

Week #4

Implementation of a Local DNS Server and Authoritative Nameserver

Team Member 1:

Name : Laxmikant Bhujang Gurav

SRN : PES1UG20CS658

Roll no.: 55

Team Member 2:

Name : Pavan Kumar Nuthi

SRN : PES1UG20CS670

Roll no.: 31

Observation 1:

Ping a computer such as www.google.com (any domain). Please use Wireshark to show the DNS query triggered by your ping command and DNS response.

WIRESHARK CAPTURE

The screenshot shows the NetworkMiner application window. The dns tab is active, displaying a list of network traffic entries. One entry is highlighted, showing a DNS query from 10.1.10.61 to 192.168.3.5 for the domain www.google.com. The query ID is 0xf4f92, and the response code is 0x0. The response data includes the HTML content of the Google search results page.

Wireshark · Packet 1108 · any

▶ Frame 1108: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
▶ Linux cooked capture
▶ Internet Protocol Version 4, Src: 192.168.3.5, Dst: 10.1.10.61
▼ User Datagram Protocol, Src Port: 53, Dst Port: 36633
 Source Port: 53
 Destination Port: 36633
 Length: 56
 Checksum: 0xac6e [unverified]
 [Checksum Status: Unverified]
 [Stream index: 9]
▼ Domain Name System (response)
 Transaction ID: 0x4f92
 ▶ Flags: 0x8180 Standard query response, No error
 Questions: 1
 Answer RRs: 1
 Authority RRs: 0
 Additional RRs: 0
 ▶ Queries
 ▶ Answers
 [Request In: 1106]
 [Time: 0.000327063 seconds]

0000 00 00 00 01 00 06 14 58 d0 d4 86 00 41 43 08 00 X . . . AC . .
0010 45 00 00 4c 5a 6e 00 00 7e 11 0a 48 c0 a8 03 05 E . . Lzn . ~ . H . . .
0020 0a 01 0a 3d 00 35 8f 19 00 38 ac 6e 4f 92 81 80 . . . = 5 . 8 . n0 . . .
0030 00 01 00 01 00 00 00 00 03 77 77 77 06 67 6f 6f www . goo . . .
0040 67 6c 65 03 63 6f 6d 00 00 01 00 01 c0 0c 00 01 gle . com
0050 00 01 00 00 00 6a 00 04 ac d9 1f c4 . . . j

Part 1: Setting Up a Local DNS Server

Task 1: Configure the User/Client Machine

1.1 Change the resolver configuration file (/etc/resolv.conf):

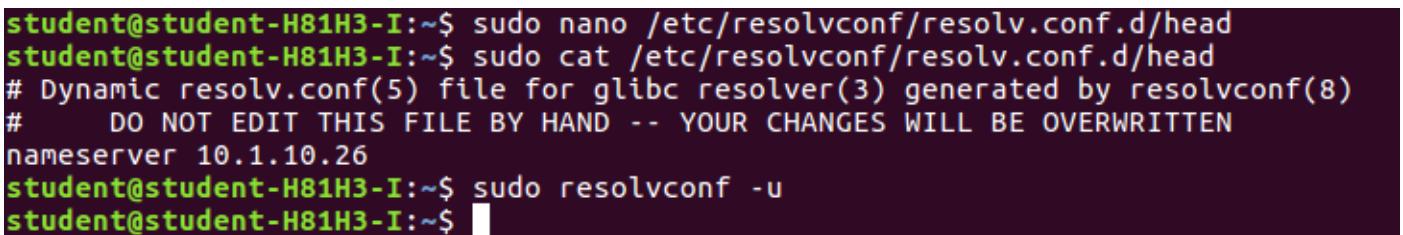


```
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
# DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 10.1.10.26
```

```
student@student-H81H3-I:~$ sudo nano /etc/resolvconf/resolv.conf.d/head
student@student-H81H3-I:~$ 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 10.1.10.26
student@student-H81H3-I:~$
```

1.2 Run the following command for the change to take effect.

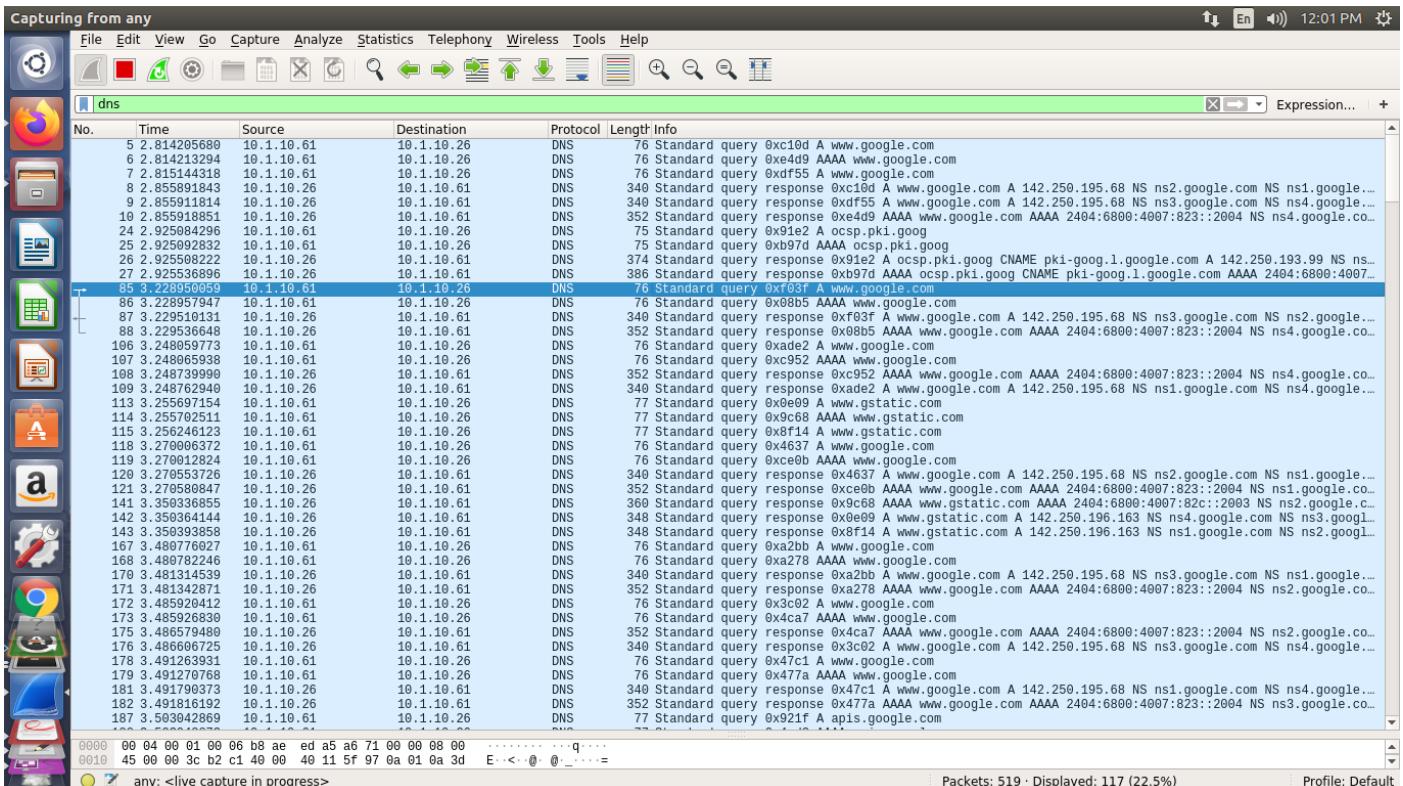
```
sudo resolvconf -u
```



```
# 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 10.1.10.26
student@student-H81H3-I:~$ sudo resolvconf -u
student@student-H81H3-I:~$
```

