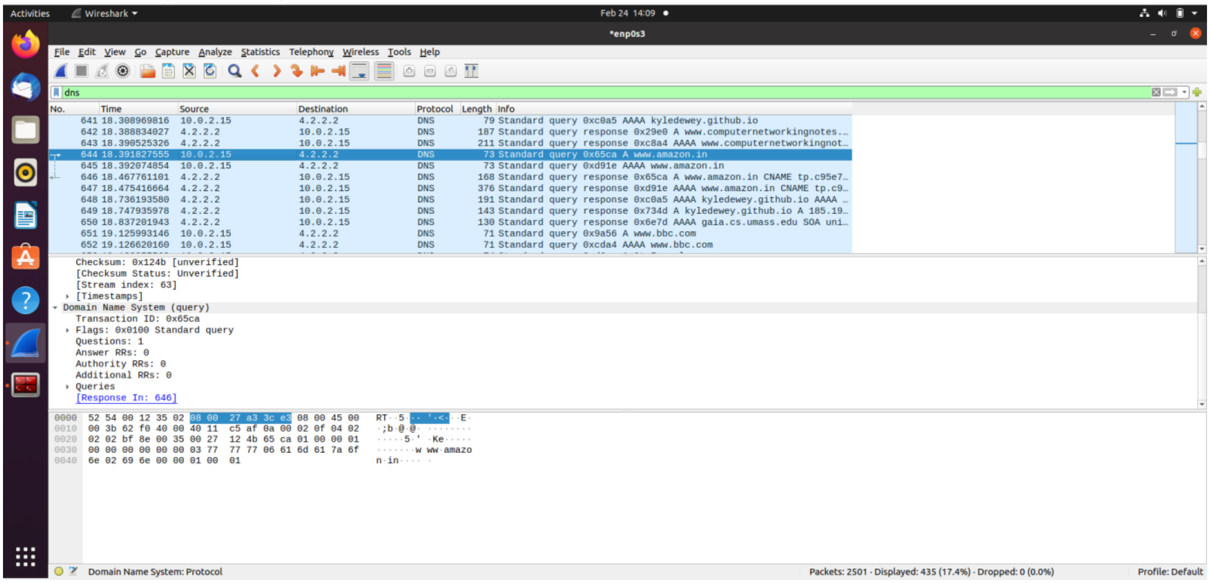
Week #4

Sriram R SRN : PES1UG20CS435 Section : H

Screenshots :

Observation 1 :


Activities
Wireshark
Feb 24 14:09
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
dns
```

```
No.  Time          Source      Destination  Protocol Length Info
 641 18.308969816  10.0.2.15   4.2.2.2      DNS       79 Standard query 0xc0a5 AAAA kyledewey.github.io
 642 18.388834027  4.2.2.2     10.0.2.15    DNS      187 Standard query response 0x29e0 A www.computernetworkingnotes.…
 643 18.390525326  4.2.2.2     10.0.2.15    DNS      211 Standard query response 0xc8a4 AAAA www.computernetworkingnot…
 644 18.391827555  10.0.2.15   4.2.2.2      DNS       73 Standard query 0x65ca A www.amazon.in
 645 18.392074854  10.0.2.15   4.2.2.2      DNS       73 Standard query 0xd91e AAAA www.amazon.in
 646 18.467761101  4.2.2.2     10.0.2.15    DNS      168 Standard query response 0x65ca A www.amazon.in CNAME tp.c95e7…
 647 18.475416664  4.2.2.2     10.0.2.15    DNS      376 Standard query response 0xd91e AAAA www.amazon.in CNAME tp.c9…
 648 18.736193580  4.2.2.2     10.0.2.15    DNS      191 Standard query response 0xc0a5 AAAA kyledewey.github.io AAAA …
 649 18.747935978  4.2.2.2     10.0.2.15    DNS      143 Standard query response 0x734d A kyledewey.github.io A 185.19…
 650 18.837201943  4.2.2.2     10.0.2.15    DNS      130 Standard query response 0x6e7d AAAA gaia.cs.umass.edu SOA uni…
 651 19.125993146  10.0.2.15   4.2.2.2      DNS       71 Standard query 0x9a56 A www.bbc.com
 652 19.126620160  10.0.2.15   4.2.2.2      DNS       71 Standard query 0xcda4 AAAA www.bbc.com
```

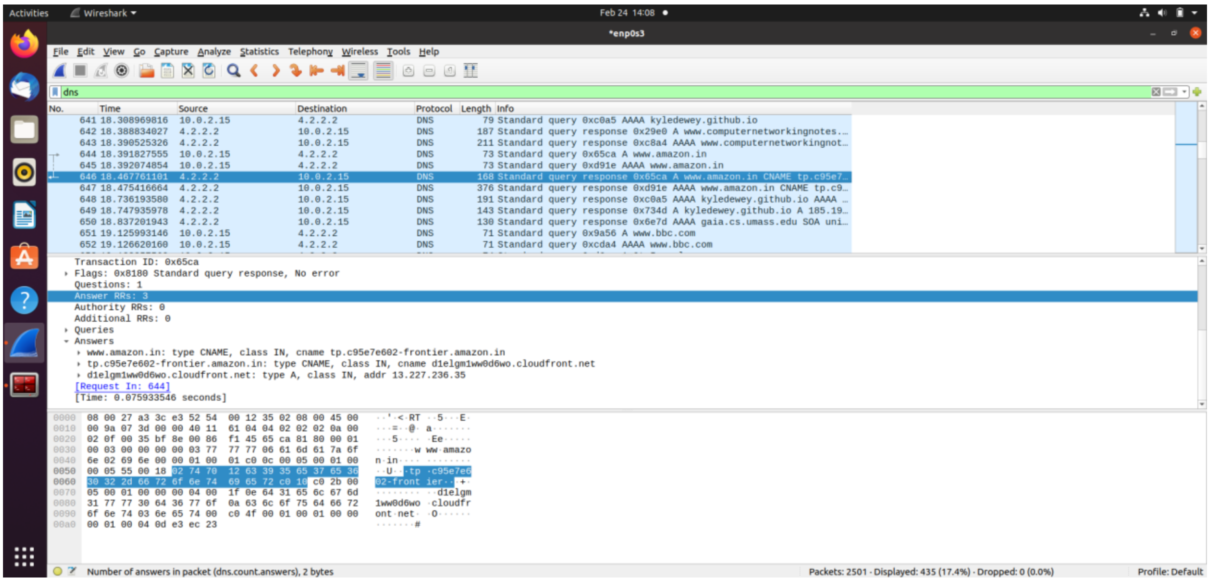
```
    Checksum: 0x124b [unverified]
    [Checksum Status: Unverified]
    [Stream index: 63]
  › [Timestamps]
⌄ Domain Name System (query)
    Transaction ID: 0x65ca
  › Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  › Queries
    [Response In: 646]
```

