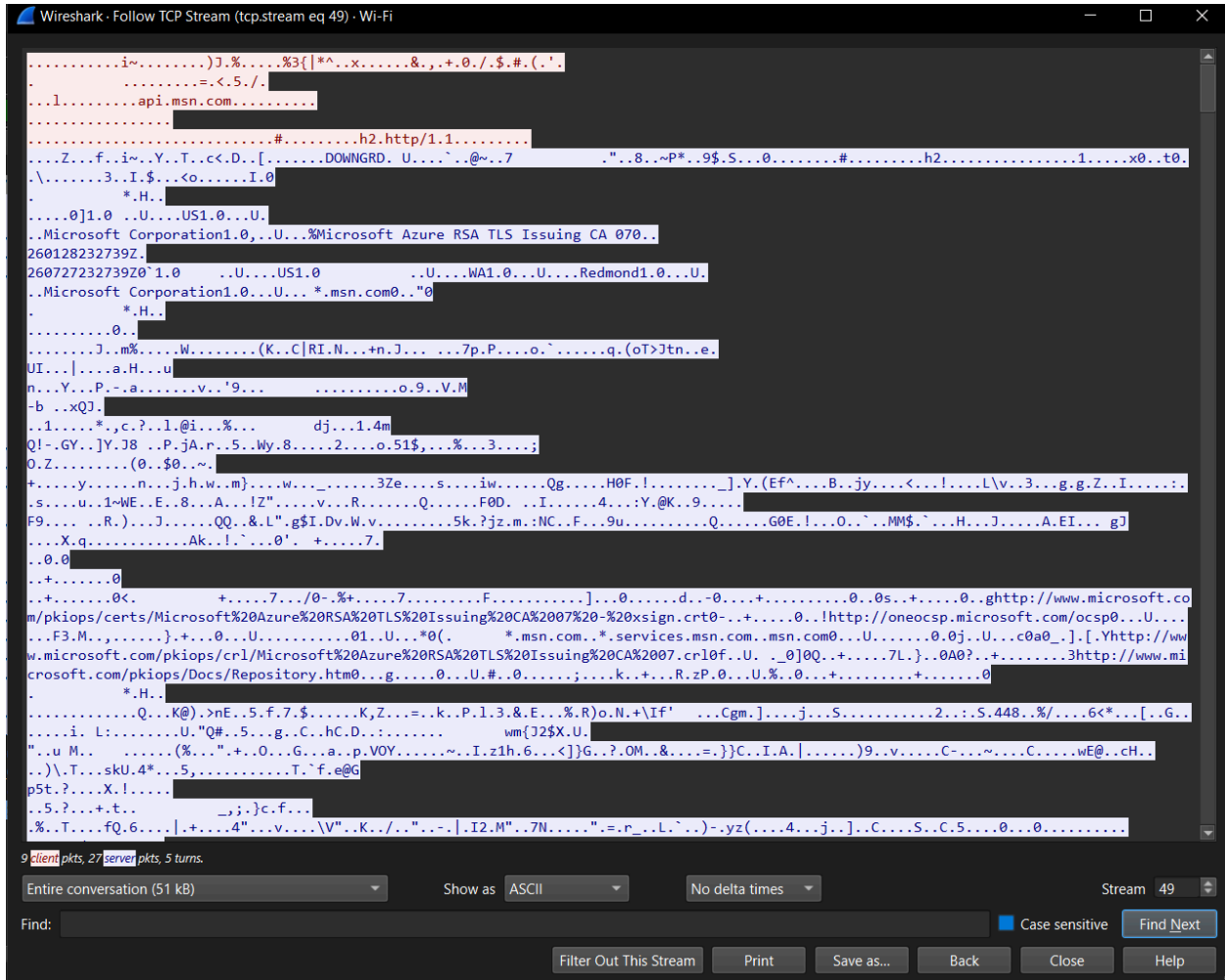


TASK 3

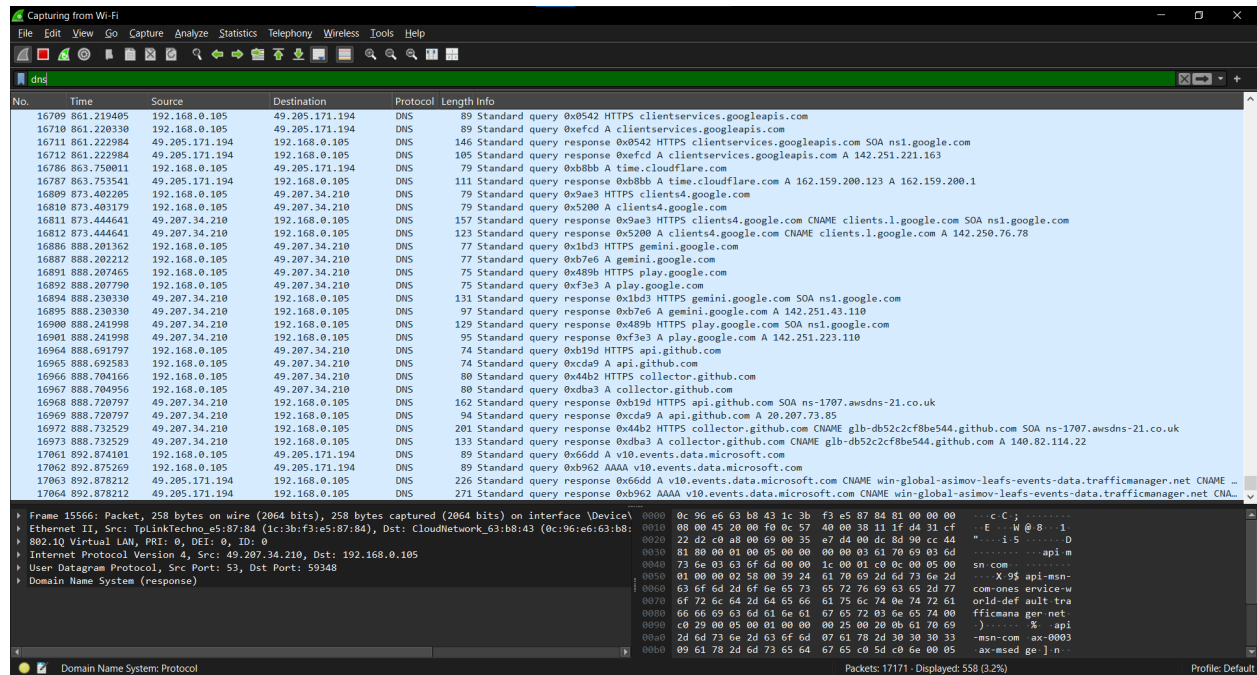
1. Observing a three-way TCP Handshake



The image shows a Wireshark packet capture window titled "Wireshark · Follow TCP Stream (tcp.stream eq 49) · Wi-Fi". The main pane displays the raw data of a TCP stream, which has been decoded into ASCII text. The text is a mix of lowercase letters, numbers, and special characters, including some non-ASCII characters like "µ" and "€". The text is organized into lines, with some lines starting with "0" or "1" indicating packet boundaries. The bottom of the window shows a summary of the stream: "9 client pkts, 27 server pkts, 5 turns." Below this, there are buttons for "Filter Out This Stream", "Print", "Save as...", "Back", "Close", and "Help".

A 3 way handshake.

2. DNS Query




The image shows a Wireshark packet capture of DNS traffic. The top pane displays a list of 27 packets, all of which are DNS queries or responses. The middle pane shows the details of the selected packet (No. 17171), which is a DNS query for 'api-ms-win-base-util-l1-1-0'. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
16709	861.219495	192.168.0.105	49.205.171.194	DNS	89	Standard query 0x0542 HTTPS clientservices.googleapis.com
16710	861.220330	192.168.0.105	49.205.171.194	DNS	89	Standard query 0xefcd A clientservices.googleapis.com
