

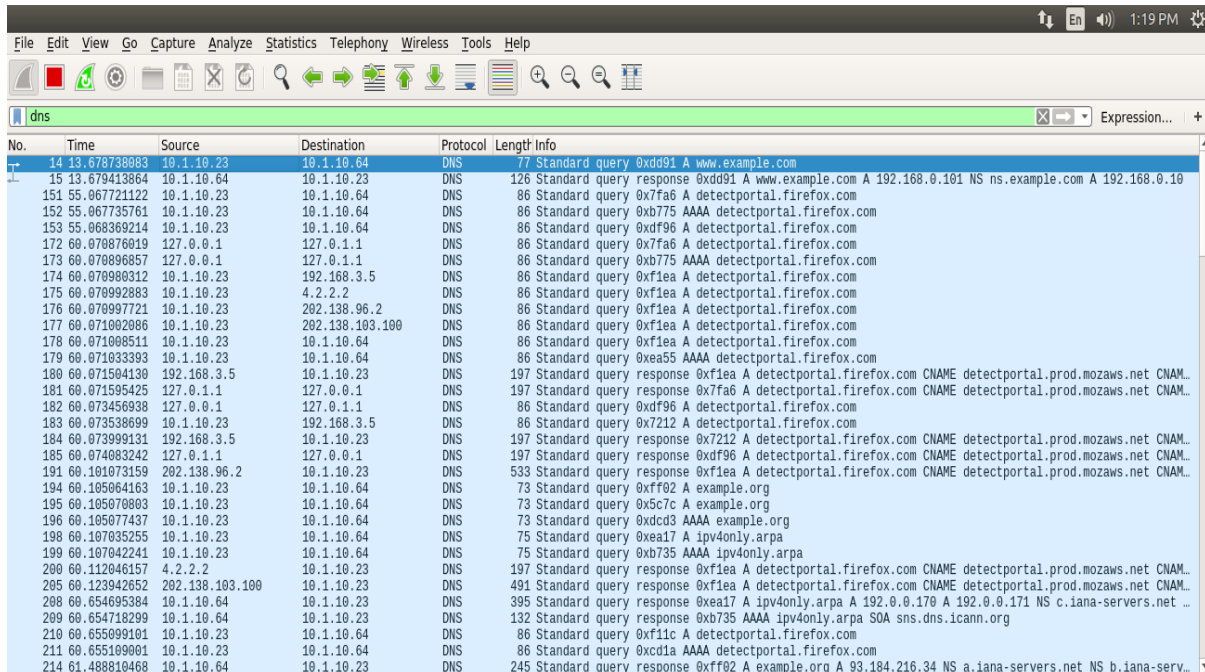
CN LAB REPORT – WEEK 4

NAME: DIVYANSHU SHARMA

PES1UG20CS806

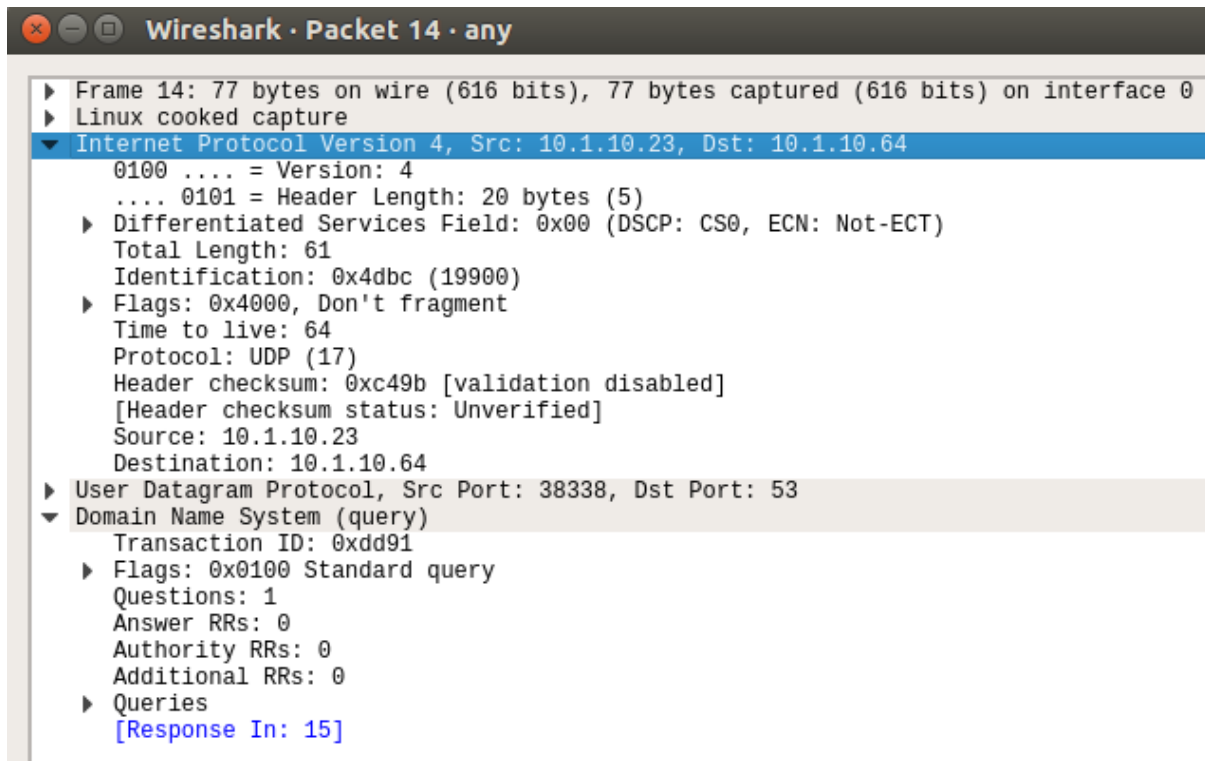
1. First Test

- 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	13.678738883	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	60.070876619	127.0.0.1	127.0.0.1	DNS	86	Standard query 0x7fa6 A detectportal.firefox.com
173	60.070896857	127.0.0.1	127.0.0.1	DNS	86	Standard query 0xb775 AAAA detectportal.firefox.com
