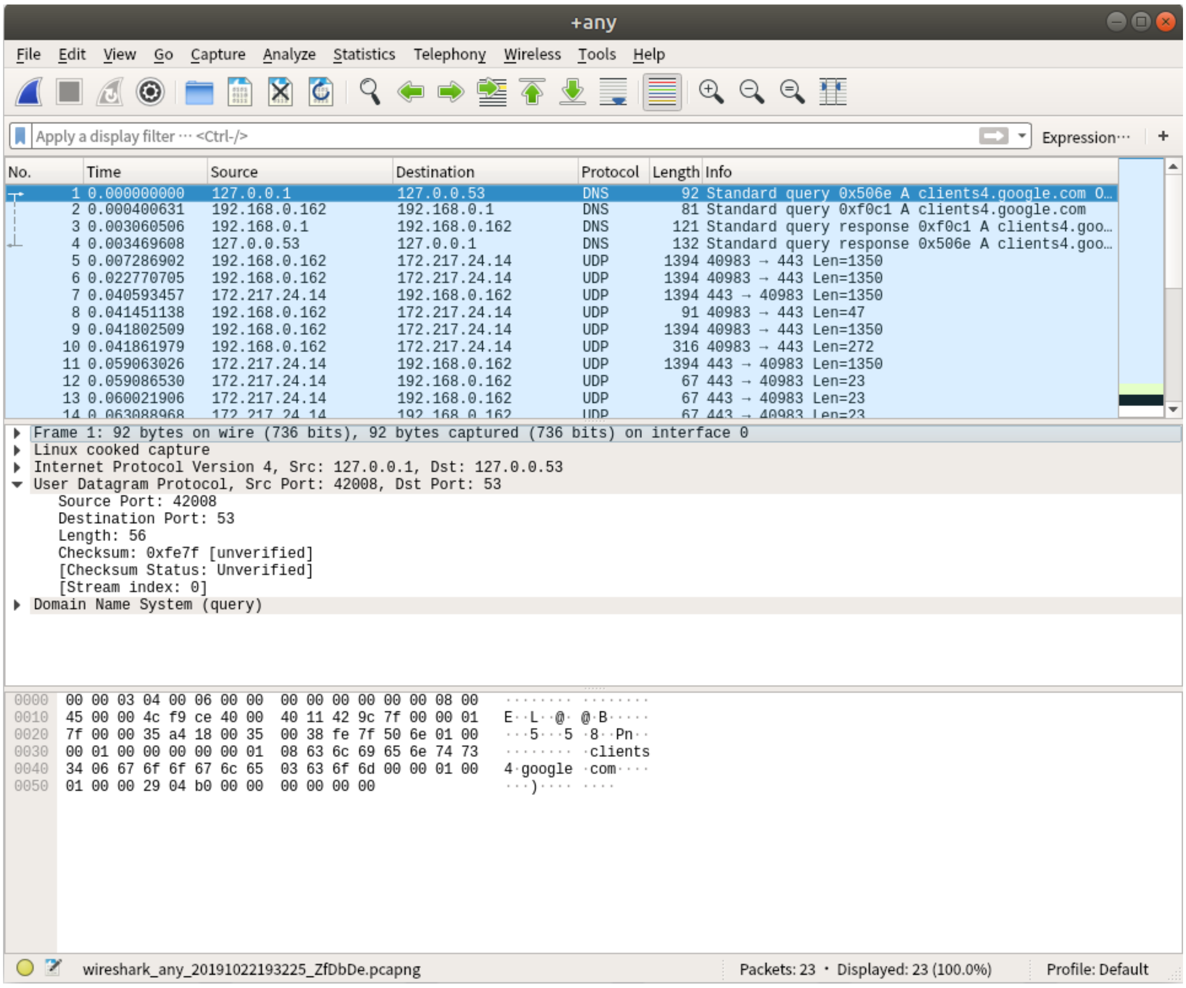
Computer Network HW1

by b06902034 黃柏諭

Problem 1


+any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

```
No.  Time         Source          Destination     Protocol Length Info
   1 0.000000000  127.0.0.1       127.0.0.53      DNS        92 Standard query 0x506e A clients4.google.com O…
   2 0.000400631  192.168.0.162   192.168.0.1     DNS        81 Standard query 0xf0c1 A clients4.google.com
   3 0.003060506  192.168.0.1     192.168.0.162   DNS       121 Standard query response 0xf0c1 A clients4.goo…
   4 0.003469608  127.0.0.53      127.0.0.1       DNS       132 Standard query response 0x506e A clients4.goo…
   5 0.007286902  192.168.0.162   172.217.24.14   UDP      1394 40983 → 443 Len=1350
   6 0.022770705  192.168.0.162   172.217.24.14   UDP      1394 40983 → 443 Len=1350
   7 0.040593457  172.217.24.14   192.168.0.162   UDP      1394 443 → 40983 Len=1350
   8 0.041451138  192.168.0.162   172.217.24.14   UDP        91 40983 → 443 Len=47
   9 0.041802509  192.168.0.162   172.217.24.14   UDP      1394 40983 → 443 Len=1350
  10 0.041861979  192.168.0.162   172.217.24.14   UDP       316 40983 → 443 Len=272
  11 0.059063026  172.217.24.14   192.168.0.162   UDP      1394 443 → 40983 Len=1350
  12 0.059086530  172.217.24.14   192.168.0.162   UDP        67 443 → 40983 Len=23
  13 0.060021906  172.217.24.14   192.168.0.162   UDP        67 443 → 40983 Len=23
  14 0.063088968  172.217.24.14   192.168.0.162   UDP        67 443 → 40983 Len=23
```

