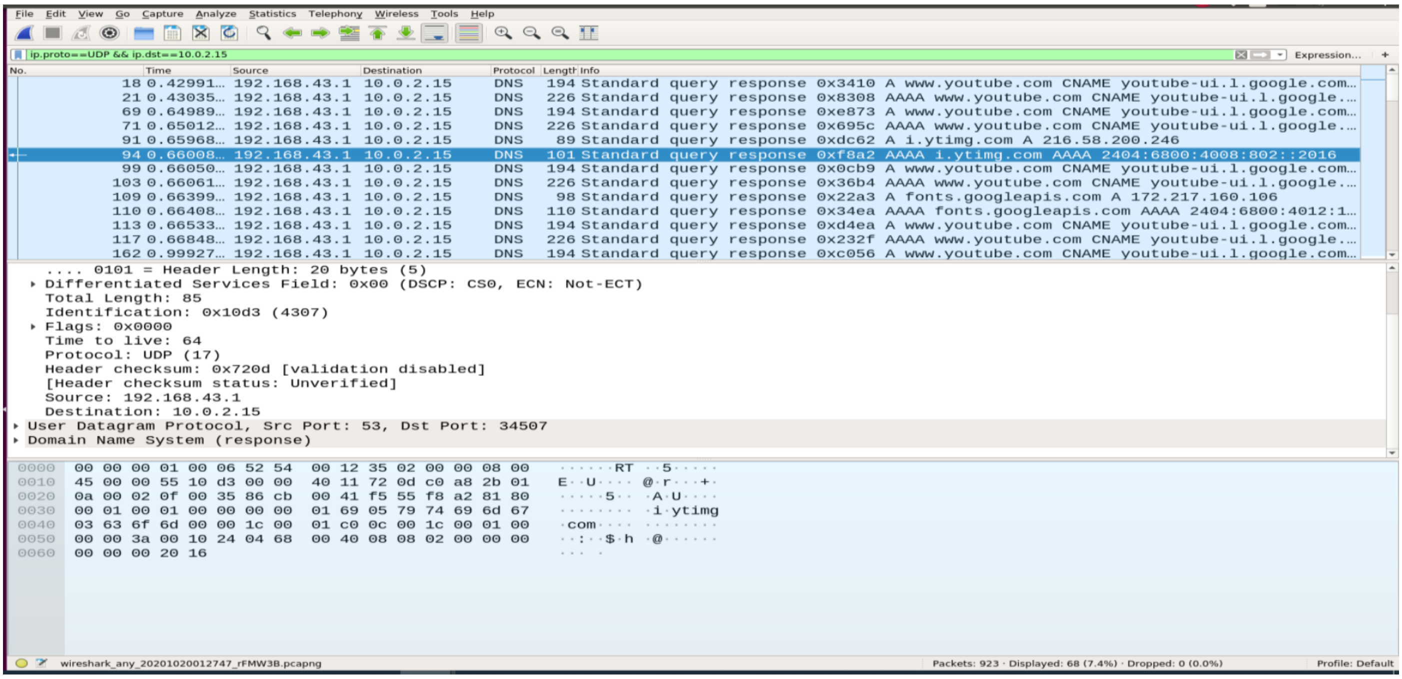
Computer Network 2020 HW1

B07902078 資工三 沈韋辰

01 Analysis of UDP packets


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

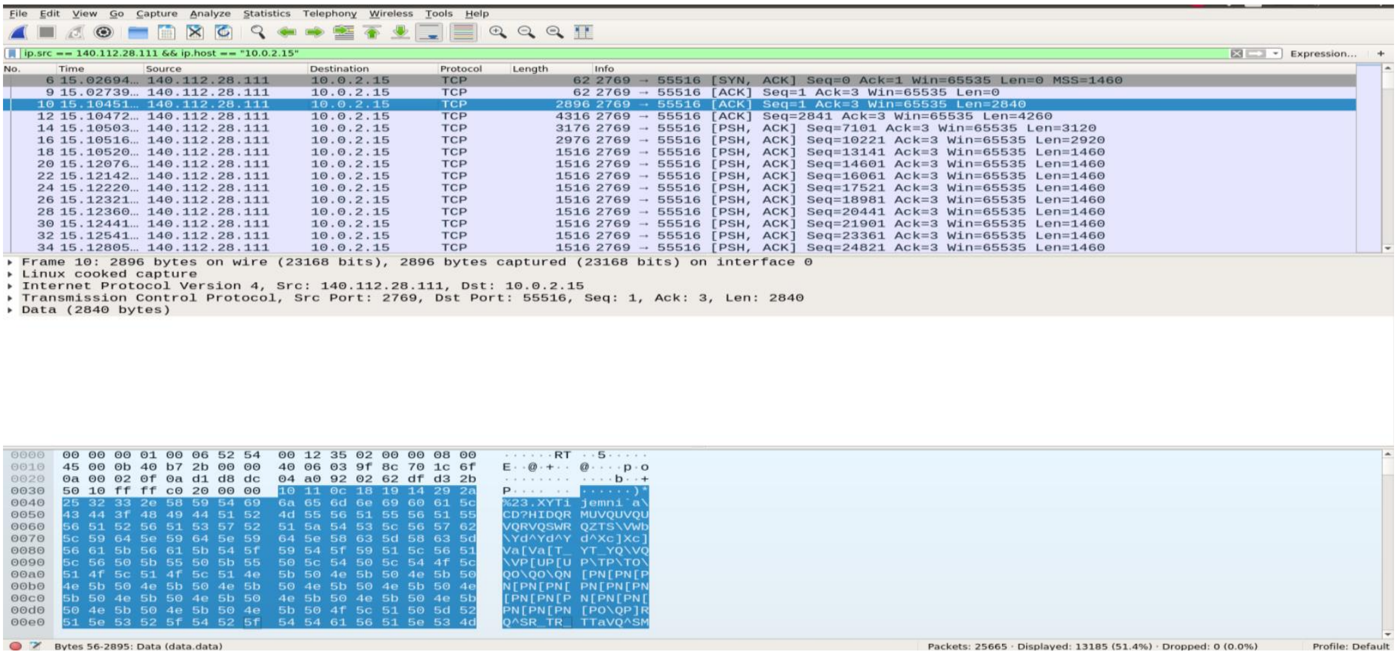
```
ip.proto==UDP && ip.dst==10.0.2.15

No.  Time       Source        Destination Protocol Length Info
  18 0.42991… 192.168.43.1 10.0.2.15   DNS  194 Standard query response 0x3410 A www.youtube.com CNAME youtube-ui.l.google.com…
  21 0.43035… 192.168.43.1 10.0.2.15   DNS  226 Standard query response 0x8308 AAAA www.youtube.com CNAME youtube-ui.l.google.…
  69 0.64989… 192.168.43.1 10.0.2.15   DNS  194 Standard query response 0xe873 A www.youtube.com CNAME youtube-ui.l.google.com…
  71 0.65012… 192.168.43.1 10.0.2.15   DNS  226 Standard query response 0x695c AAAA www.youtube.com CNAME youtube-ui.l.google.…
  91 0.65968… 192.168.43.1 10.0.2.15   DNS   89 Standard query response 0xdc62 A i.ytimg.com A 216.58.200.246
