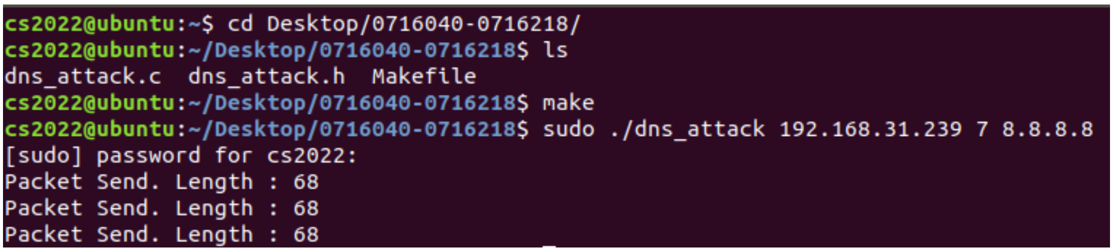
Student ID: 0716040 0716218

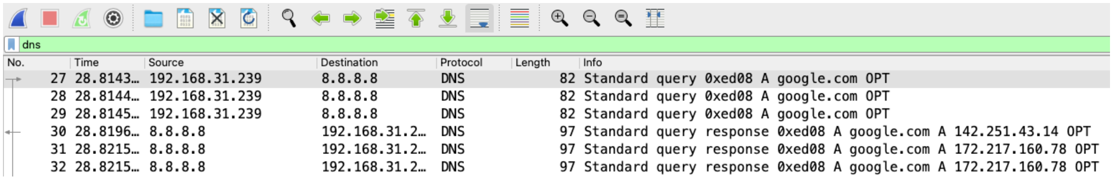
1.

Scenario:



```
cs2022@ubuntu:~$ cd Desktop/0716040-0716218/
cs2022@ubuntu:~/Desktop/0716040-0716218$ ls
dns_attack.c  dns_attack.h  Makefile
cs2022@ubuntu:~/Desktop/0716040-0716218$ make
cs2022@ubuntu:~/Desktop/0716040-0716218$ sudo ./dns_attack 192.168.31.239 7 8.8.8.8
[sudo] password for cs2022:
Packet Send. Length : 68
Packet Send. Length : 68
Packet Send. Length : 68
```

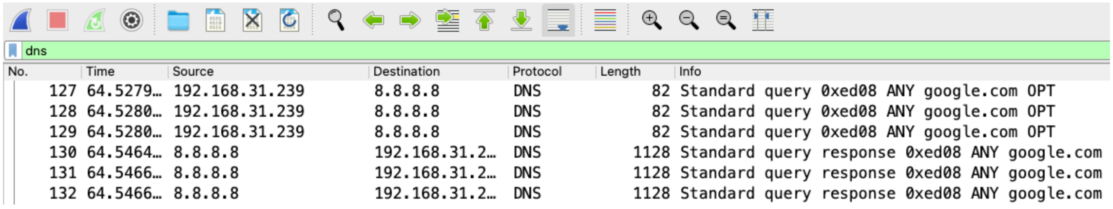
Task 1 result:



dns

No.	Time	Source	Destination	Protocol	Length	Info
27	28.8143…	192.168.31.239	8.8.8.8	DNS	82	Standard query 0xed08 A google.com OPT
28	28.8144…	192.168.31.239	8.8.8.8	DNS	82	Standard query 0xed08 A google.com OPT
29	28.8145…	192.168.31.239	8.8.8.8	DNS	82	Standard query 0xed08 A google.com OPT
30	28.8196…	8.8.8.8	192.168.31.2…	DNS	97	Standard query response 0xed08 A google.com A 142.251.43.14 OPT
31	28.8215…	8.8.8.8	192.168.31.2…	DNS	97	Standard query response 0xed08 A google.com A 172.217.160.78 OPT
32	28.8215…	8.8.8.8	192.168.31.2…	DNS	97	Standard query response 0xed08 A google.com A 172.217.160.78 OPT

Task 2 result:



dns

No.	Time	Source	Destination	Protocol	Length	Info
127	64.5279…	192.168.31.239	8.8.8.8	DNS	82	Standard query 0xed08 ANY google.com OPT
128	64.5280…	192.168.31.239	8.8.8.8	DNS	82	Standard query 0xed08 ANY google.com OPT
129	64.5280…	192.168.31.239	8.8.8.8	DNS	82	Standard query 0xed08 ANY google.com OPT
130	64.5464…	8.8.8.8	192.168.31.2…	DNS	1128	Standard query response 0xed08 ANY google.com
131	64.5466…	8.8.8.8	192.168.31.2…	DNS	1128	Standard query response 0xed08 ANY google.com
132	64.5466…	8.8.8.8	192.168.31.2…	DNS	1128	Standard query response 0xed08 ANY google.com

(amplification rate: 1128/82 = 13.75)

2.

Change the DNS query type from type A(0x0001) to ANY(0x00ff), and change the query website to a more ambiguous one, such as “google.com” (compared with “www.google.com”), which would make the DNS server reply with a much longer response.

3.

We can use port blocking method: block the unneeded ports.