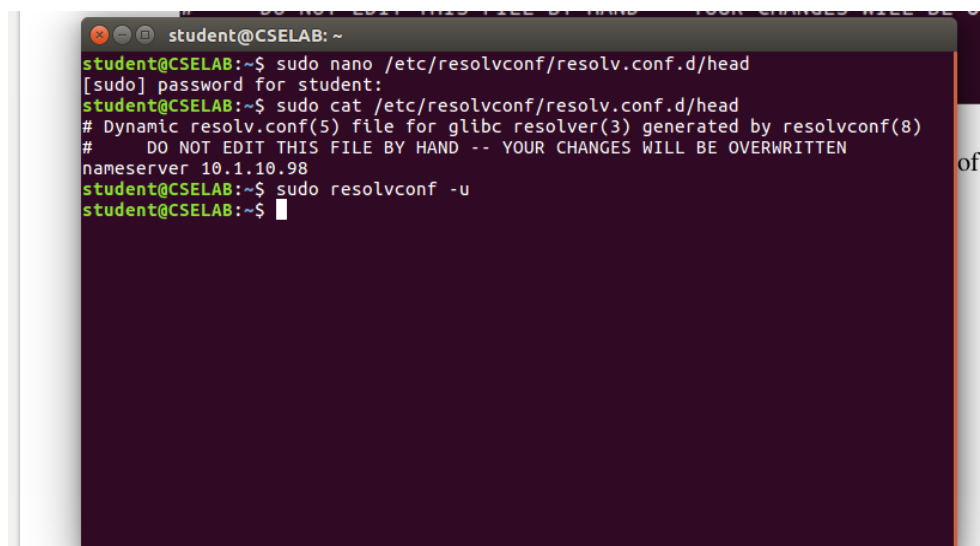
DNS Query



DNS Response

## 2. Task 1 – Configuring Client Machine

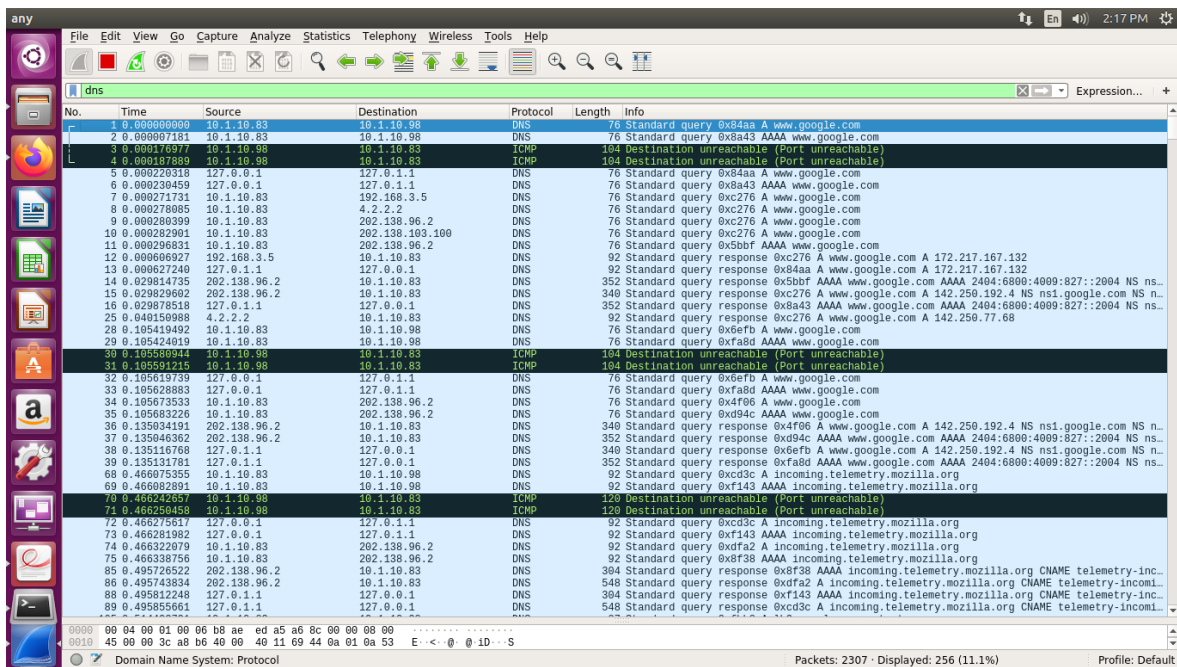
- The IP Address of the client machine is **10.0.10.98** and the IP Address of the server machine is **10.0.10.83**
- We need to add the IP Address of the custom DNS server (**10.0.10.83**) to the client machine.
- This is done by adding the IP address of the server to the file **/etc/resolvconf/resolv.conf.d/head** 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**



