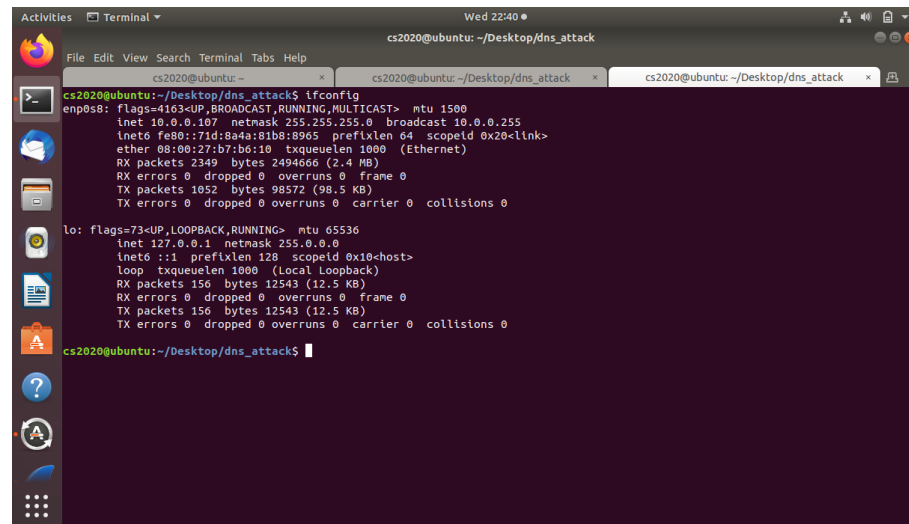


# Project 1: DNS Reflection and Amplification Attacks

Student ID: 0716085

## Part1: DNS Reflection and Amplification Attacks

Task I: DNS reflection attack:

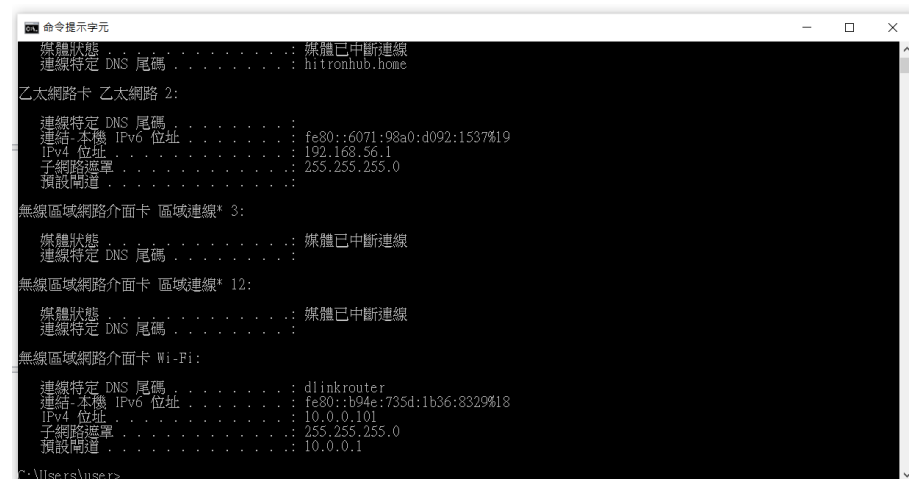


```
cs2020@ubuntu: ~/Desktop/dns_attack$ ifconfig
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.107 netmask 255.255.255.0 broadcast 10.0.0.255
    inet6 fe80::71d:984a:81b3:9965 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:b7:b6:10 txqueuelen 1000 (Ethernet)
    RX packets 2349 bytes 2494666 (2.4 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1052 bytes 98572 (98.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 156 bytes 12543 (12.5 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 156 bytes 12543 (12.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

cs2020@ubuntu: ~/Desktop/dns_attack$
```

