

Computer Networks

Assignment 1

Bo69o2o9i 資工四 羅寶瑩

01 Analysis of UDP packets

The image shows a Wireshark packet capture window titled "Wireshark · Packet 457 · any". The packet list on the left shows "Frame 457: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0". The packet details pane on the right shows the following structure:

- Linux cooked capture
- Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 62
 - Identification: 0x11d0 (4560)
 - Flags: 0x4000, Don't fragment
 - Time to live: 64
 - Protocol: UDP (17)
 - Header checksum: 0x29dd [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 127.0.0.1
 - Destination: 127.0.0.1
- User Datagram Protocol, Src Port: 42303, Dst Port: 53
 - Source Port: 42303
 - Destination Port: 53
 - Length: 42
 - Checksum: 0xff3d [unverified]
 - [Checksum Status: Unverified]
 - [Stream index: 24]
- Domain Name System (query)
 - Transaction ID: 0x24be
 - Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
- Queries
 - aus5.mozilla.org: type AAAA, class IN
 - Name: aus5.mozilla.org
 - [Name Length: 16]
 - [Label Count: 3]
 - Type: AAAA (IPv6 Address) (28)
 - Class: IN (0x0001)

[Response In: 460]

The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII. The ASCII column shows the text "E..>..@..@..).....?..5..*..=\$...aus5.mozilla-or g.....".

The webserver of the packet is aus5.mozilla.org. It is the current server that firefox would need to access for auto-update.

02 Analysis of TCP packets

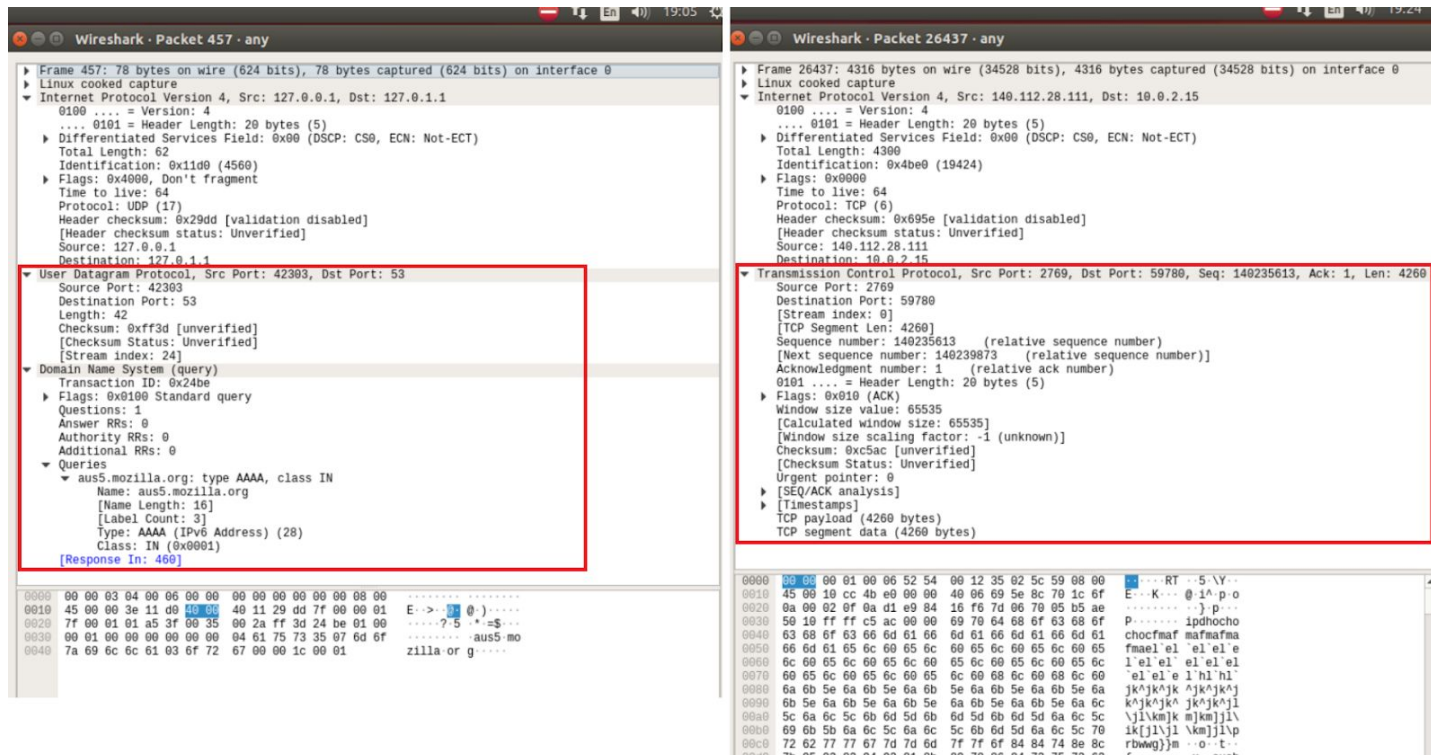
The image shows a Wireshark packet capture window titled "Wireshark · Packet 15443 · any". The packet list on the left shows "Frame 15443: 1764 bytes on wire (14112 bits), 1764 bytes captured (14112 bits) on interface 0". The packet details pane on the right shows the following structure:

