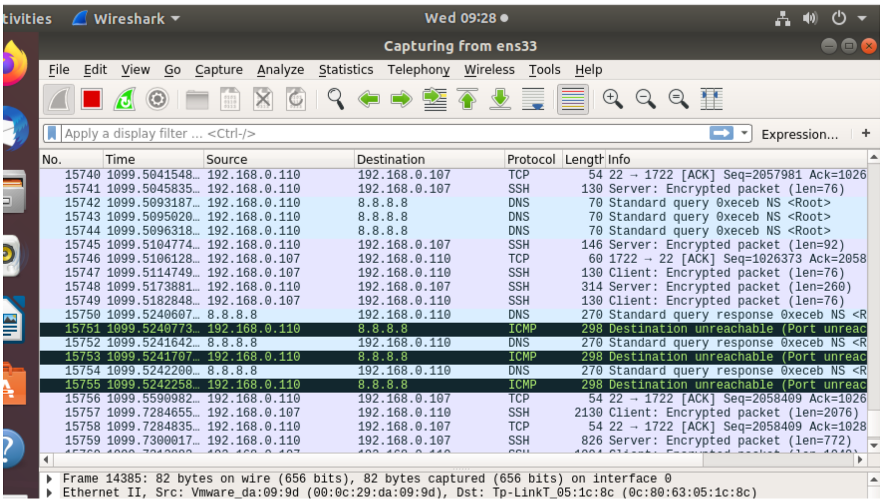
Item1:

0716011->10101110110011101011

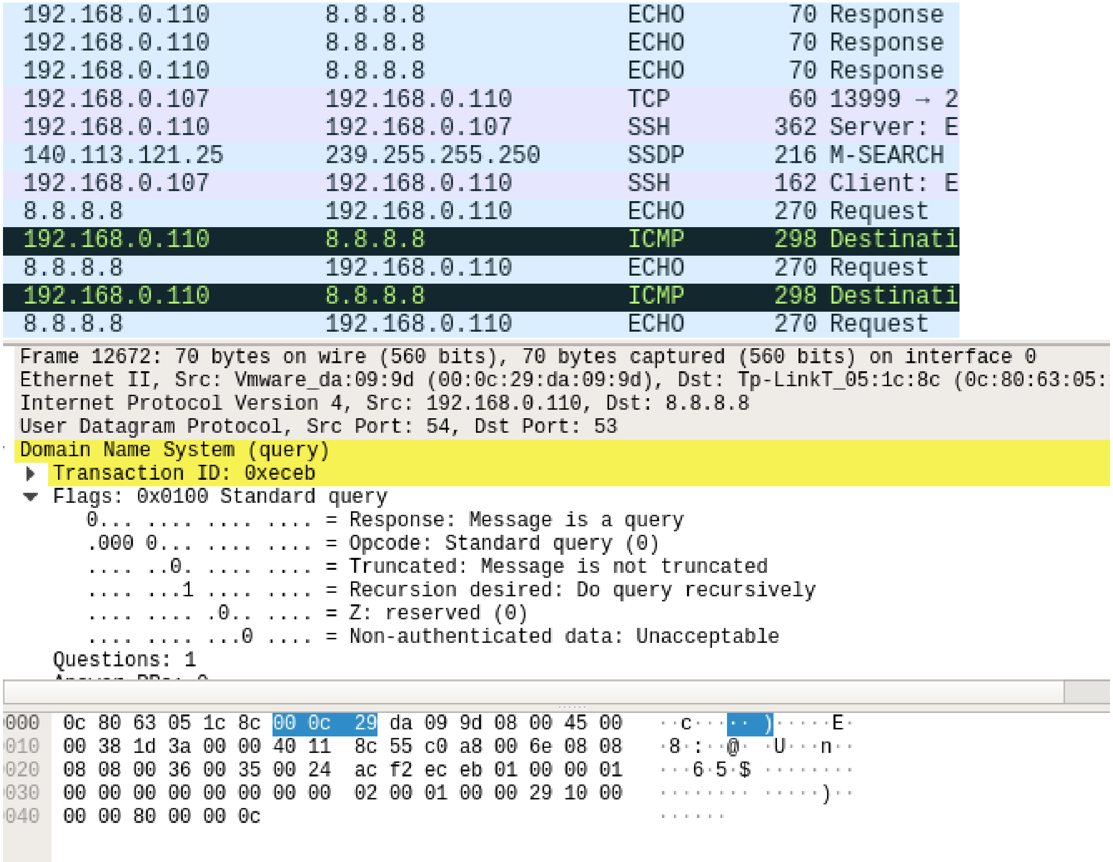
Take 16(1110110011101011)