(1) Attacker machine, ip addr = 10.0.0.107



```
命令提示字元
媒體狀態 . . . . . : 媒體已中斷連線
連線特定 DNS 尾碼 . . . . . : hitronhub.home

乙太網路卡 乙太網路 2:

連線特定 DNS 尾碼 . . . . . :
連結 本機 IPv6 位址 . . . . . : fe80::6071:98a0:d092:1537%19
IPv4 位址 . . . . . : 192.168.56.1
子網路遮罩 . . . . . : 255.255.255.0
預設閘道 . . . . . :

無線區域網路介面卡 區域連線* 3:

媒體狀態 . . . . . : 媒體已中斷連線
連線特定 DNS 尾碼 . . . . . :

無線區域網路介面卡 區域連線* 12:

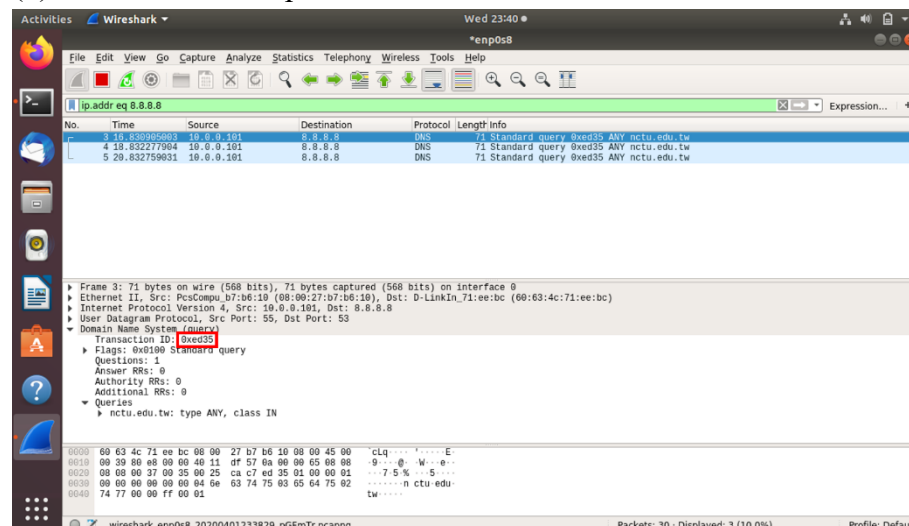
媒體狀態 . . . . . : 媒體已中斷連線
連線特定 DNS 尾碼 . . . . . :

無線區域網路介面卡 Wi-Fi:

連線特定 DNS 尾碼 . . . . . : dlinkrouter
連結 本機 IPv6 位址 . . . . . : fe80::b94e:735d:1b36:8329%18
IPv4 位址 . . . . . : 10.0.0.101
子網路遮罩 . . . . . : 255.255.255.0
預設閘道 . . . . . : 10.0.0.1

C:\Users\User>
```

(2) Victim machine, ip addr = 10.0.0.101

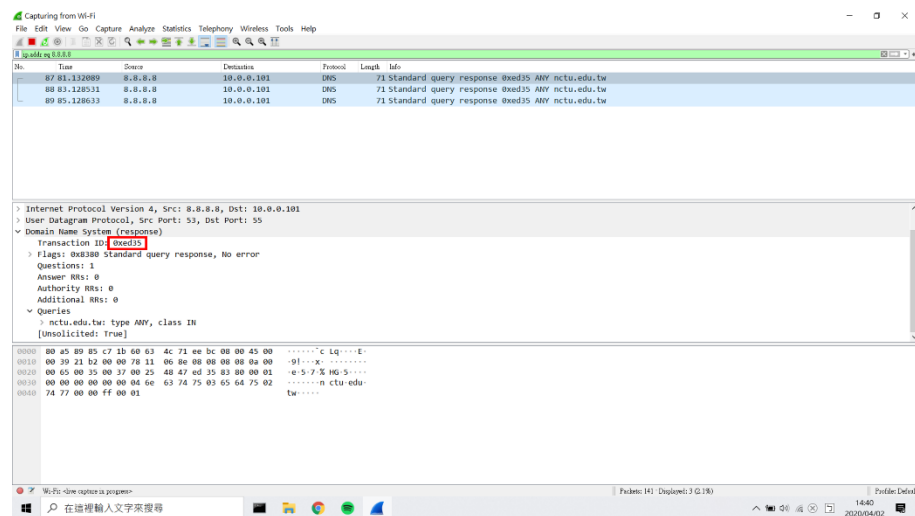


Wireshark packet capture showing a DNS query from the victim machine (10.0.0.101) to the attacker machine (10.0.0.107). The packet is a Standard query 0xed35 ANY nctu.edu.tw.