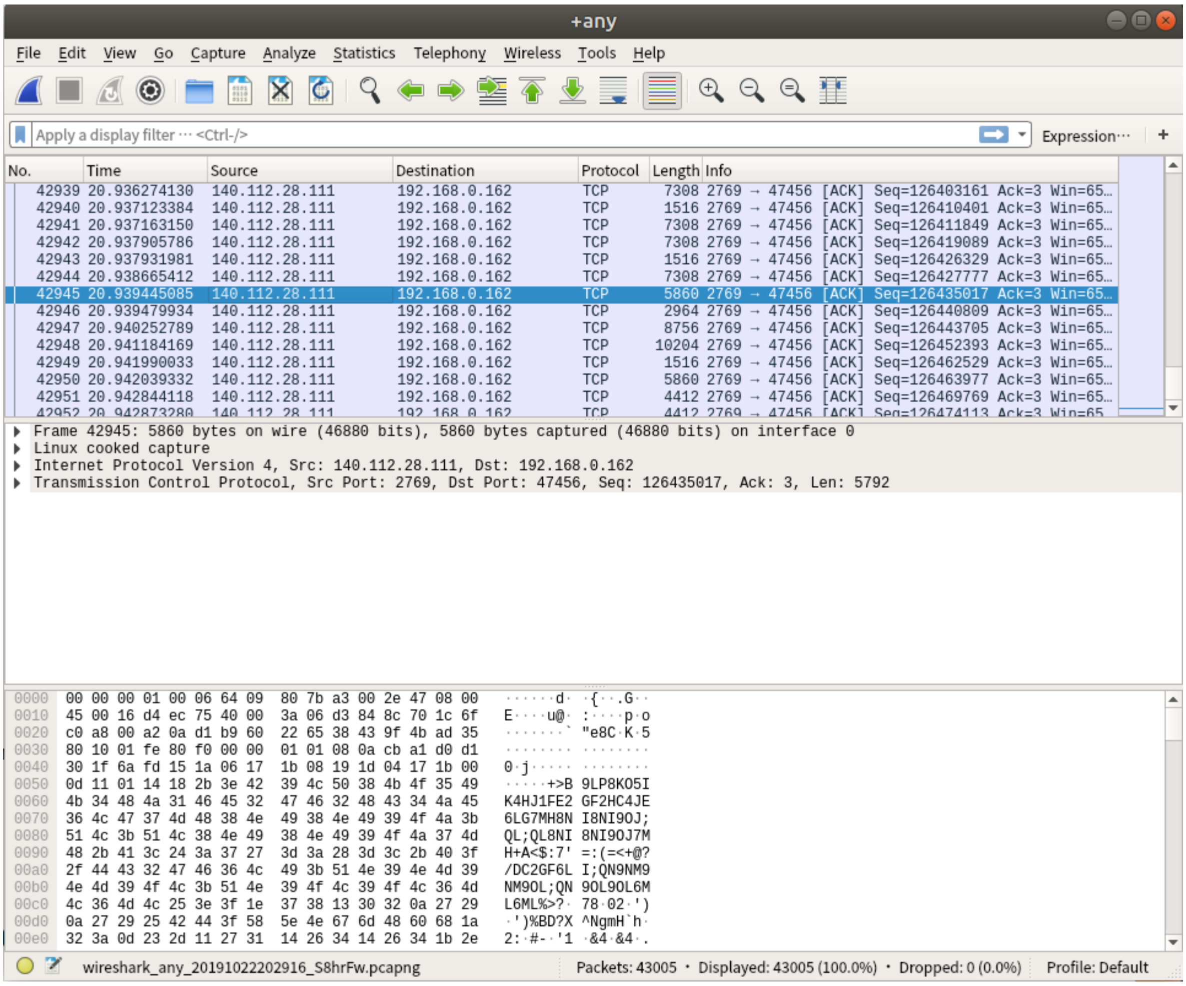
```
▸ Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.53
▾ User Datagram Protocol, Src Port: 42008, Dst Port: 53
    Source Port: 42008
    Destination Port: 53
    Length: 56
    Checksum: 0xfe7f [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
▸ Domain Name System (query)
```

```
0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 08 00   ········ ········
0010  45 00 00 4c f9 ce 40 00  40 11 42 9c 7f 00 00 01   E··L··@· @·B·····
0020  7f 00 00 35 a4 18 00 35  00 38 fe 7f 50 6e 01 00   ···5···5 ·8··Pn··
0030  00 01 00 00 00 00 00 01  08 63 6c 69 65 6e 74 73   ········ ·clients
0040  34 06 67 6f 6f 67 6c 65  03 63 6f 6d 00 00 01 00   4·google ·com····
0050  01 00 00 29 04 b0 00 00  00 00 00 00               ···)···· ····
```

```
wireshark_any_20191022193225_ZfDbDe.pcapng    Packets: 23 · Displayed: 23 (100.0%)    Profile: Default
```

- Website: www.google.com
- It's a DNS query, it provide the IP address of hostname

