

Traffic Analysis

Protocols:

Protocol is a set of rules which is used for communicating with two devices like computers, mobile ,...etc. Which devices are connected within a same network can communicate with each other using protocols.

IP (Internet Protocol) - A unique identifier number series used for communicate with other devices.

MAC (Media Access Control)-An unchangeable unique identifier for each device.

DNS (Domain Naming System)-Converts system understanding IP address to human understanding names.

TCP (Transfer Control Protocol)- Used for data transfer (reliable).

UDP (User Datagram Protocol)- Used for data transfer (unreliable).

DNS Traffic:

The image shows a Wireshark packet capture of DNS traffic. The top pane displays a list of packets, with packet 33 selected. The middle pane shows the details of the selected packet, and the bottom pane shows the raw packet data in hexadecimal and ASCII.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
25	12.755653	192.168.1.3	8.8.8.8	DNS	76	Standard query 0x366e HTTPS web.whatsapp.com
26	12.756075	192.168.1.3	8.8.8.8	DNS	76	Standard query 0xc958 A web.whatsapp.com
33	13.137433	8.8.8.8	192.168.1.3	DNS	150	Standard query response 0x366e HTTPS web.whatsapp.com CNAME mx-ds.cdn.whatsapp.net SOA a.ns.whatsapp.net
34	13.137438	8.8.8.8	192.168.1.3	DNS	129	Standard query response 0xc958 A web.whatsapp.com CNAME mx-ds.cdn.whatsapp.net A 57.144.213.32
55	14.903448	192.168.1.3	8.8.8.8	DNS	76	Standard query 0x2c6b HTTPS web.whatsapp.com
56	14.904343	192.168.1.3	8.8.8.8	DNS	76	Standard query 0x16cb A web.whatsapp.com
58	15.223385	8.8.8.8	192.168.1.3	DNS	129	Standard query response 0x16cb A web.whatsapp.com CNAME mx-ds.cdn.whatsapp.net A 57.144.213.32
59	15.223385	8.8.8.8	192.168.1.3	DNS	158	Standard query response 0x2c6b HTTPS web.whatsapp.com CNAME mx-ds.cdn.whatsapp.net SOA a.ns.whatsapp.net
231	16.666789	192.168.1.3	8.8.8.8	DNS	70	Standard query 0x286c HTTPS dns.google
232	16.667177	192.168.1.3	8.8.8.8	DNS	70	Standard query 0xe6f3 A dns.google
233	16.667731	192.168.1.3	8.8.8.8	DNS	70	Standard query 0x1226 HTTPS dns.google
234	16.668513	192.168.1.3	8.8.8.8	DNS	70	Standard query 0xd843 A dns.google
235	16.669390	192.168.1.3	8.8.8.8	DNS	70	Standard query 0xd8ce HTTPS dns.google
236	16.669823	192.168.1.3	8.8.8.8	DNS	70	Standard query 0xf43b A dns.google
247	16.892812	8.8.8.8	192.168.1.3	DNS	146	Standard query response 0x286c HTTPS dns.google SOA ns1.zdns.google
248	16.892812	8.8.8.8	192.168.1.3	DNS	102	Standard query response 0xe6f3 A dns.google A 8.8.8.8 A 8.8.4.4
249	16.892812	8.8.8.8	192.168.1.3	DNS	146	Standard query response 0x1226 HTTPS dns.google SOA ns1.zdns.google
250	16.892812	8.8.8.8	192.168.1.3	DNS	102	Standard query response 0xd843 A dns.google A 8.8.8.8 A 8.8.4.4
251	16.892812	8.8.8.8	192.168.1.3	DNS	102	Standard query response 0xf43b A dns.google A 8.8.8.8 A 8.8.4.4
252	16.892812	8.8.8.8	192.168.1.3	DNS	146	Standard query response 0xd8ce HTTPS dns.google SOA ns1.zdns.google
372	17.661303	192.168.1.3	8.8.8.8	DNS	81	Standard query 0xb624 A tm-sdk.platiniumai.net

Packet Details (Packet 33):