## 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 **10.0.10.83** but it does not receive any hence it resorts to using the default DNS server at **127.0.0.1**.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.1.10.83	10.1.10.98	DNS	76	Standard query 0x84aa A www.google.com
2	0.000000711	10.1.10.83	10.1.10.98	DNS	76	Standard query 0x84aa A www.google.com
3	0.000176977	10.1.10.83	10.1.10.83	ICMP	104	Destination unreachable (Port unreachable)
4	0.000187889	10.1.10.83	10.1.10.83	ICMP	104	Destination unreachable (Port unreachable)
5	0.000220318	127.0.0.1	127.0.0.1	DNS	76	Standard query 0x84aa A www.google.com
6	0.000230459	127.0.0.1	127.0.0.1	DNS	76	Standard query 0x84aa AAAA www.google.com
7	0.000271731	10.1.10.83	192.168.3.5	DNS	76	Standard query 0xc276 A www.google.com
8	0.000278085	10.1.10.83	4.2.2.2	DNS	76	Standard query 0xc276 A www.google.com
9	0.000280399	10.1.10.83	202.138.96.2	DNS	76	Standard query 0xc276 A www.google.com
10	0.000282901	10.1.10.83	202.138.103.100	DNS	76	Standard query 0xc276 A www.google.com
11	0.000286831	10.1.10.83	202.138.96.2	DNS	76	Standard query 0xc276 A www.google.com
12	0.000606927	192.168.3.5	10.1.10.83	DNS	92	Standard query response 0xc276 A www.google.com A 172.217.167.132
13	0.000627240	127.0.0.1	127.0.0.1	DNS	92	Standard query response 0x84aa A www.google.com A 172.217.167.132
14	0.029814735	202.138.96.2	10.1.10.83	DNS	352	Standard query response 0x50bf AAAA www.google.com AAAA 2404:6800:4009:827::2004 NS ns...
15	0.029826692	202.138.96.2	10.1.10.83	DNS	340	Standard query response 0xc276 A www.google.com A 142.250.192.4 NS nsl.google.com NS n...
16	0.029878518	127.0.0.1	127.0.0.1	DNS	352	Standard query response 0x84aa AAAA www.google.com AAAA 2404:6800:4009:827::2004 NS ns...
25	0.040150988	4.2.2.2	10.1.10.83	DNS	92	Standard query response 0xc276 A www.google.com A 142.250.77.68
28	0.105419492	10.1.10.83	10.1.10.98	DNS	76	Standard query 0x6fb A www.google.com
29	0.105424019	10.1.10.83	10.1.10.98	DNS	76	Standard query 0x6fb AAAA www.google.com
30	0.105509944	10.1.10.83	10.1.10.83	ICMP	104	Destination unreachable (Port unreachable)
31	0.105591215	10.1.10.83	10.1.10.83	ICMP	104	Destination unreachable (Port unreachable)
32	0.105619739	127.0.0.1	127.0.0.1	DNS	76	Standard query 0x6fb A www.google.com
33	0.105628883	127.0.0.1	127.0.0.1	DNS	76	Standard query 0x6fb AAAA www.google.com
34	0.105673533	10.1.10.83	202.138.96.2	DNS	76	Standard query 0x4f06 A www.google.com
35	0.105683226	10.1.10.83	202.138.96.2	DNS	76	Standard query 0xd94c AAAA www.google.com
36	0.135034191	202.138.96.2	10.1.10.83	DNS	340	Standard query response 0x4f06 A www.google.com A 142.250.192.4 NS nsl.google.com NS n...
37	0.135046392	202.138.96.2	10.1.10.83	DNS	352	Standard query response 0xd94c AAAA www.google.com AAAA 2404:6800:4009:827::2004 NS ns...
38	0.135116768	127.0.0.1	127.0.0.1	DNS	340	Standard query response 0x6fb A www.google.com A 142.250.192.4 NS nsl.google.com NS n...
39	0.135131761	127.0.0.1	127.0.0.1	DNS	352	Standard query response 0x6fb AAAA www.google.com AAAA 2404:6800:4009:827::2004 NS ns...
68	0.460875355	10.1.10.83	10.1.10.98	DNS	92	Standard query 0xcd3c A incoming.telemetry.mozilla.org
69	0.460892891	10.1.10.83	10.1.10.98	DNS	92	Standard query 0xf143 AAAA incoming.telemetry.mozilla.org
70	0.466242657	10.1.10.83	10.1.10.83	ICMP	120	Destination unreachable (Port unreachable)
71	0.466250458	10.1.10.83	10.1.10.83	ICMP	120	Destination unreachable (Port unreachable)
72	0.466275617	127.0.0.1	127.0.0.1	DNS	92	Standard query 0xcd3c A incoming.telemetry.mozilla.org
73	0.466281982	127.0.0.1	127.0.0.1	DNS	92	Standard query 0xf143 AAAA incoming.telemetry.mozilla.org
74	0.466322079	10.1.10.83	202.138.96.2	DNS	92	Standard query 0xdfa2 A incoming.telemetry.mozilla.org
75	0.466338756	10.1.10.83	202.138.96.2	DNS	92	Standard query 0x8f38 AAAA incoming.telemetry.mozilla.org
85	0.495726522	202.138.96.2	10.1.10.83	DNS	384	Standard query response 0x8f38 AAAA incoming.telemetry.mozilla.org CNAME telemetry-inc...
86	0.495743804	202.138.96.2	10.1.10.83	DNS	548	Standard query response 0xdfa2 A incoming.telemetry.mozilla.org CNAME telemetry-inc...
88	0.495812248	127.0.0.1	127.0.0.1	DNS	384	Standard query response 0xf143 AAAA incoming.telemetry.mozilla.org CNAME telemetry-inc...
89	0.495855661	127.0.0.1	127.0.0.1	DNS	548	Standard query response 0xcd3c A incoming.telemetry.mozilla.org CNAME telemetry-inc...

