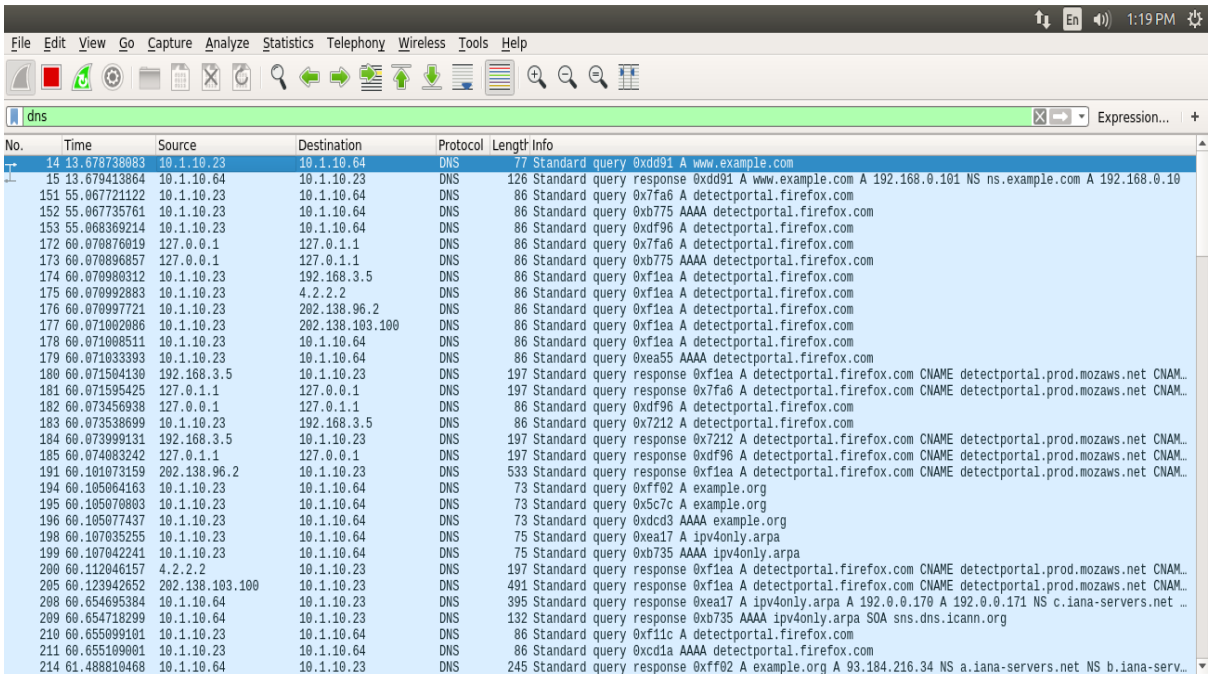
CN LAB REPORT – WEEK 4

NAME: DIVYANSHU SHARMA

PES1UG20CS806

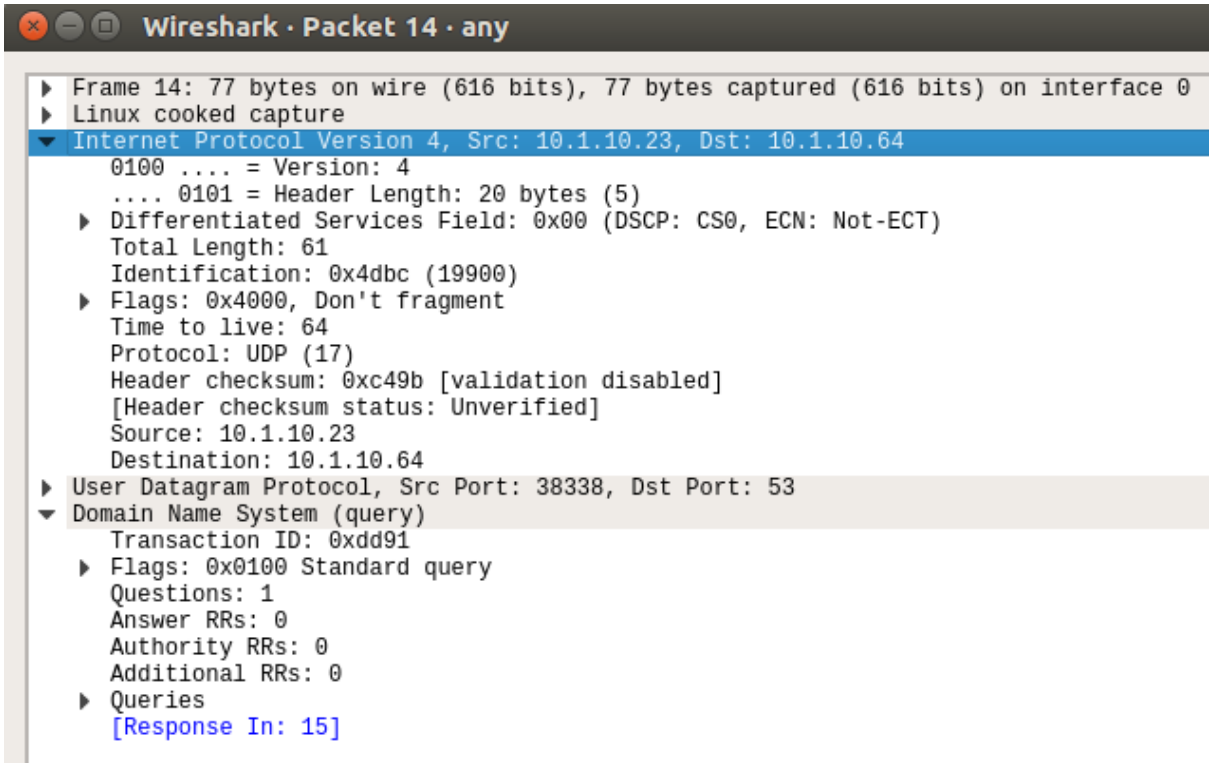
1. First Test

- Ping a computer such as www.example.com. Please use Wireshark to show the DNS query triggered by your ping command and DNS response.



