

# Computer Network Assignment 1

b06902048 資工三 李峻宇

## Analysis of UDP packets

Screenshot:

The screenshot displays the Wireshark network traffic analysis tool. The top pane shows a list of captured packets. Packet 7 is a UDP packet from 192.168.0.100 to 172.217.24.22 on port 443 to 62516. The middle pane shows the details of the selected packet, including the Ethernet II header, Internet Protocol Version 4 header, and User Datagram Protocol (UDP) header. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
6	0.170252	192.168.0.100	172.217.160.68	TCP	66	56789 → 443 [ACK] Seq=2050833823 Ack=78387571 Win=2048 L...
7	0.699856	192.168.0.100	172.217.24.22	UDP	175	62516 → 443 Len=133
8	0.711661	172.217.24.22	192.168.0.100	UDP	1400	443 → 62516 Len=1350 [ETHERNET FRAME CHECK SEQUENCE INCO...
9	0.711894	172.217.24.22	192.168.0.100	UDP	1400	443 → 62516 Len=1350 [ETHERNET FRAME CHECK SEQUENCE INCO...
10	0.711896	172.217.24.22	192.168.0.100	UDP	1400	443 → 62516 Len=1350 [ETHERNET FRAME CHECK SEQUENCE INCO...
11	0.712205	172.217.24.22	192.168.0.100	UDP	1400	443 → 62516 Len=1350 [ETHERNET FRAME CHECK SEQUENCE INCO...
12	0.712372	172.217.24.22	192.168.0.100	UDP	1400	443 → 62516 Len=1350 [ETHERNET FRAME CHECK SEQUENCE INC...
13	0.712458	172.217.24.22	192.168.0.100	UDP	1400	443 → 62516 Len=1350 [ETHERNET FRAME CHECK SEQUENCE INCO...
14	0.712782	172.217.24.22	192.168.0.100	UDP	1400	443 → 62516 Len=1350 [ETHERNET FRAME CHECK SEQUENCE INCO...
15	0.713003	172.217.24.22	192.168.0.100	UDP	1400	443 → 62516 Len=1350 [ETHERNET FRAME CHECK SEQUENCE INCO...
16	0.713048	172.217.24.22	192.168.0.100	UDP	1400	443 → 62516 Len=1350 [ETHERNET FRAME CHECK SEQUENCE INCO...
17	0.713353	192.168.0.100	172.217.24.22	UDP	71	62516 → 443 Len=29

Frame 12: 1400 bytes on wire (11200 bits), 1400 bytes captured (11200 bits) on interface 0

Ethernet II, Src: D-LinkIn\_c5:e8:b2 (90:94:e4:c5:e8:b2), Dst: Apple\_66:d9:9f (f0:18:98:66:d9:9f)

Internet Protocol Version 4, Src: 172.217.24.22, Dst: 192.168.0.100

User Datagram Protocol, Src Port: 443, Dst Port: 62516

Source Port: 443  
Destination Port: 62516  
Length: 1350  
Checksum: 0x2a84 [unverified]  
[Checksum Status: Unverified]  
[Stream index: 0]

Data (1350 bytes)  
Data: 41014ae4f6b64ff6fc7c0ad9331aaabca46c4e089d68b42c...  
[Length: 1350]

0020 00 64 01 bb f4 34 05 4e 2a 84 41 01 01 4a e4 f6 b6 -d...4-N \*A-J...  
0030 4f f6 fc 7c 0a d9 33 1a aa bc a4 6c 4e 08 9d 68 0...|...3...UN...h  
0040 b4 2c cc 01 0b 83 b9 a5 47 25 46 a3 3d aa b2 7e ,.....G%F=...~  
0050 b6 6b f1 0e 17 28 27 ce 87 3f 42 44 1b f6 7c 4d -k...(!...?BD...|M

