

HW1

b09902004 資工三 郭懷元

UDP Packets

The image shows a Wireshark packet capture window titled '*wlan0'. The packet list pane displays a series of DNS packets. The packet details pane shows the structure of a DNS query packet.

No.	Time	Source	Destination	Protocol	Length	Info
50	184113716	10.131.225.46	140.112.254.4	DNS	83	Standard query 0x9832 A dailymix-images.scdn.co
60	184137471	10.131.225.46	140.112.254.4	DNS	83	Standard query 0xdb36 AAAA dailymix-images.scdn.co
70	184508400	10.131.225.46	140.112.254.4	DNS	83	Standard query 0x6ea9 A api-partner.spotify.com
80	184520924	10.131.225.46	140.112.254.4	DNS	83	Standard query 0x88af AAAA api-partner.spotify.com
90	186915363	140.112.254.4	10.131.225.46	DNS	192	Standard query response 0x88af AAAA api-partner.spotify.com CNAME p...
100	186915638	140.112.254.4	10.131.225.46	DNS	180	Standard query response 0x6ea9 A api-partner.spotify.com CNAME part...
120	193067243	10.131.225.46	140.112.254.4	DNS	82	Standard query 0x8c72 A newjams-images.scdn.co
130	193086908	10.131.225.46	140.112.254.4	DNS	82	Standard query 0xba8e AAAA newjams-images.scdn.co
150	193796610	140.112.254.4	10.131.225.46	DNS	142	Standard query response 0x9832 A dailymix-images.scdn.co CNAME scdn...
160	196081733	140.112.254.4	10.131.225.46	DNS	277	Standard query response 0x8c72 A newjams-images.scdn.co CNAME scdn...
230	228221292	140.112.254.4	10.131.225.46	DNS	289	Standard query response 0xba8e AAAA newjams-images.scdn.co CNAME sc...
610	200000000	140.112.254.4	10.131.225.46	DNS	154	Standard query response 0xdb36 AAAA dailymix-images.scdn.co CNAME s...

Frame 5: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface wlan0, id 0
Ethernet II, Src: IntelCor_cb:72:35 (bc:17:b8:cb:72:35), Dst: ArubaaHe_04:42:60 (00:1a:1e:04:42:60)
Internet Protocol Version 4, Src: 10.131.225.46, Dst: 140.112.254.4
User Datagram Protocol, Src Port: 42964, Dst Port: 53
Domain Name System (query)

0000 00 1a 1e 04 42 60 bc 17 b8 cb 72 35 00 00 45 00 ...B...r5..E
0010 00 45 5c 45 40 00 40 11 68 3c 0a 83 e1 2e 8c 70 .EVE@ @ hc...p
0020 fe 04 a7 d4 00 35 00 31 76 69 08 32 01 00 00 015.1 vi.2...
0030 00 00 00 00 00 00 0f 64 61 69 6c 79 6d 69 78 2dd ailymix-
0040 69 6d 61 67 65 73 04 73 63 64 6e 02 63 6f 00 00 images's cdn co..
0050 01 00 01 ...

Domain Name System: Protocol Packets: 2347 - Displayed: 40 (1.7%) - Dropped: 0 (0.0%) Profile: Default

- Server address: 140.112.254.4
- Service: DNS (Domain Name System)
- Port number used: 53 on server side, 42964 on client side

TCP Packets

The image shows a Wireshark packet capture window titled 'tcp.pcapng'. The packet list pane on the left shows a list of 39 packets, all of which are SSHv2. The packet details pane on the right shows the details of the selected packet (packet 23), which is an SSHv2 packet. The packet is an SSHv2 packet, and the details pane shows the following information:

- Frame 23: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface wlan0, id 0
- Ethernet II, Src: IntelCor_cb:72:35 (bc:17:b8:cb:72:35), Dst: ArubaaHe_04:42:60 (00:1a:1e:04:42:60)
- Internet Protocol Version 4, Src: 10.131.225.46, Dst: 140.112.30.36
- Transmission Control Protocol, Src Port: 49810, Dst Port: 22, Seq: 1, Ack: 1, Len: 21
- SSH Protocol

The packet bytes pane at the bottom shows the raw data of the packet, which is an SSHv2 packet. The data is shown in hexadecimal and ASCII. The ASCII part of the data is: 'SSH-2.0-OpenSSH_9.0'.