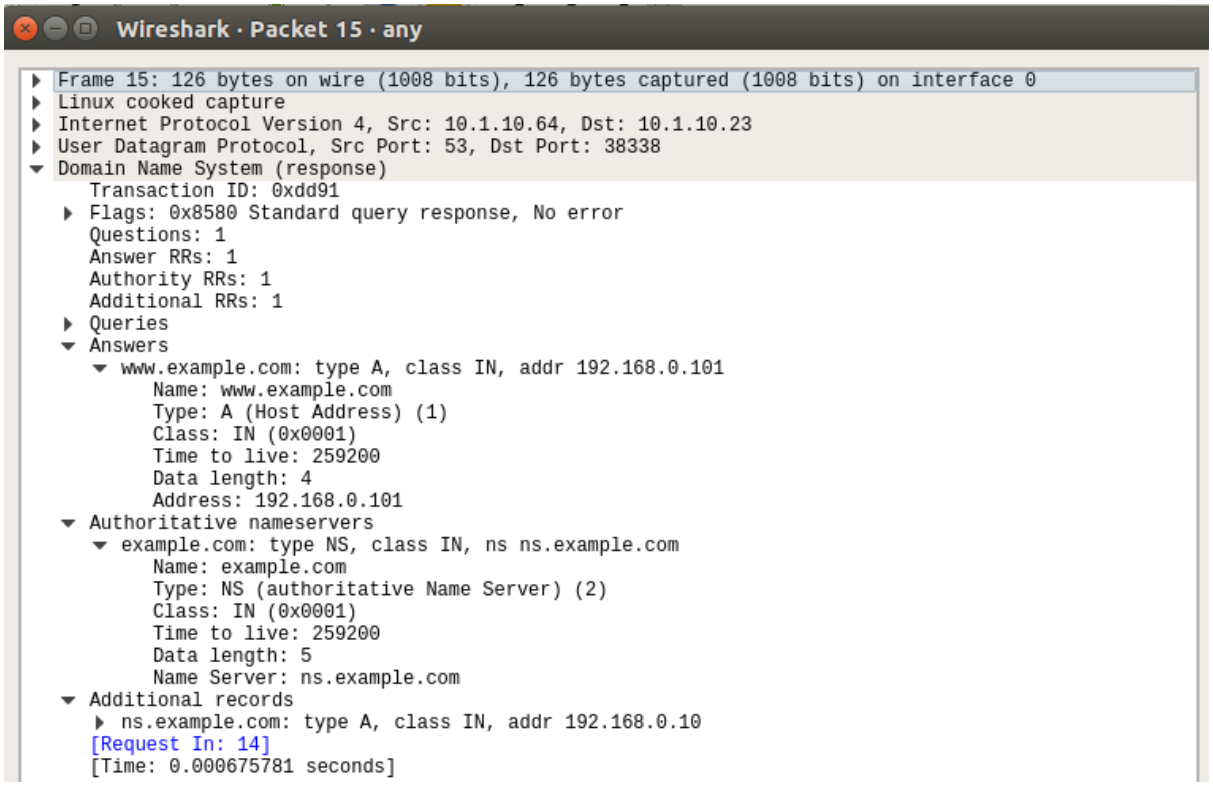
No.	Time	Source	Destination	Protocol	Length	Info
14	13.678738083	10.1.10.23	10.1.10.64	DNS	77	Standard query 0xdd91 A www.example.com
15	13.679413864	10.1.10.64	10.1.10.23	DNS	126	Standard query response 0xdd91 A www.example.com A 192.168.0.101 NS ns.example.com A 192.168.0.10
151	55.067721122	10.1.10.23	10.1.10.64	DNS	86	Standard query 0x7fa6 A detectportal.firefox.com
152	55.067735761	10.1.10.23	10.1.10.64	DNS	86	Standard query 0xb775 AAAA detectportal.firefox.com
153	55.068369214	10.1.10.23	10.1.10.64	DNS	86	Standard query 0xdf96 A detectportal.firefox.com
172	60.070876019	127.0.0.1	127.0.1.1	DNS	86	Standard query 0x7fa6 A detectportal.firefox.com
173	60.070896857	127.0.0.1	127.0.1.1	DNS	86	Standard query 0xb775 AAAA detectportal.firefox.com
174	60.070980312	10.1.10.23	192.168.3.5	DNS	86	Standard query 0xf1ea A detectportal.firefox.com
175	60.070992883	10.1.10.23	4.2.2.2	DNS	86	Standard query 0xf1ea A detectportal.firefox.com
176	60.070997721	10.1.10.23	202.138.96.2	DNS	86	Standard query 0xf1ea A detectportal.firefox.com
177	60.071002086	10.1.10.23	202.138.103.100	DNS	86	Standard query 0xf1ea A detectportal.firefox.com
178	60.071008511	10.1.10.23	10.1.10.64	DNS	86	Standard query 0xf1ea A detectportal.firefox.com
179	60.071033393	10.1.10.23	10.1.10.64	DNS	86	Standard query 0xea55 AAAA detectportal.firefox.com
180	60.071504130	192.168.3.5	10.1.10.23	DNS	197	Standard query response 0xf1ea A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAM…
181	60.071595425	127.0.1.1	127.0.0.1	DNS	197	Standard query response 0x7fa6 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAM…
182	60.073456938	127.0.0.1	127.0.1.1	DNS	86	Standard query 0xdf96 A detectportal.firefox.com
183	60.073538699	10.1.10.23	192.168.3.5	DNS	86	Standard query 0x7212 A detectportal.firefox.com
184	60.073999131	192.168.3.5	10.1.10.23	DNS	197	Standard query response 0x7212 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAM…
185	60.074083242	127.0.1.1	127.0.0.1	DNS	197	Standard query response 0xdf96 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAM…
191	60.101073159	202.138.96.2	10.1.10.23	DNS	533	Standard query response 0xf1ea A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAM…
194	60.105064163	10.1.10.23	10.1.10.64	DNS	73	Standard query 0xff02 A example.org
195	60.105070803	10.1.10.23	10.1.10.64	DNS	73	Standard query 0x5c7c A example.org
196	60.105077437	10.1.10.23	10.1.10.64	DNS	73	Standard query 0xdcd3 AAAA example.org
198	60.107035255	10.1.10.23	10.1.10.64	DNS	75	Standard query 0xea17 A ipv4only.arpa
199	60.107042241	10.1.10.23	10.1.10.64	DNS	75	Standard query 0xb735 AAAA ipv4only.arpa
200	60.112046157	4.2.2.2	10.1.10.23	DNS	197	Standard query response 0xf1ea A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAM…
205	60.123942652	202.138.103.100	10.1.10.23	DNS	491	Standard query response 0xf1ea A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAM…
208	60.654695384	10.1.10.64	10.1.10.23	DNS	395	Standard query response 0xea17 A ipv4only.arpa A 192.0.0.170 A 192.0.0.171 NS c.iana-servers.net …
209	60.654718299	10.1.10.64	10.1.10.23	DNS	132	Standard query response 0xb735 AAAA ipv4only.arpa SOA sns.dns.icann.org
210	60.655099101	10.1.10.23	10.1.10.64	DNS	86	Standard query 0xf11c A detectportal.firefox.com
211	60.655109001	10.1.10.23	10.1.10.64	DNS	86	Standard query 0xcd1a AAAA detectportal.firefox.com
214	61.488810468	10.1.10.64	10.1.10.23	DNS	245	Standard query response 0xff02 A example.org A 93.184.216.34 NS a.iana-servers.net NS b.iana-serv…