```
0000  52 54 00 12 35 02 08 00  27 a3 3c e3 08 00 45 00   RT··5··· '·<···E·
0010  00 3b 62 f0 40 00 40 11  c5 af 0a 00 02 0f 04 02   ·;b·@·@· ········
0020  02 02 bf 8e 00 35 00 27  12 4b 65 ca 01 00 00 01   ·····5·' ·Ke·····
0030  00 00 00 00 00 00 03 77  77 77 06 61 6d 61 7a 6f   ·······w ww·amazo
0040  6e 02 69 6e 00 00 01 00  01                        n·in···· ·
```

Domain Name System: Protocol

Packets: 2501 · Displayed: 435 (17.4%) · Dropped: 0 (0.0%)

Profile: Default


Activities
Wireshark
Feb 24 14:08
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
dns
```

```
No.  Time          Source      Destination  Protocol Length Info
 641 18.308969816  10.0.2.15   4.2.2.2      DNS       79 Standard query 0xc0a5 AAAA kyledewey.github.io
 642 18.388834027  4.2.2.2     10.0.2.15    DNS      187 Standard query response 0x29e0 A www.computernetworkingnotes.…
 643 18.390525326  4.2.2.2     10.0.2.15    DNS      211 Standard query response 0xc8a4 AAAA www.computernetworkingnot…
 644 18.391827555  10.0.2.15   4.2.2.2      DNS       73 Standard query 0x65ca A www.amazon.in
 645 18.392074854  10.0.2.15   4.2.2.2      DNS       73 Standard query 0xd91e AAAA www.amazon.in
 646 18.467761101  4.2.2.2     10.0.2.15    DNS      168 Standard query response 0x65ca A www.amazon.in CNAME tp.c95e7…
 647 18.475416664  4.2.2.2     10.0.2.15    DNS      376 Standard query response 0xd91e AAAA www.amazon.in CNAME tp.c9…
 648 18.736193580  4.2.2.2     10.0.2.15    DNS      191 Standard query response 0xc0a5 AAAA kyledewey.github.io AAAA …
 649 18.747935978  4.2.2.2     10.0.2.15    DNS      143 Standard query response 0x734d A kyledewey.github.io A 185.19…
 650 18.837201943  4.2.2.2     10.0.2.15    DNS      130 Standard query response 0x6e7d AAAA gaia.cs.umass.edu SOA uni…
 651 19.125993146  10.0.2.15   4.2.2.2      DNS       71 Standard query 0x9a56 A www.bbc.com
 652 19.126620160  10.0.2.15   4.2.2.2      DNS       71 Standard query 0xcda4 AAAA www.bbc.com
```

```
    Transaction ID: 0x65ca
  › Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  › Queries
  ⌄ Answers
    › www.amazon.in: type CNAME, class IN, cname tp.c95e7e602-frontier.amazon.in
    › tp.c95e7e602-frontier.amazon.in: type CNAME, class IN, cname d1elgm1ww0d6wo.cloudfront.net
    › d1elgm1ww0d6wo.cloudfront.net: type A, class IN, addr 13.227.236.35
    [Request In: 644]
    [Time: 0.075933546 seconds]
```

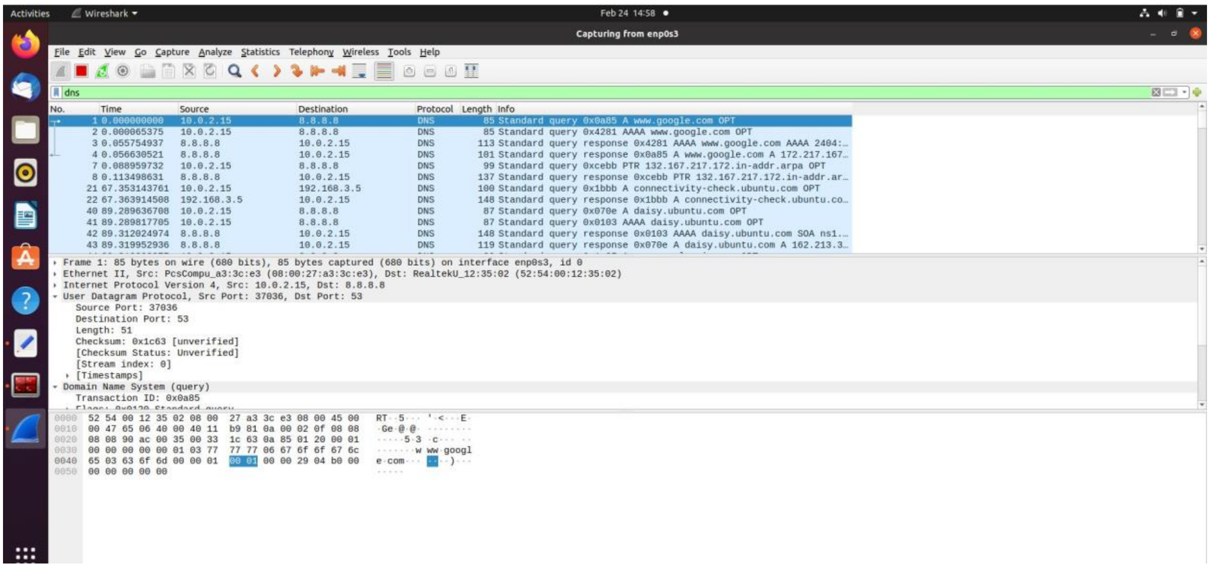
```
0000  08 00 27 a3 3c e3 52 54  00 12 35 02 08 00 45 00   ··'·<·RT ··5···E·
0010  00 9a 07 3d 00 00 40 11  61 04 04 02 02 02 0a 00   ···=··@· a·······
0020  02 0f 00 35 bf 8e 00 86  f1 45 65 ca 81 80 00 01   ···5···· ·Ee·····
0030  00 03 00 00 00 00 03 77  77 77 06 61 6d 61 7a 6f   ·······w ww·amazo
0040  6e 02 69 6e 00 00 01 00  01 c0 0c 00 05 00 01 00   n·in···· ········
0050  00 05 55 00 18 02 74 70  12 63 39 35 65 37 65 36   ··U···tp ·c95e7e6
0060  30 32 2d 66 72 6f 6e 74  69 65 72 c0 10 c0 2b 00   02-front ier···+·
0070  05 00 01 00 00 00 04 00  1f 0e 64 31 65 6c 67 6d   ········ ··d1elgm
0080  31 77 77 30 64 36 77 6f  0a 63 6c 6f 75 64 66 72   1ww0d6wo ·cloudfr
0090  6f 6e 74 03 6e 65 74 00  c0 4f 00 01 00 01 00 00   ont·net· ·O······
00a0  00 01 00 04 0d e3 ec 23                            ·······#
```