- Answer RRs: 1
- Authority RRs: 1
- Additional RRs: 0
- Queries
 - web.whatsapp.com: type HTTPS, class IN
 - Name: web.whatsapp.com
 - [Name Length: 16]
 - [Label Count: 3]
 - Type: HTTPS (65) (HTTPS Specific Service Endpoints)
 - Class: IN (0x0001)
- Answers
 - web.whatsapp.com: type CNAME, class IN, cname mx-ds.cdn.whatsapp.net
 - Name: web.whatsapp.com
 - Type: CNAME (5) (canonical NAME for an alias)
 - Class: IN (0x0001)
 - Time to live: 3352 (55 minutes, 52 seconds)
 - Data length: 25
 - CNAME: mx-ds.cdn.whatsapp.net
 - whatsapp.net: type SOA, class IN, mname a.ns.whatsapp.net
 - [Resource ID: 25]
 - [Time: 0.381785000 seconds]

Raw Packet Data (Hex):

```
0000 58 cd c9 36 58 79 8c 13 e2 44 e4 07 08 00 45 80 X . cxy . . D . . . E
0010 00 90 03 eb 00 00 7c 11 68 37 08 08 08 c0 a8 . . . . . h7 . . . . .
0020 01 03 00 35 ef 93 00 7c 98 44 3e 6e 81 80 00 01 . . . . . Dns . . . . .
0030 00 01 00 01 00 00 03 77 65 62 08 77 68 61 74 73 . . . . . eb-whats
0040 61 70 70 03 63 6f 6d 00 00 41 00 01 c0 0c 00 05 app-com . -A . . . . .
0050 00 01 00 00 0d 18 00 19 06 6d 6d 78 2d 64 73 03 . . . . . -mx-ds-
0060 63 64 6e 08 77 68 61 74 73 61 70 70 03 6e 65 74 cdn-what sapp-net
0070 00 c0 39 00 06 00 01 00 00 0e d3 00 21 01 61 02 -9 . . . . . -1 . a .
0080 6e 73 c0 39 03 64 6e 73 c0 39 fa ce b0 0c 00 00 ns-9-dns -9 . . . . .
0090 38 40 00 00 07 08 00 09 3a 80 00 00 01 2c 80 . . . . . : . . . . .
```