->ECEB->0xECEB



tivities
Wireshark
Wed 09:28
Capturing from ens33
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…

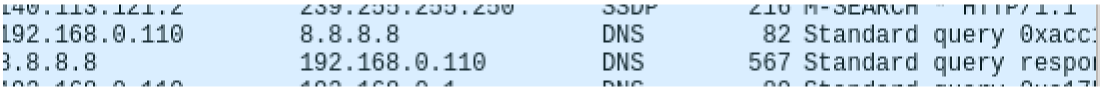
```
No.   Time             Source          Destination     Protocol Length Info
15740 1099.5041548…  192.168.0.110   192.168.0.107   TCP        54 22 → 1722 [ACK] Seq=2057981 Ack=1026
15741 1099.5045835…  192.168.0.110   192.168.0.107   SSH       130 Server: Encrypted packet (len=76)
15742 1099.5093187…  192.168.0.110   8.8.8.8         DNS        70 Standard query 0xeceb NS <Root>
15743 1099.5095020…  192.168.0.110   8.8.8.8         DNS        70 Standard query 0xeceb NS <Root>
15744 1099.5096318…  192.168.0.110   8.8.8.8         DNS        70 Standard query 0xeceb NS <Root>
15745 1099.5104774…  192.168.0.110   192.168.0.107   SSH       146 Server: Encrypted packet (len=92)
15746 1099.5106128…  192.168.0.107   192.168.0.110   TCP        60 1722 → 22 [ACK] Seq=1026373 Ack=2058
15747 1099.5114749…  192.168.0.107   192.168.0.110   SSH       130 Client: Encrypted packet (len=76)
15748 1099.5173881…  192.168.0.110   192.168.0.107   SSH       314 Server: Encrypted packet (len=260)
15749 1099.5182848…  192.168.0.107   192.168.0.110   SSH       130 Client: Encrypted packet (len=76)
15750 1099.5240607…  8.8.8.8         192.168.0.110   DNS       270 Standard query response 0xeceb NS <R
15751 1099.5240773…  192.168.0.110   8.8.8.8         ICMP      298 Destination unreachable (Port unreac
15752 1099.5241642…  8.8.8.8         192.168.0.110   DNS       270 Standard query response 0xeceb NS <R
15753 1099.5241707…  192.168.0.110   8.8.8.8         ICMP      298 Destination unreachable (Port unreac
15754 1099.5242200…  8.8.8.8         192.168.0.110   DNS       270 Standard query response 0xeceb NS <R
15755 1099.5242258…  192.168.0.110   8.8.8.8         ICMP      298 Destination unreachable (Port unreac
15756 1099.5590982…  192.168.0.110   192.168.0.107   TCP        54 22 → 1722 [ACK] Seq=2058409 Ack=1026
15757 1099.7284655…  192.168.0.107   192.168.0.110   SSH      2130 Client: Encrypted packet (len=2076)
15758 1099.7284835…  192.168.0.110   192.168.0.107   TCP        54 22 → 1722 [ACK] Seq=2058409 Ack=1028
15759 1099.7300017…  192.168.0.110   192.168.0.107   SSH       826 Server: Encrypted packet (len=772)

▸ Frame 14385: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
▸ Ethernet II, Src: Vmware_da:09:9d (00:0c:29:da:09:9d), Dst: Tp-LinkT_05:1c:8c (0c:80:63:05:1c:8c)
```