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**.

```
student@CSELAB:~
GNU nano 2.5.3 File: /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 {
        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;

    auth-nxdomain no; # conform to RFC1035
    listen-on-v6 { any; };
};

; Read 26 lines

Terminal File Edit View Search Terminal Help

student@CSELAB:~$ sudo service bind9 restart
student@CSELAB:~$ sudo rndc dumpdb -cache
student@CSELAB:~$ sudo rndc flush
student@CSELAB:~$ cat /var/cache/bind/dump.db

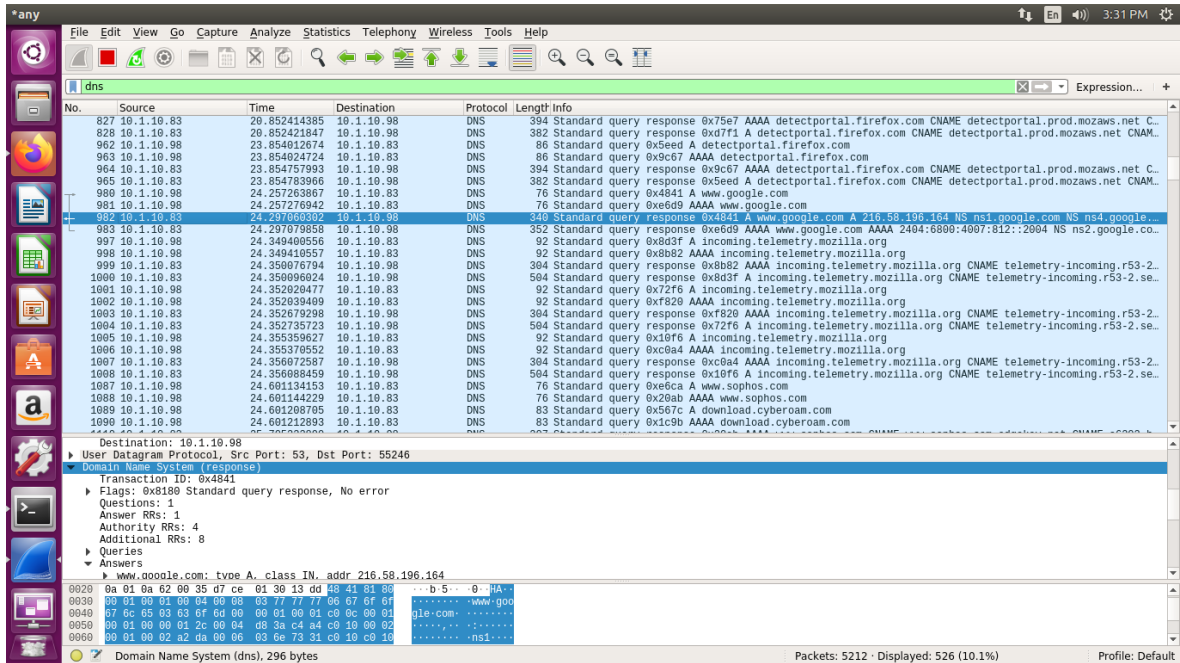
; Start view _default

; Cache dump of view '_default' (cache _default)

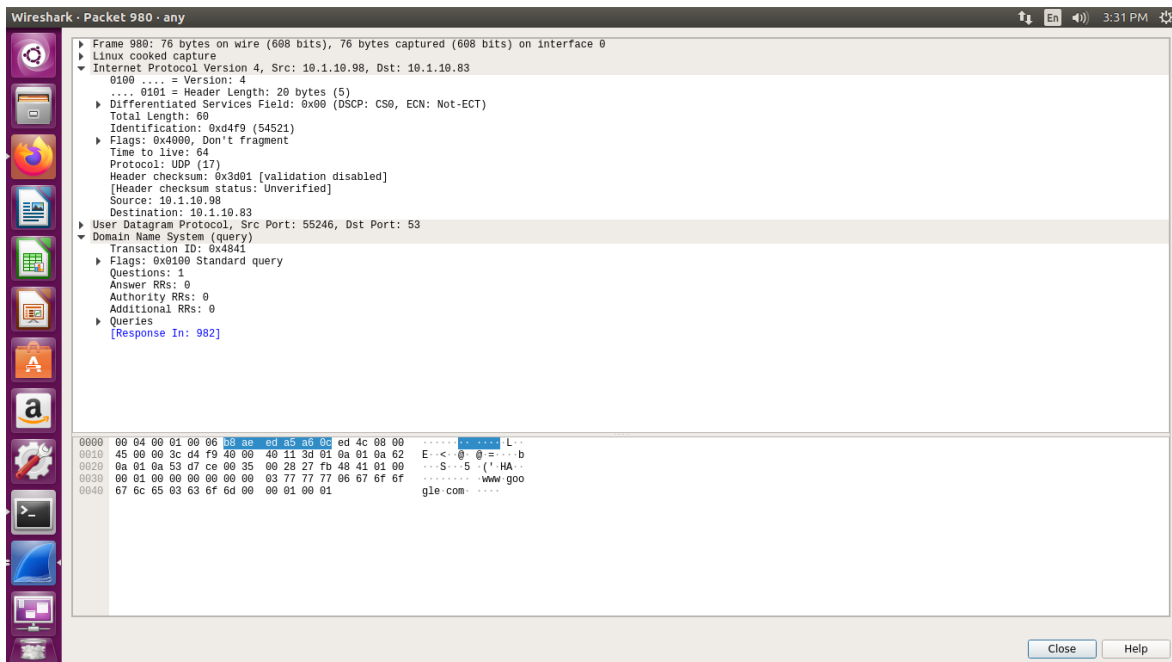
; SOA 20210219085408
; secure
518377 IN NS a.root-servers.net.
518377 IN NS b.root-servers.net.
518377 IN NS c.root-servers.net.
518377 IN NS d.root-servers.net.