- Linux cooked capture
 - Packet type: Unicast to us (0)
 - Link-layer address type: 1
 - Link-layer address length: 6
 - Source: RealtekU_12:35:02 (52:54:00:12:35:02)
 - Unused: ffff
 - Protocol: IPv4 (0x0800)
 - Internet Protocol Version 4, Src: 140.112.28.111, Dst: 10.0.2.15
 - Transmission Control Protocol, Src Port: 2769, Dst Port: 34790, Seq: 45483645, Ack: 1, Len: 1708
 - Source Port: 2769
 - Destination Port: 34790
 - [Stream index: 0]
 - [TCP Segment Len: 1708]
 - Sequence number: 45483645 (relative sequence number)
 - [Next sequence number: 45485353 (relative sequence number)]
 - Acknowledgment number: 1 (relative ack number)
 - 0101 = Header Length: 20 bytes (5)
 - Flags: 0x018 (PSH, ACK)
 - Window size value: 65535
 - [Calculated window size: 65535]
 - [Window size scaling factor: -1 (unknown)]
 - Checksum: 0xbbb4 [unverified]
 - [Checksum Status: Unverified]
 - Urgent pointer: 0
 - [SEQ/ACK analysis]
 - [Timestamps]

The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII. The first few bytes are 00 00 00 01 00 06 52 54, which correspond to the Ethernet II frame type (0x0800) and the source MAC address (52:54:00:12:35:02).

The server uses port 2769 for this application.

03 Compare the headers of transport layer between TCP and UDP



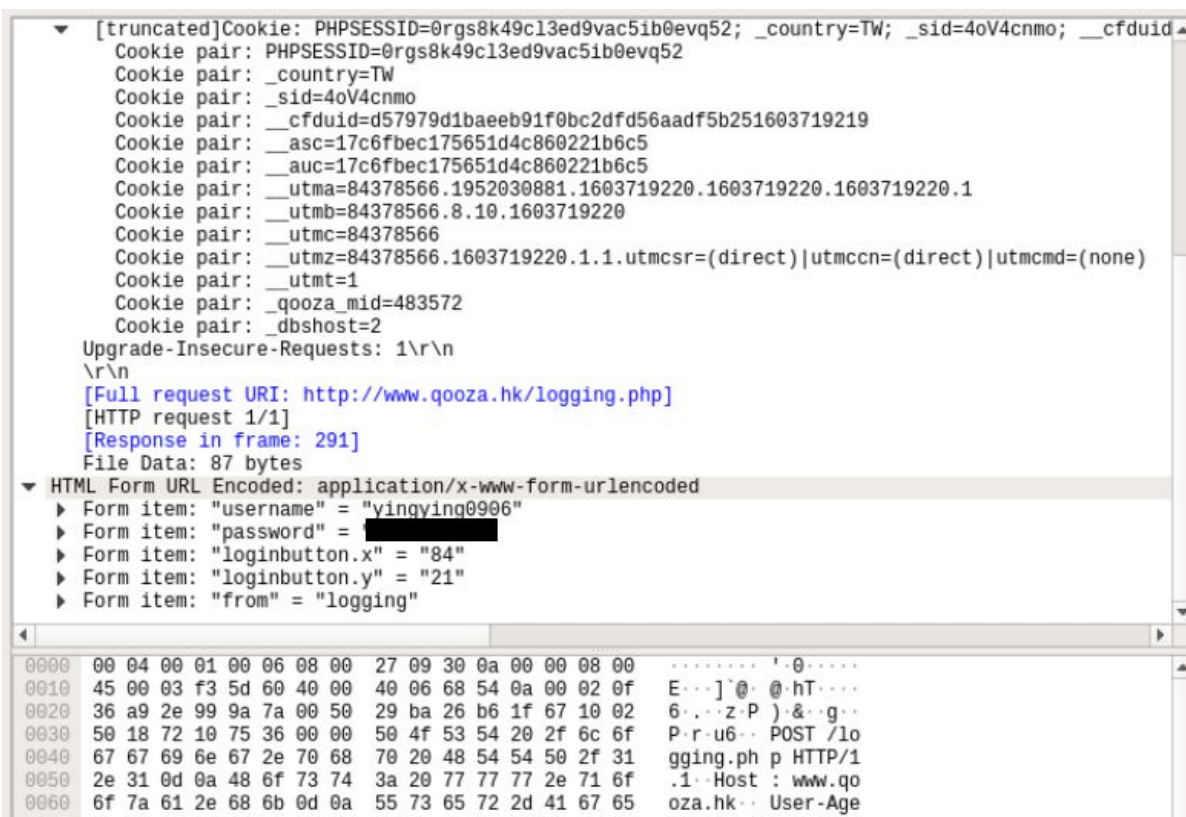
The headers of the TCP packet are similar to the headers of the UDP packet. They both have Frame, Linux cooked capture, and Internet protocol version 4. The difference between them is shown in the image above.