Observation 2:

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



Wireshark · Packet 794 · any

```

▶ Frame 794: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
▶ Linux cooked capture
▶ Internet Protocol Version 4, Src: 10.1.10.61, Dst: 10.1.10.26
└ User Datagram Protocol, Src Port: 51784, Dst Port: 53
    Source Port: 51784
    Destination Port: 53
    Length: 40
    Checksum: 0x8db3 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 59]
  ▼ Domain Name System (query)
    Transaction ID: 0xf06c
    ▼ Flags: 0x0100 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)
      .... 0.... .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▶ www.google.com: type A, class IN
    [Response In: 796]

```

| | | | | | |
|------|-------------|-------------|-------------|-------------------------|----------------------|
| 0000 | 00 04 00 01 | 00 06 | b8 ae | ed a5 a6 71 00 00 08 00 | q |
| 0010 | 45 00 00 3c | 29 53 40 00 | 40 11 e9 05 | 0a 01 0a 3d | E-<)S@ @.....= |
| 0020 | 0a 01 0a 1a | ca 48 00 35 | 00 28 8d b3 | f0 6c 01 00 |H-5 (....1... |
| 0030 | 00 01 00 00 | 00 00 00 00 | 03 77 77 77 | 06 67 6f 6f |www.goo |
| 0040 | 67 6c 65 03 | 63 6f 6d 00 | 00 01 00 01 |gle.com..... | |

Close Help

Wireshark · Packet 796 · any

```

▶ Frame 796: 340 bytes on wire (2720 bits), 340 bytes captured (2720 bits) on interface 0
▶ Linux cooked capture
▶ Internet Protocol Version 4, Src: 10.1.10.26, Dst: 10.1.10.61
└ User Datagram Protocol, Src Port: 53, Dst Port: 51784
    Source Port: 53
    Destination Port: 51784
    Length: 304
    Checksum: 0xc336 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 59]
  ▼ Domain Name System (response)
    Transaction ID: 0xf06c
    ▶ Flags: 0x8100 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 4
    Additional RRs: 8
  ▼ Queries
    ▶ www.google.com: type A, class IN
  ▼ Answers
    ▶ www.google.com: type A, class IN, addr 142.250.195.68
  ▼ Authoritative nameservers
    ▶ google.com: type NS, class IN, ns ns3.google.com
    ▶ google.com: type NS, class IN, ns ns2.google.com
    ▶ google.com: type NS, class IN, ns ns1.google.com
    ▶ google.com: type NS, class IN, ns ns4.google.com
  ▶ Additional records
    [Request In: 794]
    [Time: 0.000576947 seconds]