518377 IN NS e.root-servers.net.
518377 IN NS f.root-servers.net.
518377 IN NS g.root-servers.net.
518377 IN NS h.root-servers.net.
518377 IN NS i.root-servers.net.
518377 IN NS j.root-servers.net.
518377 IN NS k.root-servers.net.
518377 IN NS l.root-servers.net.
518377 IN NS m.root-servers.net.
; secure
518377 RRSIG NS 8 0 518400 (
20210304050000 20210219040000 42351 .
X0e4ITrSZueR1BY0DTDXjoIfJQ0gHpp8X5jp
yLYINhxxvQRuGI8FMQFO/TldNBm+XCxG2W3+
HKu9zpgdNK0BRT5RqN4DV4sbxauwplizqw3v
aht/vvsgTKxEIcGVfumeQpN1HhxxR1ddRfPt
lKVUTjTcCxZ5SN1xh2GxV5PURITEjIphLzvf
RZnHMTGcw7INF8VQmN34R+apQCjja1018nun
gigFkdV9H/vSHVIM2xKFDcMVsbB8Z3moPuQ
z4nmvzVxqZ3zbg0jPkL9EuESK8orD5HBLbbK
FuoXfbwBnPgIPbcGDkTL3PkR1tF+tByN25rt
jx88rJvBoGn864fdow== )
; secure
172777 DNSKEY 256 3 8 (
AwEAAABGKkqC1VAvQr48LPf9Nd39f337Mltg
gxFOAB9KLKRNSuq9jo0EPC/R6PD/4LTzUms8
```