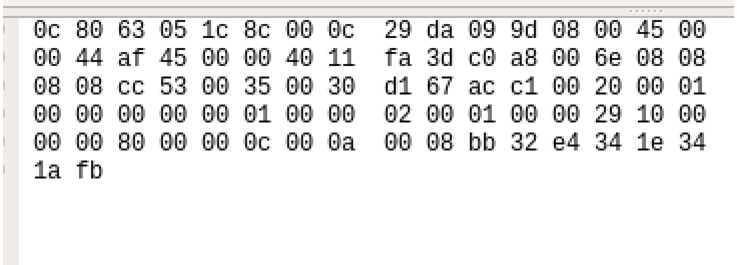
```
192.168.0.110      8.8.8.8            ECHO       70 Response
192.168.0.110      8.8.8.8            ECHO       70 Response
192.168.0.110      8.8.8.8            ECHO       70 Response
192.168.0.107      192.168.0.110      TCP        60 13999 → 2
192.168.0.110      192.168.0.107      SSH       362 Server: E
140.113.121.25     239.255.255.250    SSDP      216 M-SEARCH
192.168.0.107      192.168.0.110      SSH       162 Client: E
8.8.8.8            192.168.0.110      ECHO      270 Request
192.168.0.110      8.8.8.8            ICMP      298 Destinati
8.8.8.8            192.168.0.110      ECHO      270 Request
192.168.0.110      8.8.8.8            ICMP      298 Destinati
8.8.8.8            192.168.0.110      ECHO      270 Request

 Frame 12672: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
 Ethernet II, Src: Vmware_da:09:9d (00:0c:29:da:09:9d), Dst: Tp-LinkT_05:1c:8c (0c:80:63:05:
 Internet Protocol Version 4, Src: 192.168.0.110, Dst: 8.8.8.8
 User Datagram Protocol, Src Port: 54, Dst Port: 53
 Domain Name System (query)
 ▸ Transaction ID: 0xeceb
 ▾ 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

000  0c 80 63 05 1c 8c 00 0c  29 da 09 9d 08 00 45 00   ··c····· )·····E·
010  00 38 1d 3a 00 00 40 11  8c 55 c0 a8 00 6e 08 08   ·8·:··@· ·U···n··
020  08 08 00 36 00 35 00 24  ac f2 ec eb 01 00 00 01   ···6·5·$ ········
030  00 00 00 00 00 00 00 00  02 00 01 00 00 29 10 00   ········ ·····)··
040  00 00 80 00 00 0c                                   ······
```

Item2:

I find out the Internet says that using Dig … +trace can get huge message, so I type "dig @8.8.8.8 www.google.com +trace" and use wireshark to see what kind of packet pc actually send to dns server, and I type the hex bytes as the packet shown. However, the last few bytes are cookies, so I abandon them. The additional RRs should be 1,but it will make the response weak. And I accidentally put it to 0, which make the packet big.



```
140.113.121.2        239.255.255.250      SSDP       216 M-SEARCH * HTTP/1.1
192.168.0.110        8.8.8.8              DNS         82 Standard query 0xacc
8.8.8.8              192.168.0.110        DNS        567 Standard query respo
```



```
0c 80 63 05 1c 8c 00 0c  29 da 09 9d 08 00 45 00
00 44 af 45 00 00 40 11  fa 3d c0 a8 00 6e 08 08
08 08 cc 53 00 35 00 30  d1 67 ac c1 00 20 00 01
00 00 00 00 00 01 00 00  02 00 01 00 00 29 10 00
00 00 80 00 00 0c 00 0a  00 08 bb 32 e4 34 1e 34
1a fb
```

Item3:

Make the source ip verified by ISP is the most effective way.

Disable the recursion echo

only accept trusted ip when the packet is using DNS protocol

set a limit for flow control to each ip user, when exceed the limit reject packets from the ip.