174	60.070908312	10.1.10.23	192.168.3.5	DNS	86	Standard query 0xf1ea A detectportal.firefox.com
175	60.07092883	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	127.0.0.1	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	127.0.0.1	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	127.0.0.1	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 0xcd3 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

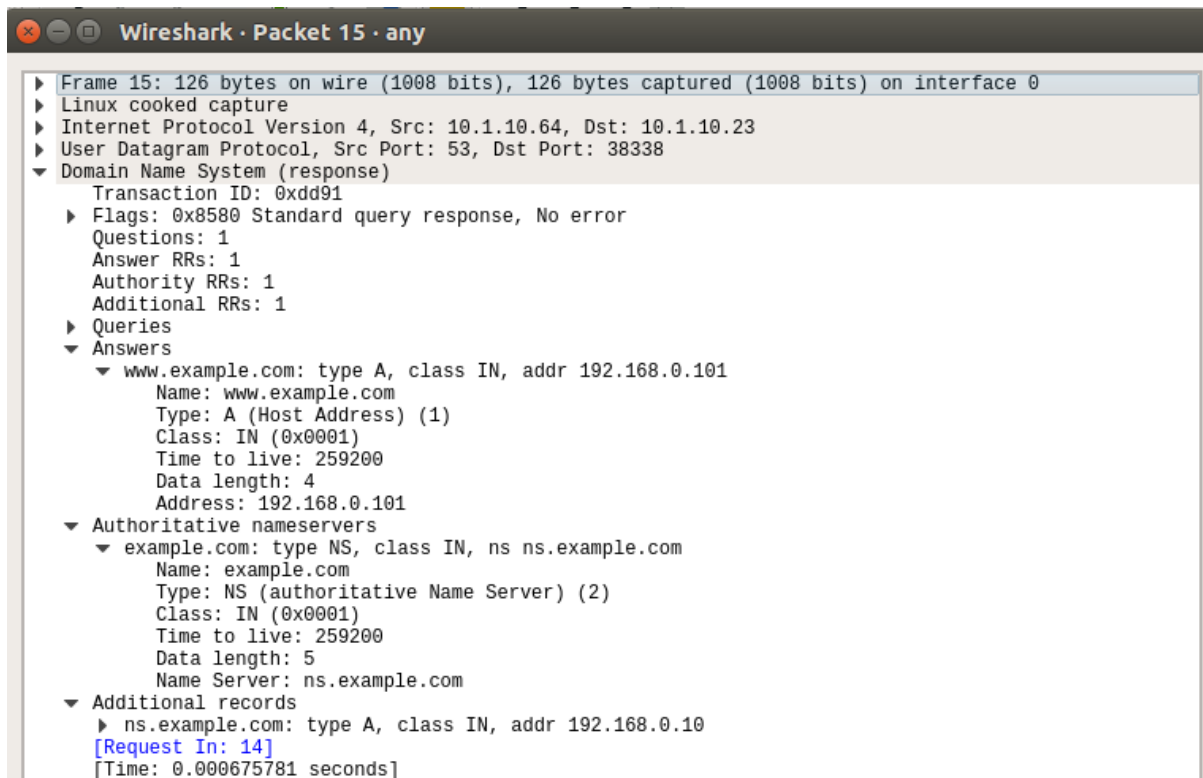
▶ Frame 14: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0