```

Close Help

Task 2: Set Up a Local DNS Server

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

\$ sudo apt-get update

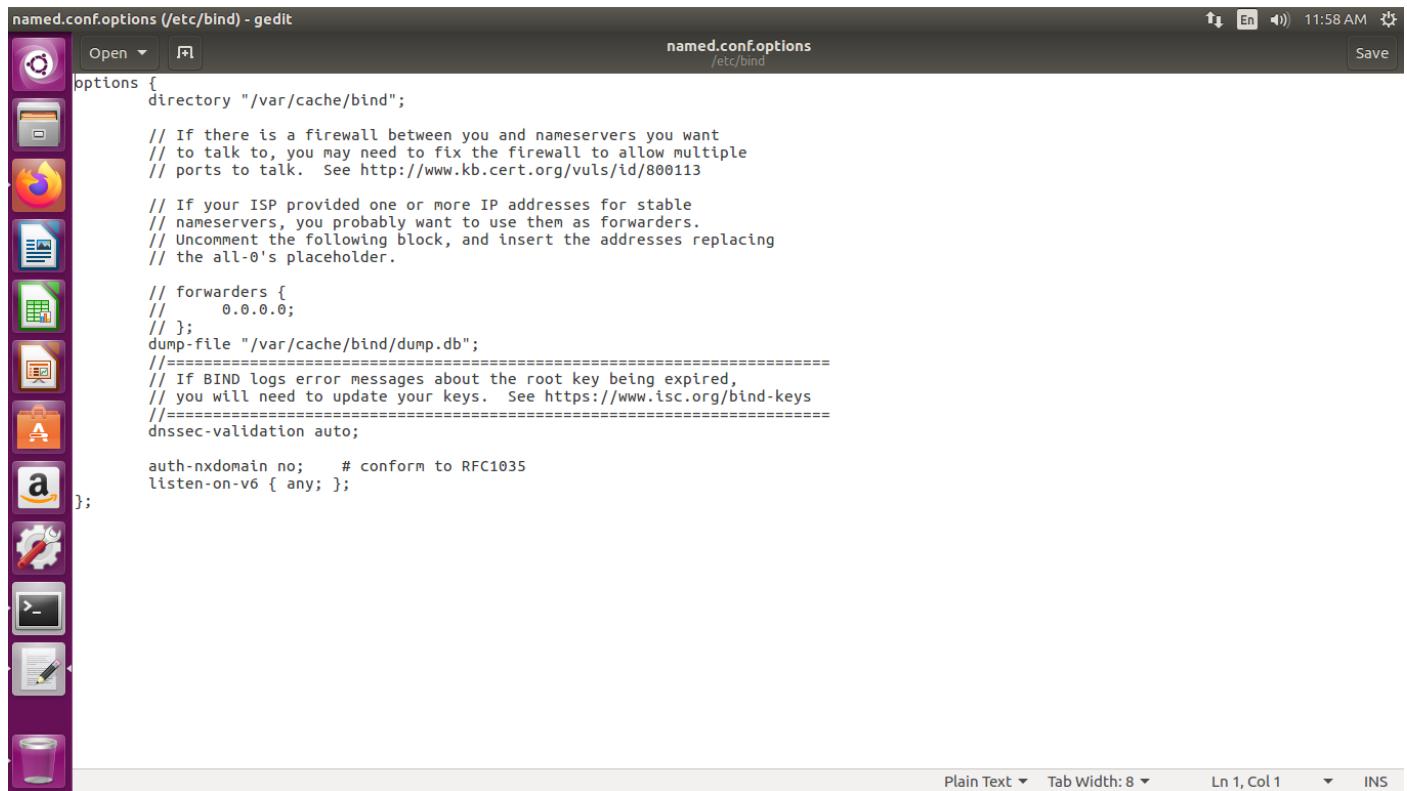
```
student@student-H81H3-I:~$ sudo apt-get update
[sudo] password for student:
Ign:1 http://dl.google.com/linux/chrome/deb stable InRelease
Hit:4 http://in.archive.ubuntu.com/ubuntu xenial InRelease
Ign:3 http://dl.google.com/linux/chrome/deb stable Release
Hit:5 http://in.archive.ubuntu.com/ubuntu xenial-updates InRelease
Ign:6 http://dl.google.com/linux/chrome/deb stable/main amd64 Packages
Ign:7 http://dl.google.com/linux/chrome/deb stable/main all Packages
Hit:8 http://in.archive.ubuntu.com/ubuntu xenial-backports InRelease
Ign:9 http://dl.google.com/linux/chrome/deb stable/main Translation-en_IN
Ign:10 http://dl.google.com/linux/chrome/deb stable/main Translation-en
Ign:11 http://dl.google.com/linux/chrome/deb stable/main amd64 DEP-11 Metadata
Ign:12 http://dl.google.com/linux/chrome/deb stable/main DEP-11 64x64 Icons
Ign:6 http://dl.google.com/linux/chrome/deb stable/main amd64 Packages
Ign:7 http://dl.google.com/linux/chrome/deb stable/main all Packages
Ign:9 http://dl.google.com/linux/chrome/deb stable/main Translation-en_IN
Ign:10 http://dl.google.com/linux/chrome/deb stable/main Translation-en
Ign:11 http://dl.google.com/linux/chrome/deb stable/main amd64 DEP-11 Metadata
Ign:12 http://dl.google.com/linux/chrome/deb stable/main DEP-11 64x64 Icons
Ign:6 http://dl.google.com/linux/chrome/deb stable/main amd64 Packages
Ign:2 https://www.apache.org/dist/cassandra/debian 31ix InRelease
Ign:7 http://dl.google.com/linux/chrome/deb stable/main all Packages
Ign:9 http://dl.google.com/linux/chrome/deb stable/main Translation-en_IN
Hit:14 http://ppa.launchpad.net/deadsnakes/ppa/ubuntu xenial InRelease
Ign:10 http://dl.google.com/linux/chrome/deb stable/main Translation-en
Ign:11 http://dl.google.com/linux/chrome/deb stable/main amd64 DEP-11 Metadata
Ign:12 http://dl.google.com/linux/chrome/deb stable/main DEP-11 64x64 Icons
Ign:6 http://dl.google.com/linux/chrome/deb stable/main amd64 Packages
Ign:7 http://dl.google.com/linux/chrome/deb stable/main all Packages
Ign:9 http://dl.google.com/linux/chrome/deb stable/main Translation-en_IN
Ign:10 http://dl.google.com/linux/chrome/deb stable/main Translation-en
Ign:11 http://dl.google.com/linux/chrome/deb stable/main amd64 DEP-11 Metadata
Ign:12 http://dl.google.com/linux/chrome/deb stable/main DEP-11 64x64 Icons
Ign:6 http://dl.google.com/linux/chrome/deb stable/main amd64 Packages
Ign:7 http://dl.google.com/linux/chrome/deb stable/main all Packages
Ign:9 http://dl.google.com/linux/chrome/deb stable/main Translation-en_IN
Ign:10 http://dl.google.com/linux/chrome/deb stable/main Translation-en
Ign:11 http://dl.google.com/linux/chrome/deb stable/main amd64 DEP-11 Metadata
Ign:12 http://dl.google.com/linux/chrome/deb stable/main DEP-11 64x64 Icons
Ign:6 http://dl.google.com/linux/chrome/deb stable/main amd64 Packages
Ign:7 http://dl.google.com/linux/chrome/deb stable/main all Packages
Ign:9 http://dl.google.com/linux/chrome/deb stable/main Translation-en_IN
Ign:10 http://dl.google.com/linux/chrome/deb stable/main Translation-en
Ign:11 http://dl.google.com/linux/chrome/deb stable/main amd64 DEP-11 Metadata
Ign:12 http://dl.google.com/linux/chrome/deb stable/main DEP-11 64x64 Icons
Err:6 http://dl.google.com/linux/chrome/deb stable/main amd64 Packages
  404  File not found
```

\$ sudo apt-get install bind9

```
student@student-H81H3-I:~$ sudo apt-get install bind9
Reading package lists... Done
Building dependency tree
Reading state information... Done
bind9 is already the newest version (1:9.10.3.dfsg.P4-8ubuntu1.19).
The following package was automatically installed and is no longer required:
  snapd-login-service
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 20 not upgraded.
student@student-H81H3-I:~$ ;2-
```

2.2 Configure the BIND9 Server :

student@student-H81H3-I:~\$ sudo gedit /etc/bind/named.conf.options



The screenshot shows a Gedit text editor window titled "named.conf.options (/etc/bind) - gedit". The file contains the following configuration code for a BIND9 nameserver:

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

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

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

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

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

};
```

The status bar at the bottom of the window shows "Plain Text" and "Tab Width: 8".

2.3 Start DNS server :