  94 0.66008… 192.168.43.1 10.0.2.15   DNS  101 Standard query response 0xf8a2 AAAA i.ytimg.com AAAA 2404:6800:4008:802::2016
  99 0.66050… 192.168.43.1 10.0.2.15   DNS  194 Standard query response 0x0cb9 A www.youtube.com CNAME youtube-ui.l.google.com…
 103 0.66061… 192.168.43.1 10.0.2.15   DNS  226 Standard query response 0x36b4 AAAA www.youtube.com CNAME youtube-ui.l.google.…
 109 0.66399… 192.168.43.1 10.0.2.15   DNS   98 Standard query response 0x22a3 A fonts.googleapis.com A 172.217.160.106
 110 0.66408… 192.168.43.1 10.0.2.15   DNS  110 Standard query response 0x34ea AAAA fonts.googleapis.com AAAA 2404:6800:4012:1…
 113 0.66533… 192.168.43.1 10.0.2.15   DNS  194 Standard query response 0xd4ea A www.youtube.com CNAME youtube-ui.l.google.com…
 117 0.66848… 192.168.43.1 10.0.2.15   DNS  226 Standard query response 0x232f AAAA www.youtube.com CNAME youtube-ui.l.google.…
 162 0.99927… 192.168.43.1 10.0.2.15   DNS  194 Standard query response 0xc056 A www.youtube.com CNAME youtube-ui.l.google.com…

    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 85
    Identification: 0x10d3 (4307)
  ▸ Flags: 0x0000
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0x720d [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.43.1
    Destination: 10.0.2.15
▸ User Datagram Protocol, Src Port: 53, Dst Port: 34507
▸ Domain Name System (response)

0000  00 00 00 01 00 06 52 54  00 12 35 02 00 00 08 00   ······RT ··5·····
0010  45 00 00 55 10 d3 00 00  40 11 72 0d c0 a8 2b 01   E··U···· @·r···+·
0020  0a 00 02 0f 00 35 86 cb  00 41 f5 55 f8 a2 81 80   ·····5·· ·A·U····
0030  00 01 00 01 00 00 00 00  01 69 05 79 74 69 6d 67   ········ ·i·ytimg
0040  03 63 6f 6d 00 00 1c 00  01 c0 0c 00 1c 00 01 00   ·com···· ········
0050  00 00 3a 00 10 24 04 68  00 40 08 08 02 00 00 00   ··:··$·h ·@······
0060  00 00 00 20 16                                     ··· ·

wireshark_any_20201020012747_rFMW3B.pcapng    Packets: 923 · Displayed: 68 (7.4%) · Dropped: 0 (0.0%)    Profile: Default
```