Number of answers in packet (dns.count.answers), 2 bytes

Packets: 2501 · Displayed: 435 (17.4%) · Dropped: 0 (0.0%)

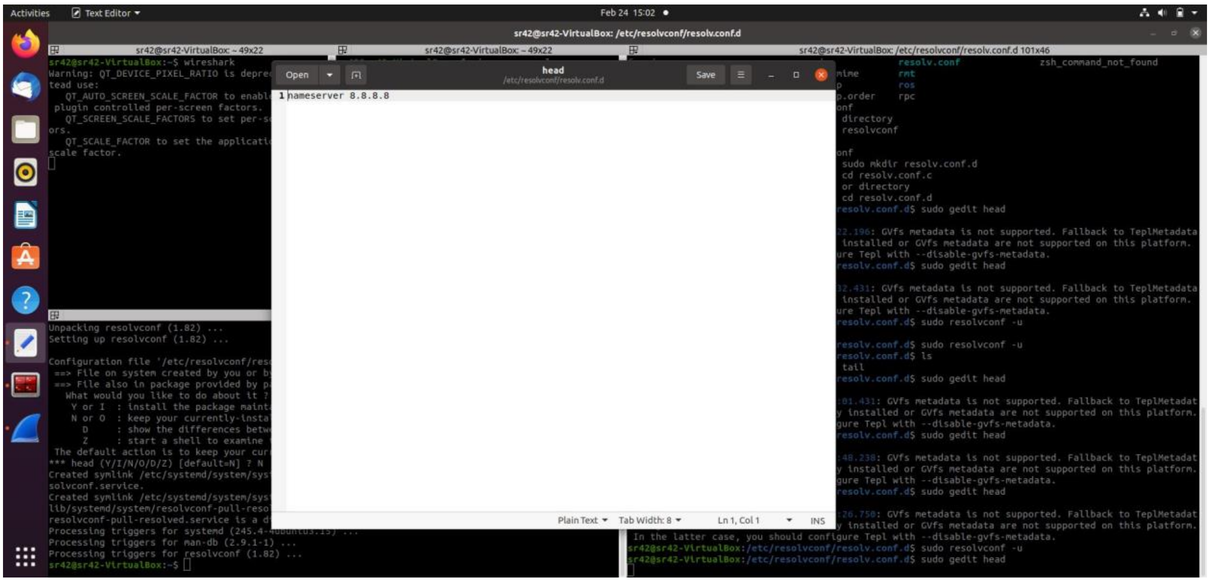
Profile: Default

Observation 2 :



Activities
Wireshark
Feb 24 14:58
Capturing from enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
dns

No.    Time          Source        Destination   Protocol Length Info
     1 0.000000000   10.0.2.15     8.8.8.8       DNS        85 Standard query 0x0a85 A www.google.com OPT
     2 0.000065375   10.0.2.15     8.8.8.8       DNS        85 Standard query 0x4281 AAAA www.google.com OPT
     3 0.055754937   8.8.8.8       10.0.2.15     DNS       113 Standard query response 0x4281 AAAA www.google.com AAAA 2404:…
     4 0.056630521   8.8.8.8       10.0.2.15     DNS       101 Standard query response 0x0a85 A www.google.com A 172.217.167…
     7 0.088959732   10.0.2.15     8.8.8.8       DNS        99 Standard query 0xcebb PTR 132.167.217.172.in-addr.arpa OPT
     8 0.113498631   8.8.8.8       10.0.2.15     DNS       137 Standard query response 0xcebb PTR 132.167.217.172.in-addr.ar…
    21 67.353143761  10.0.2.15     192.168.3.5   DNS       100 Standard query 0x1bbb A connectivity-check.ubuntu.com OPT
    22 67.363914508  192.168.3.5   10.0.2.15     DNS       148 Standard query response 0x1bbb A connectivity-check.ubuntu.co…
    40 89.289636708  10.0.2.15     8.8.8.8       DNS        87 Standard query 0x070e A daisy.ubuntu.com OPT
    41 89.289817705  10.0.2.15     8.8.8.8       DNS        87 Standard query 0x0103 AAAA daisy.ubuntu.com OPT
    42 89.312024974  8.8.8.8       10.0.2.15     DNS       148 Standard query response 0x0103 AAAA daisy.ubuntu.com SOA ns1.…
    43 89.319952936  8.8.8.8       10.0.2.15     DNS       119 Standard query response 0x070e A daisy.ubuntu.com A 162.213.3…

▸ Frame 1: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface enp0s3, id 0
▸ Ethernet II, Src: PcsCompu_a3:3c:e3 (08:00:27:a3:3c:e3), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 8.8.8.8
▾ User Datagram Protocol, Src Port: 37036, Dst Port: 53
    Source Port: 37036
    Destination Port: 53
    Length: 51
    Checksum: 0x1c63 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  ▸ [Timestamps]
▾ Domain Name System (query)
    Transaction ID: 0x0a85
  ▸ Flags: 0x0120 Standard query