▶ 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:~$
```

Editing Ethernet connection 1

Connection name: **Ethernet connection 1**

General | **Ethernet** | 802.1x Security | DCB | IPv4 Settings | IPv6 Settings

Method: **Automatic (DHCP)**

Addresses

Address	Netmask	Gateway

Additional DNS servers: **10.1.10.64**

Additional search domains:

DHCP client ID:

☐ Require IPv4 addressing for this connection to complete

Routes...

Cancel **Save**

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).

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
406	116.738139511	10.1.10.23	192.168.0.101	ICMP	100	Echo (ping) request id=0x0f40, seq=85/21760, ttl=64 (no response found!)
407	117.746119423	10.1.10.23	192.168.0.101	ICMP	100	Echo (ping) request id=0x0f40, seq=86/22016, ttl=64 (no response found!)
408	118.754144500	10.1.10.23	192.168.0.101	ICMP	100	Echo (ping) request id=0x0f40, seq=87/22272, ttl=64 (no response found!)
412	119.762140593	10.1.10.23	192.168.0.101	ICMP	100	Echo (ping) request id=0x0f40, seq=88/22528, ttl=64 (no response found!)
414	120.770100875	10.1.10.23	192.168.0.101	ICMP	100	Echo (ping) request id=0x0f40, seq=89/22784, ttl=64 (no response found!)
115	40.130130070	10.1.10.23	192.168.0.101	ICMP	100	Echo (ping) request id=0x0f40, seq=9/2304, ttl=64 (no response found!)
416	121.778123543	10.1.10.23	192.168.0.101	ICMP	100	Echo (ping) request id=0x0f40, seq=90/23296, ttl=64 (no response found!)
417	122.786136394	10.1.10.23	192.168.0.101	ICMP	100	Echo (ping) request id=0x0f40, seq=91/23552, ttl=64 (no response found!)
418	123.794106866	10.1.10.23	192.168.0.101	ICMP	100	Echo (ping) request id=0x0f40, seq=92/23808, ttl=64 (no response found!)
420	124.802102794	10.1.10.23	192.168.0.101	ICMP	100	Echo (ping) request id=0x0f40, seq=93/24064, ttl=64 (no response found!)
333	72.878565939	10.1.10.23	52.89.14.226	TLv1.2	99	Encrypted Alert
335	73.170070564	52.89.14.226	10.1.10.23	TLv1.2	99	Encrypted Alert
238	67.743405208	52.89.14.226	10.1.10.23	TLv1.2	2868	Server Hello
254	68.014131949	52.89.14.226	10.1.10.23	TLv1.2	2868	Server Hello
263	65.410954637	fe80::4119:667d:c14...	ff02::fb	MDNS	182	Standard query 0x0000 PTR _ftp._tcp.local, "QM" question PTR _nfs._tcp.local, "QM" question PTR _...
294	65.41010083	10.1.10.23	224.0.0.251	MDNS	162	Standard query 0x0000 PTR _ftp._tcp.local, "QM" question PTR _nfs._tcp.local, "QM" question PTR _...