Webserver : DNS server (192.168.43.1)

Service: Mapping the domain name I requested (www.youtube.com) to IPv4 (216.58.200.238) address.

Why DNS prefer to use UDP? : UDP is faster and has less overhead than TCP. A DNS query is simple for the client. Therefore, if the request or response is not too large, using UDP is more economic. (Still exists a few cases use TCP for DNS.) Even though UDP is unreliable, it has good extensibility. We can add timeout or resend on the application layer to make it reliable.

02 Analysis of TCP packets


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

```
ip.src == 140.112.28.111 && ip.host == "10.0.2.15"

No. Time       Source          Destination Protocol Length Info
  6 15.02694… 140.112.28.111 10.0.2.15   TCP     62 2769 → 55516 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
  9 15.02739… 140.112.28.111 10.0.2.15   TCP     62 2769 → 55516 [ACK] Seq=1 Ack=3 Win=65535 Len=0
 10 15.10451… 140.112.28.111 10.0.2.15   TCP   2896 2769 → 55516 [ACK] Seq=1 Ack=3 Win=65535 Len=2840
 12 15.10472… 140.112.28.111 10.0.2.15   TCP   4316 2769 → 55516 [ACK] Seq=2841 Ack=3 Win=65535 Len=4260
 14 15.10503… 140.112.28.111 10.0.2.15   TCP   3176 2769 → 55516 [PSH, ACK] Seq=7101 Ack=3 Win=65535 Len=3120
 16 15.10516… 140.112.28.111 10.0.2.15   TCP   2976 2769 → 55516 [PSH, ACK] Seq=10221 Ack=3 Win=65535 Len=2920
 18 15.10520… 140.112.28.111 10.0.2.15   TCP   1516 2769 → 55516 [PSH, ACK] Seq=13141 Ack=3 Win=65535 Len=1460
 20 15.12076… 140.112.28.111 10.0.2.15   TCP   1516 2769 → 55516 [PSH, ACK] Seq=14601 Ack=3 Win=65535 Len=1460
 22 15.12142… 140.112.28.111 10.0.2.15   TCP   1516 2769 → 55516 [PSH, ACK] Seq=16061 Ack=3 Win=65535 Len=1460
 24 15.12220… 140.112.28.111 10.0.2.15   TCP   1516 2769 → 55516 [PSH, ACK] Seq=17521 Ack=3 Win=65535 Len=1460
 26 15.12321… 140.112.28.111 10.0.2.15   TCP   1516 2769 → 55516 [PSH, ACK] Seq=18981 Ack=3 Win=65535 Len=1460
 28 15.12360… 140.112.28.111 10.0.2.15   TCP   1516 2769 → 55516 [PSH, ACK] Seq=20441 Ack=3 Win=65535 Len=1460
 30 15.12441… 140.112.28.111 10.0.2.15   TCP   1516 2769 → 55516 [PSH, ACK] Seq=21901 Ack=3 Win=65535 Len=1460
 32 15.12541… 140.112.28.111 10.0.2.15   TCP   1516 2769 → 55516 [PSH, ACK] Seq=23361 Ack=3 Win=65535 Len=1460
 34 15.12805… 140.112.28.111 10.0.2.15   TCP   1516 2769 → 55516 [PSH, ACK] Seq=24821 Ack=3 Win=65535 Len=1460

▸ Frame 10: 2896 bytes on wire (23168 bits), 2896 bytes captured (23168 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 140.112.28.111, Dst: 10.0.2.15
▸ Transmission Control Protocol, Src Port: 2769, Dst Port: 55516, Seq: 1, Ack: 3, Len: 2840
▸ Data (2840 bytes)

0000  00 00 00 01 00 06 52 54  00 12 35 02 00 00 08 00   ······RT ··5·····
0010  45 00 0b 40 b7 2b 00 00  40 06 03 9f 8c 70 1c 6f   E··@·+·· @····p·o
0020  0a 00 02 0f 0a d1 d8 dc  04 a0 92 02 62 df d3 2b   ········ ····b··+
0030  50 10 ff ff c0 20 00 00  10 11 0c 18 19 14 29 2a   P······· ······)*
0040  25 32 33 2e 58 59 54 69  6a 65 6d 6e 69 60 61 5c   %23.XYTi jemni`a\
0050  43 44 3f 48 49 44 51 52  4d 55 56 51 55 56 51 55   CD?HIDQR MUVQUVQU
0060  56 51 52 56 51 53 57 52  51 5a 54 53 5c 56 57 62   VQRVQSWR QZTS\VWb
0070  5c 59 64 5e 59 64 5e 59  64 5e 58 63 5d 58 63 5d   \Yd^Yd^Y d^Xc]Xc]
0080  56 61 5b 56 61 5b 54 5f  59 54 5f 59 51 5c 56 51   Va[Va[T_ YT_YQ\VQ
0090  5c 56 50 5b 55 50 5b 55  50 5c 54 50 5c 54 4f 5c   \VP[UP[U P\TP\TO\
00a0  51 4f 5c 51 4f 5c 51 4e  5b 50 4e 5b 50 4e 5b 50   QO\QO\QN [PN[PN[P
00b0  4e 5b 50 4e 5b 50 4e 5b  50 4e 5b 50 4e 5b 50 4e   N[PN[PN[ PN[PN[PN
00c0  5b 50 4e 5b 50 4e 5b 50  4e 5b 50 4e 5b 50 4e 5b   [PN[PN[P N[PN[PN[
00d0  50 4e 5b 50 4e 5b 50 4e  5b 50 4f 5c 51 50 5d 52   PN[PN[PN [PO\QP]R
00e0  51 5e 53 52 5f 54 52 5f  54 54 61 56 51 5e 53 4d   Q^SR_TR_ TTaVQ^SM

Bytes 56-2895: Data (data.data)    Packets: 25665 · Displayed: 13185 (51.4%) · Dropped: 0 (0.0%)    Profile: Default
```