Wireshark Packet Capture



```
Wireshark · Packet 14 · any
▸ Frame 14: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0
▸ Linux cooked capture
▾ Internet Protocol Version 4, Src: 10.1.10.23, Dst: 10.1.10.64
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 61
    Identification: 0x4dbc (19900)
  ▸ Flags: 0x4000, Don't fragment
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0xc49b [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.1.10.23
    Destination: 10.1.10.64
▸ User Datagram Protocol, Src Port: 38338, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0xdd91
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▸ Queries
    [Response In: 15]
```

DNS Query

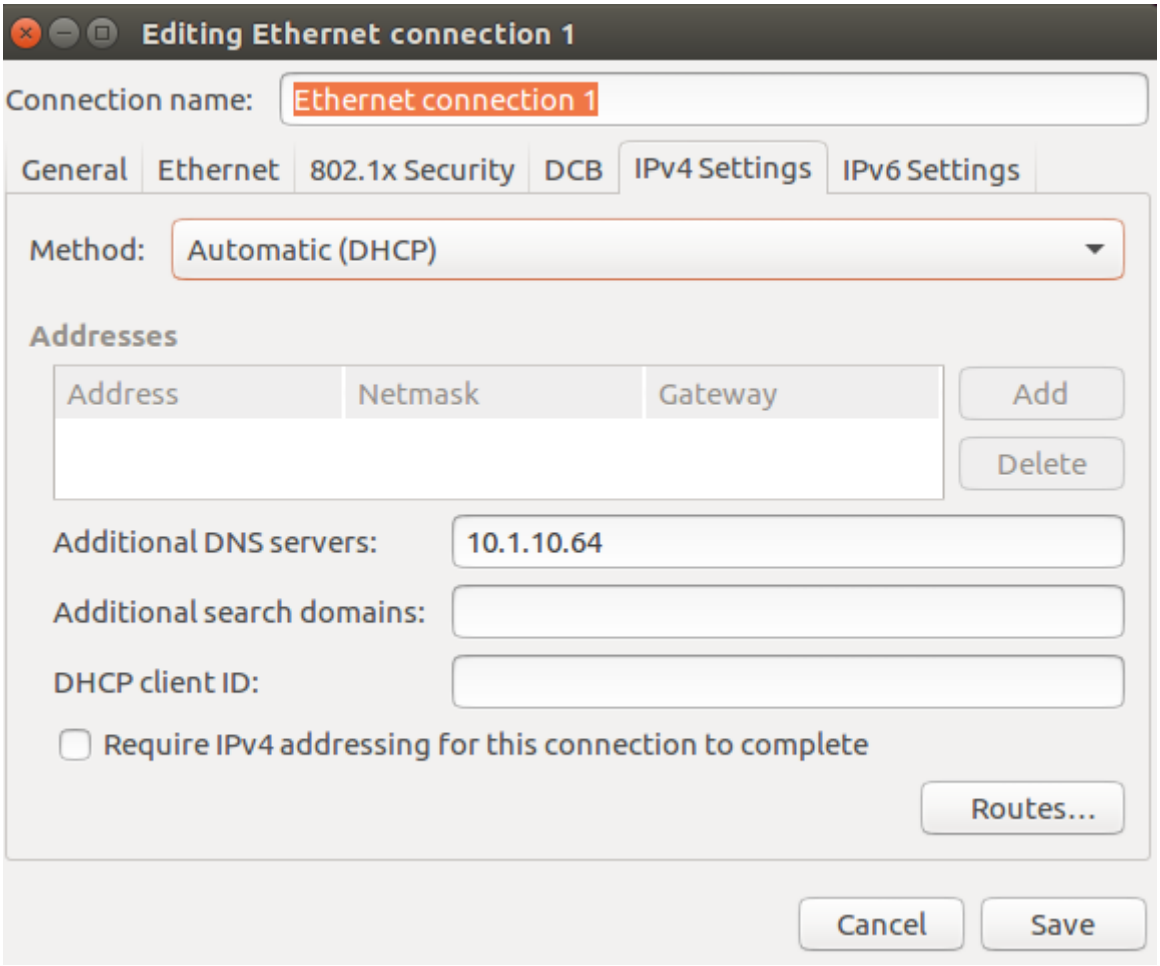


DNS Response

1. Task 1: Configure the User Machine

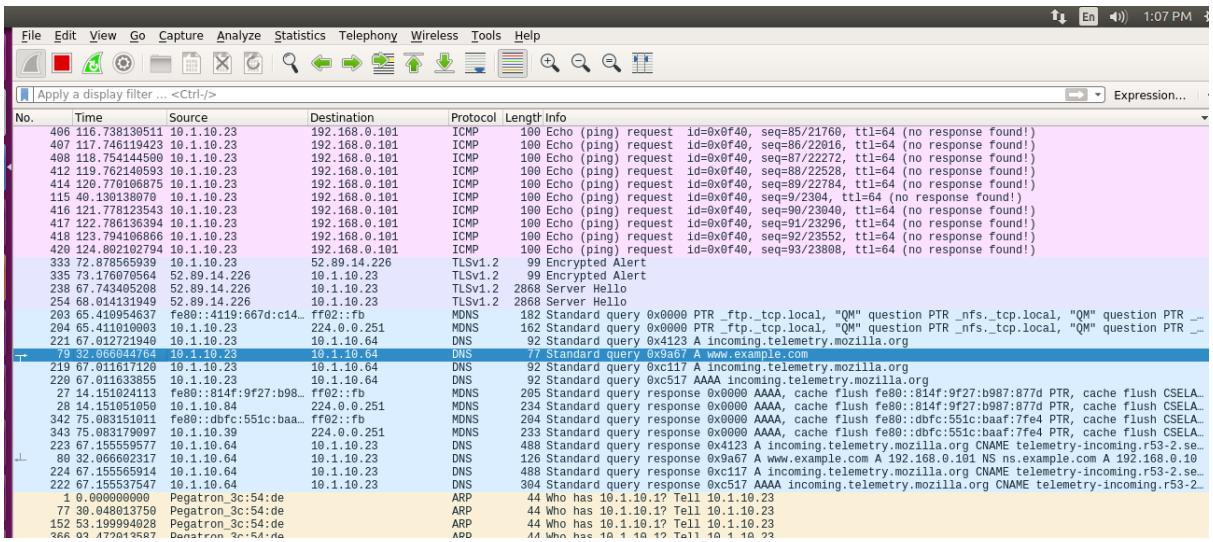
- The IP Address of the client machine is 10.1.10.23 and the IP Address of the server machine is 10.1.10.64
- We need to add the IP Address of the custom DNS server (10.1.10.64) to the client machine.
- This is done by adding the IP address of the server to the file **/etc/resolvconf/resolv.conf.d/head** 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**

```
student@CSELAB:~$ sudo 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
nameserver 10.1.10.96
student@CSELAB:~$ sudo resolvconf -u
student@CSELAB:~$
```



2. **Second Test**:

- Ping a computer such as www.example.com.
- Please use Wireshark to show the DNS query triggered by your ping command and DNS response. Describe your observation. (Take a screenshot).



3. Task 2 – Setting Up Local DNS Server

Note: If bind9 server is not already installed, install using the command

$ sudo apt-get update

$ sudo apt-get install bind9

```
student@CSELAB:~$ sudo apt-get update
[sudo] password for student:
Hit:1 http://in.archive.ubuntu.com/ubuntu xenial InRelease
Get:2 http://in.archive.ubuntu.com/ubuntu xenial-updates InRelease [109 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu xenial-backports InRelease [107 kB]
Get:4 http://security.ubuntu.com/ubuntu xenial-security InRelease [109 kB]
Get:5 http://dl.google.com/linux/chrome/deb stable InRelease [1,811 B]
Get:6 http://in.archive.ubuntu.com/ubuntu xenial-updates/main amd64 Packages [1,946 kB]
Ign:5 http://dl.google.com/linux/chrome/deb stable InRelease
Hit:7 https://dl.winehq.org/wine-builds/ubuntu xenial InRelease
Get:8 http://dl.google.com/linux/chrome/deb stable/main amd64 Packages [1,084 B]
Get:9 http://security.ubuntu.com/ubuntu xenial-security/main amd64 DEP-11 Metadata [93.1 kB]
Get:10 http://security.ubuntu.com/ubuntu xenial-security/universe amd64 DEP-11 Metadata [130 kB]
Get:11 http://security.ubuntu.com/ubuntu xenial-security/multiverse amd64 DEP-11 Metadata [2,464 B]
Get:12 http://in.archive.ubuntu.com/ubuntu xenial-updates/main i386 Packages [1,481 kB]
