

Wireshark – Webpage Traffic

Host IP: 192.138.1.3

Subnet Mask: 255.255.255.0

Default Gateway: 192.138.1.2

DNS Server: 192.138.1.2

A capture is started on Ethernet0 interface.

Navigate to google.com.

Once the page fully loads, the capture is ended.

When examining the capture, a DNS Query was made by the host to the DNS server.

163	3.016446	192.138.1.3	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
164	3.088812	192.138.1.2	192.138.1.3	DNS	146 Standard query response 0x3dd6 HTTPS clientservices.googleapis.com SOA ns1.google.com
165	3.088859	192.138.1.3	192.138.1.2	ICMP	174 Destination unreachable (Port unreachable)
166	3.112469	192.138.1.3	192.138.1.2	DNS	74 Standard query 0x8d7b A www.google.com
167	3.114189	192.138.1.3	192.138.1.2	DNS	74 Standard query 0xb855 HTTPS www.google.com
168	3.117076	192.138.1.2	192.138.1.3	DNS	170 Standard query response 0x8d7b A www.google.com A 142.250.114.103 A 142.250.114.99 A 142.250.114.147
169	3.140309	192.138.1.2	192.138.1.3	DNS	99 Standard query response 0xb855 HTTPS www.google.com HTTPS
170	3.142376	192.138.1.3	142.250.114.103	QUIC	1292 Initial. DCTID=67e8eb352abd5b29. PKN: 1. CRVPTO

This query is made for the host to resolve the URL “google.com” to an IP address that the browser can navigate to.

The DNS Server then sends a response packet.

When clicking the packet and investigating the packet details, a collection of IP Addresses can be found as answers to the query.

```
> Internet Protocol Version 4, Src: 192.138.1.2, Dst: 192.138.1.3
> User Datagram Protocol, Src Port: 53, Dst Port: 50462
▼ Domain Name System (response)
  Transaction ID: 0x8d7b
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 6
  Authority RRs: 0
  Additional RRs: 0
  > Queries
  ▼ Answers
    > www.google.com: type A, class IN, addr 142.250.114.103
    > www.google.com: type A, class IN, addr 142.250.114.99
    > www.google.com: type A, class IN, addr 142.250.114.147
    > www.google.com: type A, class IN, addr 142.250.114.104
    > www.google.com: type A, class IN, addr 142.250.114.106
    > www.google.com: type A, class IN, addr 142.250.114.105
    [Request In: 166]
    [Time: 0.004607000 seconds]
```

When entering each of these IP Addresses directly into the browser, we confirm that all 6 of these addresses are assigned to google.com.

When examining the capture further, multiple TCP packets can be found being sent between the host and the first IP Address in DNS Response.

The capture is filtered for TCP packets for easier analysis.

181	3.203339	192.138.1.3	142.250.114.103	TCP	66 49855 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
188	3.230461	142.250.114.103	192.138.1.3	TCP	60 443 → 49855 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
189	3.230548	192.138.1.3	142.250.114.103	TCP	54 49855 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
190	3.231191	192.138.1.3	142.250.114.103	TLSv1.3	1874 Client Hello (SNI=www.google.com)

The next 3 packets are evidence of the host attempting to make a connection with google.com with a 3-Way Handshake, which is completed.

The next packets in the capture are sent using TLS.

The capture is filtered for TLS packets for easier analysis.