There are two headers called “user datagram protocol” and “domain name system” in the UDP packet. However, this kind of information in the TCP packets is combined in one header called “transmission control protocol”.

By comparing the fields in these headers, there are some fields in the TCP packet that the UDP packet doesn't exist, such as acknowledgment number, next sequence number, sequence number, timestamp, SEQ/ACK analysis, etc.

Also, there are some fields in the UDP packet that TCP packet doesn't exist, such as questions, answer RRs, authority RRs, additional RRs etc.

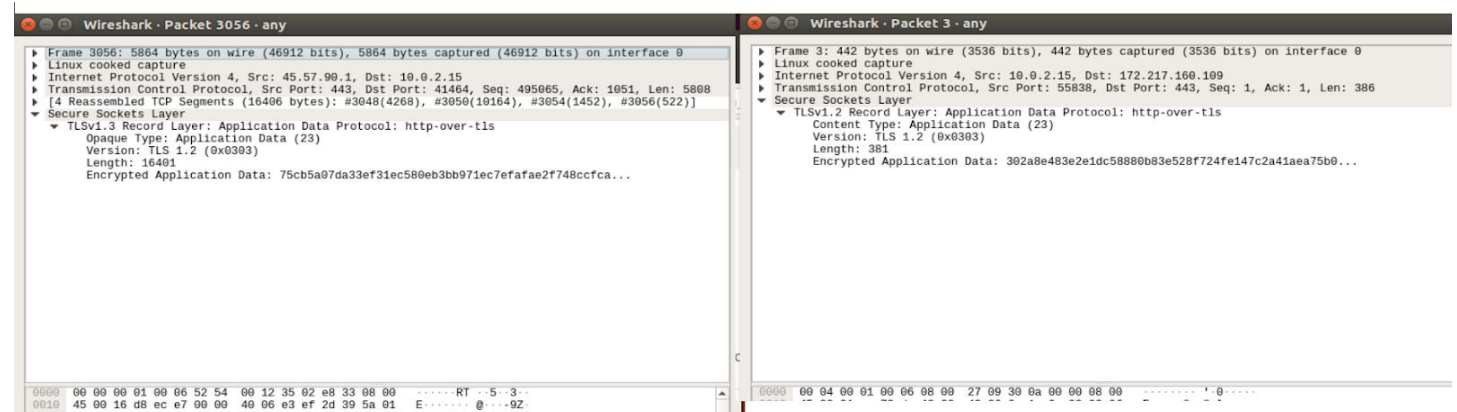
04 Find out a plaintext password



The website is called Qooza. It is a blog/weblog which was famous in Hong Kong since 2004 and it is still using HTTP. I typed my qooza account and found this packet in Wireshark.

It is not safe to send passwords in plaintext since the other people may get our password by capturing the packet that we send to the server. Once other people get our password, they can use our password to access the server to steal our personal information or carry out financial-related activities.

05 Other observations



I have tried to use the browser to browse two famous websites: Netflix and Gmail, and capture the packets of them. Both of them have a header called “secure sockets layer” and it shows that they are using http over tls.

Reference:

1. <https://support.mozilla.org/bm/questions/1224757> (question 1)
2. <http://www.qooza.hk/>