221	67.012721940	10.1.10.23	10.1.10.64	DNS	92	Standard query 0x4123 A incoming.telemetry.mozilla.org
79	32.860844764	10.1.10.23	10.1.10.64	DNS	77	Standard query 0x9a67 A www.example.com
219	67.011617120	10.1.10.23	10.1.10.64	DNS	92	Standard query 0xc117 A incoming.telemetry.mozilla.org
220	67.011633855	10.1.10.23	10.1.10.64	DNS	92	Standard query 0xc517 AAAA incoming.telemetry.mozilla.org
27	14.151024113	fe80::814f:9f27:b98...	ff02::fb	MDNS	205	Standard query response 0x0000 AAAA, cache flush fe80::814f:9f27:b987:877d PTR, cache flush CSELA...
28	14.151051050	10.1.10.84	224.0.0.251	MDNS	234	Standard query response 0x0000 AAAA, cache flush fe80::814f:9f27:b987:877d PTR, cache flush CSELA...
342	75.083151011	fe80::dbfc:551c:baa...	ff02::fb	MDNS	204	Standard query response 0x0000 AAAA, cache flush fe80::dbfc:551c:baaf:7fe4 PTR, cache flush CSELA...
343	75.083179997	10.1.10.39	224.0.0.251	MDNS	233	Standard query response 0x0000 AAAA, cache flush fe80::dbfc:551c:baaf:7fe4 PTR, cache flush CSELA...
232	67.155559577	10.1.10.64	10.1.10.23	DNS	488	Standard query response 0x4123 A incoming.telemetry.mozilla.org CNAME telemetry-incoming.r53-2.se...
80	32.066602317	10.1.10.64	10.1.10.23	DNS	126	Standard query response 0x9a67 A www.example.com A 192.168.0.101 NS ns.example.com A 192.168.0.10...
224	67.155565914	10.1.10.64	10.1.10.23	DNS	488	Standard query response 0xc117 A incoming.telemetry.mozilla.org CNAME telemetry-incoming.r53-2.se...
222	67.155537547	10.1.10.64	10.1.10.23	DNS	304	Standard query response 0xc517 AAAA incoming.telemetry.mozilla.org CNAME telemetry-incoming.r53-2.se...
1	0.000000000	Pegatron.3c:54:de		ARP	44	Who has 10.1.10.1? Tell 10.1.10.23
77	30.048013750	Pegatron.3c:54:de		ARP	44	Who has 10.1.10.1? Tell 10.1.10.23
152	53.199994028	Pegatron.3c:54:de		ARP	44	Who has 10.1.10.1? Tell 10.1.10.23
368	92.4770413587	Pegatron.3c:54:de		ARP	44	Who has 10.1.10.1? Tell 10.1.10.23

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
  be authenticated: NO_PUBKEY 78BD65473CB3BD13
W: The repository 'http://dl.google.com/linux/chrome/deb stable InRelease' is not signed.
W: Data from such a repository can't be authenticated and is therefore potentially dangerous to use.
W: See apt-get(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 libwscodec3 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 .
                        XOe4ITrSZueR1BY0DIDXjoIfJQ0gHpp8XSjp
```