Get:13 http://in.archive.ubuntu.com/ubuntu xenial-updates/main amd64 DEP-11 Metadata [326 kB]
Get:14 http://in.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 DEP-11 Metadata [281 kB]
Get:15 http://in.archive.ubuntu.com/ubuntu xenial-updates/universe DEP-11 64x64 Icons [435 kB]
Get:16 http://in.archive.ubuntu.com/ubuntu xenial-updates/multiverse amd64 DEP-11 Metadata [5,960 B]
Get:17 http://in.archive.ubuntu.com/ubuntu xenial-backports/main amd64 DEP-11 Metadata [3,328 B]
Get:18 http://in.archive.ubuntu.com/ubuntu xenial-backports/universe amd64 DEP-11 Metadata [6,612 B]
Fetched 5,038 kB in 12s (404 kB/s)
Reading package lists... Done
W: GPG error: http://dl.google.com/linux/chrome/deb stable InRelease: The following signatures couldn't
ot available: NO_PUBKEY 78BD65473CB3BD13
W: The repository 'http://dl.google.com/linux/chrome/deb stable InRelease' is not signed.
N: Data from such a repository can't be authenticated and is therefore potentially dangerous to use.
N: See apt-secure(8) manpage for repository creation and user configuration details
```

```
student@CSELAB:~$ sudo apt-get install bind9
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libevent-core-2.0-5 libpango1.0-0 libqmi-glib1 libqpdf17 libwireshark8
  libwiretap6 libwscodecs1 libwsutil7
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  bind9utils libirs141
Suggested packages:
  bind9-doc
The following NEW packages will be installed:
  bind9 bind9utils libirs141
0 upgraded, 3 newly installed, 0 to remove and 2 not upgraded.
Need to get 592 kB of archives.
After this operation, 2,960 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu xenial-updates/main amd64 libirs141 amd64 1:9.10.3.dfsg.P4-8ubuntu1.17 [18.0 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu xenial-updates/main amd64 bind9utils amd64 1:9.10.3.dfsg.P4-8ubuntu1.17 [201 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu xenial-updates/main amd64 bind9 amd64 1:9.10.3.dfsg.P4-8ubuntu1.17 [373 kB]
Fetched 592 kB in 1s (552 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libirs141:amd64.
(Reading database ... 228561 files and directories currently installed.)
Preparing to unpack .../libirs141_1%3a9.10.3.dfsg.P4-8ubuntu1.17_amd64.deb ...
Unpacking libirs141:amd64 (1:9.10.3.dfsg.P4-8ubuntu1.17) ...
Selecting previously unselected package bind9utils.
Preparing to unpack .../bind9utils_1%3a9.10.3.dfsg.P4-8ubuntu1.17_amd64.deb ...
Unpacking bind9utils (1:9.10.3.dfsg.P4-8ubuntu1.17) ...
Selecting previously unselected package bind9.
Preparing to unpack .../bind9_1%3a9.10.3.dfsg.P4-8ubuntu1.17_amd64.deb ...
Unpacking bind9 (1:9.10.3.dfsg.P4-8ubuntu1.17) ...
Processing triggers for libc-bin (2.23-0ubuntu11.2) ...
Processing triggers for man-db (2.7.5-1) ...
Processing triggers for ufw (0.35-0ubuntu2) ...
Rules updated for profile 'Apache Full'
```

