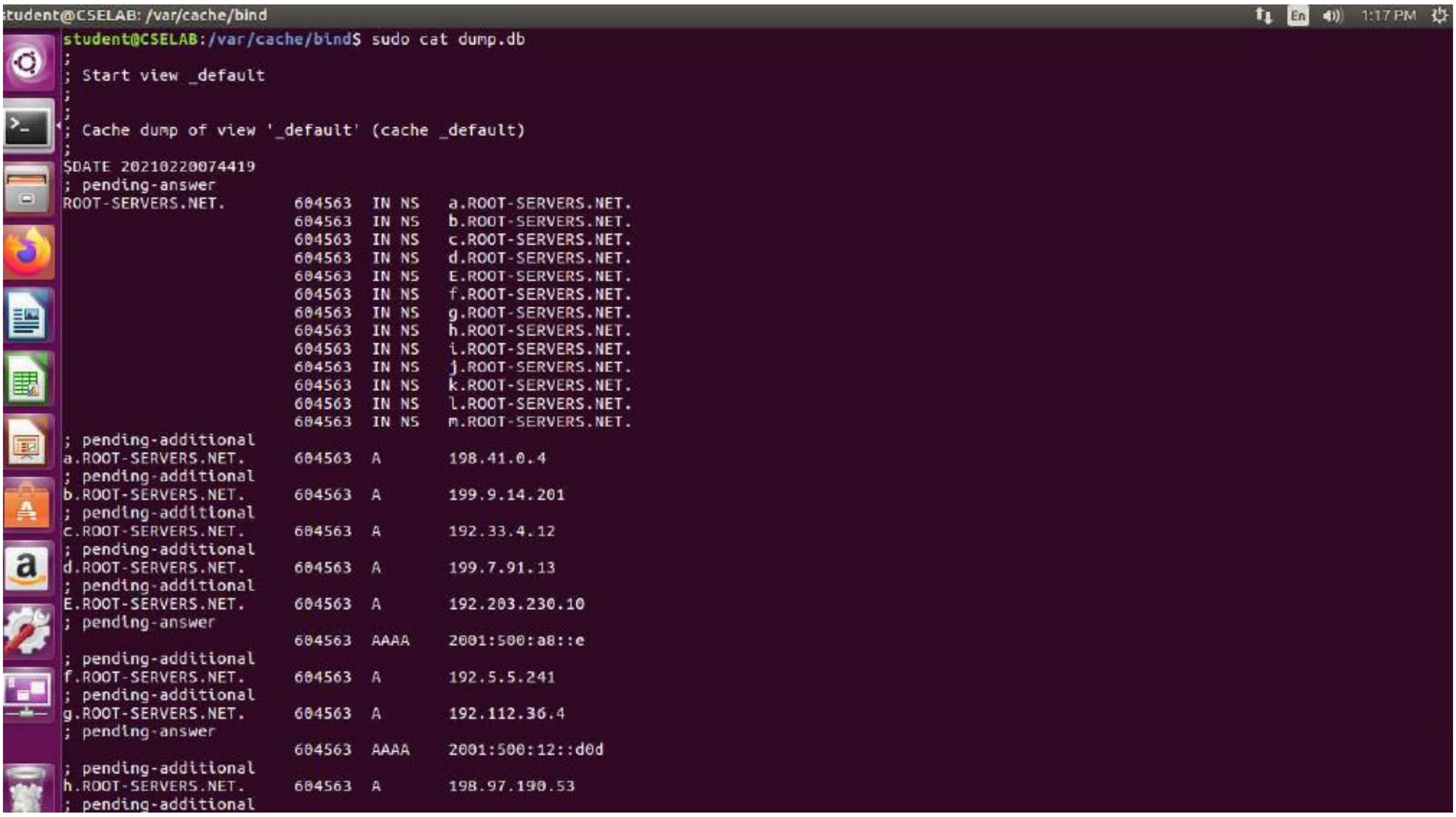
Computer networks laboratory week 4

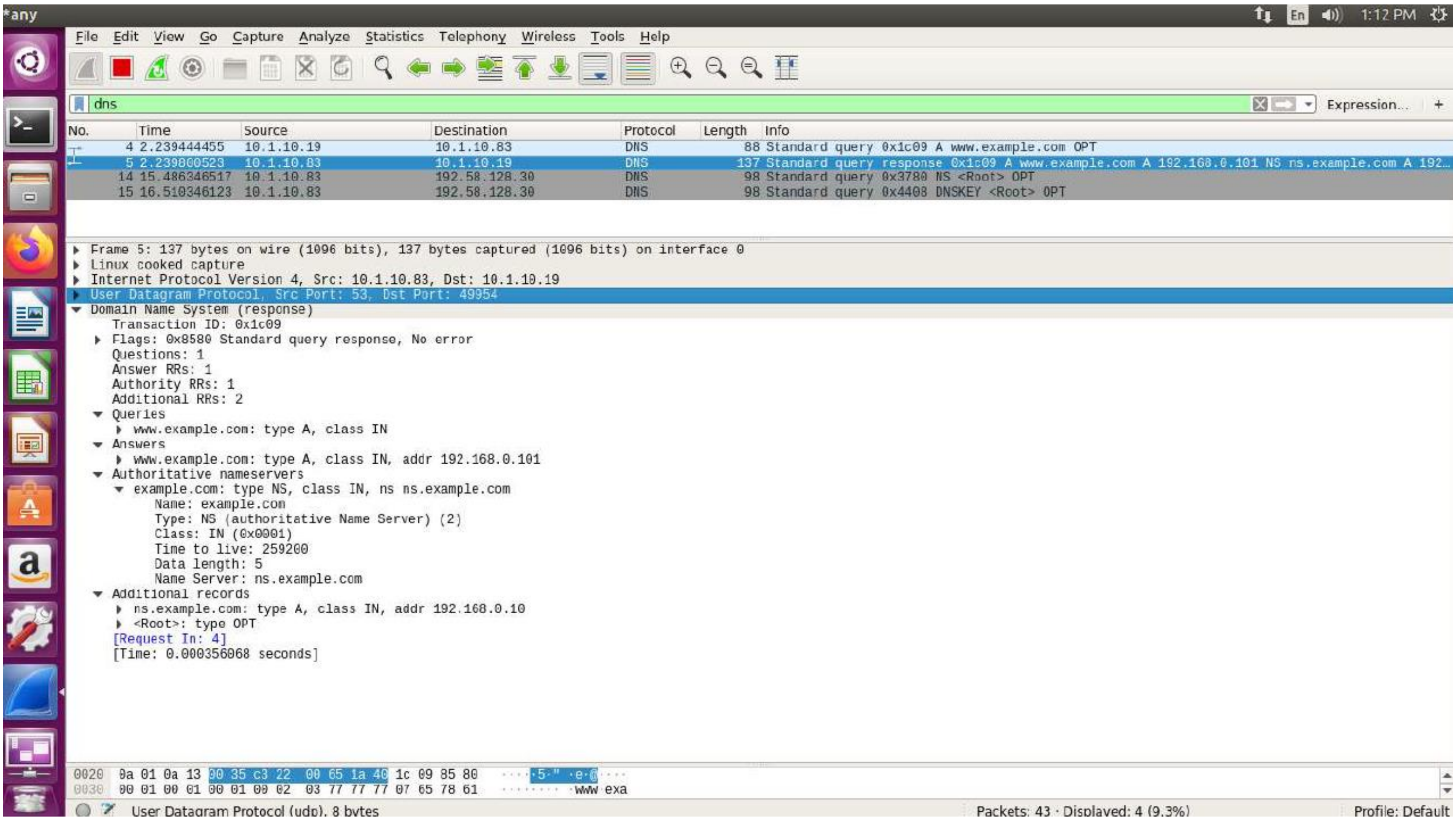
Name: Pranav R. Hegde SRN: PES1UG19CS343 Section: F

DNS Implementation



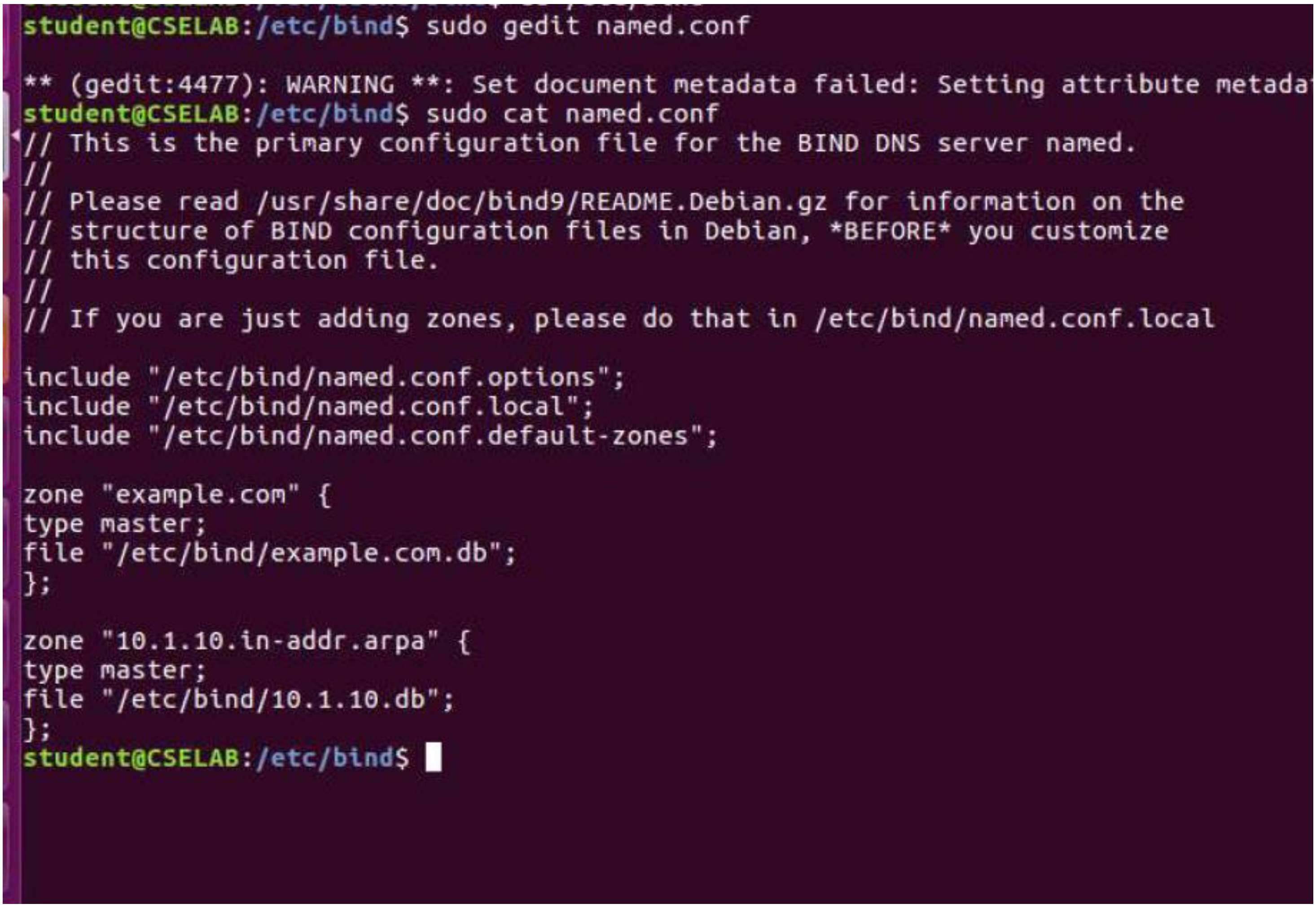
```
student@CSELAB:/var/cache/bind$ sudo cat dump.db
;
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
$DATE 20210220074419
; pending-answer
ROOT-SERVERS.NET.        604563  IN NS    a.ROOT-SERVERS.NET.
                         604563  IN NS    b.ROOT-SERVERS.NET.
                         604563  IN NS    c.ROOT-SERVERS.NET.
                         604563  IN NS    d.ROOT-SERVERS.NET.
                         604563  IN NS    E.ROOT-SERVERS.NET.
                         604563  IN NS    f.ROOT-SERVERS.NET.
                         604563  IN NS    g.ROOT-SERVERS.NET.
                         604563  IN NS    h.ROOT-SERVERS.NET.
                         604563  IN NS    i.ROOT-SERVERS.NET.
                         604563  IN NS    j.ROOT-SERVERS.NET.
                         604563  IN NS    k.ROOT-SERVERS.NET.
                         604563  IN NS    l.ROOT-SERVERS.NET.
                         604563  IN NS    m.ROOT-SERVERS.NET.
; pending-additional
a.ROOT-SERVERS.NET.      604563  A        198.41.0.4