```
student@student-H81H3-I:~$ sudo service bind9 restart
student@student-H81H3-I:~$ █
```

Observation 3:

Now, go back to your user machine (10.2.22.195), and ping a computer such as www.google.com and describe your observation. Please use Wireshark to show the DNS query triggered by your ping command. Please also indicate when the DNS cache is used. (Take a screenshot).

Capturing from any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|------------|-------------|----------|--------|-----------------------------------------------------------------------------------------------------------------------------|
| 10 | 3.058121597 | 10.1.10.61 | 10.1.10.26 | DNS | 76 | Standard query 0xddc3 A www.google.com |
| 11 | 3.058133284 | 10.1.10.61 | 10.1.10.26 | DNS | 76 | Standard query 0xbde8 AAAA www.google.com |
| 12 | 3.058306784 | 10.1.10.26 | 10.1.10.61 | DNS | 352 | Standard query response 0x8de8 AAAA www.google.com AAAA 2404:6800:4007:823::2004 NS ns2.google.com |
| 13 | 3.058398957 | 10.1.10.26 | 10.1.10.61 | DNS | 348 | Standard query response 0xddc3 A www.google.com A 142.250.195.68 NS ns4.google.com NS ns2.google.com |
| 48 | 3.298751957 | 10.1.10.61 | 10.1.10.26 | DNS | 76 | Standard query 0x7829 A www.google.com |
| 49 | 3.298762951 | 10.1.10.61 | 10.1.10.26 | DNS | 76 | Standard query 0xb235 AAAA www.google.com |
| 50 | 3.299802135 | 10.1.10.26 | 10.1.10.61 | DNS | 352 | Standard query response 0xb235 AAAA www.google.com AAAA 2404:6800:4007:823::2004 NS ns3.google.com |
| 51 | 3.299822454 | 10.1.10.26 | 10.1.10.61 | DNS | 348 | Standard query response 0x7829 A www.google.com A 142.250.195.68 NS ns2.google.com NS ns1.google.com |
| 71 | 3.325306784 | 10.1.10.61 | 10.1.10.26 | DNS | 76 | Standard query 0xb235 AAAA www.google.com |
| 72 | 3.325308492 | 10.1.10.61 | 10.1.10.26 | DNS | 76 | Standard query 0xddc3 AAAA www.google.com |
| 73 | 3.325564732 | 10.1.10.26 | 10.1.10.61 | DNS | 348 | Standard query response 0x5f2f A www.google.com AAAA 2404:6800:4007:823::2004 NS ns4.google.com NS ns1.google.com |
| 74 | 3.325532326 | 10.1.10.26 | 10.1.10.61 | DNS | 352 | Standard query response 0xddc3 AAAA www.google.com AAAA 2404:6800:4007:823::2004 NS ns3.google.com |
| 76 | 3.330753733 | 10.1.10.61 | 10.1.10.26 | DNS | 77 | Standard query 0xf99 A www.gstatic.com |
| 77 | 3.330761183 | 10.1.10.61 | 10.1.10.26 | DNS | 77 | Standard query 0x8136 AAAA www.gstatic.com |
| 80 | 3.337558544 | 10.1.10.61 | 10.1.10.26 | DNS | 76 | Standard query 0x8dff A www.google.com |
| 81 | 3.337561528 | 10.1.10.61 | 10.1.10.26 | DNS | 76 | Standard query 0xcd23 AAAA www.google.com |
| 82 | 3.337726873 | 10.1.10.26 | 10.1.10.61 | DNS | 340 | Standard query response 0x8dff A www.google.com A 142.250.195.68 NS ns4.google.com NS ns3.google.com |
| 83 | 3.337755177 | 10.1.10.26 | 10.1.10.61 | DNS | 352 | Standard query response 0xcd23 AAAA www.google.com AAAA 2404:6800:4007:823::2004 NS ns1.google.com |
| 95 | 3.473603889 | 10.1.10.26 | 10.1.10.61 | DNS | 360 | Standard query response 0x8136 AAAA www.gstatic.com AAAA 2404:6800:4007:82c::2003 NS ns4.google.com |
| 96 | 3.495263099 | 10.1.10.61 | 10.1.10.26 | DNS | 77 | Standard query 0xe0c A apis.google.com |
| 97 | 3.495269316 | 10.1.10.61 | 10.1.10.26 | DNS | 77 | Standard query 0x3af1 AAAA apis.google.com |
| 102 | 3.536625091 | 10.1.10.26 | 10.1.10.61 | DNS | 362 | Standard query response 0xee0e A apis.google.com CNAME plus.l.google.com A 142.250.182.78 NS ns1.google.com |
| 103 | 3.537094633 | 10.1.10.26 | 10.1.10.61 | DNS | 374 | Standard query response 0x3af1 AAAA apis.google.com CNAME plus.l.google.com AAAA 2404:6800:4007:823::2004 NS ns4.google.com |
| 104 | 3.538156844 | 10.1.10.61 | 10.1.10.26 | DNS | 76 | Standard query 0xc755 A www.google.com |
| 105 | 3.538157034 | 10.1.10.61 | 10.1.10.26 | DNS | 76 | Standard query 0xbdf2 AAAA www.google.com |
| 106 | 3.538572410 | 10.1.10.26 | 10.1.10.61 | DNS | 352 | Standard query response 0x0df2 AAAA www.google.com AAAA 2404:6800:4007:823::2004 NS ns4.google.com |
| 107 | 3.538579594 | 10.1.10.26 | 10.1.10.61 | DNS | 349 | Standard query response 0xc755 A www.google.com A 142.250.195.68 NS ns4.google.com NS ns3.google.com |
| 109 | 3.542975787 | 10.1.10.61 | 10.1.10.26 | DNS | 76 | Standard query 0x8d04 A www.google.com |
| 110 | 3.542981852 | 10.1.10.61 | 10.1.10.26 | DNS | 76 | Standard query 0xbdf8 AAAA www.google.com |
| 111 | 3.543257492 | 10.1.10.26 | 10.1.10.61 | DNS | 352 | Standard query response 0xbdf8 AAAA www.google.com AAAA 2404:6800:4007:823::2004 NS ns3.google.com |
| 112 | 3.543288656 | 10.1.10.26 | 10.1.10.61 | DNS | 349 | Standard query response 0x8d04 A www.google.com A 142.250.195.68 NS ns2.google.com NS ns4.google.com |
| 116 | 3.551410661 | 10.1.10.61 | 10.1.10.26 | DNS | 76 | Standard query 0xd0fb A www.google.com |
| 117 | 3.551417161 | 10.1.10.61 | 10.1.10.26 | DNS | 76 | Standard query 0xca14 AAAA www.google.com |
| 119 | 3.551750681 | 10.1.10.26 | 10.1.10.61 | DNS | 352 | Standard query response 0xca14 AAAA www.google.com AAAA 2404:6800:4007:823::2004 NS ns3.google.com |
| 120 | 3.551778451 | 10.1.10.26 | 10.1.10.61 | DNS | 349 | Standard query response 0xd0fb A www.google.com A 142.250.195.68 NS ns3.google.com NS ns2.google.com |
| 139 | 3.692985179 | 10.1.10.61 | 10.1.10.26 | DNS | 76 | Standard query 0xdfc4 A www.google.com |
| 140 | 3.692991236 | 10.1.10.61 | 10.1.10.26 | DNS | 76 | Standard query 0x1b1 AAAA www.google.com |
| 141 | 3.692540359 | 10.1.10.26 | 10.1.10.61 | DNS | 352 | Standard query response 0x71b1 AAAA www.google.com AAAA 2404:6800:4007:823::2004 NS ns4.google.com |
| 142 | 3.692544648 | 10.1.10.26 | 10.1.10.61 | DNS | 348 | Standard query response 0xdfcb A www.google.com A 142.250.195.68 NS ns1.google.com NS ns4.google.com |
| 143 | 3.693047749 | 10.1.10.61 | 10.1.10.26 | DNS | 76 | Standard query 0x832a A www.google.com |
| 144 | 3.6930851525 | 10.1.10.61 | 10.1.10.26 | DNS | 76 | Standard query 0xc56a AAAA www.google.com |

0000 00 00 01 00 06 b8 ae ed a5 a6 71 00 00 08 00 q . . .
0010 45 00 00 44 42 db 00 00 40 11 0e 76 0a 01 0a 3d E . < . @ . @ Y . . . =
0020 0a 01 0a 1a 89 73 00 35 00 28 e1 31 dd c3 01 00 . . . s . 5 . (. 1 . . .

Packets: 2321 · Displayed: 84 (3.6%)

Profile: Default

Wireshark · Packet 10 · any

Frame 10: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0

Linux cooked capture

Internet Protocol Version 4, Src: 10.1.10.61, Dst: 10.1.10.26

User Datagram Protocol, Src Port: 35187, Dst Port: 53

Source Port: 35187
Destination Port: 53
Length: 40
Checksum: 0xe131 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]

Domain Name System (query)
Transaction ID: 0xddc3
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0

Queries
www.google.com: type A, class IN
[Response In: 13]

0000 00 04 00 01 00 06 b8 ae ed a5 a6 71 00 00 08 00 q . . .
0010 45 00 00 3c b8 d0 40 00 40 11 59 88 0a 01 0a 3d E . < . @ . @ Y . . . =
0020 0a 01 0a 1a 89 73 00 35 00 28 e1 31 dd c3 01 00 . . . s . 5 . (. 1 . . .

Close Help