No.	Time	Source	Destination	Protocol	Length	Info
3	18.83995983	10.0.0.101	8.8.8.8	DNS	71	Standard query 0xed35 ANY nctu.edu.tw
4	18.832277904	10.0.0.101	8.8.8.8	DNS	71	Standard query 0xed35 ANY nctu.edu.tw
5	29.832759931	10.0.0.101	8.8.8.8	DNS	71	Standard query 0xed35 ANY nctu.edu.tw

Transaction ID: 0xed35  
Flags: 0x0190 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries  
nctu.edu.tw: type ANY, class IN

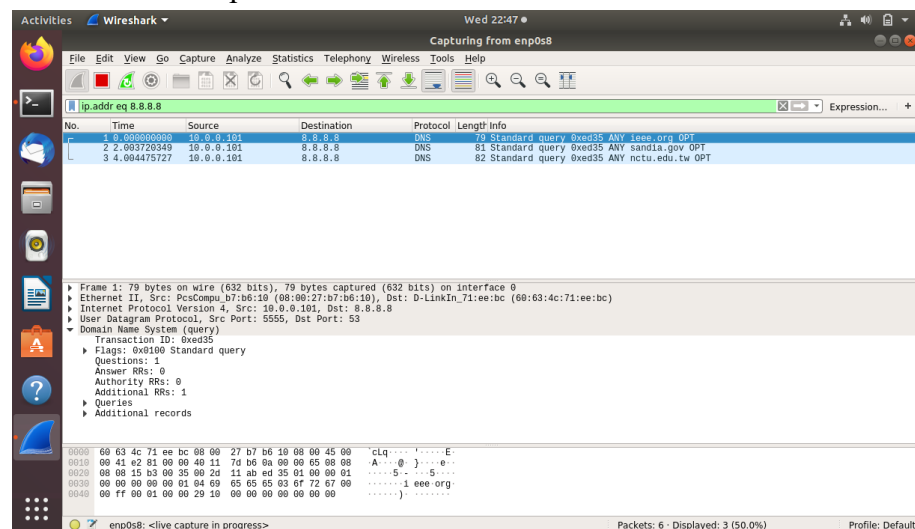
### (3-1) Capture packet at attacker machine



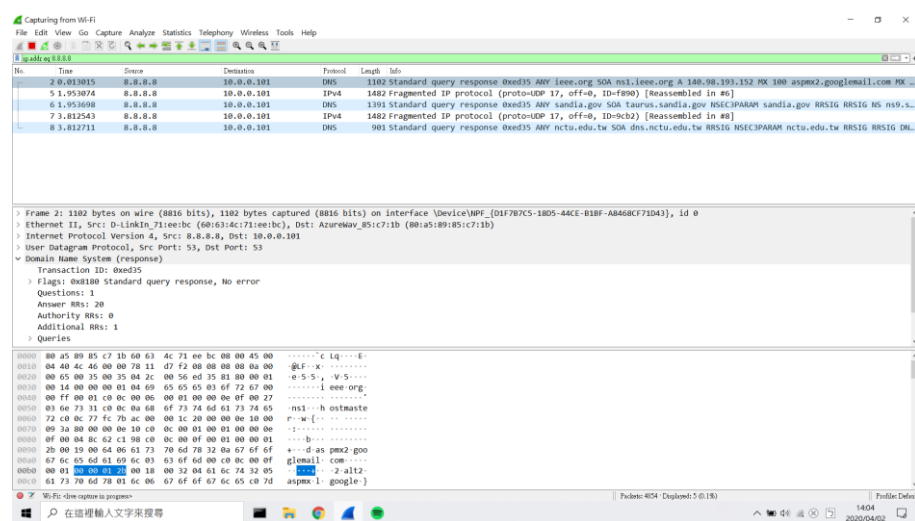
### (3-2) Capture packet at victim machine

By picture (3-1) and (3-2), it can show that DNS reflection attack is success.