; pending-additional
b.ROOT-SERVERS.NET.      604563  A        199.9.14.201
; pending-additional
c.ROOT-SERVERS.NET.      604563  A        192.33.4.12
; pending-additional
d.ROOT-SERVERS.NET.      604563  A        199.7.91.13
; pending-additional
E.ROOT-SERVERS.NET.      604563  A        192.203.230.10
; pending-answer
                         604563  AAAA     2001:500:a8::e
; pending-additional
f.ROOT-SERVERS.NET.      604563  A        192.5.5.241
; pending-additional
g.ROOT-SERVERS.NET.      604563  A        192.112.36.4
; pending-answer
                         604563  AAAA     2001:500:12::d0d
; pending-additional
h.ROOT-SERVERS.NET.      604563  A        198.97.190.53
; pending-additional
```

Wireshark capture:

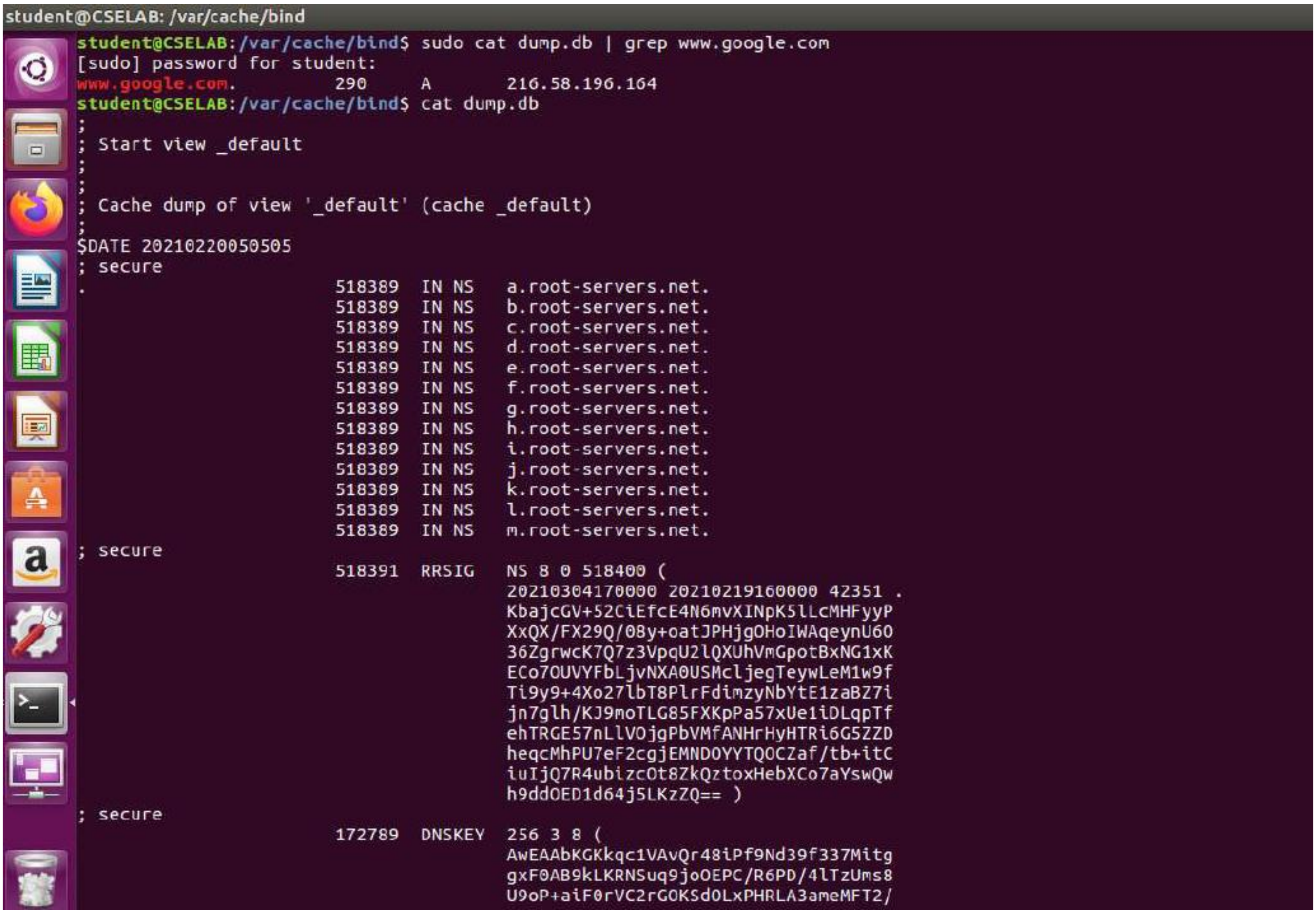


*any
1:12 PM
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

```
dns

No.  Time           Source       Destination    Protocol Length Info
   4 2.239444455    10.1.10.19   10.1.10.83     DNS         88 Standard query 0x1c09 A www.example.com OPT
   5 2.239800523    10.1.10.83   10.1.10.19     DNS        137 Standard query response 0x1c09 A www.example.com A 192.168.0.101 NS ns.example.com A 192…
  14 15.486346517   10.1.10.83   192.58.128.30  DNS         98 Standard query 0x3780 NS <Root> OPT