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
```

No.	Time	Source	Destination	Protocol	Length	Info
24	3.027548136	10.1.10.63	10.1.10.96	DNS	75	Standard query 0xb8dd AAAA ipv4only.arpa
25	3.027725824	10.1.10.96	10.1.10.63	ICMP	103	Destination unreachable (Port unreachable)
26	3.027749393	10.1.10.96	10.1.10.63	ICMP	103	Destination unreachable (Port unreachable)
27	3.027759682	127.0.0.1	127.0.1.1	DNS	75	Standard query 0xb8dd AAAA ipv4only.arpa
28	3.027769639	127.0.0.1	127.0.1.1	DNS	75	Standard query 0xb8dd AAAA ipv4only.arpa
29	3.027796147	10.1.10.63	202.138.96.2	DNS	75	Standard query 0x740c A ipv4only.arpa
30	3.027812071	10.1.10.63	202.138.96.2	DNS	75	Standard query 0x8c44 AAAA ipv4only.arpa
31	3.056947127	202.138.96.2	10.1.10.63	DNS	132	Standard query response 0x8c44 AAAA ipv4only.arpa SOA sns.dns.icann.org
32	3.056964694	202.138.96.2	10.1.10.63	DNS	373	Standard query response 0x740c A ipv4only.arpa A 192.0.0.170 A 192.0.0.171 NS a.iana-servers.net ...
33	3.057094695	127.0.1.1	127.0.0.1	DNS	132	Standard query response 0xb8dd AAAA ipv4only.arpa SOA sns.dns.icann.org
34	3.057022738	127.0.1.1	127.0.0.1	DNS	373	Standard query response 0xb8dd A ipv4only.arpa A 192.0.0.170 A 192.0.0.171 NS a.iana-servers.net ...
50	15.729551911	10.1.10.63	10.1.10.96	DNS	76	Standard query 0x968a A www.google.com
51	15.729742698	10.1.10.96	10.1.10.63	ICMP	104	Destination unreachable (Port unreachable)
52	15.729775127	127.0.0.1	127.0.1.1	DNS	76	Standard query 0x968a A www.google.com
53	15.729830436	10.1.10.63	192.168.3.5	DNS	76	Standard query 0x88ab A www.google.com
54	15.729835303	10.1.10.63	4.2.2.2	DNS	76	Standard query 0x88ab A www.google.com
55	15.729837978	10.1.10.63	202.138.96.2	DNS	76	Standard query 0x88ab A www.google.com
56	15.729840448	10.1.10.63	202.138.103.100	DNS	76	Standard query 0x88ab A www.google.com
57	15.729842888	10.1.10.63	10.0.10.96	DNS	76	Standard query 0x88ab A www.google.com
58	15.730199922	192.168.3.5	10.1.10.63	DNS	92	Standard query response 0x88ab A www.google.com A 142.250.192.4
59	15.730260959	127.0.1.1	127.0.0.1	DNS	92	Standard query response 0x968a A www.google.com A 142.250.192.4
61	15.733517499	192.168.4.1	10.1.10.63	ICMP	104	Time-to-live exceeded (time to live exceeded in transit)
63	15.751807309	10.1.10.63	10.1.10.96	DNS	88	Standard query 0xa408 PTR 4.192.250.142.in-addr.arpa
64	15.752019670	10.1.10.96	10.1.10.63	ICMP	116	Destination unreachable (Port unreachable)
65	15.752095407	127.0.0.1	127.0.1.1	DNS	88	Standard query 0xa408 PTR 4.192.250.142.in-addr.arpa
66	15.752176947	10.1.10.63	192.168.3.5	DNS	88	Standard query 0xc4d5 PTR 4.192.250.142.in-addr.arpa
67	15.752625080	192.168.3.5	10.1.10.63	DNS	126	Standard query response 0xc4d5 PTR 4.192.250.142.in-addr.arpa PTR bom12s14-in-f4.1e100.net
68	15.752653721	127.0.1.1	127.0.0.1	DNS	126	Standard query response 0xa408 PTR 4.192.250.142.in-addr.arpa PTR bom12s14-in-f4.1e100.net
69	15.771162073	4.2.2.2	10.1.10.63	DNS	92	Standard query response 0x88ab A www.google.com A 142.250.183.68
70	15.792120330	202.138.103.100	10.1.10.63	DNS	340	Standard query response 0x88ab A www.google.com A 142.250.76.36 NS ns1.google.com NS ns3.google.c...
71	15.810435645	202.138.96.2	10.1.10.63	DNS	340	Standard query response 0x88ab A www.google.com A 142.250.67.196 NS ns1.google.com NS ns4.google.c...

Wireshark Packet Capture

rk · Packet 57 · any

- ▶ Frame 57: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
- ▶ Linux cooked capture
- ▶ Internet Protocol Version 4, Src: 10.1.10.63, Dst: 10.0.10.96
- ▶ User Datagram Protocol, Src Port: 57709, Dst Port: 53
- ▼ Domain Name System (query)
 - Transaction ID: 0x88ab
 - ▶ Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - ▼ Queries
 - www.google.com: type A, class IN
 - Name: www.google.com
 - [Name Length: 14]
 - [Label Count: 3]
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)

DNS Query Packet

rk · Packet 57 · any