Step 1: Configure the BIND9 Server.

- BIND9 gets its configuration from a file called **/etc/bind/named.conf.**
- This file is the primary configuration file, and it usually contains several "include" entries.
- One of the included files is called **/etc/bind/named.conf.options**. This is where we typically set up the configuration options.
- Let us first set up an option related to DNS cache by adding a dump-file entry to the options block. The above option specifies where the cache content should be dumped to if BIND is asked to dump its cache.

```
@CSELAB: ~
student@CSELAB:~$ sudo nano /etc/bind/named.conf.options
```

```
@CSELAB: ~
student@CSELAB:~$ sudo nano /etc/bind/named.conf.options
Use "fg" to return to nano.

[4]+  Stopped                 sudo nano /etc/bind/named.conf.options
student@CSELAB:~$ sudo nano /etc/bind/named.conf.options
student@CSELAB:~$ sudo cat /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; };
};
```

- The above option specifies where the cache content should be dumped to if BIND is asked to dump its cache. If this option is not specified, BIND dumps the cache to a default file called **/var/cache/bind/named_dump.db**

Step 2: Start DNS server

- We start the DNS server using the command**: $ sudo service bind9 restart**

```
student@CSELAB:~$ sudo service bind9 restart
student@CSELAB:~$
```

- The two commands shown below are related to DNS cache.
- The first command is **sudo rndc dumpdb -cache**, dumps the content of the cache to the file specified above.
- And the second command is **sudo rndc flush** which clears the cache.

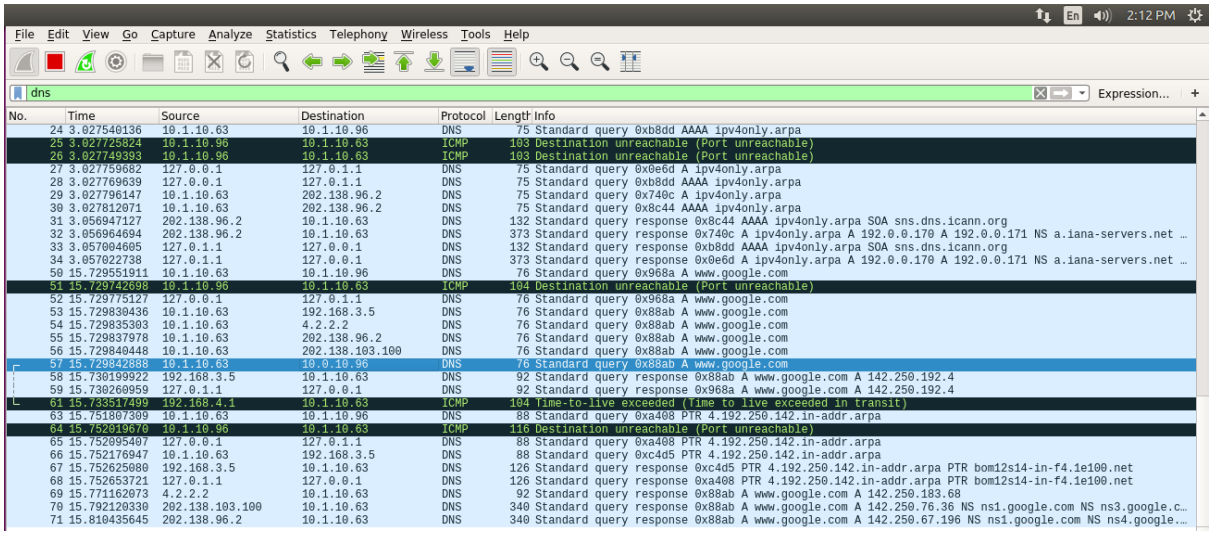
```
student@CSELAB:~$ sudo rndc dumpdb -cache
student@CSELAB:~$ sudo rndc flush
student@CSELAB:~$ cat /var/cache/bind/dump.db
;
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
$DATE 20210219074231
; secure
.                       518378  IN NS   a.root-servers.net.
                        518378  IN NS   b.root-servers.net.
                        518378  IN NS   c.root-servers.net.
                        518378  IN NS   d.root-servers.net.
                        518378  IN NS   e.root-servers.net.
                        518378  IN NS   f.root-servers.net.
                        518378  IN NS   g.root-servers.net.
                        518378  IN NS   h.root-servers.net.
                        518378  IN NS   i.root-servers.net.
                        518378  IN NS   j.root-servers.net.
                        518378  IN NS   k.root-servers.net.
                        518378  IN NS   l.root-servers.net.
                        518378  IN NS   m.root-servers.net.
; secure
                        518400  RRSIG   NS 8 0 518400 (
                                        20210304050000 20210219040000 42351 .
                                        XOe4ITrSZueR1BY0DTDXjoIfJQ0gHpp8XSjp
```