  15 16.510346123   10.1.10.83   192.58.128.30  DNS         98 Standard query 0x4408 DNSKEY <Root> OPT

▸ Frame 5: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.1.10.83, Dst: 10.1.10.19
▸ User Datagram Protocol, Src Port: 53, Dst Port: 49954
▾ Domain Name System (response)
    Transaction ID: 0x1c09
  ▸ 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
  ▾ Answers
    ▸ www.example.com: type A, class IN, addr 192.168.0.101
  ▾ 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 192.168.0.10
    ▸ <Root>: type OPT
    [Request In: 4]
    [Time: 0.000356068 seconds]

0020  0a 01 0a 13 00 35 c3 22  00 65 1a 40 1c 09 85 80   ·····5·" ·e·@····
0030  00 01 00 01 00 01 00 02  03 77 77 77 07 65 78 61   ········ ·www·exa

User Datagram Protocol (udp), 8 bytes          Packets: 43 · Displayed: 4 (9.3%)          Profile: Default
```

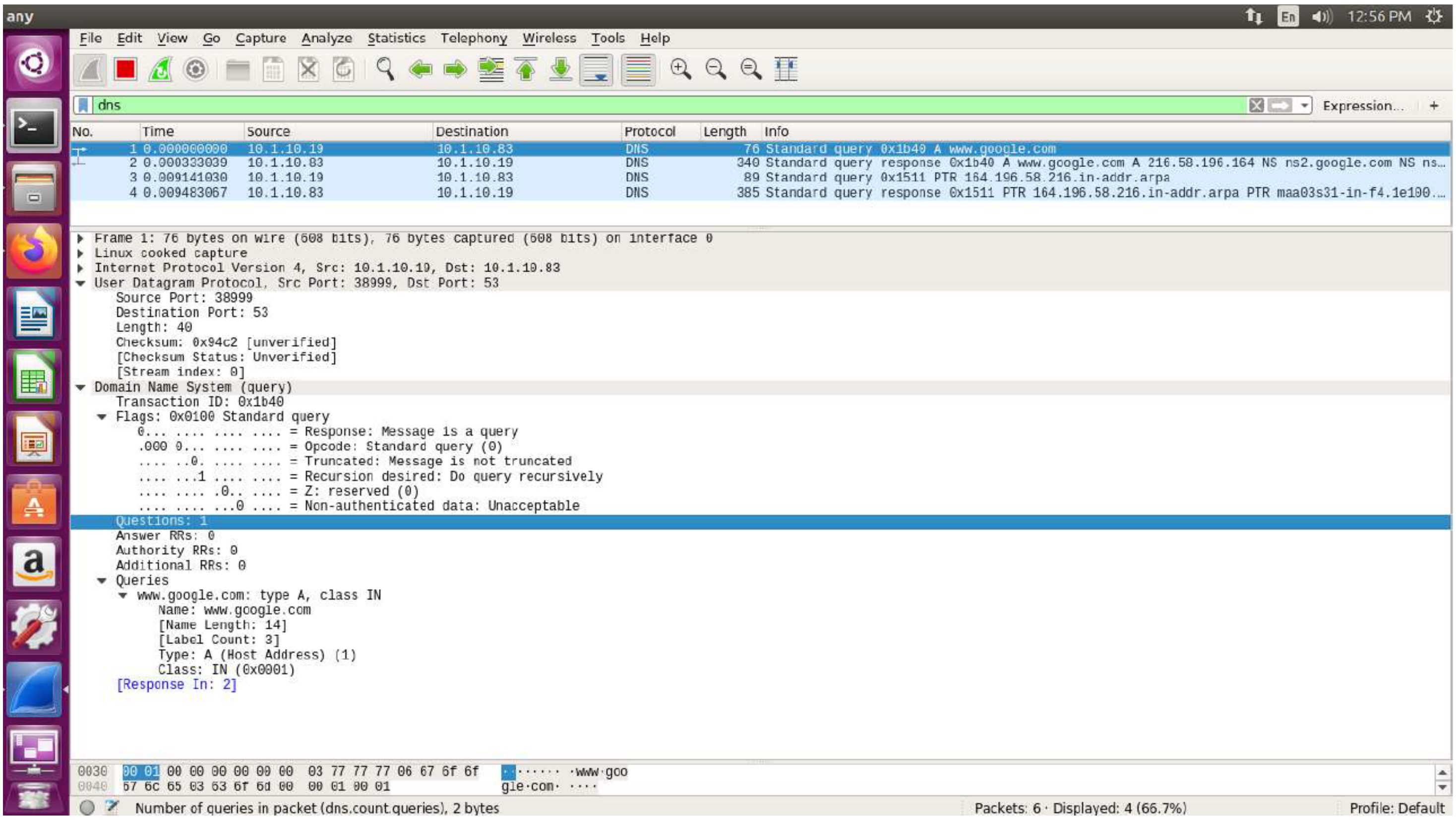


```
student@CSELAB:/etc/bind$ sudo gedit named.conf

** (gedit:4477): WARNING **: Set document metadata failed: Setting attribute metada
student@CSELAB:/etc/bind$ sudo cat 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@CSELAB:/etc/bind$ 
```



```
student@CSELAB: /var/cache/bind