```
Frame 13: 340 bytes on wire (2720 bits), 340 bytes captured (2720 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.1.10.26, Dst: 10.1.10.61
User Datagram Protocol, Src Port: 53, Dst Port: 35187
Domain Name System (response)
    Transaction ID: 0xddc3
    Flags: 0x8100 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 4
    Additional RRs: 8
    Queries
        www.google.com: type A, class IN
    Answers
        www.google.com: type A, class IN, addr 142.250.195.68
    Authoritative nameservers
        google.com: type NS, class IN, ns ns4.google.com
        google.com: type NS, class IN, ns ns2.google.com
        google.com: type NS, class IN, ns ns3.google.com
        google.com: type NS, class IN, ns ns1.google.com
    Additional records
        ns1.google.com: type A, class IN, addr 216.239.32.10
        ns1.google.com: type AAAA, class IN, addr 2001:4860:4802:32::a
        ns2.google.com: type A, class IN, addr 216.239.34.10
        ns2.google.com: type AAAA, class IN, addr 2001:4860:4802:34::a
        ns3.google.com: type A, class IN, addr 216.239.36.10
        ns3.google.com: type AAAA, class IN, addr 2001:4860:4802:36::a
        ns4.google.com: type A, class IN, addr 216.239.38.10
        ns4.google.com: type AAAA, class IN, addr 2001:4860:4802:38::a
[Request In: 10]
[Time: 0.000276460 seconds]
```

Observation 4:

The two commands shown below are related to DNS cache. The first command dumps the content of the cache to the file specified above, and the second command clears the cache. You need extract the DNS cache using 'grep' command and take screenshot of www.google.com DNS cache.

```
student@student-H81H3-I:~$ sudo rndc dumpdb -cache
student@student-H81H3-I:~$ sudo rndc flush
student@student-H81H3-I:~$ █
```

DNS Cache using 'grep' command:

```
student@student-H81H3-I:~  
** (gedit:3309): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported  
^C  
student@student-H81H3-I:~$ sudo rndc flush  
student@student-H81H3-I:~$ sudo rndc dumpdb -cache  
student@student-H81H3-I:~$ grep google.com "/var/cache/bind/named_dump.db"  
grep: /var/cache/bind/named_dump.db: No such file or directory  
student@student-H81H3-I:~$ grep google.com "/var/cache/bind/dump.db"  
student@student-H81H3-I:~$ sudo rndc flush  
student@student-H81H3-I:~$ sudo rndc dumpdb -cache  
student@student-H81H3-I:~$ grep google.com "/var/cache/bind/dump.db"  
google.com. 172794 NS ns1.google.com.  
google.com. 172794 NS ns2.google.com.  
google.com. 172794 NS ns3.google.com.  
google.com. 172794 NS ns4.google.com.  
adservice.google.com. 296 A 142.250.205.226  
apis.google.com. 604796 CNAME plus.l.google.com.  
plus.l.google.com. 296 A 142.250.182.110  
ns1.google.com. 172794 A 216.239.32.10  
ns2.google.com. 172794 A 216.239.34.10  
ns3.google.com. 172794 A 216.239.36.10  
ns4.google.com. 172794 A 216.239.38.10  
www.google.com. 296 A 142.250.195.68  
gstatic.com. 172795 NS ns1.google.com.  
gstatic.com. 172795 NS ns2.google.com.  
gstatic.com. 172795 NS ns3.google.com.  
gstatic.com. 172795 NS ns4.google.com.  
google.co.in. 86395 NS ns1.google.com.  
google.co.in. 86395 NS ns2.google.com.  
google.co.in. 86395 NS ns3.google.com.  
google.co.in. 86395 NS ns4.google.com.  
doubleclick.net. 172796 NS ns1.google.com.  
doubleclick.net. 172796 NS ns2.google.com.  
doubleclick.net. 172796 NS ns3.google.com.  
doubleclick.net. 172796 NS ns4.google.com.  
; ns3.google.com [v4 TTL 5] [v6 TTL 5] [v4 success] [v6 success]  
; ns3.google.com [v4 TTL 4] [v6 TTL 4] [v4 success] [v6 success]  
; ns1.google.com [v4 TTL 5] [v6 TTL 5] [v4 success] [v6 success]  
; ns1.google.com [v4 TTL 4] [v6 TTL 4] [v4 success] [v6 success]  
; ns4.google.com [v4 TTL 5] [v6 TTL 5] [v4 success] [v6 success]  
; ns4.google.com [v4 TTL 4] [v6 TTL 4] [v4 success] [v6 success]  
; ns2.google.com [v4 TTL 5] [v6 TTL 5] [v4 success] [v6 success]  
; ns2.google.com [v4 TTL 4] [v6 TTL 4] [v4 success] [v6 success]  
student@student-H81H3-I:~$
```

Part 2: Setting Up an Authoritative Nameserver for example.com domain

Task 3: Host a Zone in the Local DNS server.

3.1 Create Zones :

```
student@student-H81H3-I:~$ sudo nano /etc/bind/named.conf  
student@student-H81H3-I:~$ 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 "10.1.10.in-addr.arpa" {  
    type master;  
    file "/etc/bind/10.1.10.db";  
};  
student@student-H81H3-I:~$
```

3.2 Setup the forward lookup zone file :