Problem 2



```
No.   Time        Source          Destination     Protocol Length Info
42939 20.936274130 140.112.28.111 192.168.0.162   TCP       7308 2769 → 47456 [ACK] Seq=126403161 Ack=3 Win=65…
42940 20.937123384 140.112.28.111 192.168.0.162   TCP       1516 2769 → 47456 [ACK] Seq=126410401 Ack=3 Win=65…
42941 20.937163150 140.112.28.111 192.168.0.162   TCP       7308 2769 → 47456 [ACK] Seq=126411849 Ack=3 Win=65…
42942 20.937905786 140.112.28.111 192.168.0.162   TCP       7308 2769 → 47456 [ACK] Seq=126419089 Ack=3 Win=65…
42943 20.937931981 140.112.28.111 192.168.0.162   TCP       1516 2769 → 47456 [ACK] Seq=126426329 Ack=3 Win=65…
42944 20.938665412 140.112.28.111 192.168.0.162   TCP       7308 2769 → 47456 [ACK] Seq=126427777 Ack=3 Win=65…
42945 20.939445085 140.112.28.111 192.168.0.162   TCP       5860 2769 → 47456 [ACK] Seq=126435017 Ack=3 Win=65…
42946 20.939479934 140.112.28.111 192.168.0.162   TCP       2964 2769 → 47456 [ACK] Seq=126440809 Ack=3 Win=65…
42947 20.940252789 140.112.28.111 192.168.0.162   TCP       8756 2769 → 47456 [ACK] Seq=126443705 Ack=3 Win=65…
42948 20.941184169 140.112.28.111 192.168.0.162   TCP      10204 2769 → 47456 [ACK] Seq=126452393 Ack=3 Win=65…
42949 20.941990033 140.112.28.111 192.168.0.162   TCP       1516 2769 → 47456 [ACK] Seq=126462529 Ack=3 Win=65…
42950 20.942039332 140.112.28.111 192.168.0.162   TCP       5860 2769 → 47456 [ACK] Seq=126463977 Ack=3 Win=65…
42951 20.942844118 140.112.28.111 192.168.0.162   TCP       4412 2769 → 47456 [ACK] Seq=126469769 Ack=3 Win=65…
42952 20.942873280 140.112.28.111 192.168.0.162   TCP       4412 2769 → 47456 [ACK] Seq=126474113 Ack=3 Win=65
```

```
▸ Frame 42945: 5860 bytes on wire (46880 bits), 5860 bytes captured (46880 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 140.112.28.111, Dst: 192.168.0.162
▸ Transmission Control Protocol, Src Port: 2769, Dst Port: 47456, Seq: 126435017, Ack: 3, Len: 5792
```

```
0000  00 00 00 01 00 06 64 09  80 7b a3 00 2e 47 08 00   ······d· ·{··.G··
0010  45 00 16 d4 ec 75 40 00  3a 06 d3 84 8c 70 1c 6f   E····u@· :····p·o
0020  c0 a8 00 a2 0a d1 b9 60  22 65 38 43 9f 4b ad 35   ·······` "e8C·K·5
0030  80 10 01 fe 80 f0 00 00  01 01 08 0a cb a1 d0 d1   ········ ········
0040  30 1f 6a fd 15 1a 06 17  1b 08 19 1d 04 17 1b 00   0·j····· ········
0050  0d 11 01 14 18 2b 3e 42  39 4c 50 38 4b 4f 35 49   ·····+>B 9LP8KO5I
0060  4b 34 48 4a 31 46 45 32  47 46 32 48 43 34 4a 45   K4HJ1FE2 GF2HC4JE
0070  36 4c 47 37 4d 48 38 4e  49 38 4e 49 39 4f 4a 3b   6LG7MH8N I8NI9OJ;
0080  51 4c 3b 51 4c 38 4e 49  38 4e 49 39 4f 4a 37 4d   QL;QL8NI 8NI9OJ7M
0090  48 2b 41 3c 24 3a 37 27  3d 3a 28 3d 3c 2b 40 3f   H+A<$:7' =:(=<+@?
00a0  2f 44 43 32 47 46 36 4c  49 3b 51 4e 39 4e 4d 39   /DC2GF6L I;QN9NM9
00b0  4e 4d 39 4f 4c 3b 51 4e  39 4f 4c 39 4f 4c 36 4d   NM9OL;QN 9OL9OL6M
00c0  4c 36 4d 4c 25 3e 3f 1e  37 38 13 30 32 0a 27 29   L6ML%>?· 78·02·')
00d0  0a 27 29 25 42 44 3f 58  5e 4e 67 6d 48 60 68 1a   ·')%BD?X ^NgmH`h·
00e0  32 3a 0d 23 2d 11 27 31  14 26 34 14 26 34 1b 2e   2:·#-·'1 ·&4·&4·.
```