0000  52 54 00 12 35 02 08 00  27 a3 3c e3 08 00 45 00   RT··5···'·<···E·
0010  00 47 65 06 40 00 40 11  b9 81 0a 00 02 0f 08 08   ·Ge·@·@·········
0020  08 08 90 ac 00 35 00 33  1c 63 0a 85 01 20 00 01   ·····5·3·c··· ··
0030  00 00 00 00 00 01 03 77  77 77 06 67 6f 6f 67 6c   ·······w ww·googl
0040  65 03 63 6f 6d 00 00 01  00 01 00 00 29 04 b0 00   e·com·······)···
0050  00 00 00 00 00                                     ·····
```



Activities
Text Editor
Feb 24 15:02
sr42@sr42-VirtualBox: /etc/resolvconf/resolv.conf.d
sr42@sr42-VirtualBox: ~ 49x22
sr42@sr42-VirtualBox: ~ 49x22
sr42@sr42-VirtualBox: /etc/resolvconf/resolv.conf.d 101x46
Open
head
/etc/resolvconf/resolv.conf.d
Save
Plain Text
Tab Width: 8
Ln 1, Col 1
INS

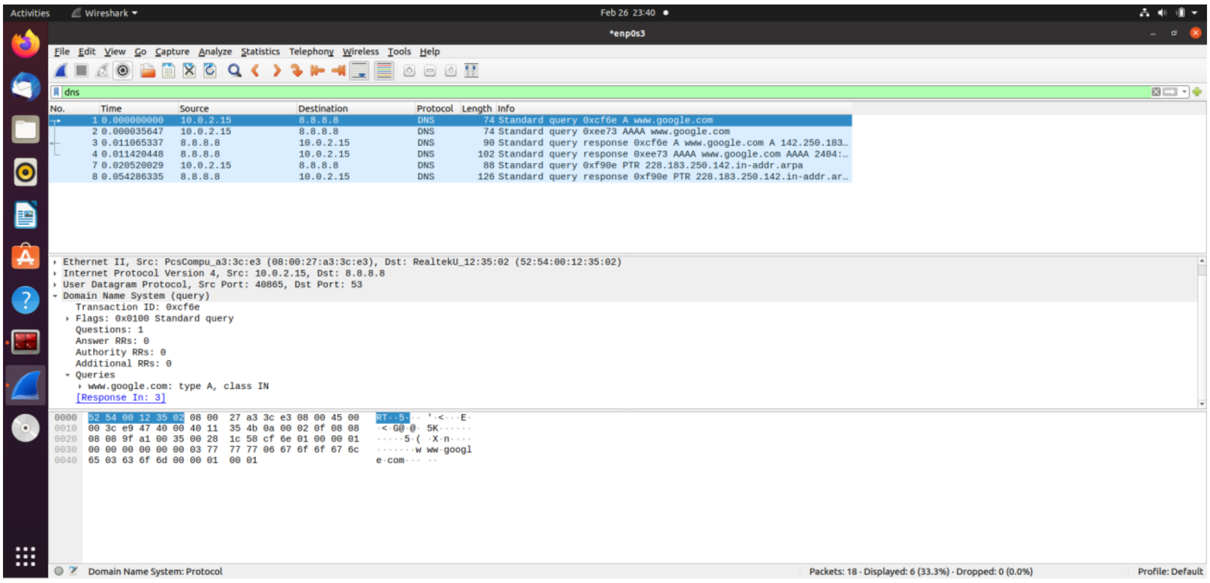
```
1 nameserver 8.8.8.8
```

```
sr42@sr42-VirtualBox:~$ wireshark
Warning: QT_DEVICE_PIXEL_RATIO is deprec
tead use:
   QT_AUTO_SCREEN_SCALE_FACTOR to enabl
 plugin controlled per-screen factors.
   QT_SCREEN_SCALE_FACTORS to set per-s
ors.
   QT_SCALE_FACTOR to set the applicati
scale factor.
```

```
Unpacking resolvconf (1.82) ...
Setting up resolvconf (1.82) ...

Configuration file '/etc/resolvconf/res
 ==> File on system created by you or b
 ==> File also in package provided by p
   What would you like to do about it ?
    Y or I  : install the package maint
    N or O  : keep your currently-insta
      D     : show the differences betw
      Z     : start a shell to examine
 The default action is to keep your cur
*** head (Y/I/N/O/D/Z) [default=N] ? N
Created symlink /etc/systemd/system/sys
solvconf.service.
Created symlink /etc/systemd/system/sys
lib/systemd/system/resolvconf-pull-reso
resolvconf-pull-resolved.service is a d
Processing triggers for systemd (245.4-4ubuntu3.15) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for resolvconf (1.82) ...
sr42@sr42-VirtualBox:~$
```

```
              resolv.conf                 zsh_command_not_found
mime          rmt
p             ros
p.order       rpc
onf
 directory
 resolvconf

onf
 sudo mkdir resolv.conf.d
 cd resolv.conf.c
 or directory
 cd resolv.conf.d
resolv.conf.d$ sudo gedit head

22.196: GVfs metadata is not supported. Fallback to TeplMetadata
 installed or GVfs metadata are not supported on this platform.
ure Tepl with --disable-gvfs-metadata.
resolv.conf.d$ sudo gedit head

32.431: GVfs metadata is not supported. Fallback to TeplMetadata
 installed or GVfs metadata are not supported on this platform.
ure Tepl with --disable-gvfs-metadata.
resolv.conf.d$ sudo resolvconf -u

resolv.conf.d$ sudo resolvconf -u
resolv.conf.d$ ls
 tail
resolv.conf.d$ sudo gedit head

:01.431: GVfs metadata is not supported. Fallback to TeplMetadat
y installed or GVfs metadata are not supported on this platform.
gure Tepl with --disable-gvfs-metadata.
resolv.conf.d$ sudo gedit head

:48.238: GVfs metadata is not supported. Fallback to TeplMetadat
y installed or GVfs metadata are not supported on this platform.
gure Tepl with --disable-gvfs-metadata.
resolv.conf.d$ sudo gedit head