```
$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 10.1.10.101
mail IN A 10.1.10.102
ns IN A 10.1.10.10
*.example.com. IN A 10.1.10.100
```

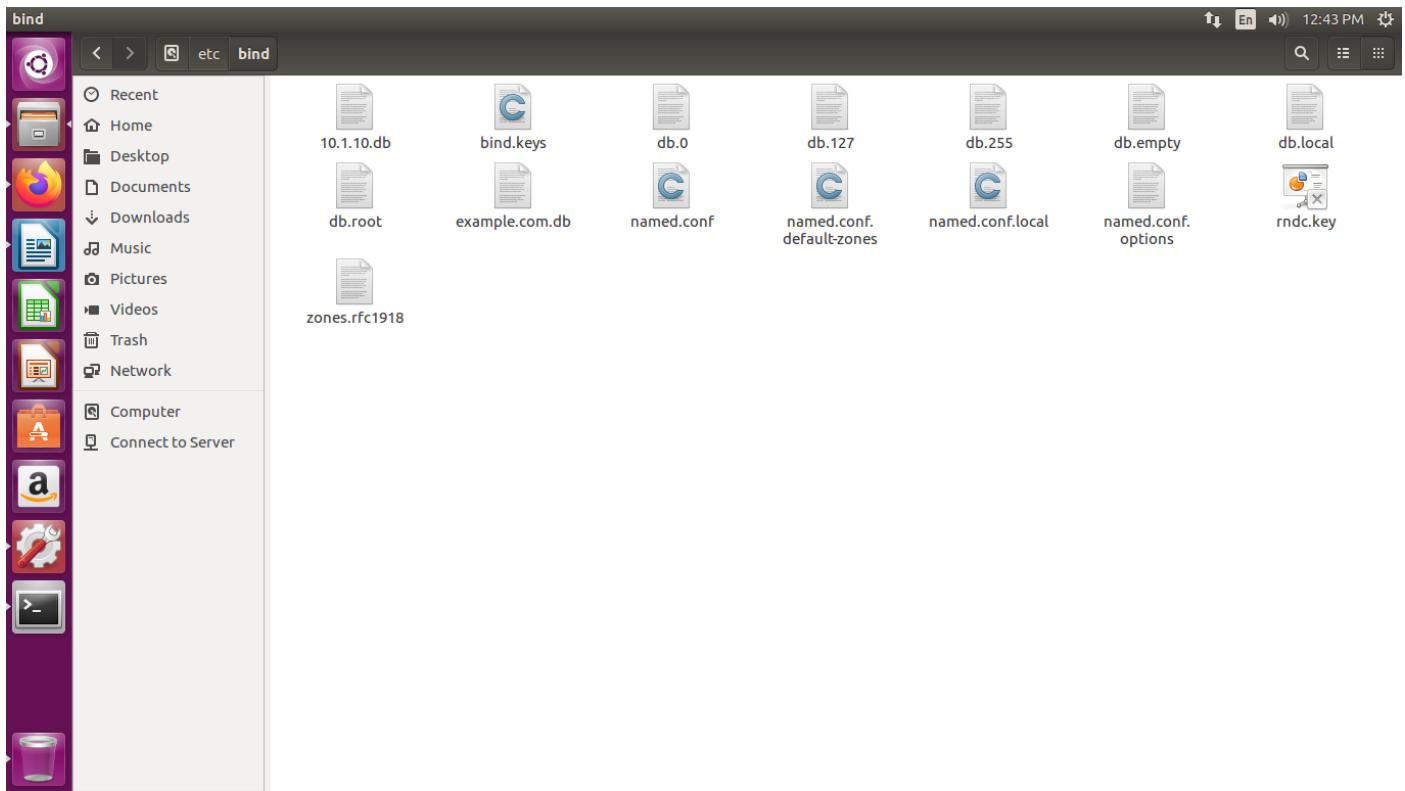
The screenshot shows a terminal window titled "example.com.db" displaying a forward DNS zone file. The file contains records for the domain example.com, including an SOA record, an NS record pointing to ns.example.com, an MX record for mail.example.com, an A record for the www subdomain, an A record for the mail subdomain, an A record for the ns subdomain, and a wildcard A record for *.example.com.

3.3 Setup the reverse lookup zone file :



```
$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.
```

The screenshot shows a terminal window titled "10.1.10.db" displaying a reverse DNS zone file. The file contains PTR records for the IP addresses 10.1.10.101, 10.1.10.102, and 10.1.10.10, all pointing to their respective subdomains www.example.com, mail.example.com, and ns.example.com.



Task 4: Restart the BIND server and test

4.1 When all the changes are made, remember to restart the BIND server. Now we will restart the DNS server using the following command:

```
student@student-H81H3-I:~$ sudo service bind9 restart  
student@student-H81H3-I:~$
```

4.2 Now, go back to the client machine and ask the local DNS server for the IP address of www.example.com using the dig command.

```
student@student@localhost: ~  
student@student@localhost:~$ sudo nano /etc/resolvconf/resolv.conf.d/head  
student@student@localhost:~$ dig www.example.com  
  
; <>> DiG 9.10.3-P4-Ubuntu <>> www.example.com  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 48415  
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2  
  
;; OPT PSEUDOSECTION:  
;; EDNS: version: 0, flags:; udp: 4096  
;; QUESTION SECTION:  
;www.example.com. IN A  
  
;; ANSWER SECTION:  
www.example.com. 259200 IN A 192.168.0.101  
  
;; AUTHORITY SECTION:  
example.com. 259200 IN NS ns.example.com.  
  
;; ADDITIONAL SECTION:  
ns.example.com. 259200 IN A 192.168.0.10  
  
;; Query time: 0 msec  
;; SERVER: 10.1.10.107#53(10.1.10.107)  
;; WHEN: Thu Mar 03 12:51:10 IST 2022  
;; MSG SIZE rcvd: 93  
  