```
▶ Frame 57: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
▼ Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Elitegro_a5:a5:a7 (b8:ae:ed:a5:a5:a7)
  Unused: 0000
  Protocol: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 10.1.10.63, Dst: 10.0.10.96
▼ User Datagram Protocol, Src Port: 57709, Dst Port: 53
  Source Port: 57709
  Destination Port: 53
  Length: 40
  Checksum: 0xde08 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 11]
▼ Domain Name System (query)
  Transaction ID: 0x88ab
  ▼ Flags: 0x0100 Standard query
    0... .. = Response: Message is a query
    .000 0... .. = Opcode: Standard query (0)
    .... .. = Truncated: Message is not truncated
    ....1... .. = Recursion desired: Do query recursively
    .... ..0... .. = Z: reserved (0)
    .... ..0... .. = Non-authenticated data: Unacceptable
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▼ www.google.com: type A, class IN
      Name: www.google.com
      [Name Length: 14]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
```

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

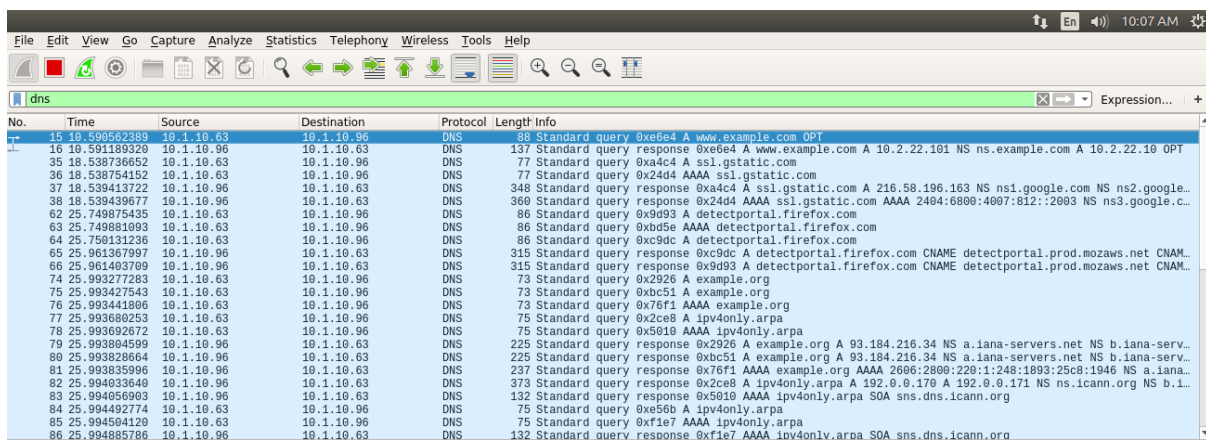
```
student@CSELAB:~$ sudo cat /etc/bind/10.0.63.db
$TTL 3D
@      IN      SOA      ns.example.com. admin.example.com. (
2008111001
      8H
      2H
      4W
      1D)
@      IN      NS       ns.example.com.