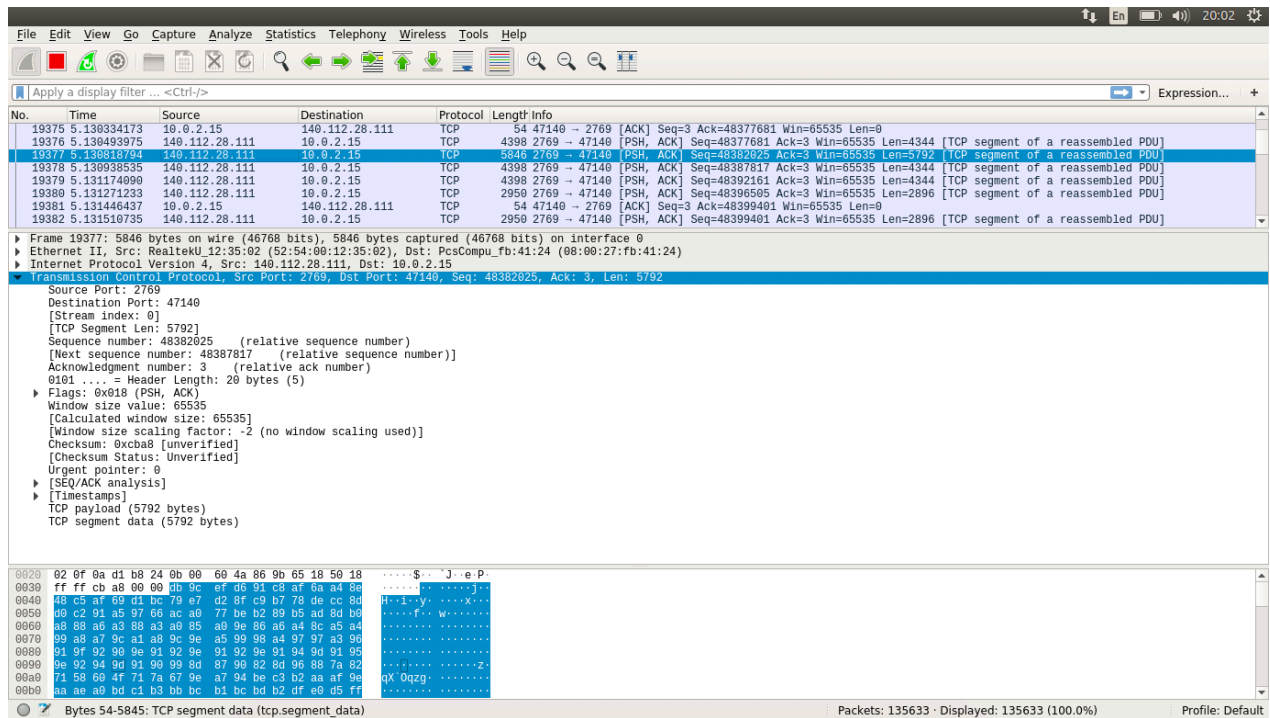
User Datagram Protocol (udp), 8 bytes

Packets: 50656 · Displayed: 50656 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

I used wireshark while I was watching youtube vedio by google chrome. Youtube usually provides lots of vedioes to watch.

# Analysis of TCP packets

Screenshot :



The port which the server used for this application is 2769. We can find it in Source IP in the screenshot.

## Compare the header between UDP and TCP

There are source port, destination port, length and check sum in both UDP and TCP.

But there is something only existing in TCP, like sequence number, ACK information, which TCP use to remember packets' order and insure stable connection.

# Find out a plaintext assword

Screenshot:

Wireshark packet capture showing a login attempt on eyny.com. The packet list shows an HTTP POST request (packet 11) to /member.php?mod=logging&action=login. The packet details pane shows the form data, including 'loginfield=username' and 'password=Aimer\_saikou'. The packet bytes pane shows the raw data with a red box highlighting the password field.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.103.254.240	216.58.200.33	TCP	62	50868 → 8443 [SYN] Seq=1013475612 Win=65535 Len=0 MSS=14...
2	0.548256	10.103.254.240	140.112.254.4	DNS	72	Standard query 0x8e71 A www.eyny.com
3	0.561647	140.112.254.4	10.103.254.240	DNS	164	Standard query response 0x8e71 A www.eyny.com CNAME 100t...
4	1.924605	10.103.254.240	216.58.200.33	TCP	62	[TCP Retransmission] 50868 → 8443 [SYN] Seq=1013475612 W...
5	2.467022	10.103.254.240	169.44.67.231	TCP	78	50869 → 80 [SYN] Seq=53818241 Win=65535 Len=0 MSS=1460 W...
6	2.772102	169.44.67.231	10.103.254.240	TCP	82	80 → 50869 [SYN, ACK] Seq=3978067168 Ack=53818242 Win=65...
7	2.772231	10.103.254.240	169.44.67.231	TCP	66	50869 → 80 [ACK] Seq=53818242 Ack=3978067169 Win=131520 ...
8	2.773175	10.103.254.240	169.44.67.231	TCP	1436	50869 → 80 [ACK] Seq=53818242 Ack=3978067169 Win=131520 ...
9	2.773177	10.103.254.240	169.44.67.231	TCP	762	50869 → 80 [PSH, ACK] Seq=53819612 Ack=3978067169 Win=13...
10	2.773757	10.103.254.240	169.44.67.231	HTTP	765	POST /member.php?mod=logging&action=login&loginsubmit=y...
11	3.075059	169.44.67.231	10.103.254.240	TCP	74	80 → 50869 [ACK] Seq=3978067169 Ack=53819612 Win=655360 ...

Referer: http://www.eyny.com/member.php?mod=logging&action=login\r\n  
Content-Length: 699\r\n  
[truncated]Cookie: 606e55XbD\_e8d7\_inlang=zh; 606e55XbD\_e8d7\_lastact=1571138542%09home.php%09misc; 606e55XbD\_e8d7\_lastvisit=1571134942; 606e55XbD\_e8d7\_loginfield=username; 606e55XbD\_e8d7\_password=Aimer\_saikou\r\n  
[Full request URI: http://www.eyny.com/member.php?mod=logging&action=login&loginsubmit=yes&loginhash=Lzr6D&inajax=1]  
[HTTP request 1/2]  
[Next request in frame: 20]  
File Data: 699 bytes  
▼ HTML Form URL Encoded: application/x-www-form-urlencoded  
▶ Form item: "formhash" = "70c95d8a"  
▶ Form item: "referer" = "http://www.eyny.com/./"  
▶ Form item: "loginfield" = "username"  
▶ Form item: "username" = "Aimer"  
▶ Form item: "password" = "Aimer\_saikou"  
▶ Form item: "questionid" = "0"  
▶ Form item: "answer" = ""  
▶ Form item: "cookietime" = "2592000"  
▶ Form item: "g-recaptcha-response" = "03A0LTBLReoa06xx025KCFbhFW-H6Gy-GKd71eMoT6hdaTsK8K-7eHN3IhT5yHE2piD-MC10bhtThBd5xc7ob94PvhVUa3k0ZP-trwMHIrA"  
▶ Form item: "loginsubmit" = "true"

0840 79 2e 63 6f 6d 25 32 46 2e 25 32 46 26 6c 6f 67 y.com%2F.%2F&log  
0850 69 6e 66 69 65 6c 64 3d 75 73 65 72 6e 61 6d 65 infield= username  
0860 26 75 73 65 72 6e 61 6d 65 3d 41 69 6d 65 72 26 &username=Aimer&

I connected to eyny.com and change the URL from https: to http: , and then logged in while wireshark opening. We can find our username and password in this packets, so can someone do, that is why it is unsafe.