43	1.135645	192.138.1.3	142.250.115.94	TLSv1.3	1857 Client Hello (SNI=clientservices.googleapis.com)
58	1.193357	192.138.1.3	142.250.114.84	TLSv1.3	1783 Client Hello (SNI=accounts.google.com)
64	1.198892	142.250.115.94	192.138.1.3	TLSv1.3	1514 Server Hello, Change Cipher Spec
75	1.238991	142.250.115.94	192.138.1.3	TLSv1.3	70 Application Data
78	1.246111	142.250.114.84	192.138.1.3	TLSv1.3	1514 Server Hello, Change Cipher Spec
82	1.250640	142.250.114.84	192.138.1.3	TLSv1.3	1158 Application Data
84	1.268441	192.138.1.3	142.250.115.94	TLSv1.3	128 Change Cipher Spec, Application Data
87	1.297216	142.250.115.94	192.138.1.3	TLSv1.3	1042 Application Data, Application Data
91	1.317340	192.138.1.3	142.250.115.94	TLSv1.3	146 Application Data
93	1.318835	192.138.1.3	142.250.115.94	TLSv1.3	85 Application Data
95	1.319103	192.138.1.3	142.250.115.94	TLSv1.3	421 Application Data
97	1.322008	192.138.1.3	142.250.114.84	TLSv1.3	128 Change Cipher Spec, Application Data
99	1.344859	142.250.115.94	192.138.1.3	TLSv1.3	85 Application Data
100	1.348314	142.250.114.84	192.138.1.3	TLSv1.3	1022 Application Data, Application Data
103	1.401876	142.250.115.94	192.138.1.3	TLSv1.3	252 Application Data, Application Data
107	1.668018	142.250.115.94	192.138.1.3	TLSv1.3	93 Application Data
108	1.669031	192.138.1.3	142.250.115.94	TLSv1.3	93 Application Data

These packets are evidence of a TLS Handshake between google.com and the host in order to establish a secure connection.

When attempting to investigate the Application data sent by the Google server, we find that it is cyphertext.

>	Frame 75: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{E1CA5079-}
>	Ethernet II, Src: VMware_f6:06:37 (00:50:56:f6:06:37), Dst: VMware_ef:eb:ae (00:0c:29:ef:eb:ae)
>	Internet Protocol Version 4, Src: 142.250.115.94, Dst: 192.138.1.3
>	Transmission Control Protocol, Src Port: 443, Dst Port: 49852, Seq: 5745, Ack: 1804, Len: 16
>	[5 Reassembled TCP Segments (4539 bytes): #64(239), #65(1364), #73(1460), #74(1460), #75(16)]
▼	Transport Layer Security
▼	TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
	Opaque Type: Application Data (23)
	Version: TLS 1.2 (0x0303)
	Length: 4534
	Encrypted Application Data [truncated]: 83be3945f2e59b88b5df5f3b32eed95960b9856459e2d40648ec14581e
	[Application Data Protocol: Hypertext Transfer Protocol]

HTTPS uses TLS to encrypt Application Layer data and maintain confidentiality if network traffic is captured.

The host has now established a secure connection with google.com.

A new capture is started on Ethernet0.

Navigate to <http://http.badssl.com/>.

Once the page fully loads, the capture is ended.

The packets captured are mostly similar to those from Google, but there are some key differences.

When examining the DNS packets, the browser attempts to relay the host to the website using HTTPS instead of HTTP for a secure connection.

Unfortunately, the DNS server can only respond with the IP Address of the website using HTTP.

2614	20.136463	104.154.89.105	192.138.1.3	HTTP	654	HTTP/1.1 200 OK	(text/html)
------	-----------	----------------	-------------	------	-----	-----------------	-------------

Because of this, the Application Layer data is visible in complete plaintext in the packet details.

```
▼ Line-based text data: text/html (20 lines)
<!DOCTYPE html>\n
<html>\n
<head>\n
  <meta charset="utf-8">\n
  <meta name="viewport" content="width=device-width, initial-scale=1">\n
  <link rel="shortcut icon" href="/icons/favicon-red.ico"/>\n
  <link rel="apple-touch-icon" href="/icons/icon-red.png"/>\n
  <title>http.badssl.com</title>\n
  <link rel="stylesheet" href="/style.css">\n
  <style>body { background: red; }</style>\n
</head>\n
<body>\n
<div id="content">\n
  <h1 style="font-size: 8vw;">\n
    http.badssl.com\n
  </h1>\n
</div>\n
\n
</body>\n
```