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



No.	Time	Source	Destination	Protocol	Length	Info
15	10.590562389	10.1.10.63	10.1.10.96	DNS	88	Standard query 0xe6e4 A www.example.com OPT
16	10.591189320	10.1.10.96	10.1.10.63	DNS	137	Standard query response 0xe6e4 A www.example.com A 10.2.22.101 NS ns.example.com A 10.2.22.10 OPT
35	18.538736652	10.1.10.63	10.1.10.96	DNS	77	Standard query 0xa4c4 A ssl.gstatic.com
36	18.538754152	10.1.10.63	10.1.10.96	DNS	77	Standard query 0x24d4 AAAA ssl.gstatic.com
37	18.539413722	10.1.10.96	10.1.10.63	DNS	348	Standard query response 0xa4c4 A ssl.gstatic.com A 216.58.196.163 NS ns1.google.com NS ns2.google.c...
38	18.539439677	10.1.10.96	10.1.10.63	DNS	360	Standard query response 0x24d4 AAAA ssl.gstatic.com AAAA 2404:6800:4007:812::2003 NS ns3.google.c...
62	25.749875435	10.1.10.63	10.1.10.96	DNS	86	Standard query 0x9d93 A detectportal.firefox.com
63	25.749881093	10.1.10.63	10.1.10.96	DNS	86	Standard query 0xbd5e AAAA detectportal.firefox.com
64	25.750131236	10.1.10.63	10.1.10.96	DNS	86	Standard query 0xc9dc A detectportal.firefox.com
65	25.961367997	10.1.10.96	10.1.10.63	DNS	315	Standard query response 0xc9dc A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAM...
66	25.961403709	10.1.10.96	10.1.10.63	DNS	315	Standard query response 0x9d93 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAM...
74	25.993277283	10.1.10.63	10.1.10.96	DNS	73	Standard query 0x2926 A example.org
75	25.993427543	10.1.10.63	10.1.10.96	DNS	73	Standard query 0xbc51 A example.org
76	25.993441806	10.1.10.63	10.1.10.96	DNS	73	Standard query 0x76f1 AAAA example.org
77	25.993680253	10.1.10.63	10.1.10.96	DNS	75	Standard query 0x2ce8 A ipv4only.arpa
78	25.993692672	10.1.10.63	10.1.10.96	DNS	75	Standard query 0x5010 AAAA ipv4only.arpa
79	25.993804599	10.1.10.96	10.1.10.63	DNS	225	Standard query response 0x2926 A example.org A 93.184.216.34 NS a.iana-servers.net NS b.iana-serv...
80	25.993828064	10.1.10.96	10.1.10.63	DNS	225	Standard query response 0xbc51 A example.org A 93.184.216.34 NS a.iana-servers.net NS b.iana-serv...
81	25.993835996	10.1.10.96	10.1.10.63	DNS	237	Standard query response 0x76f1 AAAA example.org AAAA 2606:2800:220:1:248:1803:25c8:1946 NS a.iana...
82	25.994033640	10.1.10.96	10.1.10.63	DNS	373	Standard query response 0x2ce8 A ipv4only.arpa A 192.0.0.170 A 192.0.0.171 NS ns.icann.org NS b.i...
83	25.994056903	10.1.10.96	10.1.10.63	DNS	132	Standard query response 0x5010 AAAA ipv4only.arpa SOA sns.dns.icann.org
84	25.994492774	10.1.10.63	10.1.10.96	DNS	75	Standard query 0xe56b A ipv4only.arpa
85	25.994504120	10.1.10.63	10.1.10.96	DNS	75	Standard query 0xf1e7 AAAA ipv4only.arpa
86	25.994885786	10.1.10.96	10.1.10.63	DNS	132	Standard query response 0xf1e7 AAAA ipv4only.arpa SOA sns.dns.icann.org

Wireshark Packet Capture

k · Packet 15 · any

- ▶ Frame 15: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0
- ▶ Linux cooked capture
- ▼ Internet Protocol Version 4, Src: 10.1.10.63, Dst: 10.1.10.96
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 72
 - Identification: 0xc4b4 (50356)
 - ▶ Flags: 0x0000
 - Time to live: 64
 - Protocol: UDP (17)
 - Header checksum: 0x8d50 [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 10.1.10.63
 - Destination: 10.1.10.96
- ▼ User Datagram Protocol, Src Port: 52138, Dst Port: 53
 - Source Port: 52138
 - Destination Port: 53
 - Length: 52
 - Checksum: 0xc97a [unverified]
 - [Checksum Status: Unverified]
 - [Stream index: 2]
- ▼ Domain Name System (query)
 - Transaction ID: 0xe6e4
 - ▶ Flags: 0x0120 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 1
 - ▶ Queries
 - ▶ Additional records
 - [Response In: 16]

DNS Response Packet

k · Packet 16 · any

- ▶ Frame 16: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits) on interface 0
- ▶ Linux cooked capture
- ▼ Internet Protocol Version 4, Src: 10.1.10.96, Dst: 10.1.10.63
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 121
 - Identification: 0x6453 (25683)
 - ▶ Flags: 0x0000
 - Time to live: 64
 - Protocol: UDP (17)
 - Header checksum: 0xed80 [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 10.1.10.96
 - Destination: 10.1.10.63
- ▶ User Datagram Protocol, Src Port: 53, Dst Port: 52138
- ▼ Domain Name System (response)
 - Transaction ID: 0xe6e4
 - ▶ 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
 - Name: www.example.com
 - [Name Length: 15]
 - [Label Count: 3]
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)
 - ▼ Answers
 - ▼ www.example.com: type A, class IN, addr 10.2.22.101
 - Name: www.example.com
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)
 - Time to live: 259200
 - Data length: 4
 - Address: 10.2.22.101
 - ▶ Authoritative nameservers
 - ▶ Additional records
 - [Request In: 15]
 - [Time: 0.000626931 seconds]

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.