student@CSELAB:/var/cache/bind$ sudo cat dump.db | grep www.google.com
[sudo] password for student:
www.google.com.         290     A       216.58.196.164
student@CSELAB:/var/cache/bind$ cat dump.db
;
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
$DATE 20210220050505
; secure
.                       518389  IN NS   a.root-servers.net.
                        518389  IN NS   b.root-servers.net.
                        518389  IN NS   c.root-servers.net.
                        518389  IN NS   d.root-servers.net.
                        518389  IN NS   e.root-servers.net.
                        518389  IN NS   f.root-servers.net.
                        518389  IN NS   g.root-servers.net.
                        518389  IN NS   h.root-servers.net.
                        518389  IN NS   i.root-servers.net.
                        518389  IN NS   j.root-servers.net.
                        518389  IN NS   k.root-servers.net.
                        518389  IN NS   l.root-servers.net.
                        518389  IN NS   m.root-servers.net.
; secure
                        518391  RRSIG   NS 8 0 518400 (
                                        20210304170000 20210219160000 42351 .
                                        KbajcGV+52CiEfcE4N6mvXINpK5lLcMHFyyP
                                        XxQX/FX29Q/08y+oatJPHjgOHoIWAqeynU6O
                                        36ZgrwcK7Q7z3VpqU2lQXUhVmGpotBxNG1xK
                                        ECo7OUVYFbLjvNXA0USMcljegTeywLeM1w9f
                                        Ti9y9+4Xo27lbT8PlrFdimzyNbYtE1zaBZ7i
                                        jn7glh/KJ9moTLG85FXKpPa57xUe1iDLqpTf
                                        ehTRGE57nLlVOjgPbVMfANHrHyHTRi6G5ZZD
                                        heqcMhPU7eF2cgjEMNDOYYTQOCZaf/tb+itC
                                        iuIjQ7R4ubizcOt8ZkQztoxHebXCo7aYswQw
                                        h9ddOED1d64j5LKzZQ== )
; secure
                        172789  DNSKEY  256 3 8 (
                                        AwEAAbKGKkqc1VAvQr48iPf9Nd39f337Mitg
                                        gxF0AB9kLKRNSuq9joOEPC/R6PD/4lTzUms8
                                        U9oP+aiF0rVC2rGOKSdOLxPHRLA3ameMFT2/
```

Wireshark captures:



any
12:56 PM
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

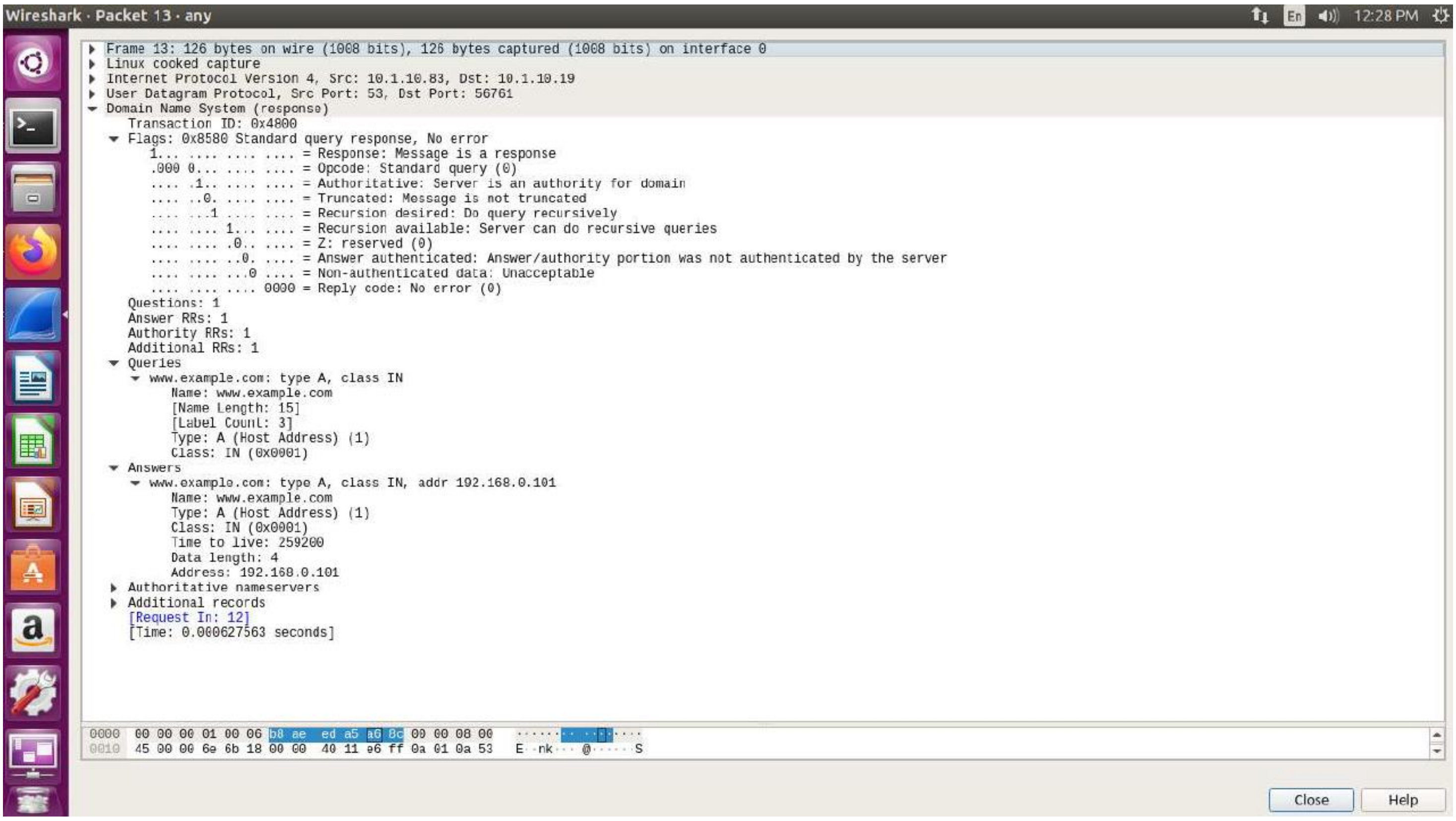
```
dns
```

```
No.  Time         Source       Destination  Protocol  Length Info