## 5. Third Test

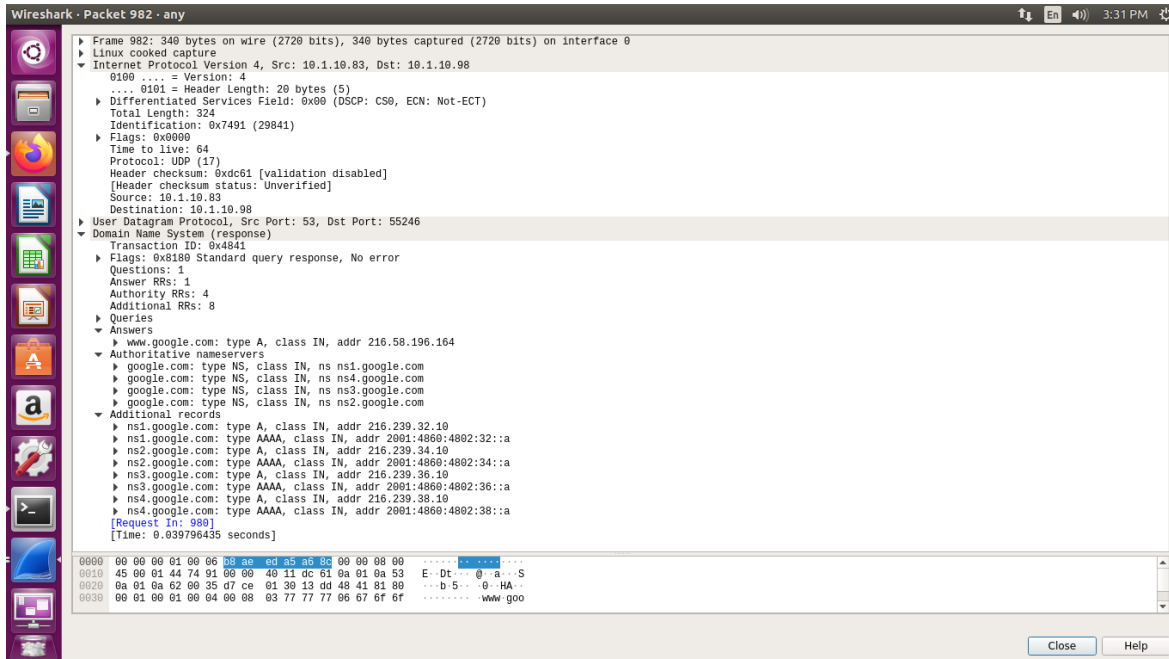
- The Flipkart website is pinged again with Wireshark running in the background.
- The IP Address of the local DNS server is clearly seen in the screenshots below.
- The cache is dumped into the dumpfile so it can be seen.
- The cache file also contains the canonical hostname and the A type records with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