Step 3: Use the DNS server

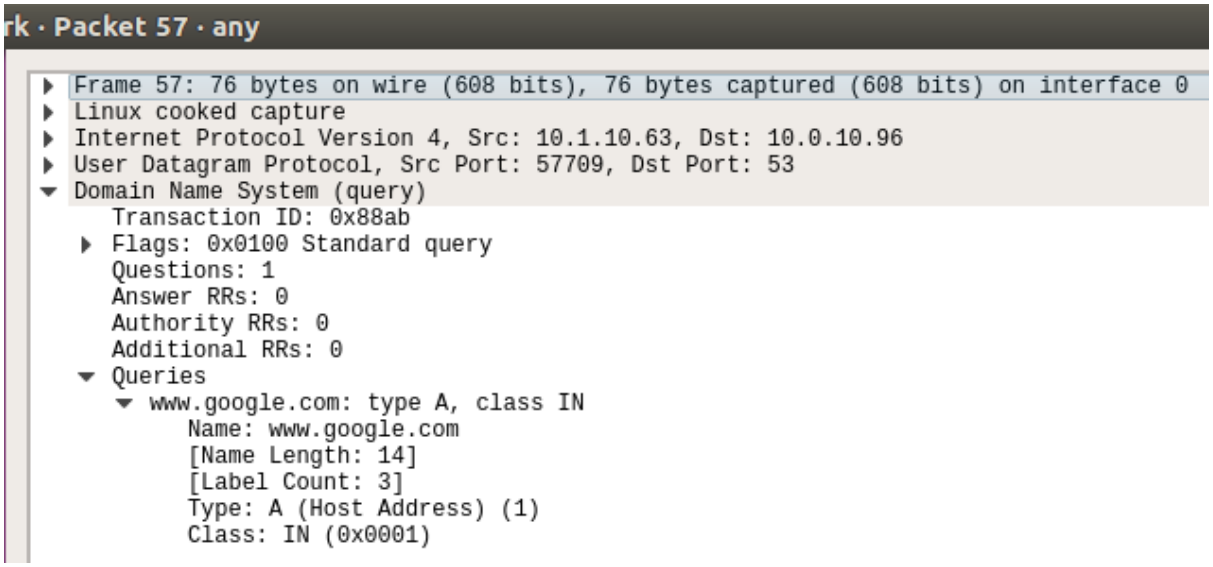
4. Third Test:

- Now, go back to your user machine, and ping a computer such as www.google.com
- 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

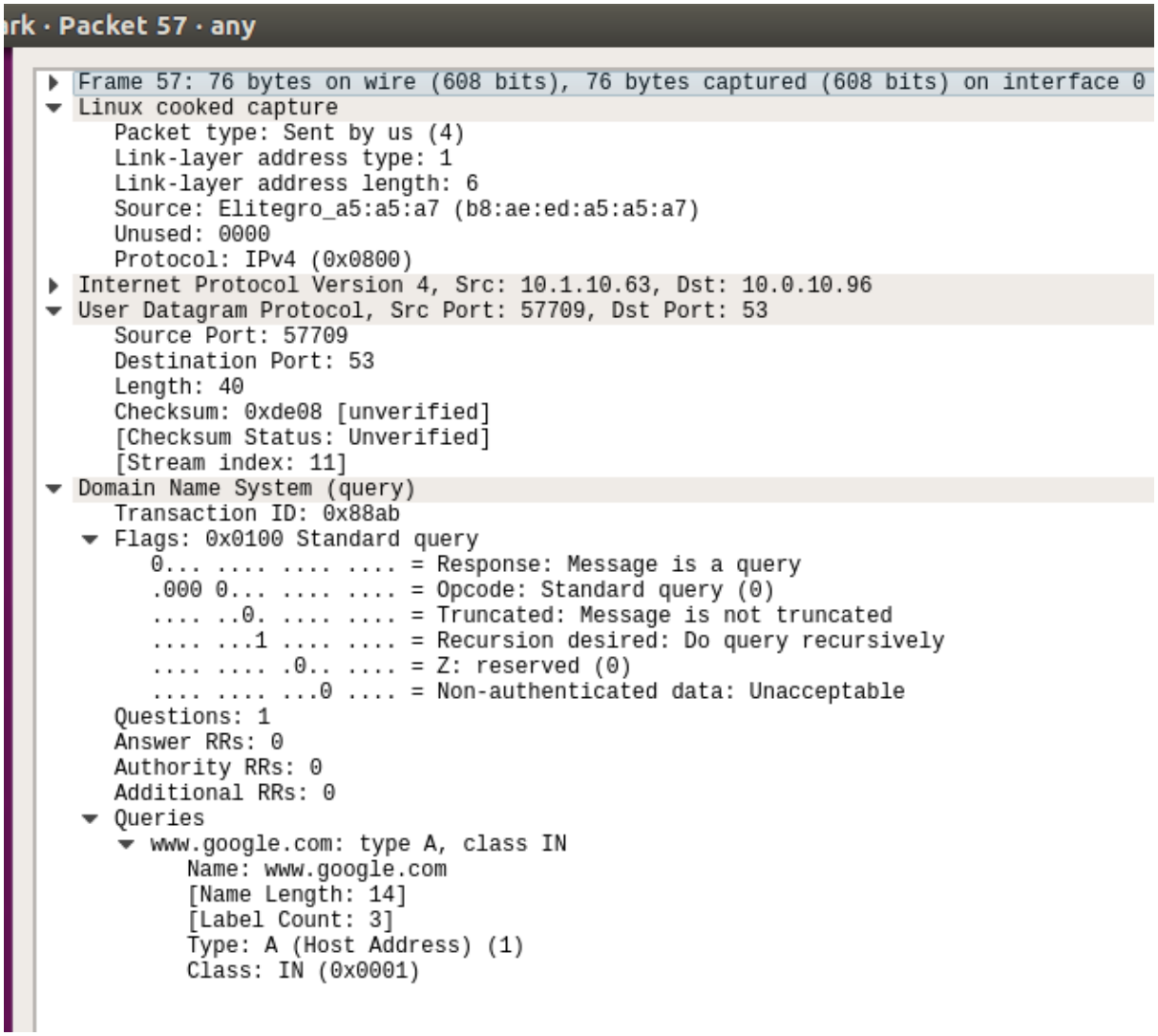
```
@CSELAB: ~
student@CSELAB:~$ ping www.google.com
PING www.google.com (142.250.192.4) 56(84) bytes of data.
64 bytes from bom12s14-in-f4.1e100.net (142.250.192.4): icmp_seq=1 ttl=116 time=21.3 ms
64 bytes from bom12s14-in-f4.1e100.net (142.250.192.4): icmp_seq=2 ttl=116 time=20.6 ms
64 bytes from bom12s14-in-f4.1e100.net (142.250.192.4): icmp_seq=3 ttl=116 time=20.3 ms
64 bytes from bom12s14-in-f4.1e100.net (142.250.192.4): icmp_seq=4 ttl=116 time=20.3 ms
64 bytes from bom12s14-in-f4.1e100.net (142.250.192.4): icmp_seq=5 ttl=116 time=20.2 ms
64 bytes from bom12s14-in-f4.1e100.net (142.250.192.4): icmp_seq=6 ttl=116 time=20.3 ms
64 bytes from bom12s14-in-f4.1e100.net (142.250.192.4): icmp_seq=7 ttl=116 time=20.3 ms
64 bytes from bom12s14-in-f4.1e100.net (142.250.192.4): icmp_seq=8 ttl=116 time=20.5 ms
64 bytes from bom12s14-in-f4.1e100.net (142.250.192.4): icmp_seq=9 ttl=116 time=20.3 ms
```