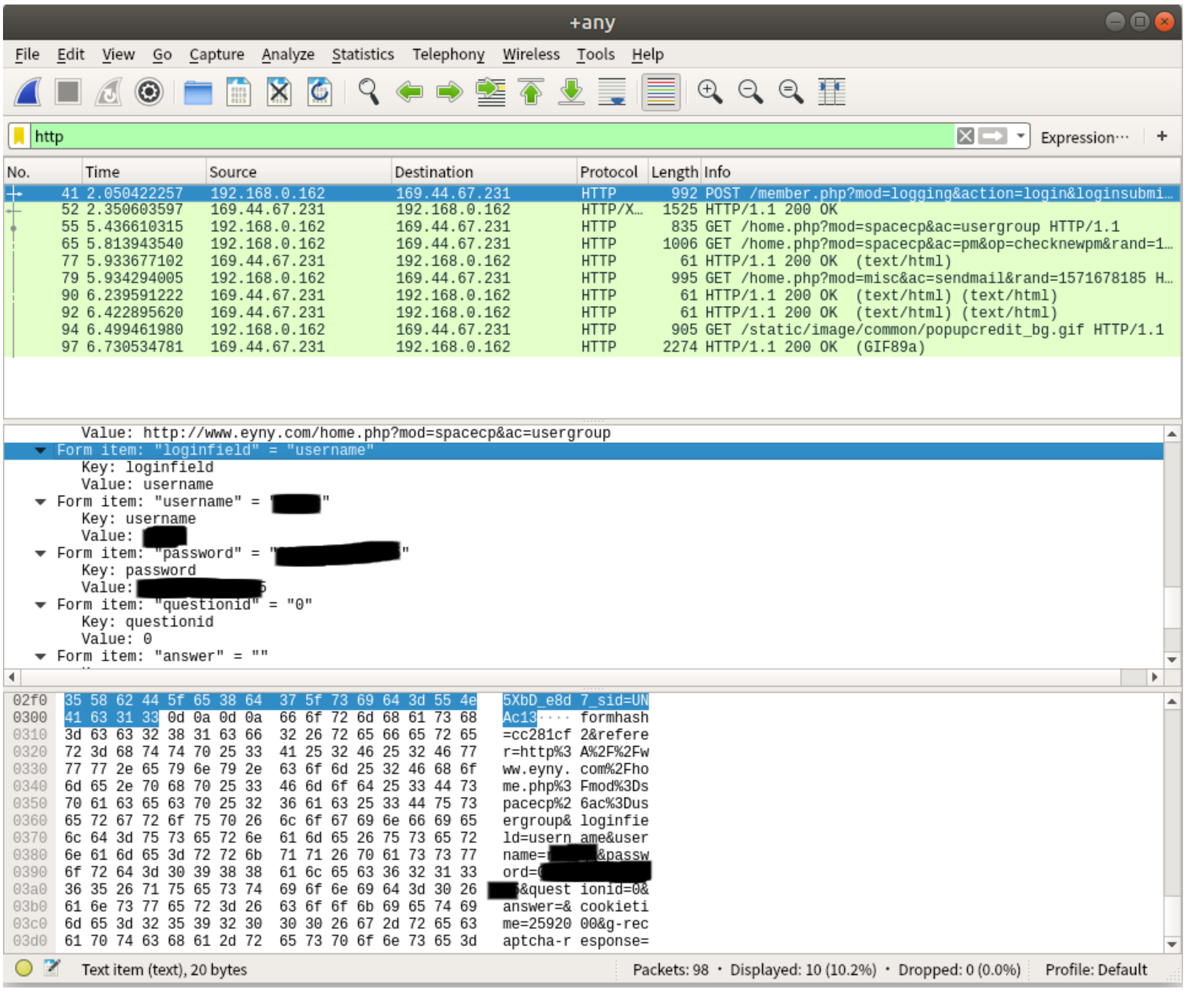
wireshark_any_20191022202916_S8hrFw.pcapng | Packets: 43005 · Displayed: 43005 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

- The port which server use is 2796

Problem 3

- Only TCP header contains: sequence number, acknowledgement number, flags, window size, urgent pointer
- Only UDP header contains: length
- Both of them contains source/destination port, check sum.