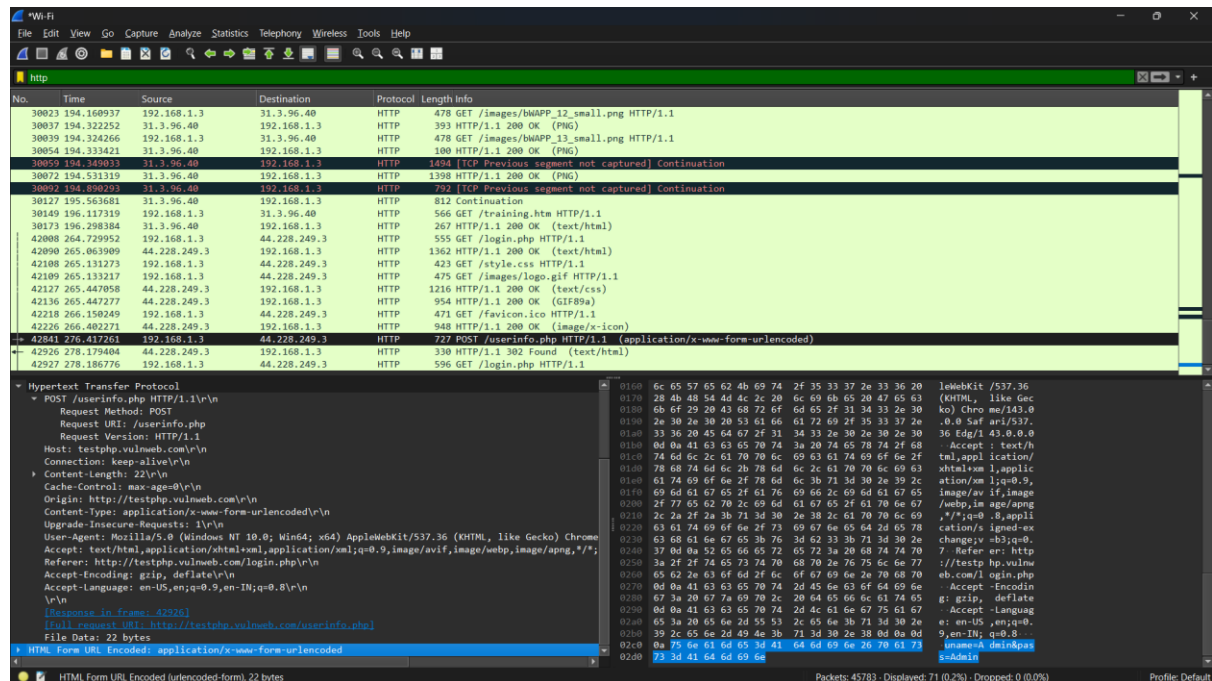
Own device-192.168.1.3

DNS Server-8.8.8.8

192.168.1.3 request for a website's IP to 8.8.8.8

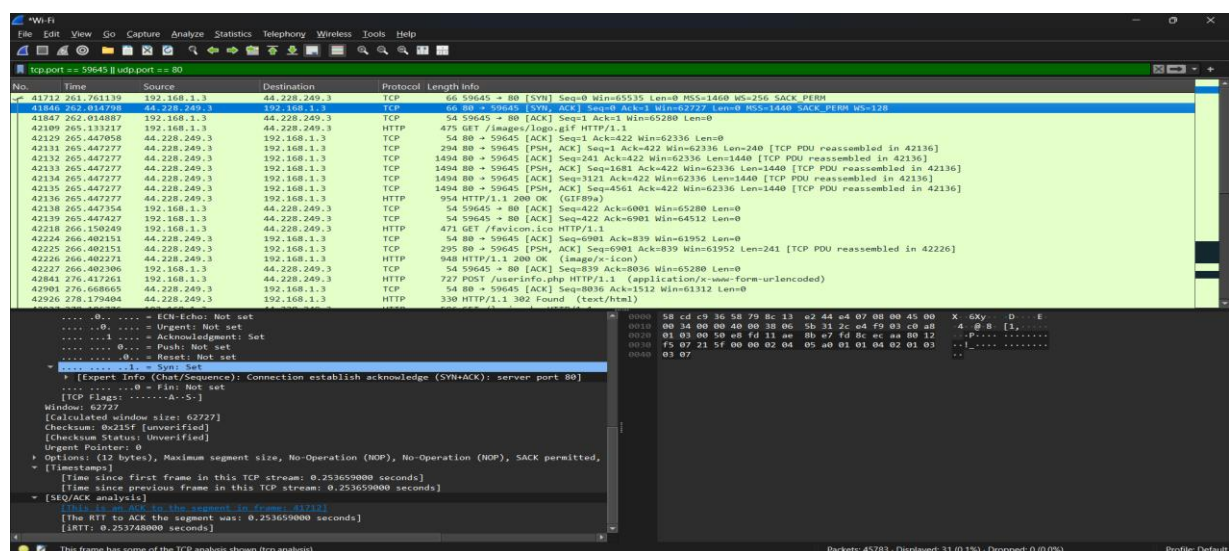
8.8.8.8 responded for the request from 192.168.1.3

HTTP Traffic:



HTTP stands for Hyper Text Transfer Protocol. It used for share html pages (Website). In this event, the user logged in the website named “vulnweb.com”.

TCP Traffic:



TCP is used for transfer data. In this event, the user device transferred data using port 80. The responder device (44.228.243.3) received the data using its port 59645. Port 80 was used for http protocol. So it might be a webpage activity.

Encrypted vs Plain data:

Encrypted Text	Plain Text
Hard to read it.	Easily read the data.
Non-vulnerable for man-in-middle attacks.	Vulnerable for man-in-middle attacks.
Data exposing might be difficult.	Data are exposed easily.
Most secured.	Unsecured

Plain Text:

The image shows a Wireshark packet capture of an HTTP POST request. The packet list on the left shows a POST request to /userinfo.php. The packet details pane on the right shows the request body as an HTML form URL-encoded string. The body contains the following data:

```

HTML Form URL Encoded (application/x-www-form-urlencoded)
--
username=admin&password=admin
  
```

The packet bytes pane on the right shows the raw data of the request body, which is the URL-encoded string: `username=admin&password=admin`.