student@student@localhost:~$
```

4.3 Observe the results in Wireshark capture :

Capturing from any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|-------------------------|-------------|----------|--------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| 1 | 0.000000000 | Elitegro_a5.. | | ARP | 62 | Who has 10.1.10.192? Tell 10.1.10.70 |
| 2 | 0.077706811 | Elitegro_a5.. | | ARP | 62 | Who has 10.1.10.113? Tell 10.1.10.55 |
| 3 | 0.606856937 | Elitegro_a5.. | | ARP | 62 | Who has 10.1.10.160? Tell 10.1.10.164 |
| 4 | 1.103791282 | Elitegro_a5.. | | ARP | 62 | Who has 10.1.10.113? Tell 10.1.10.55 |
| 5 | 1.108863657 | fe80::d6ce:... ff02::fb | MDNS | 135 | Standard query 0x0000 SRV UBUNTU18.04._smb._tcp.local, "QM" question SRV 0 0 445 linux.local | |
| 6 | 1.438893771 | Elitegro_a5.. | | ARP | 62 | Who has 10.1.10.95? Tell 10.1.10.164 |
| 7 | 1.630862452 | Elitegro_a5.. | | ARP | 62 | Who has 10.1.10.160? Tell 10.1.10.164 |
| 8 | 1.950873405 | Elitegro_a5.. | | ARP | 62 | Who has 10.1.10.102? Tell 10.1.10.164 |
| 9 | 2.462853856 | Elitegro_a5.. | | ARP | 62 | Who has 10.1.10.95? Tell 10.1.10.164 |
| 10 | 2.654979282 | Elitegro_a5.. | | ARP | 62 | Who has 10.1.10.160? Tell 10.1.10.164 |
| 11 | 2.974846994 | Elitegro_a5.. | | ARP | 62 | Who has 10.1.10.102? Tell 10.1.10.164 |
| 12 | 3.486861388 | Elitegro_a5.. | | ARP | 62 | Who has 10.1.10.95? Tell 10.1.10.164 |
| 13 | 3.678827181 | Elitegro_a5.. | | ARP | 62 | Who has 10.1.10.160? Tell 10.1.10.164 |
| 14 | 3.998845769 | Elitegro_a5.. | | ARP | 62 | Who has 10.1.10.102? Tell 10.1.10.164 |
| 15 | 4.702859240 | Elitegro_a5.. | | ARP | 62 | Who has 10.1.10.160? Tell 10.1.10.164 |
| 16 | 5.726961777 | Elitegro_a5.. | | ARP | 62 | Who has 10.1.10.160? Tell 10.1.10.164 |
| 17 | 5.857556219 | 127.0.0.1 | 127.0.0.1 | UDP | 76 | 47314 - 47314 Len=32 |
| 18 | 5.870002912 | 127.0.0.1 | 127.0.0.1 | UDP | 68 | 47314 - 47314 Len=24 |
| 19 | 5.873012546 | 127.0.0.1 | 127.0.0.1 | UDP | 76 | 47314 - 47314 Len=32 |
| 20 | 5.883849880 | 127.0.0.1 | 127.0.0.1 | UDP | 988 | 47314 - 47314 Len=936 |
| 21 | 5.883874139 | 127.0.0.1 | 127.0.0.1 | UDP | 420 | 47314 - 47314 Len=376 |
| 22 | 5.883889968 | 127.0.0.1 | 127.0.0.1 | UDP | 532 | 47314 - 47314 Len=488 |
| 23 | 6.750870962 | Elitegro_a5.. | | ARP | 62 | Who has 10.1.10.160? Tell 10.1.10.164 |
| 24 | 7.725613016 | 127.0.0.1 | 127.0.0.1 | UDP | 45 | 54649 - 54649 Len=1 |
| 25 | 7.725644565 | ::1 | ::1 | UDP | 65 | 50869 - 50869 Len=1 |
| 26 | 7.725681867 | 10.1.10.47 | 10.1.10.107 | DNS | 88 | Standard query 0xd993 A www.example.com OPT |
| 27 | 7.726215071 | 10.1.10.107 | 10.1.10.47 | DNS | 137 | Standard query response 0xd993 A www.example.com A 10.1.10.101 NS ns.example.com A 10.1.10.10 OPT |
| 28 | 7.774792702 | Elitegro_a5.. | | ARP | 62 | Who has 10.1.10.160? Tell 10.1.10.164 |
| 29 | 8.606872473 | Elitegro_a5.. | | ARP | 62 | Who has 10.1.10.102? Tell 10.1.10.164 |
| 30 | 8.798931641 | Elitegro_a5.. | | ARP | 62 | Who has 10.1.10.160? Tell 10.1.10.164 |
| 31 | 8.924744509 | 10.1.10.149 | 224.0.0.251 | MDNS | 115 | Standard query 0x0000 SRV UBUNTU18.04._smb._tcp.local, "QM" question SRV 0 0 445 linux.local |
| 32 | 9.401111944 | fe80::862f:ff02::fb | MDNS | 227 | Standard query 0x0000 PTR _ftp._tcp.local, "QM" question TXT UBUNTU18.04._smb._tcp.local, "QM" question PTR _nfs.. | |
| 33 | 9.461235246 | 10.1.10.24 | 224.0.0.251 | MDNS | 207 | Standard query 0x0000 PTR _ftp._tcp.local, "QM" question TXT UBUNTU18.04._smb._tcp.local, "QM" question PTR _nfs.. |
| 34 | 9.630836266 | Elitegro_a5.. | | ARP | 62 | Who has 10.1.10.192? Tell 10.1.10.164 |
| 35 | 9.822817233 | Elitegro_a5.. | | ARP | 62 | Who has 10.1.10.160? Tell 10.1.10.164 |
| 36 | 10.654849795 | Elitegro_a5.. | | ARP | 62 | Who has 10.1.10.102? Tell 10.1.10.164 |

Frame 33: 207 bytes on wire (1656 bits), 207 bytes captured (1656 bits) on interface 0

Linux cooked capture

Internet Protocol Version 4, Src: 10.1.10.24, Dst: 224.0.0.251

User Datagram Protocol, Src Port: 5353, Dst Port: 5353

Multicast Domain Name System (query)

0000 00 02 00 01 00 b8 ae ed a5 97 00 00 08 00

0010 45 00 00 bf df dc 40 00 ff 11 c6 3c 0a 01 0a 18 E

any any <live capture in progress> Packets: 51 · Displayed: 51 (100.0%) Profile: Default

*any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

Frame 27: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits) on interface 0

Linux cooked capture

Internet Protocol Version 4, Src: 10.1.10.107, Dst: 10.1.10.47

User Datagram Protocol, Src Port: 53, Dst Port: 43079

Domain Name System (response)

Transaction ID: 0xd993

Flags: 0x8580 Standard query response, No error

- 1.... = Response: Message is a response
- .000 0.... = Opcode: Standard query (0)
-1.... = Authoritative: Server is an authority for domain
-0.... = Truncated: Message is not truncated
-1.... = Recursion desired: Do query recursively
-1.... = Recursion available: Server can do recursive queries
-0.... = Z: reserved (0)
-0.... = Answer authenticated: Answer/authority portion was not authenticated by the server
-0.... = Non-authenticated data: Unacceptable
-0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 1

Authority RRs: 1

Additional RRs: 2

Queries

Answers

- www.example.com: type A, class IN, addr 10.1.10.101
 - Name: www.example.com
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)
 - Time to live: 259200
 - Data length: 4
 - Address: 10.1.10.101
- Authoritative nameservers
 - example.com: type NS, class IN, ns ns.example.com
 - Name: example.com
 - Type: NS (Authoritative Name Server) (2)
 - Class: IN (0x0001)
 - Time to live: 259200
 - Data length: 5
 - Name Server: ns.example.com
- Additional records
 - ns.example.com: type A, class IN, addr 10.1.10.10
 - Name: ns.example.com
 - Type: A (Host Address) (1)

0070 00 01 00 01 00 03 f4 80 00 04 0a 01 0a 0a 00 00

0080 29 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Response Class (dns.resp.class), 2 bytes Packets: 160 · Displayed: 160 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

4.4 DNS cache on server machine after dig command :