   1 0.000000000  10.1.10.19   10.1.10.83   DNS        76 Standard query 0x1b40 A www.google.com
   2 0.000333039  10.1.10.83   10.1.10.19   DNS       340 Standard query response 0x1b40 A www.google.com A 216.58.196.164 NS ns2.google.com NS ns…
   3 0.009141030  10.1.10.19   10.1.10.83   DNS        89 Standard query 0x1511 PTR 164.196.58.216.in-addr.arpa
   4 0.009483067  10.1.10.83   10.1.10.19   DNS       385 Standard query response 0x1511 PTR 164.196.58.216.in-addr.arpa PTR maa03s31-in-f4.1e100.…
```

```
▸ Frame 1: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.1.10.19, Dst: 10.1.10.83
▾ User Datagram Protocol, Src Port: 38999, Dst Port: 53
     Source Port: 38999
     Destination Port: 53
     Length: 40
     Checksum: 0x94c2 [unverified]
     [Checksum Status: Unverified]
     [Stream index: 0]
▾ Domain Name System (query)
     Transaction ID: 0x1b40
   ▾ 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
           Name: www.google.com
           [Name Length: 14]
           [Label Count: 3]
           Type: A (Host Address) (1)
           Class: IN (0x0001)
     [Response In: 2]
```

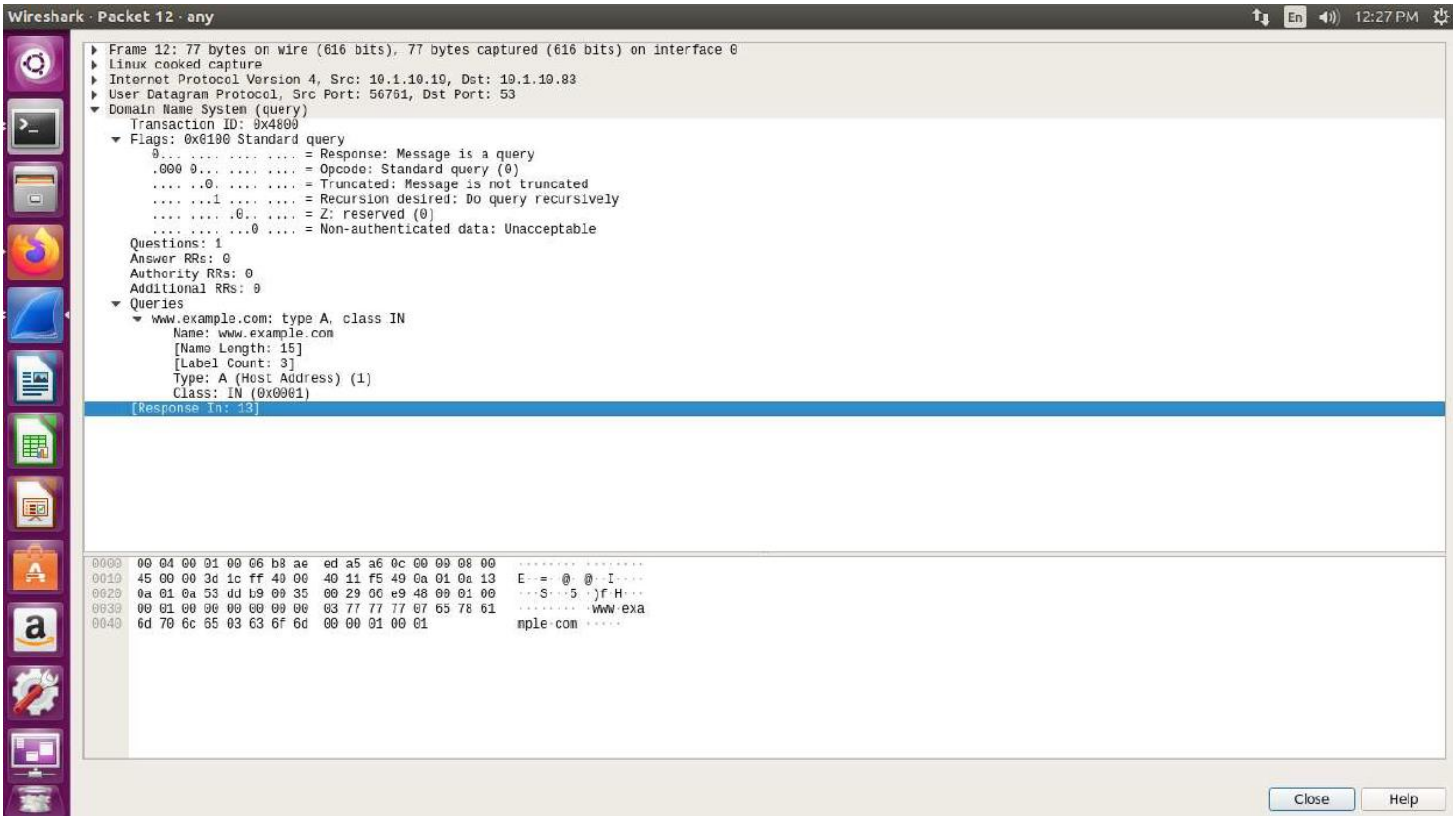
```
0030  00 01 00 00 00 00 00 00  03 77 77 77 06 67 6f 6f   ········ ·www·goo
0040  67 6c 65 03 63 6f 6d 00  00 01 00 01               gle·com· ····