Wireshark packet capture



Request

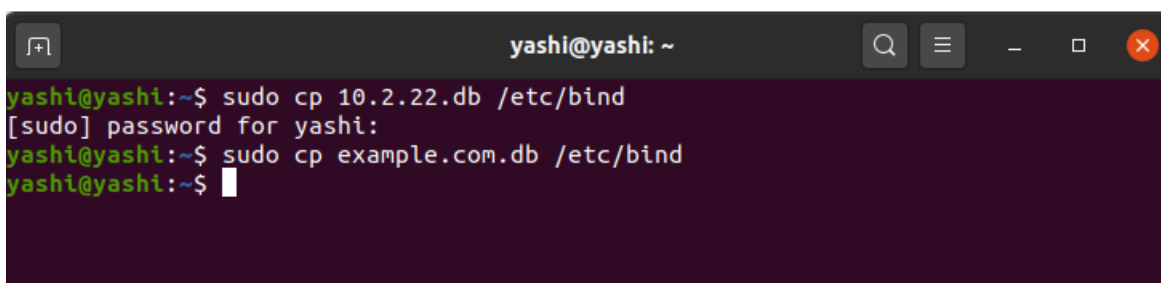


Response

## 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).

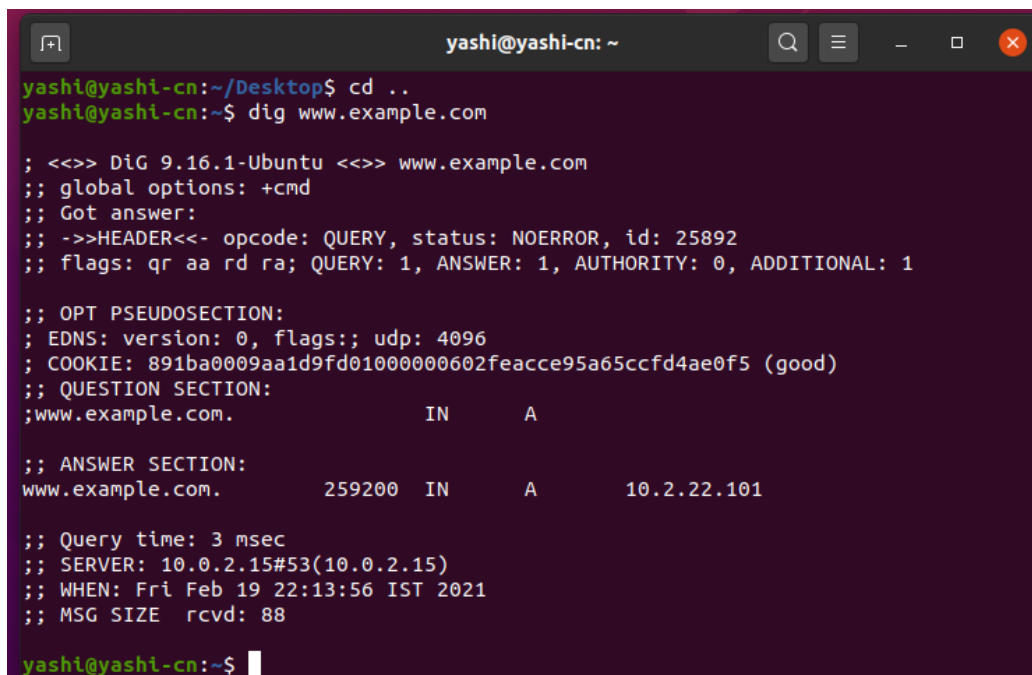


## 6.2 Forward and Reverse Lookup

- 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.
- 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.

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

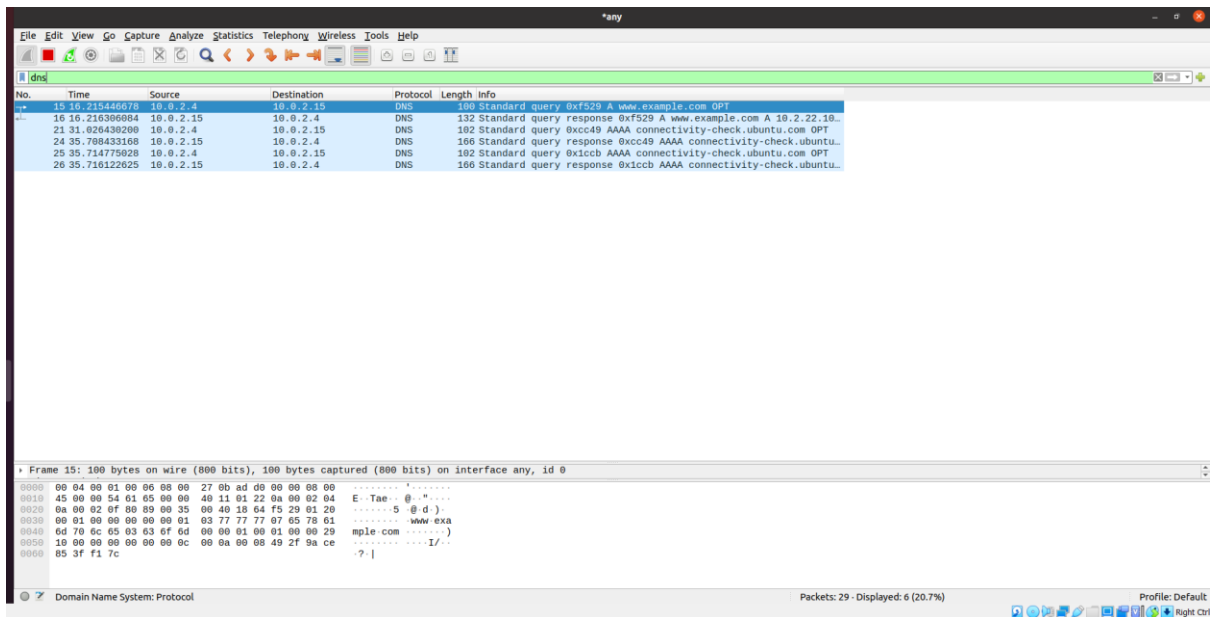
- The dig command is used to lookup name servers specified in the file **/etc/resolv.conf**
- Wireshark is used to capture the packets while running the command **dig www.example.com**
- The IP Address of the DNS Server and the returned IP Address of the domain set by us can be seen in the query and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



```
yashi@yashi-cn: ~  
yashi@yashi-cn:~/Desktop$ cd ..  
yashi@yashi-cn:~$ dig www.example.com  
  
; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25892  
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 4096  
; COOKIE: 891ba0009aa1d9fd01000000602feacce95a65ccfd4ae0f5 (good)  
;; QUESTION SECTION:  
;www.example.com.                IN      A  
  
;; ANSWER SECTION:  
www.example.com.                259200  IN      A      10.2.22.101  
  
;; Query time: 3 msec  
;; SERVER: 10.0.2.15#53(10.0.2.15)  
;; WHEN: Fri Feb 19 22:13:56 IST 2021  
;; MSG SIZE rcvd: 88  
  
yashi@yashi-cn:~$
```