### Task II: DNS amplification attack:



### (4-1) DNS request sent by attacker machine

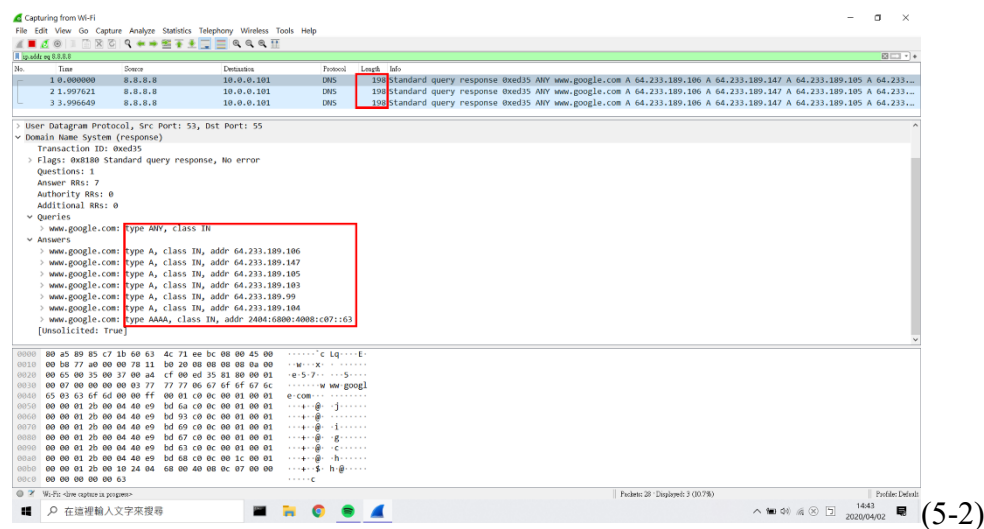
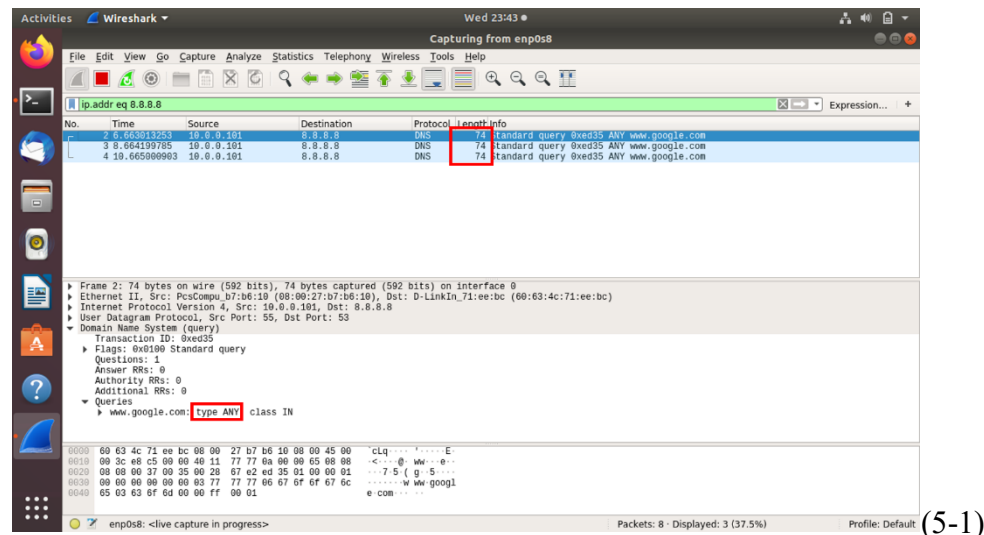


### (4-2) DNS response received by victim machine

By picture (4-1) and (4-2), it can show that DNS amplification attack is success.