:26.750: GVfs metadata is not supported. Fallback to TeplMetadat
y installed or GVfs metadata are not supported on this platform.
 In the latter case, you should configure Tepl with --disable-gvfs-metadata.
sr42@sr42-VirtualBox:/etc/resolvconf/resolv.conf.d$ sudo resolvconf -u
sr42@sr42-VirtualBox:/etc/resolvconf/resolv.conf.d$ sudo gedit head
```

Observation 3 :



Activities
Wireshark
Feb 26 23:40
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

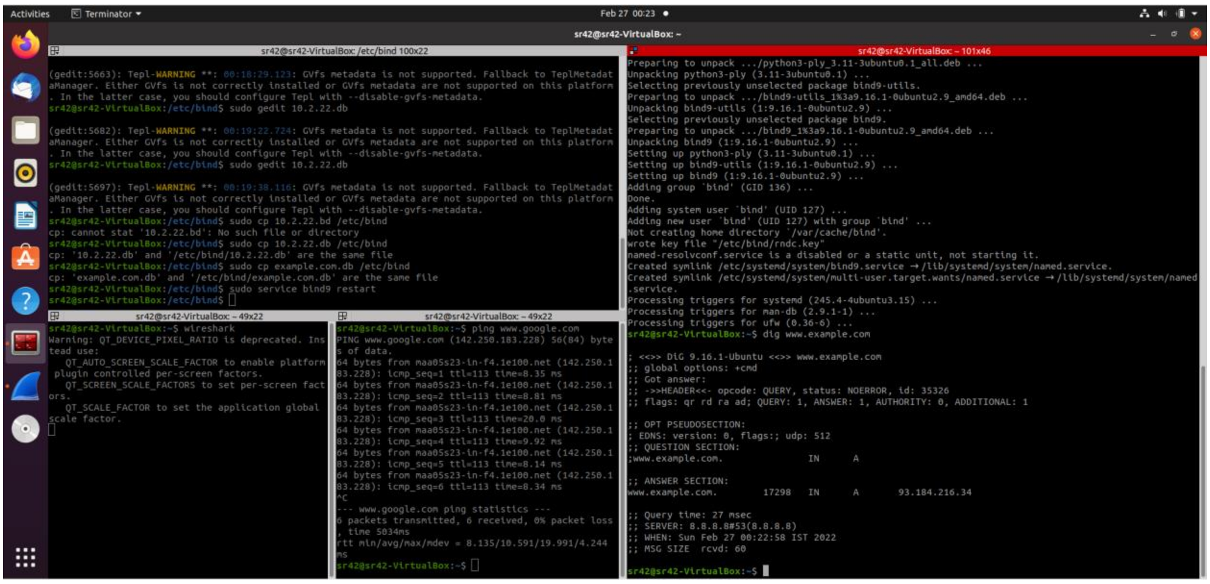
```
dns

No.    Time          Source        Destination   Protocol Length Info
     1 0.000000000   10.0.2.15     8.8.8.8       DNS        74 Standard query 0xcf6e A www.google.com
     2 0.000035647   10.0.2.15     8.8.8.8       DNS        74 Standard query 0xee73 AAAA www.google.com
     3 0.011065337   8.8.8.8       10.0.2.15     DNS        90 Standard query response 0xcf6e A www.google.com A 142.250.183…
     4 0.011420448   8.8.8.8       10.0.2.15     DNS       102 Standard query response 0xee73 AAAA www.google.com AAAA 2404:…
     7 0.020520029   10.0.2.15     8.8.8.8       DNS        88 Standard query 0xf90e PTR 228.183.250.142.in-addr.arpa
     8 0.054286335   8.8.8.8       10.0.2.15     DNS       126 Standard query response 0xf90e PTR 228.183.250.142.in-addr.ar…

▸ Ethernet II, Src: PcsCompu_a3:3c:e3 (08:00:27:a3:3c:e3), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 8.8.8.8
▸ User Datagram Protocol, Src Port: 40865, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0xcf6e
  ▸ 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: 3]

0000  52 54 00 12 35 02 08 00  27 a3 3c e3 08 00 45 00   RT··5···'·<···E·
0010  00 3c e9 47 40 00 40 11  35 4b 0a 00 02 0f 08 08   ·<·G@·@·5K······
0020  08 08 9f a1 00 35 00 28  1c 58 cf 6e 01 00 00 01   ·····5·(·X·n····
0030  00 00 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c   ·······w ww·googl
0040  65 03 63 6f 6d 00 00 01  00 01                     e·com·····

Domain Name System: Protocol        Packets: 18 · Displayed: 6 (33.3%) · Dropped: 0 (0.0%)        Profile: Default
```

Observation 4 (DNS cache) :