- SSH server: linux5.csie.ntu.edu.tw at 140.112.30.36
- SSH server port: 22
- My machine used private IP address in the tcp packets, because the subnet 10.0.0.0/8 is reserved for private network in IPv4, and my source ip address is 10.131.225.46

TCP & UDP Comparison

Same fields

- Source port and destination port
- Checksum

Different fields

- Flags (only in TCP)
- Sequence number (only in TCP)
- Acknowledgement number (only in TCP)

Plaintext Password in Packets

The image shows a Wireshark packet capture window titled '*wlan0'. The packet list pane shows two packets. Packet 22 is an HTTP 200 OK response from 10.131.225.46 to 163.23.240.53. The packet details pane shows the following information:

- Cookie: cookie_year=111; cookie_sem=1\r\n
- Upgrade-Insecure-Requests: 1\r\n
- \r\n
- [Full request URI: http://schinfo.ccut.edu.tw/login_x.php]
- [HTTP request 1/1]
- [Response in frame: 22]
- File Data: 93 bytes
- HTML Form URL Encoded: application/x-www-form-urlencoded
- Form item: "Kind" = "2"
- Form item: "UserID" = "b09902004"
- Form item: "Passwd" = "CN2022{a1w@y5_u5e_ht7p5_f0r_10gin}"
- Form item: "B1" = "0n0j0t00"

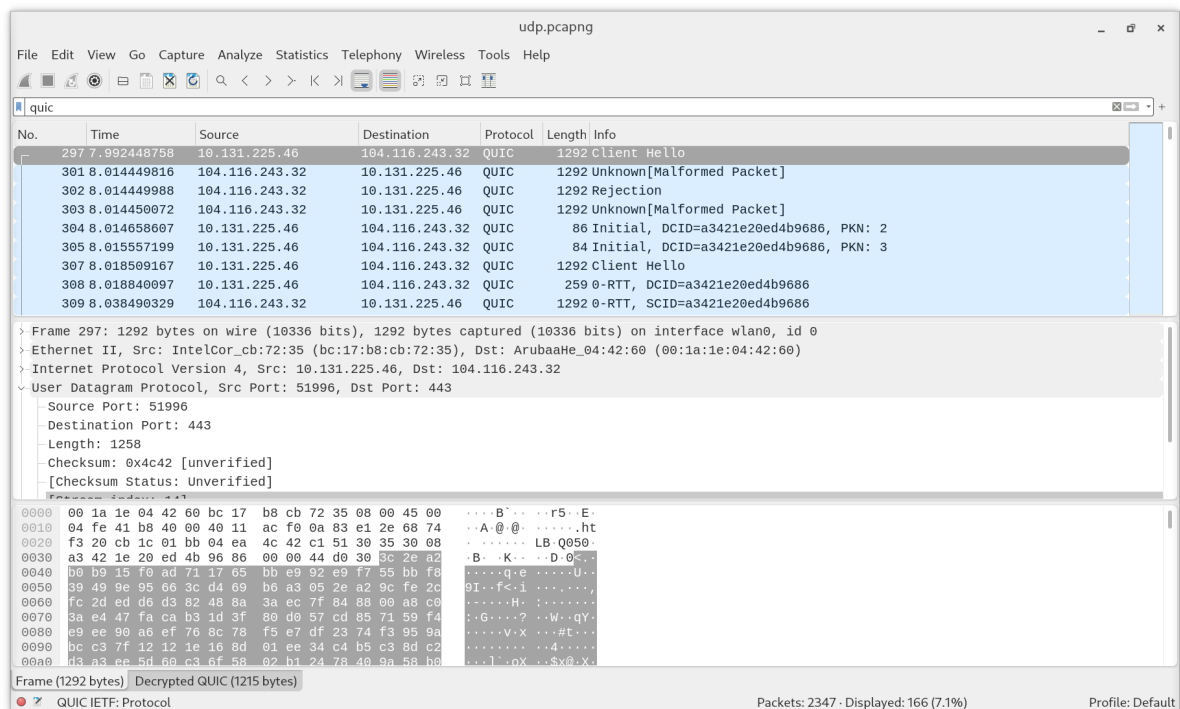
The packet bytes pane shows the raw data of the response, including the status line: HTTP/1.1 200 OK (text/html).

- Website: [中州科技大學校園網路資訊系統](#)
- If an attacker can capture packets going through their campus's router, then any user of this website that is connected to the router would have their passwords leaked.

Other Discoveries

Refs:

- <https://en.wikipedia.org/wiki/QUIC>
- <https://en.wikipedia.org/wiki/HTTP/3>



I found a protocol called "QUIC" that I hadn't heard of. It's a relatively new transport layer protocol running on top of UDP. It aims to improve performance of web apps that uses TCP now.

QUIC is used in the newly proposed HTTP/3. Previous versions of HTTP uses TCP as the transport layer protocol.