```

Number of queries in packet (dns.count.queries), 2 bytes   Packets: 6 · Displayed: 4 (66.7%)   Profile: Default



```
▸ Frame 13: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.1.10.83, Dst: 10.1.10.19
▸ User Datagram Protocol, Src Port: 53, Dst Port: 56761
▾ Domain Name System (response)
     Transaction ID: 0x4800
   ▾ 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: 1
   ▾ 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 192.168.0.101
           Name: www.example.com
           Type: A (Host Address) (1)
           Class: IN (0x0001)
           Time to live: 259200
           Data length: 4
           Address: 192.168.0.101
   ▸ Authoritative nameservers
   ▸ Additional records
     [Request In: 12]
     [Time: 0.000627563 seconds]
```

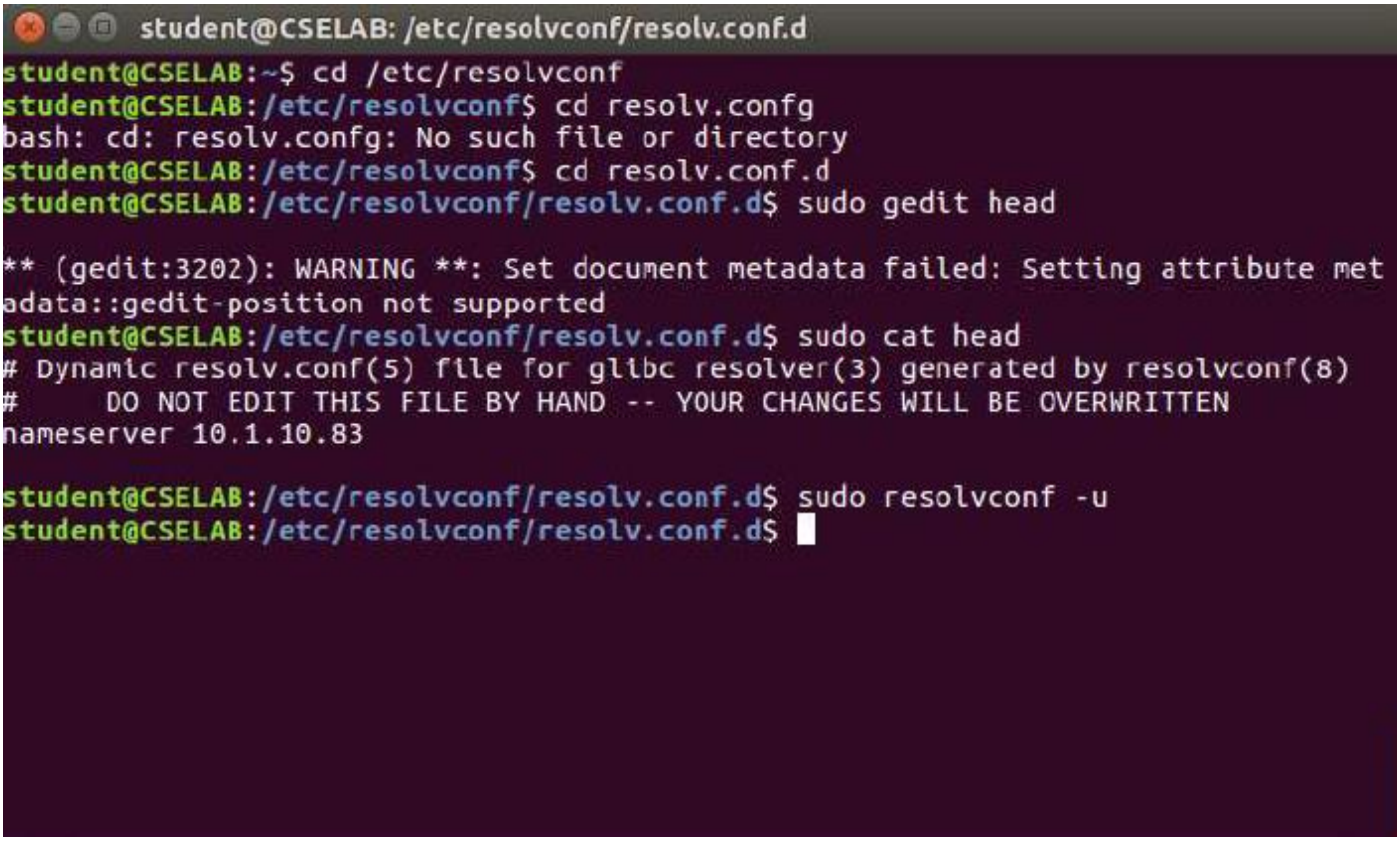
```
0000  00 00 00 01 00 06 b8 ae  ed a5 a6 8c 00 00 08 00   ········ ········
0010  45 00 00 6e 6b 18 00 00  40 11 e6 ff 0a 01 0a 53   E··nk··· @······S
```



```
▸ Frame 12: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.1.10.19, Dst: 10.1.10.83
▸ User Datagram Protocol, Src Port: 56761, Dst Port: 53
▾ Domain Name System (query)
     Transaction ID: 0x4800