```
;
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
; using a 604800 second stale ttl
$DATE 20220219182533
; secure
.                       1122239         IN NS  a.root-servers.net.
                        1122239         IN NS  b.root-servers.net.
                        1122239         IN NS  c.root-servers.net.
                        1122239         IN NS  d.root-servers.net.
                        1122239         IN NS  e.root-servers.net.
                        1122239         IN NS  f.root-servers.net.
                        1122239         IN NS  g.root-servers.net.
                        1122239         IN NS  h.root-servers.net.
                        1122239         IN NS  i.root-servers.net.
                        1122239         IN NS  j.root-servers.net.
                        1122239         IN NS  k.root-servers.net.
                        1122239         IN NS  l.root-servers.net.
                        1122239         IN NS  m.root-servers.net.
; secure
                        1122239         RRSIGNS 8 0 518400 (
                                        20220311170000 20220226160000 9799 .
                                        EZ02Y6Bomku5fk9N5w2JaaVYoBc2t6wuP74+
                                        c4mGEUzYpVr6M05Yltxm+W+txe+grByh/0Ny
                                        FIrQ5aK3r2jaqJebKmhmTyeReKhS2vX1M2RZ
                                        8Uazx5NlPbe66Omj6k13uZvEizTkF9mFlQ/3
                                        T/QS6d+Z821tS9vYSwd5YcUYVAKQ0vnOnwrX
                                        vMMfe0kxro0OvrksvgQMNLdGFli8ItP6iaHh
                                        gBH1vRemFWHGI/ao69eHQOO8QWXIqBXulkYB
                                        +VDFXgt4IugD71PCxSnTakwz0Ml0LxiT6Ped
                                        VDj4IFxHjoc6Gtp1sHRBVPPhSNNq4VuFYsuU
                                        LUdPb5RZO+yzzUp0/A== )
; secure
                        776639          DNSKEY       256 3 8 (
                                        AwEAAZym4HCWiTAAl2Mv1izgTyn9sKwgi5eB
                                        xpG29bVlefq/r+TGCtmUElvFyBWHRjvf9mBg
                                        lIlTBRse22dvzNOI+cYrkjD6LOHuxMoc/d4W
                                        tXWKdviNmrtWF2GpjmDOI98gLd4BZ0U/lY84
                                        7mJP9LypFABZcEn3zM3vce4Ee1A3upSlFQ2T
                                        FyJSD9HvMnP4XneFexBxV96RpLcy2O+u2W6C
                                        hIiDCjlrowPCcU3zXfXxyWy/VKM6TOa8gNf+
                                        aKaVkcv/eIh5er8rrsqAi9KT8O5hmhzYLkUO
                                        QEXVSRORV0RMt9l3JSwWxT1MebEDvtfBag3u
                                        o+mZwWSFlpc9kuzyWBd72Ec=
                                        ) ; ZSK; alg = RSASHA256 ; key id = 9799
                        776639          DNSKEY      257 3 8 (
                                        AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvk
                                        MgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRixH
                                        lFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8O
                                        g8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n9WG
                                        e2R8PzgCmr3EgVLrjyBxWezF0jLHwVN8efS3
                                        rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eN
                                        buv7pr+eoZG+SrDK6nWeL3c6H5Apxz7LjVc1
                                        uTIdsIXxuOLYA4/ilBmSVIzuDWfdRUfhHdY6
                                        +cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa
                                        8subX2Nn6UwNR1AkUTV74bU=
                                        ) ; KSK; alg = RSASHA256 ; key id = 20326
; secure
                        776639          RRSIGDNSKEY 8 0 172800 (
                                        20220313000000 20220220000000 20326 .
                                        VhdGJ/WGqEEtOoRHalnxxy19ASlnzOIM9D4i
                                        Ri5bvBo3MdUFRE1pVCqVGF627MIVsFH10/Xz
                                        ntV0jIEU0Ft5kdSTxqBdj0YlQpnisEBFAp+o
                                        elReMxVoHQYuwyNG6rmtZnj6RctVfajdC3DP
                                        e4t48O7vggAK4vfpB/HW125hAP2xaeqOInDc
                                        ZVIQogYM7kBxeTB3ZxUmRJcN57am4MP+k6bR
                                        A50xyiRpuLdMKIsaf/Gpjmvj16yxG19ojTvC
                                        oUQu853mI6ul79T8sh5J9bwC+FmXQXgPBg8O
                                        ZOIFudng6GN1QC4dEhZtFMIV4Bw9Tl2KKjfB
                                        OBGai6f0OWurlfNfMg== )
; glue
a.root-servers.net.     1122239         A           198.41.0.4
; glue
                        1122239         AAAA2001:503:ba3e::2:30
; glue
b.root-servers.net.     1122239         A           199.9.14.201
; glue
                        1122239         AAAA2001:500:200::b
; glue
c.root-servers.net.     1122239         A           192.33.4.12
; glue
                        1122239         AAAA2001:500:2::c
; glue
d.root-servers.net.     1122239         A           199.7.91.13
; glue
                        1122239         AAAA2001:500:2d::d
; glue
e.root-servers.net.     1122239         A           192.203.230.10
; glue
                        1122239         AAAA2001:500:a8::e
; glue
f.root-servers.net.     1122239         A           192.5.5.241
; glue
                        1122239         AAAA2001:500:2f::f
; glue
```