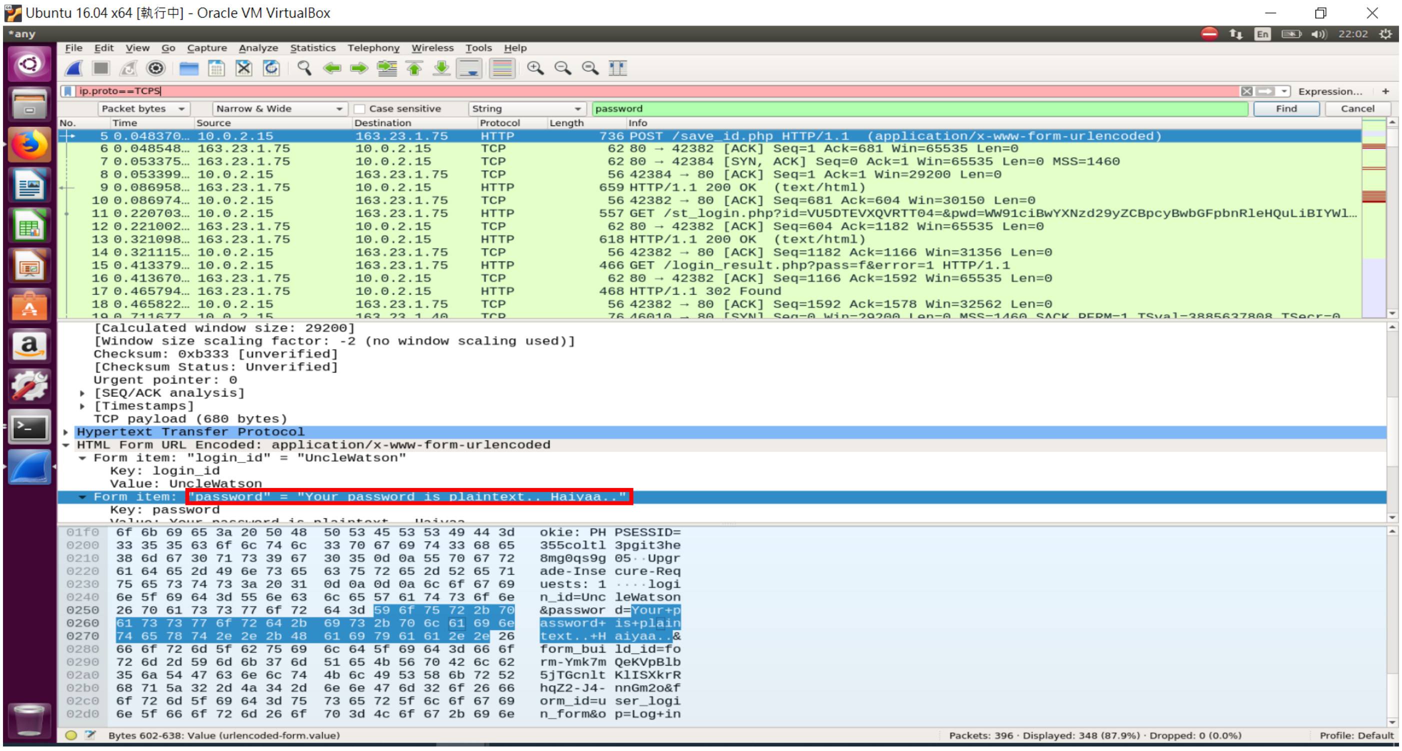
The server uses the port 2769.

03 Compare the headers of transport layer between TCP and UDP

- The average length of packet used TCP is larger than used UDP.
- TCP can transmit encrypted packets; while UDP usually transmit in plaintext.
- UDP only provides checksum; while TCP provides checksum, flags, sequence number, time stamp, etc.