Login credentials are exposed- Username: Admin, Password: Admin

Encrypted Text:

The image shows a Wireshark packet capture of a TLS handshake. The packet list on the left shows a sequence of packets, with packet 42971 (105 bytes) selected. The packet details pane on the right shows the structure of the packet, including the TLSv1.2 Record Layer, Handshake Protocol, Encrypted Handshake Message, and the Change Cipher Spec (20) and Version: TLS 1.2 (0x0303) fields. The packet bytes pane on the right shows the raw data of the packet, with the encrypted handshake message highlighted in blue.

Current filter: null

No.	Time	Source	Destination	Protocol	Length	Info
42964	279.015377	192.168.1.3	150.171.28.11	TLSv1.2	682	Client Hello (SNI=edge.microsoft.com)
42970	279.072428	150.171.28.11	192.168.1.3	TLSv1.2	288	Server Hello, Change Cipher Spec, Encrypted Handshake Message
42971	279.072931	192.168.1.3	150.171.28.11	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
42972	279.073181	192.168.1.3	150.171.28.11	TLSv1.2	153	Application Data
42974	279.073433	192.168.1.3	150.171.28.11	TLSv1.2	881	Application Data
42978	279.073530	192.168.1.3	150.171.28.11	TLSv1.2	397	Application Data
42980	279.314390	150.171.28.11	192.168.1.3	TLSv1.2	123	Application Data
42983	279.314851	192.168.1.3	150.171.28.11	TLSv1.2	92	Application Data
43000	283.718955	192.168.1.3	104.46.162.225	TLSv1.3	193	Application Data
43010	283.718997	192.168.1.3	104.46.162.225	TLSv1.3	93	Application Data
43026	283.934426	104.46.162.225	192.168.1.3	TLSv1.3	93	Application Data
43037	283.934571	192.168.1.3	104.46.162.225	TLSv1.3	1494	Application Data
43046	284.208972	104.46.162.225	192.168.1.3	TLSv1.3	89	Application Data
43055	284.201121	192.168.1.3	104.46.162.225	TLSv1.3	1367	Application Data
43057	284.201121	192.168.1.3	104.46.162.225	TLSv1.3	299	Application Data
43065	284.368260	104.46.162.225	192.168.1.3	TLSv1.3	89	Application Data
43067	284.370056	192.168.1.3	104.46.162.225	TLSv1.3	1292	Initial, DCID=6a9deba4577551f9, PKN: 2, CRYPTO, PADDING, PING, PING, PING, PING, CRYPTO, PADDING, CRYPTO, CRYPTO, PADDING
43092	288.210841	192.168.1.3	104.86.189.81	QUIC	1292	Initial, DCID=6a9deba4577551f9, PKN: 2, CRYPTO, PADDING, PING, PING, PING, PING, CRYPTO, PADDING, CRYPTO, CRYPTO, PADDING
43099	288.322086	104.86.189.81	192.168.1.3	QUIC	1292	Initial, DCID=6a9deba4577551f9, PKN: 2, CRYPTO, PADDING, PING, PING, PING, PING, CRYPTO, PADDING, CRYPTO, CRYPTO, PADDING
43108	288.326230	192.168.1.3	104.86.189.120	QUIC	1292	Initial, DCID=6a9deba4577551f9, PKN: 2, CRYPTO, PADDING, PING, PING, PING, PING, CRYPTO, PADDING, CRYPTO, CRYPTO, PADDING

Frame 42971: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface \Device\NPF{...} Ethernet II, Src: CloudNetwork 36:58:79 (58:cd:c9:36:58:79), Dst: NetlinkIct_44:e4:07 (8c:13:e2:44:e4:07) Destination: NetlinkIct_44:e4:07 (8c:13:e2:44:e4:07) Source: CloudNetwork 36:58:79 (58:cd:c9:36:58:79) Type: IPv4 (0x0800) [Stream index: 1] Internet Protocol Version 4, Src: 192.168.1.3, Dst: 150.171.28.11 Transmission Control Protocol, Src Port: 51188, Dst Port: 443, Seq: 2069, Ack: 155, Len: 51 Transport Layer Security Content Type: Change Cipher Spec (20) Version: TLS 1.2 (0x0303) Length: 1 Change Cipher Spec Message TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message Content Type: Handshake (22) Version: TLS 1.2 (0x0303) Length: 40 Handshake Protocol: Encrypted Handshake Message

Packets: 45783 · Displayed: 8681 (19.0%) · Dropped: 0 (0.0%) Profile: Default

Login credentials are encrypted. We need to do some more works to find it.