Wireshark Packet Capture



DNS Query Packet



DNS Response Packet

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

Step 1: Create Zones

- We had two zone entries in the DNS server by adding the following contents to **/etc/bind/named.conf** as shown in the below screenshot.
- The **first zone is for forward lookup** (from hostname to IP),
- And the **second zone is for reverse lookup** (from IP to hostname).

```
student@CSELAB:~$ sudo nano /etc/bind/named.conf
[sudo] password for student:
student@CSELAB:~$ sudo cat /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/10.0.63.db";
};
student@CSELAB:~$
```

Step 2: Setup the forward lookup zone file

- We create **example.com.db** zone file with the following contents in the **/etc/bind/** directory where the actual DNS resolution is stored
- 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

```
student@CSELAB:~$ 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       192.168.0.101
mail    IN      A       192.168.0.102
ns      IN      A       192.168.0.10
*.example.com.  IN      A 192.168.0.100
```

Forward Lookup file

Step 3: Setup the reverse lookup zone file

- We create a reverse DNS lookup file called **10.0.63.db for** the example.net domain to support DNS reverse lookup, i.e., from IP address to hostname in the /etc/bind/ directory with the following contents

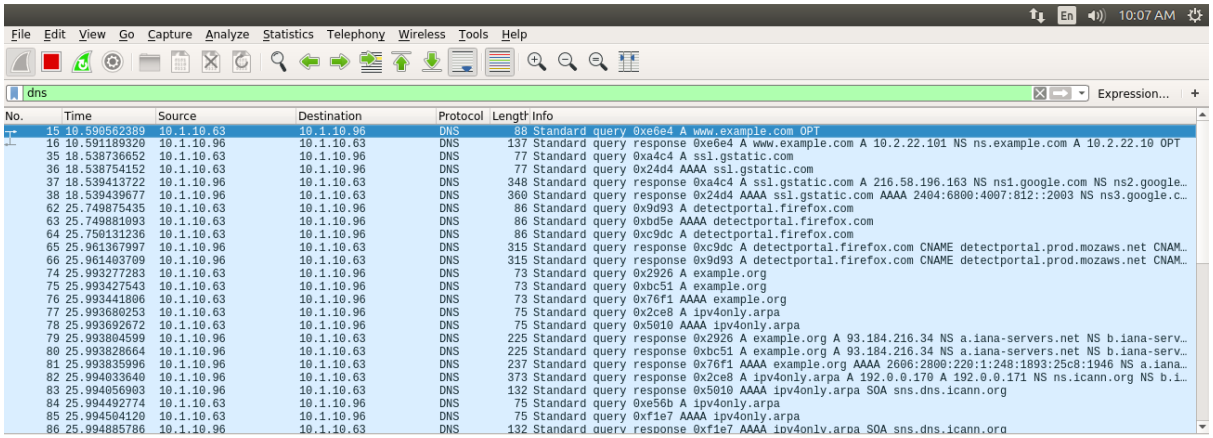
```
student@CSELAB:~$ sudo cat /etc/bind/10.0.63.db
$TTL 3D
@       IN      SOA     ns.example.com. admin.example.com. (
                        2008111001
                        8H
                        2H
                        4W
                        1D)
@       IN      NS      ns.example.com.

101     IN      PTR     www.example.com.
102     IN      PTR     mail.example.com.
10      IN      PTR     ns.example.com.
student@CSELAB:~$
```