04 Find out a plaintext password

- Screenshot of a packet



Ubuntu 16.04 x64 [執行中] - Oracle VM VirtualBox
*any
En
22:02
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
Find
Cancel

ip.proto==TCPS

Packet bytes | Narrow & Wide | ☐ Case sensitive | String | password

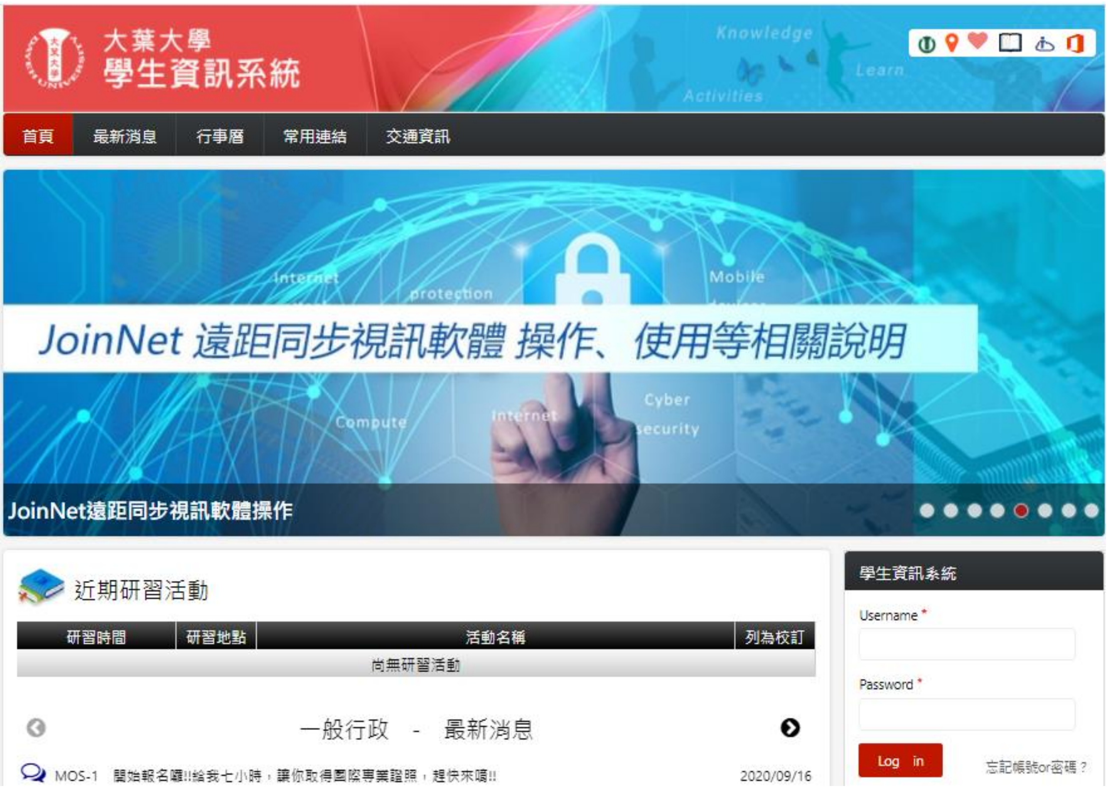
```
No.  Time        Source       Destination  Protocol Length Info
  5 0.048370… 10.0.2.15    163.23.1.75  HTTP     736 POST /save_id.php HTTP/1.1  (application/x-www-form-urlencoded)
  6 0.048548… 163.23.1.75  10.0.2.15    TCP       62 80 → 42382 [ACK] Seq=1 Ack=681 Win=65535 Len=0
  7 0.053375… 163.23.1.75  10.0.2.15    TCP       62 80 → 42384 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
  8 0.053399… 10.0.2.15    163.23.1.75  TCP       56 42384 → 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0
  9 0.086958… 163.23.1.75  10.0.2.15    HTTP     659 HTTP/1.1 200 OK  (text/html)
 10 0.086974… 10.0.2.15    163.23.1.75  TCP       56 42382 → 80 [ACK] Seq=681 Ack=604 Win=30150 Len=0
 11 0.220703… 10.0.2.15    163.23.1.75  HTTP     557 GET /st_login.php?id=VU5DTEVXQVRTT04=&pwd=WW91ciBwYXNzd29yZCBpcyBwbGFpbnRleHQuLiBIYWl…
 12 0.221002… 163.23.1.75  10.0.2.15    TCP       62 80 → 42382 [ACK] Seq=604 Ack=1182 Win=65535 Len=0
 13 0.321098… 163.23.1.75  10.0.2.15    HTTP     618 HTTP/1.1 200 OK  (text/html)
 14 0.321115… 10.0.2.15    163.23.1.75  TCP       56 42382 → 80 [ACK] Seq=1182 Ack=1166 Win=31356 Len=0
 15 0.413379… 10.0.2.15    163.23.1.75  HTTP     466 GET /login_result.php?pass=f&error=1 HTTP/1.1
 16 0.413670… 163.23.1.75  10.0.2.15    TCP       62 80 → 42382 [ACK] Seq=1166 Ack=1592 Win=65535 Len=0
 17 0.465794… 163.23.1.75  10.0.2.15    HTTP     468 HTTP/1.1 302 Found
 18 0.465822… 10.0.2.15    163.23.1.75  TCP       56 42382 → 80 [ACK] Seq=1592 Ack=1578 Win=32562 Len=0