```
student@localhost:~  
** (gedit:29089): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported  
student@localhost:~$ sudo cat /var/cache/bind/named_dump.db  
sudo: CAT: command not found  
student@localhost:~$ sudo cat /var/cache/bind/named_dump.db  
;  
; Start view _default  
;  
; Cache dump of view '_default' (cache _default)  
$DATE 20220303065554  
; secure  
.  
      518357 IN NS  a.root-servers.net.  
      518357 IN NS  b.root-servers.net.  
      518357 IN NS  c.root-servers.net.  
      518357 IN NS  d.root-servers.net.  
      518357 IN NS  e.root-servers.net.  
      518357 IN NS  f.root-servers.net.  
      518357 IN NS  g.root-servers.net.  
      518357 IN NS  h.root-servers.net.  
      518357 IN NS  i.root-servers.net.  
      518357 IN NS  j.root-servers.net.  
      518357 IN NS  k.root-servers.net.  
      518357 IN NS  l.root-servers.net.  
      518357 IN NS  m.root-servers.net.  
; secure  
      518394 RRSIG  NS 0 518400 (  
          20220316050000 20220303040000 9799 .  
          WHZ//zKRCr0aFze+haFlCSa0GwaCwCsopDKM  
          LzMr0TTvejeb96R01h+2mLnsd4qtvrbop0a  
          7FBz+Vs/m+YVOPku+vCO/fnZ+NW/KgrtxPho  
          PopeEWayXrfwtEC+Iu/G7gD1bePihXqeEMSYL  
          fLD84g7ezASexC4q3Yrfw3+sSnKkc/vwlZ3I  
          FcSw90bqyYoV597fRLZYdEoUzDjp9onU/Ncw  
          qnWJ6muVMs2107kHtaUFM07z6ngf5PGC2yLT  
          ywz+4WZLFd6t80vZypEMGFwPSxJ2W865dh2Q  
          JSdznh3V5CFW3tW+s9ZzKsJHuGlHTwqem+eg  
          ipZMx0Mu9y+F08ZVlg== )  
; secure  
      172757 DNSKEY 256 3 8 (  
          AwEAAZym4HCWiTAAl2MviizgTyn9sKwg5eB  
          xpG29bVlefq/r+TGctmUElvFyBWHRjvf9mBg
```

Observation Notebook Requirements:

For 'ping www.flipkart.com', answer the following questions

1) Locate the DNS query and response messages. Are then sent over UDP or TCP?

→ DNS Query 0x7939. It uses UDP Protocol.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------------------------|---------------|---------------|----------|--------|---------------------------------------------------|
| 6 | 2022-03-11 03:08:38.0251523... | 10.0.2.15 | 172.16.10.1 | DNS | 78 | Standard query 0x7939 A www.flipkart.com |
| 7 | 2022-03-11 03:08:43.0306997... | 127.0.0.1 | 127.0.1.1 | DNS | 78 | Standard query 0x7939 A www.flipkart.com |
| 8 | 2022-03-11 03:08:43.0308119... | 10.0.2.15 | 192.168.0.177 | DNS | 78 | Standard query 0x4f71 A www.flipkart.com |
| 9 | 2022-03-11 03:08:43.0308516... | 10.0.2.15 | 172.16.10.1 | DNS | 78 | Standard query 0x4f71 A www.flipkart.com |
| 12 | 2022-03-11 03:08:43.3897749... | 192.168.0.177 | 10.0.2.15 | DNS | 108 | Standard query response 0x4f71 A www.flipkart... |
| 13 | 2022-03-11 03:08:43.3899461... | 127.0.1.1 | 127.0.0.1 | DNS | 108 | Standard query response 0x7939 A www.flipkart... |
| 80 | 2022-03-11 03:09:40.7291465... | 10.0.2.15 | 172.16.10.1 | DNS | 88 | Standard query 0x1cc2 PTR 177.0.168.192.in-add... |
| 81 | 2022-03-11 03:09:45.7343521... | 127.0.0.1 | 127.0.1.1 | DNS | 88 | Standard query 0x1cc2 PTR 177.0.168.192.in-add... |
| 82 | 2022-03-11 03:09:45.7344468... | 10.0.2.15 | 192.168.0.177 | DNS | 88 | Standard query 0x3504 PTR 177.0.168.192.in-add... |
| 83 | 2022-03-11 03:09:45.7344845... | 10.0.2.15 | 172.16.10.1 | DNS | 88 | Standard query 0x3504 PTR 177.0.168.192.in-add... |
| 84 | 2022-03-11 03:09:45.8506324... | 192.168.0.177 | 10.0.2.15 | DNS | 147 | Standard query response 0x3504 No such name PT... |
| 85 | 2022-03-11 03:09:45.8507767... | 127.0.1.1 | 127.0.0.1 | DNS | 147 | Standard query response 0x1cc2 No such name PT... |
| 88 | 2022-03-11 03:09:45.8900102... | 10.0.2.15 | 172.16.10.1 | DNS | 88 | Standard query 0x366d PTR 110.78.53.163.in-add... |
| 89 | 2022-03-11 03:09:50.8902723... | 127.0.0.1 | 127.0.1.1 | DNS | 88 | Standard query 0x366d PTR 110.78.53.163.in-add... |
| 90 | 2022-03-11 03:09:50.8903663... | 10.0.2.15 | 192.168.0.177 | DNS | 88 | Standard query 0x2bbe PTR 110.78.53.163.in-add... |
| 91 | 2022-03-11 03:09:50.9344576... | 192.168.0.177 | 10.0.2.15 | DNS | 176 | Standard query response 0x2bbe No such name PT... |
| 92 | 2022-03-11 03:09:50.9346007... | 127.0.1.1 | 127.0.0.1 | DNS | 176 | Standard query response 0x366d No such name PT... |
| 251 | 2022-03-11 03:11:17.6176104... | 10.0.2.15 | 172.16.10.1 | DNS | 83 | Standard query 0x7d3e PTR 2.2.0.10.in-addr.arpa |
| 253 | 2022-03-11 03:11:22.6232092... | 127.0.0.1 | 127.0.1.1 | DNS | 83 | Standard query 0x7d3e PTR 2.2.0.10.in-addr.arpa |
| 254 | 2022-03-11 03:11:22.6233030... | 10.0.2.15 | 192.168.0.177 | DNS | 83 | Standard query 0x2b95 PTR 2.2.0.10.in-addr.arpa |
| 255 | 2022-03-11 03:11:22.6233384... | 10.0.2.15 | 172.16.10.1 | DNS | 83 | Standard query 0x2b95 PTR 2.2.0.10.in-addr.arpa |
| 258 | 2022-03-11 03:11:27.6283840... | 10.0.2.15 | 172.16.10.1 | DNS | 83 | Standard query 0x7d3e PTR 2.2.0.10.in-addr.arpa |
| 263 | 2022-03-11 03:11:32.6301704... | 127.0.0.1 | 127.0.1.1 | DNS | 83 | Standard query 0x7d3e PTR 2.2.0.10.in-addr.arpa |
| | | 10.0.2.15 | 192.168.0.177 | DNS | 83 | Standard query 0x2b95 PTR 2.2.0.10.in-addr.arpa |

```

▶ Frame 6: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
▶ Linux cooked capture
▼ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 172.16.10.1
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 62
  Identification: 0x690b (26891)
  Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 64
  Protocol: UDP (17)
  Header checksum: 0x0f84 [validation disabled]
  [Header checksum status: Unverified]
  Source: 10.0.2.15
  Destination: 172.16.10.1
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
▼ User Datagram Protocol, Src Port: 35612, Dst Port: 53
  Source Port: 35612
  Destination Port: 53
  Length: 42
  Checksum: 0xc25b [unverified]
  [Checksum Status: Unverified]
  [Stream index: 3]
▶ Domain Name System (query)

```

2) What is the destination port for the DNS query message? What is the source port of DNS response message?

→ Destination port for the DNS query message : 172.16.10.1

Source port of DNS response message : 127.0.1.1

3) To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

→ The DNS Query is sent to IP address 172.16.10.1. YES , both IP addresses are the same.

4) Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

→ Type of the Query is Standard. NO, it does not contain any answers.

```

▼ Domain Name System (query)
  Transaction ID: 0x7939
  ▼ Flags: 0x0100 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)
    .... ....0.... = Non-authenticated data: Unacceptable
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ 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)

```

5) Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

→ There are 2 answers provided.

- a. Canonical name for the given query
- b. IP address for the given query

```
▼ Domain Name System (response)
[Request In: 7]
[Time: 0.359246413 seconds]
Transaction ID: 0x7939
▼ Flags: 0x8180 Standard query response, No error
  1... .... .... = Response: Message is a response
  .000 0... .... .... = Opcode: Standard query (0)
  .... 0. .... .... = Authoritative: Server is not an authority for domain
  .... ..0. .... .... = Truncated: Message is not truncated
  .... ..1 .... .... = Recursion desired: Do query recursively
  .... .1... .... = Recursion available: Server can do recursive queries
  .... ..0. .... = Z: reserved (0)
  .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
  .... ..0. .... = Non-authenticated data: Unacceptable
  .... .... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
▼ 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
  ▶ flipkart.com: type A, class IN, addr 163.53.78.110
```

6) Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

→ NO