   ▾ 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.example.com: type A, class IN
           Name: www.example.com
           [Name Length: 15]
           [Label Count: 3]
           Type: A (Host Address) (1)
           Class: IN (0x0001)
     [Response In: 13]
```

```
0000  00 04 00 01 00 06 b8 ae  ed a5 a6 0c 00 00 08 00   ········ ········
0010  45 00 00 3d 1c ff 40 00  40 11 f5 49 0a 01 0a 13   E··=··@· @··I····
0020  0a 01 0a 53 dd b9 00 35  00 29 66 e9 48 00 01 00   ···S···5 ·)f·H···
0030  00 01 00 00 00 00 00 00  03 77 77 77 07 65 78 61   ········ ·www·exa
0040  6d 70 6c 65 03 63 6f 6d  00 00 01 00 01            mple·com ·····
```

Local DNS cache on server:



```
student@CSELAB:~$ cd /etc/resolvconf
student@CSELAB:/etc/resolvconf$ cd resolv.confg
bash: cd: resolv.confg: No such file or directory
student@CSELAB:/etc/resolvconf$ cd resolv.conf.d
student@CSELAB:/etc/resolvconf/resolv.conf.d$ sudo gedit head

** (gedit:3202): WARNING **: Set document metadata failed: Setting attribute met
adata::gedit-position not supported
student@CSELAB:/etc/resolvconf/resolv.conf.d$ sudo cat 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 10.1.10.83

student@CSELAB:/etc/resolvconf/resolv.conf.d$ sudo resolvconf -u
student@CSELAB:/etc/resolvconf/resolv.conf.d$ █
```