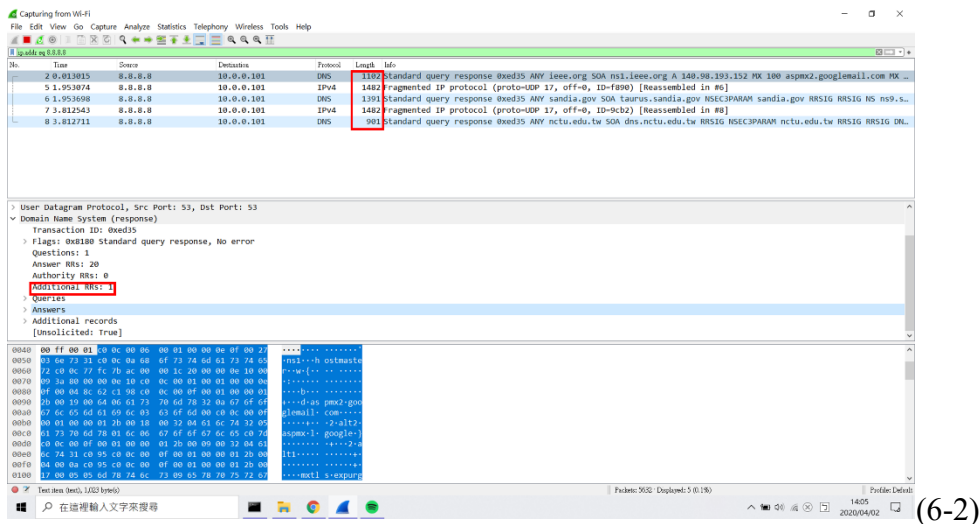
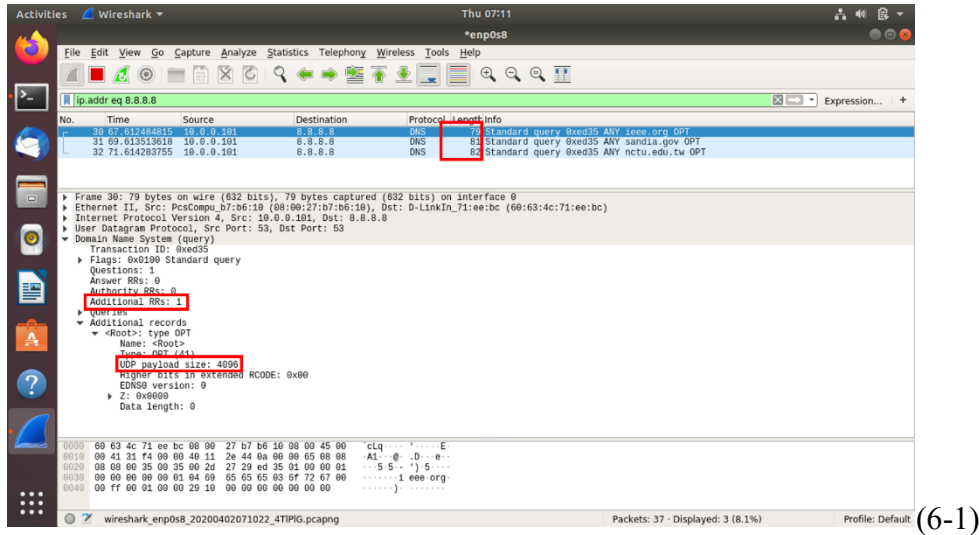
## Part 2: Way to amplify the DNS response

In DNS query, different query type will return different response. There is a query type called ANY, which will return all records of all types known. By using this type, response packet may be larger than request packet.



Picture (5-1) and (5-2) are the example of using type ANY and query name is “www.google.com”. It shows that amplification ratio is  $198/74 = 2.0$ .

Although the above method can amplify the response packet, the amplification ratio is quite small. To make the response packet much larger, we can use the additional section in DNS structure to increase the upper limit of UDP payload size.



Picture (6-1) and (6-2) are the example of using additional section and using 3 different query name “ieee.org”, “sandia.gov”, “nctu.edu.tw”. Their amplification ratio is  $1102/79 = 13.9$ ,  $1391/81 = 17.2$ ,  $901/82 = 11.0$  (only calculate DNS protocol). It is clearly that the second method’s response packet is larger than the first method. By the way, I don’t use the “www.google.com” as query name in second method is because the amplification ratio has only 2.5, it can’t see a big different between two methods.

### Part 3: Solution to defend against DoS attack based on the DNS reflection

We can’t completely defend the DNS reflection attack because of the importance of the DNS service. However, we can try to mitigate this kind of attack. One of the methods is disable the recursive query or setting access control list (ACL) to allow the trusted ip address on the list can use recursive query. Another way is once the server detected the DNS reflection attacks, the server can block these specific DNS servers that are used by the attacker.