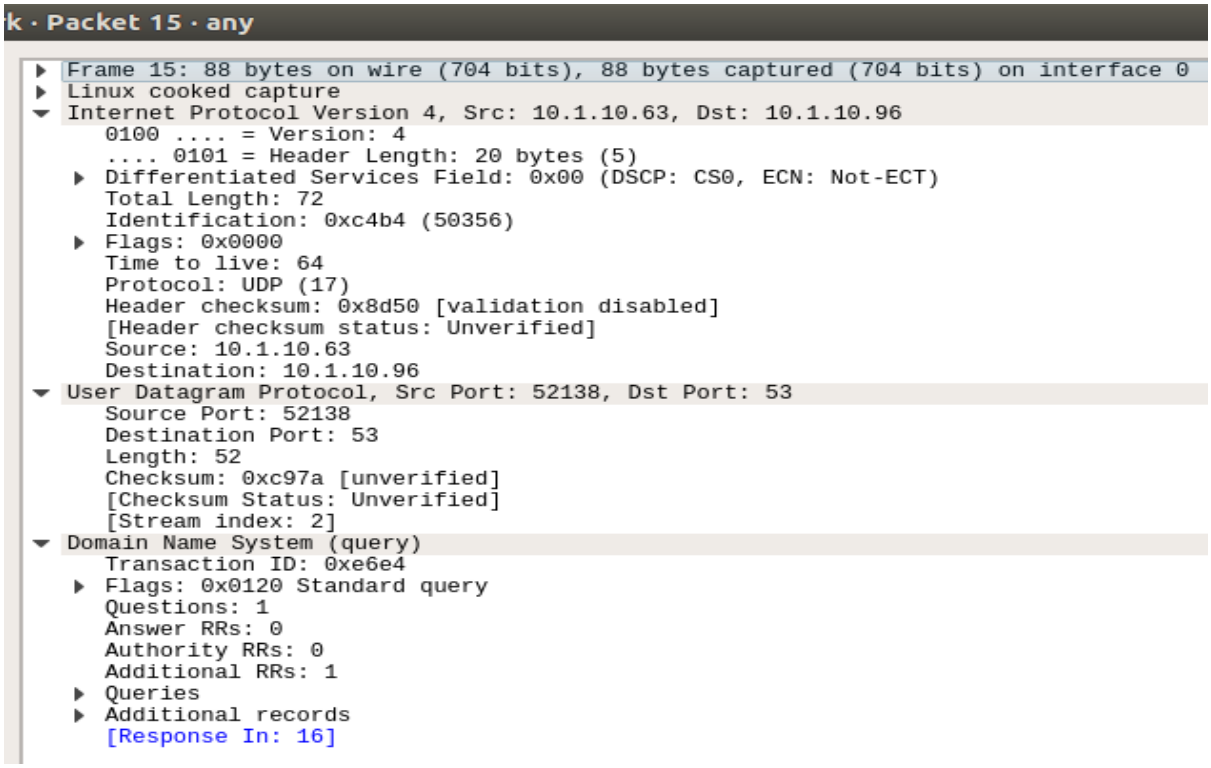
Reverse Lookup file

6. Fourth Test – Testing www.example.com

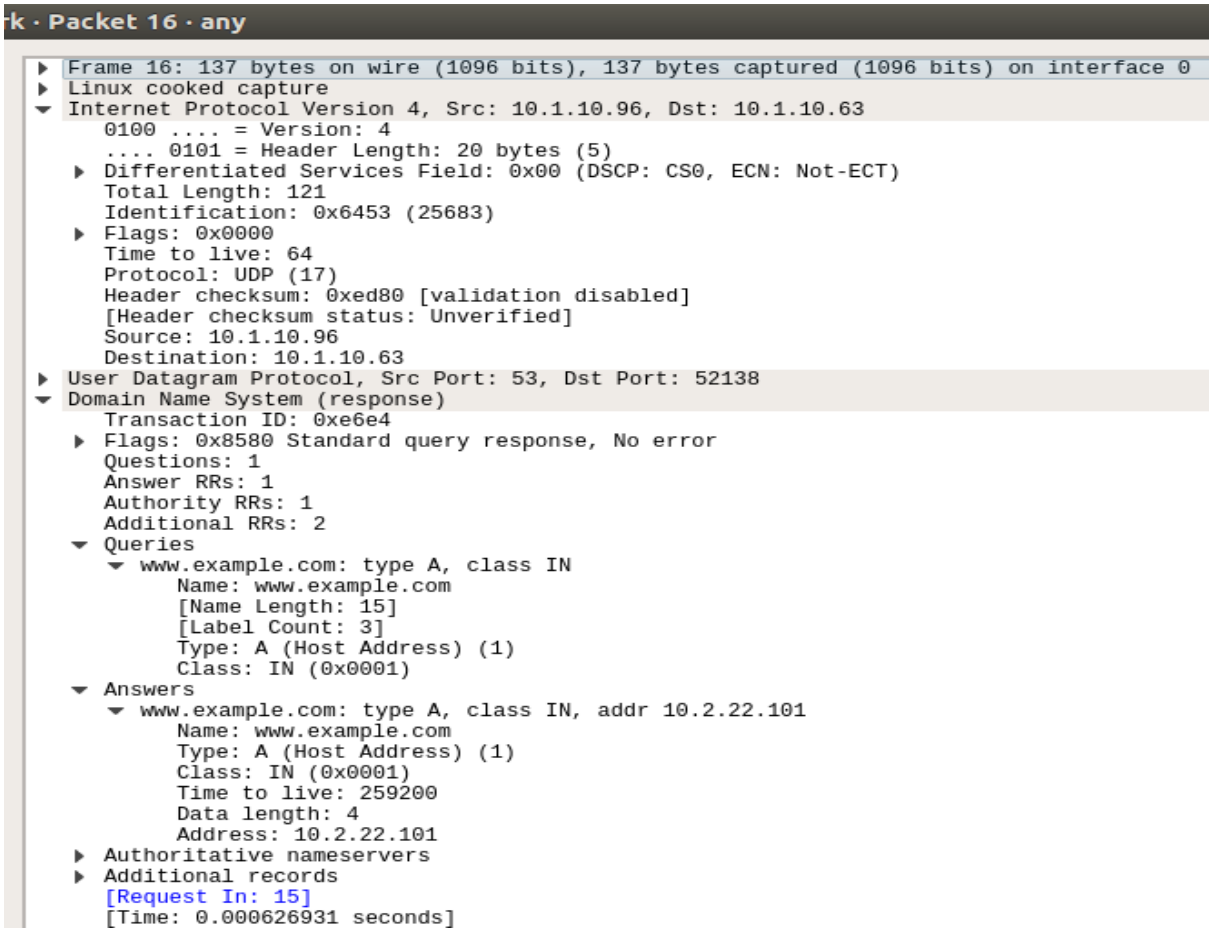
- The dig command is used to lookup name servers specified in the file **/etc/resolv.conf**



Wireshark Packet Capture



DNS Response Packet



DNS Response Packet

7. 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 10.0.2.63. 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 example.com refers to the canonical hostname www.example.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.example.com) retrieved from the response message.

Q7. *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

Q8. *To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?*

Answer – The DNS query message sent to the IP 10.1.10.96. No, this is not the IP address of your default local DNS server.

Q9. *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.

Q10. *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 example.com refers to the canonical hostname www.example.com.
- **A type RR:** This provides the IP Address of the canonical hostname.