 19 0.711677… 10.0.2.15    163.23.1.40  TCP       76 46010 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3885637808 TSecr=0
```

```
    [Calculated window size: 29200]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0xb333 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ [SEQ/ACK analysis]
  ▸ [Timestamps]
    TCP payload (680 bytes)
▸ Hypertext Transfer Protocol
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▾ Form item: "login_id" = "UncleWatson"
      Key: login_id
      Value: UncleWatson
  ▾ Form item: "password" = "Your password is plaintext.. Haiyaa.."
      Key: password
      Value: Your password is plaintext.. Haiyaa..
```

```
01f0  6f 6b 69 65 3a 20 50 48  50 53 45 53 53 49 44 3d   okie: PH PSESSID=
0200  33 35 35 63 6f 6c 74 6c  33 70 67 69 74 33 68 65   355coltl 3pgit3he
0210  38 6d 67 30 71 73 39 67  30 35 0d 0a 55 70 67 72   8mg0qs9g 05··Upgr
0220  61 64 65 2d 49 6e 73 65  63 75 72 65 2d 52 65 71   ade-Inse cure-Req
0230  75 65 73 74 73 3a 20 31  0d 0a 0d 0a 6c 6f 67 69   uests: 1 ····logi
0240  6e 5f 69 64 3d 55 6e 63  6c 65 57 61 74 73 6f 6e   n_id=Unc leWatson
0250  26 70 61 73 73 77 6f 72  64 3d 59 6f 75 72 2b 70   &passwor d=Your+p
0260  61 73 73 77 6f 72 64 2b  69 73 2b 70 6c 61 69 6e   assword+ is+plain
0270  74 65 78 74 2e 2e 2b 48  61 69 79 61 61 2e 2e 26   text..+H aiyaa..&
0280  66 6f 72 6d 5f 62 75 69  6c 64 5f 69 64 3d 66 6f   form_bui ld_id=fo
0290  72 6d 2d 59 6d 6b 37 6d  51 65 4b 56 70 42 6c 62   rm-Ymk7m QeKVpBlb
02a0  35 6a 54 47 63 6e 6c 74  4b 6c 49 53 58 6b 72 52   5jTGcnlt KlISXkrR
02b0  68 71 5a 32 2d 4a 34 2d  6e 6e 47 6d 32 6f 26 66   hqZ2-J4- nnGm2o&f
02c0  6f 72 6d 5f 69 64 3d 75  73 65 72 5f 6c 6f 67 69   orm_id=u ser_logi
02d0  6e 5f 66 6f 72 6d 26 6f  70 3d 4c 6f 67 2b 69 6e   n_form&o p=Log+in
```