dig www.example.com

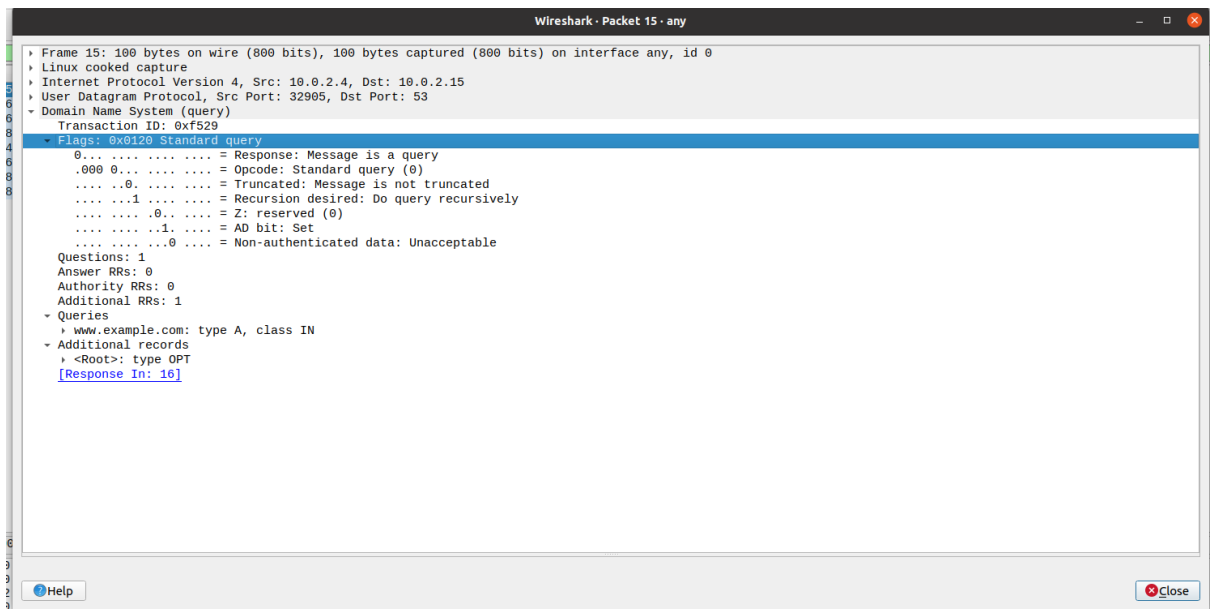


No.	Time	Source	Destination	Protocol	Length	Info
15	15.16.215446678	10.0.2.4	10.0.2.15	DNS	100	Standard query 0xf529 A www.example.com OPT
16	16.216390884	10.0.2.15	10.0.2.4	DNS	132	Standard query response 0xf529 A www.example.com A 10.2.22.10...
21	31.026439269	10.0.2.4	10.0.2.15	DNS	102	Standard query 0xc049 AAAA connectivity-check.ubuntu.com OPT
24	35.789433168	10.0.2.15	10.0.2.4	DNS	166	Standard query response 0xc049 AAAA connectivity-check.ubuntu...
25	35.714775828	10.0.2.4	10.0.2.15	DNS	102	Standard query 0x1c0b AAAA connectivity-check.ubuntu.com OPT
26	35.716122625	10.0.2.15	10.0.2.4	DNS	166	Standard query response 0x1c0b AAAA connectivity-check.ubuntu...

Frame 15: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0

```
0000  00 04 00 01 00 06 08 00 27 0b ad 09 00 00 00 00  .....
0010  45 00 00 54 01 05 00 00 40 11 01 22 0a 00 02 04  E-Tae- 0 ".....
0020  0a 00 02 0f 00 09 00 35 09 40 18 64 f5 29 01 20  ..... 5 0 d )
0030  00 01 00 00 00 00 00 01 03 77 77 77 07 65 78 61  ..... www exa
0040  0d 70 6c 65 03 03 0f 6d 00 00 01 00 01 00 00 29  mple.com .....
0050  10 00 00 00 00 00 00 0c 00 0a 00 00 49 2f 0a ce  ..... I/..
0060  85 3f f1 7c                                     :?..|
```

## Wireshark Packet Capture



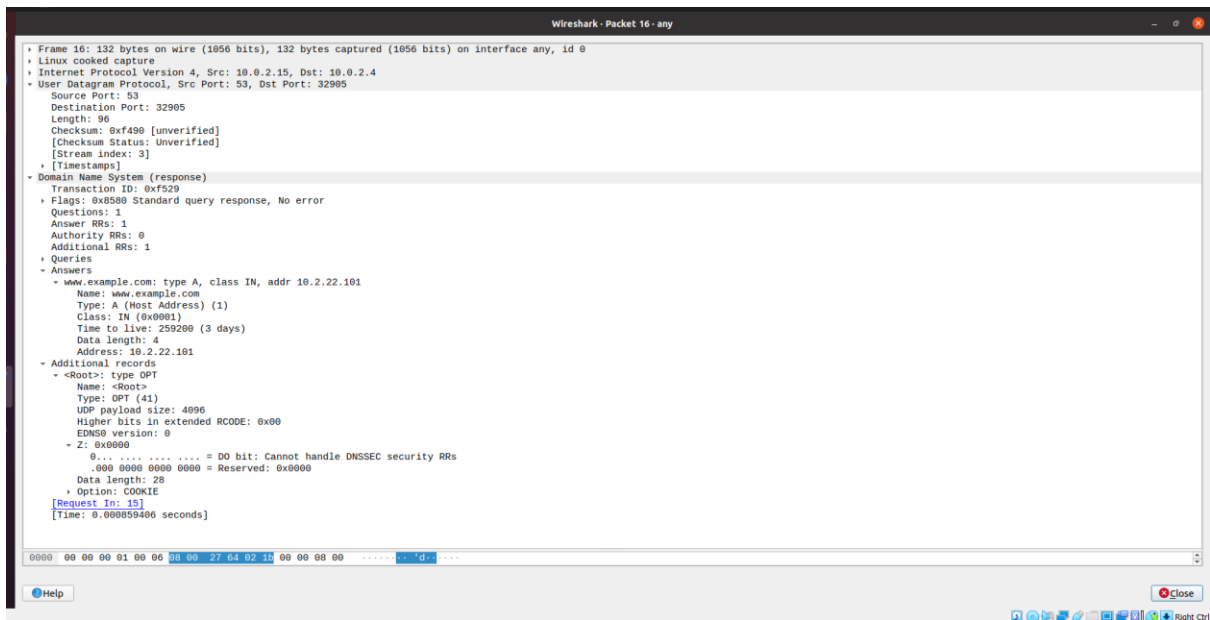
Wireshark - Packet 15 - any

Frame 15: 100 bytes on wire (800 bits), 100 bytes captured (800 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: 32905, Dst Port: 53
- Domain Name System (query)
  - Transaction ID: 0xf529
  - 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.example.com: type A, class IN
  - Additional records
    - <Root>: type OPT
  - [Response In: 16]

## Request





Response

## 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.