Problem 4



+any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

```
http
```

```
No.  Time          Source          Destination     Protocol Length Info
  41 2.050422257   192.168.0.162   169.44.67.231   HTTP        992 POST /member.php?mod=logging&action=login&loginsubmi…
  52 2.350603597   169.44.67.231   192.168.0.162   HTTP/X…    1525 HTTP/1.1 200 OK
  55 5.436610315   192.168.0.162   169.44.67.231   HTTP        835 GET /home.php?mod=spacecp&ac=usergroup HTTP/1.1
  65 5.813943540   192.168.0.162   169.44.67.231   HTTP       1006 GET /home.php?mod=spacecp&ac=pm&op=checknewpm&rand=1…
  77 5.933677102   169.44.67.231   192.168.0.162   HTTP         61 HTTP/1.1 200 OK  (text/html)
  79 5.934294005   192.168.0.162   169.44.67.231   HTTP        995 GET /home.php?mod=misc&ac=sendmail&rand=1571678185 H…
  90 6.239591222   169.44.67.231   192.168.0.162   HTTP         61 HTTP/1.1 200 OK  (text/html) (text/html)
  92 6.422895620   169.44.67.231   192.168.0.162   HTTP         61 HTTP/1.1 200 OK  (text/html) (text/html)
  94 6.499461980   192.168.0.162   169.44.67.231   HTTP        905 GET /static/image/common/popupcredit_bg.gif HTTP/1.1
  97 6.730534781   169.44.67.231   192.168.0.162   HTTP       2274 HTTP/1.1 200 OK  (GIF89a)
```

```
      Value: http://www.eyny.com/home.php?mod=spacecp&ac=usergroup
  ▾ Form item: "loginfield" = "username"
      Key: loginfield
      Value: username
  ▾ Form item: "username" = "[redacted]"
      Key: username
      Value: [redacted]
  ▾ Form item: "password" = "[redacted]"
      Key: password
      Value: [redacted]
  ▾ Form item: "questionid" = "0"
      Key: questionid
      Value: 0
  ▾ Form item: "answer" = ""
```

```
02f0  35 58 62 44 5f 65 38 64  37 5f 73 69 64 3d 55 4e   5XbD_e8d 7_sid=UN
0300  41 63 31 33 0d 0a 0d 0a  66 6f 72 6d 68 61 73 68   Ac13···· formhash
0310  3d 63 63 32 38 31 63 66  32 26 72 65 66 65 72 65   =cc281cf 2&refere
0320  72 3d 68 74 74 70 25 33  41 25 32 46 25 32 46 77   r=http%3 A%2F%2Fw
0330  77 77 2e 65 79 6e 79 2e  63 6f 6d 25 32 46 68 6f   ww.eyny. com%2Fho
0340  6d 65 2e 70 68 70 25 33  46 6d 6f 64 25 33 44 73   me.php%3 Fmod%3Ds
0350  70 61 63 65 63 70 25 32  36 61 63 25 33 44 75 73   pacecp%2 6ac%3Dus
0360  65 72 67 72 6f 75 70 26  6c 6f 67 69 6e 66 69 65   ergroup& loginfie
0370  6c 64 3d 75 73 65 72 6e  61 6d 65 26 75 73 65 72   ld=usern ame&user
0380  6e 61 6d 65 3d 72 72 6b  71 71 26 70 61 73 73 77   name=[redacted]&passw
0390  6f 72 64 3d 30 39 38 38  61 6c 65 63 36 32 31 33   ord=[redacted]
03a0  36 35 26 71 75 65 73 74  69 6f 6e 69 64 3d 30 26   [redacted]&quest ionid=0&
03b0  61 6e 73 77 65 72 3d 26  63 6f 6f 6b 69 65 74 69   answer=& cookieti
03c0  6d 65 3d 32 35 39 32 30  30 30 26 67 2d 72 65 63   me=25920 00&g-rec
03d0  61 70 74 63 68 61 2d 72  65 73 70 6f 6e 73 65 3d   aptcha-r esponse=
```

Text item (text), 20 bytes · Packets: 98 · Displayed: 10 (10.2%) · Dropped: 0 (0.0%) · Profile: Default

- Login website: http://www.eyny.com/member.php?mod=logging&action=login
- Attacker might use packet sniffer to get the password

Other Observation

- When using https instead of http, I cannot find plain text password via wireshark, hence https might be safer.