```
g.root-servers.net.     1122239         A       192.112.36.4
; glue
                        1122239         AAAA2001:500:12::d0d
; glue
h.root-servers.net.     1122239         A       198.97.190.53
; glue
                        1122239         AAAA2001:500:1::53
; glue
i.root-servers.net.     1122239         A       192.36.148.17
; glue
                        1122239         AAAA2001:7fe::53
; glue
j.root-servers.net.     1122239         A       192.58.128.30
; glue
                        1122239         AAAA2001:503:c27::2:30
; glue
k.root-servers.net.     1122239         A       193.0.14.129
; glue
                        1122239         AAAA2001:7fd::1
; glue
l.root-servers.net.     1122239         A       199.7.83.42
; glue
                        1122239         AAAA2001:500:9f::42
; glue
m.root-servers.net.     1122239         A       202.12.27.33
; glue
                        1122239         AAAA2001:dc3::35
;
; Address database dump
;
; [edns success/4096 timeout/1432 timeout/1232 timeout/512 timeout]
; [plain success/timeout]
;
;
; Unassociated entries
;
;       192.58.128.30 [srtt 3] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 839]
;       2001:500:a8::e [srtt 48140] [flags 00000000] [edns 0/2/2/2/2] [plain 0/0] [ttl 839]
;       192.36.148.17 [srtt 24] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 839]
;       192.5.5.241 [srtt 20362] [flags 00004000] [edns 2/0/0/0/0] [plain 0/0] [udpsize 512]
[ttl 839]
;       2001:500:2d::d [srtt 142840] [flags 00000000] [edns 0/2/2/2/2] [plain 0/0] [ttl 839]
;       199.7.83.42 [srtt 3] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 839]
;       2001:500:200::b [srtt 41700] [flags 00000000] [edns 0/2/2/2/2] [plain 0/0] [ttl 839]
;       193.0.14.129 [srtt 11] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 839]
;       192.112.36.4 [srtt 23] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 839]
;       202.12.27.33 [srtt 4] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 839]
;       198.97.190.53 [srtt 28] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 839]
;       192.203.230.10 [srtt 29] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 839]
;       2001:500:2::c [srtt 155760] [flags 00000000] [edns 0/2/2/2/2] [plain 0/0] [ttl 839]
;       2001:500:12::d0d [srtt 45800] [flags 00000000] [edns 0/2/2/2/2] [plain 0/0] [ttl 839]
;       2001:500:1::53 [srtt 30580] [flags 00000000] [edns 0/2/2/2/2] [plain 0/0] [ttl 839]
;       199.9.14.201 [srtt 20] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 839]
;       2001:500:2f::f [srtt 85780] [flags 00000000] [edns 0/2/2/2/2] [plain 0/0] [ttl 839]
;       2001:500:9f::42 [srtt 179730] [flags 00000000] [edns 0/2/2/2/2] [plain 0/0] [ttl 839]
;       2001:503:ba3e::2:30 [srtt 114620] [flags 00000000] [edns 0/2/2/2/2] [plain 0/0] [ttl
839]
;       2001:7fd::1 [srtt 196730] [flags 00000000] [edns 0/2/2/2/2] [plain 0/0] [ttl 839]
;       2001:7fe::53 [srtt 74720] [flags 00000000] [edns 0/2/2/2/2] [plain 0/0] [ttl 839]
;       199.7.91.13 [srtt 24] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 839]
;       2001:dc3::35 [srtt 251240] [flags 00000000] [edns 0/2/2/2/2] [plain 0/0] [ttl 839]
;       198.41.0.4 [srtt 23] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 839]
;       2001:503:c27::2:30 [srtt 167370] [flags 00000000] [edns 0/2/2/2/2] [plain 0/0] [ttl
839]
;       192.33.4.12 [srtt 8] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 839]
;
; Bad cache
;
;
; SERVFAIL cache
;
;
; Start view _bind
;
;
; Cache dump of view '_bind' (cache _bind)
;
; using a 604800 second stale ttl
$DATE 20220219182533
;
; Address database dump
;
; [edns success/4096 timeout/1432 timeout/1232 timeout/512 timeout]
; [plain success/timeout]
;
;
; Unassociated entries
;
;
; Bad cache
;
;
; SERVFAIL cache
;
; Dump complete
```

Observation 5 (dig www.example.com) :



Activities
Terminator
Feb 27 00:23
sr42@sr42-VirtualBox: ~
sr42@sr42-VirtualBox: /etc/bind 100x22
sr42@sr42-VirtualBox: ~ 49x22
sr42@sr42-VirtualBox: ~ 49x22
sr42@sr42-VirtualBox: ~ 101x46

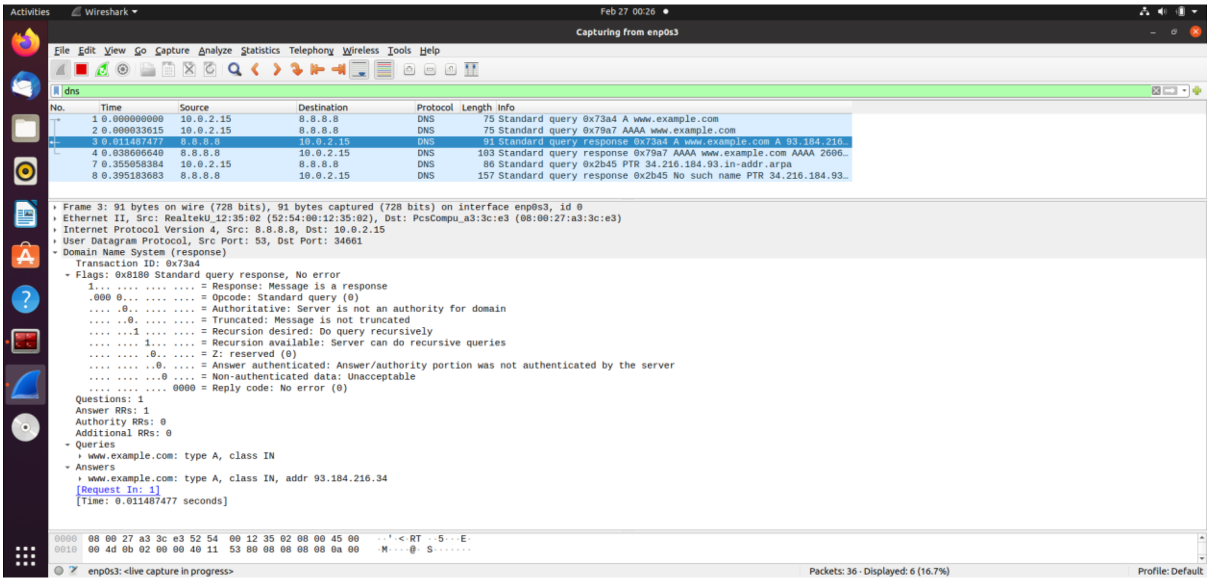
```
(gedit:5663): Tepl-WARNING **: 00:18:29.123: GVfs metadata is not supported. Fallback to TeplMetadat
aManager. Either GVfs is not correctly installed or GVfs metadata are not supported on this platform
. In the latter case, you should configure Tepl with --disable-gvfs-metadata.
sr42@sr42-VirtualBox:/etc/bind$ sudo gedit 10.2.22.db

(gedit:5682): Tepl-WARNING **: 00:19:22.724: GVfs metadata is not supported. Fallback to TeplMetadat
aManager. Either GVfs is not correctly installed or GVfs metadata are not supported on this platform
. In the latter case, you should configure Tepl with --disable-gvfs-metadata.
sr42@sr42-VirtualBox:/etc/bind$ sudo gedit 10.2.22.db

(gedit:5697): Tepl-WARNING **: 00:19:38.116: GVfs metadata is not supported. Fallback to TeplMetadat
aManager. Either GVfs is not correctly installed or GVfs metadata are not supported on this platform
. In the latter case, you should configure Tepl with --disable-gvfs-metadata.
sr42@sr42-VirtualBox:/etc/bind$ sudo cp 10.2.22.bd /etc/bind
cp: cannot stat '10.2.22.bd': No such file or directory
sr42@sr42-VirtualBox:/etc/bind$ sudo cp 10.2.22.db /etc/bind
cp: '10.2.22.db' and '/etc/bind/10.2.22.db' are the same file
sr42@sr42-VirtualBox:/etc/bind$ sudo cp example.com.db /etc/bind
cp: 'example.com.db' and '/etc/bind/example.com.db' are the same file
sr42@sr42-VirtualBox:/etc/bind$ sudo service bind9 restart
sr42@sr42-VirtualBox:/etc/bind$
```