Bytes 602-638: Value (urlencoded-form.value) | Packets: 396 · Displayed: 348 (87.9%) · Dropped: 0 (0.0%) | Profile: Default

- website: 大葉大學學生資訊系統 http://sis.dyu.edu.tw/RWD/



近期研習活動

研習時間	研習地點	活動名稱	列為校訂
尚無研習活動			

一般行政 - 最新消息

MOS-1 開始報名囉!!給我七小時，讓你取得國際專業證照，趕快來喔!! 2020/09/16

學生資訊系統

Username *

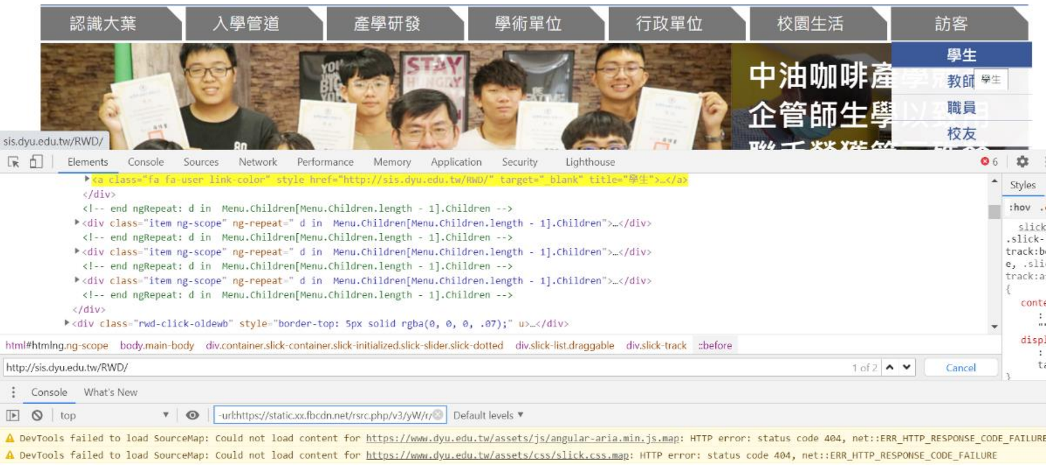
Password *

Log in

忘記帳號or密碼？

- Why is it not safe?
  Transporting the packet may pass over many routers. If there is an attacker sniffer between the link of the user and server, he may get the plaintext of password and be able to access the user's account.

Bonus



```
<a class="fa fa-user link-color" style href="http://sis.dyu.edu.tw/RWD/" target="_blank" title="學生">…</a>
</div>
<!-- end ngRepeat: d in  Menu.Children[Menu.Children.length - 1].Children -->
<div class="item ng-scope" ng-repeat=" d in  Menu.Children[Menu.Children.length - 1].Children">…</div>
<!-- end ngRepeat: d in  Menu.Children[Menu.Children.length - 1].Children -->
<div class="item ng-scope" ng-repeat=" d in  Menu.Children[Menu.Children.length - 1].Children">…</div>
<!-- end ngRepeat: d in  Menu.Children[Menu.Children.length - 1].Children -->
<div class="item ng-scope" ng-repeat=" d in  Menu.Children[Menu.Children.length - 1].Children">…</div>
<!-- end ngRepeat: d in  Menu.Children[Menu.Children.length - 1].Children -->
</div>
<div class="rwd-click-oldewb" style="border-top: 5px solid rgba(0, 0, 0, .07);" u>…</div>
```

http://sis.dyu.edu.tw/RWD/ 1 of 2

-url:https://static.xx.fbcdn.net/rsrc.php/v3/yW/r/

```
DevTools failed to load SourceMap: Could not load content for https://www.dyu.edu.tw/assets/js/angular-aria.min.js.map: HTTP error: status code 404, net::ERR_HTTP_RESPONSE_CODE_FAILURE
DevTools failed to load SourceMap: Could not load content for https://www.dyu.edu.tw/assets/css/slick.css.map: HTTP error: status code 404, net::ERR_HTTP_RESPONSE_CODE_FAILURE
```

- I found that the student system is insecure due to the homepage which jumps to the student system has an insecure HTML code: the href attribute uses **http** rather than **https.** https will encrypt the packet while http won't.