```
sr42@sr42-VirtualBox:~$ wireshark
Warning: QT_DEVICE_PIXEL_RATIO is deprecated. Ins
tead use:
   QT_AUTO_SCREEN_SCALE_FACTOR to enable platform
 plugin controlled per-screen factors.
   QT_SCREEN_SCALE_FACTORS to set per-screen fact
ors.
   QT_SCALE_FACTOR to set the application global
scale factor.
```

```
sr42@sr42-VirtualBox:~$ ping www.google.com
PING www.google.com (142.250.183.228) 56(84) byte
s of data.
64 bytes from maa05s23-in-f4.1e100.net (142.250.1
83.228): icmp_seq=1 ttl=113 time=8.35 ms
64 bytes from maa05s23-in-f4.1e100.net (142.250.1
83.228): icmp_seq=2 ttl=113 time=8.81 ms
64 bytes from maa05s23-in-f4.1e100.net (142.250.1
83.228): icmp_seq=3 ttl=113 time=20.0 ms
64 bytes from maa05s23-in-f4.1e100.net (142.250.1
83.228): icmp_seq=4 ttl=113 time=9.92 ms
64 bytes from maa05s23-in-f4.1e100.net (142.250.1
83.228): icmp_seq=5 ttl=113 time=8.14 ms
64 bytes from maa05s23-in-f4.1e100.net (142.250.1
83.228): icmp_seq=6 ttl=113 time=8.34 ms
^C
--- www.google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss
, time 5034ms
rtt min/avg/max/mdev = 8.135/10.591/19.991/4.244
ms
sr42@sr42-VirtualBox:~$
```

```
Preparing to unpack .../python3-ply_3.11-3ubuntu0.1_all.deb ...
Unpacking python3-ply (3.11-3ubuntu0.1) ...
Selecting previously unselected package bind9-utils.
Preparing to unpack .../bind9-utils_1%3a9.16.1-0ubuntu2.9_amd64.deb ...
Unpacking bind9-utils (1:9.16.1-0ubuntu2.9) ...
Selecting previously unselected package bind9.
Preparing to unpack .../bind9_1%3a9.16.1-0ubuntu2.9_amd64.deb ...
Unpacking bind9 (1:9.16.1-0ubuntu2.9) ...
Setting up python3-ply (3.11-3ubuntu0.1) ...
Setting up bind9-utils (1:9.16.1-0ubuntu2.9) ...
Setting up bind9 (1:9.16.1-0ubuntu2.9) ...
Adding group `bind' (GID 136) ...
Done.
Adding system user `bind' (UID 127) ...
Adding new user `bind' (UID 127) with group `bind' ...
Not creating home directory `/var/cache/bind'.
wrote key file "/etc/bind/rndc.key"
named-resolvconf.service is a disabled or a static unit, not starting it.
Created symlink /etc/systemd/system/bind9.service → /lib/systemd/system/named.service.
Created symlink /etc/systemd/system/multi-user.target.wants/named.service → /lib/systemd/system/named
.service.
Processing triggers for systemd (245.4-4ubuntu3.15) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for ufw (0.36-6) ...
sr42@sr42-VirtualBox:~$ dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35326
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        17298   IN      A       93.184.216.34

;; Query time: 27 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun Feb 27 00:22:58 IST 2022
;; MSG SIZE  rcvd: 60

sr42@sr42-VirtualBox:~$
```

Observation 6 (www.example.com wireshark capture):



Activities
Wireshark
Feb 27 00:26
Capturing from enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
enp0s3: <live capture in progress>
Packets: 36 · Displayed: 6 (16.7%)
Profile: Default

```
No.   Time          Source       Destination   Protocol  Length Info
    1 0.000000000   10.0.2.15    8.8.8.8       DNS           75 Standard query 0x73a4 A www.example.com
    2 0.000033615   10.0.2.15    8.8.8.8       DNS           75 Standard query 0x79a7 AAAA www.example.com
    3 0.011487477   8.8.8.8      10.0.2.15     DNS           91 Standard query response 0x73a4 A www.example.com A 93.184.216…
    4 0.038606640   8.8.8.8      10.0.2.15     DNS          103 Standard query response 0x79a7 AAAA www.example.com AAAA 2606…
    7 0.355058384   10.0.2.15    8.8.8.8       DNS           86 Standard query 0x2b45 PTR 34.216.184.93.in-addr.arpa
    8 0.395183683   8.8.8.8      10.0.2.15     DNS          157 Standard query response 0x2b45 No such name PTR 34.216.184.93…
```

```
› Frame 3: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface enp0s3, id 0
› Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_a3:3c:e3 (08:00:27:a3:3c:e3)
› Internet Protocol Version 4, Src: 8.8.8.8, Dst: 10.0.2.15
› User Datagram Protocol, Src Port: 53, Dst Port: 34661
⌄ Domain Name System (response)
    Transaction ID: 0x73a4
  ⌄ 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: 1
    Authority RRs: 0
    Additional RRs: 0
  ⌄ Queries
    › www.example.com: type A, class IN
  ⌄ Answers
    › www.example.com: type A, class IN, addr 93.184.216.34
    [Request In: 1]
    [Time: 0.011487477 seconds]
```

```
0000  08 00 27 a3 3c e3 52 54  00 12 35 02 08 00 45 00   ··'·<·RT ··5···E·
0010  00 4d 0b 02 00 00 40 11  53 80 08 08 08 08 0a 00   ·M····@· S·······
```

Questions :

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

2) What is the destination port for the DNS query message? What is the source port of DNS response message? – **53 & 36727 respectively.**

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? – **8.8.8.8. This is the same as that of the local DNS server.**

4) Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”? - **Standard query, no answers.**

5) Examine the DNS response message. How many “answers” are provided? What do each of these answers contain? – **1 answer.**

Data contained -

www.flipkart.com: type CNAME, class IN, cname flipkart.com

Name: www.flipkart.com

Type: CNAME (Canonical NAME for an alias) (5)

Class: IN (0x0001)

Time to live: 33 (33 seconds)

Data length: 2

CNAME: flipkart.com