16711	861.222984	49.205.171.194	192.168.0.105	DNS	146	Standard query response 0x0542 HTTPS clientservices.googleapis.com SOA ns1.google.com
16712	861.222984	49.205.171.194	192.168.0.105	DNS	105	Standard query response 0xefcd A clientservices.googleapis.com A 142.251.221.163
16786	861.750011	192.168.0.105	49.205.171.194	DNS	79	Standard query 0xb8bb A time.cloudflare.com
16787	861.753541	49.205.171.194	192.168.0.105	DNS	111	Standard query response 0xb8bb A time.cloudflare.com A 162.159.200.123 A 162.159.200.1
16809	873.402205	192.168.0.105	49.207.34.210	DNS	79	Standard query 0x9ae3 HTTPS clients4.google.com
16810	873.403179	192.168.0.105	49.207.34.210	DNS	79	Standard query 0x5200 A clients4.google.com
16811	873.444641	49.207.34.210	192.168.0.105	DNS	157	Standard query response 0x9ae3 HTTPS clients4.google.com CNAME clients1.google.com SOA ns1.google.com
16812	873.444641	49.207.34.210	192.168.0.105	DNS	123	Standard query response 0x5200 A clients4.google.com CNAME clients1.google.com A 142.250.76.78
16806	888.201362	192.168.0.105	49.207.34.210	DNS	77	Standard query 0x1bd3 HTTPS gemini.google.com
16887	888.202212	192.168.0.105	49.207.34.210	DNS	77	Standard query 0xb76d A gemini.google.com
16891	888.207465	192.168.0.105	49.207.34.210	DNS	75	Standard query 0x489b HTTPS play.google.com
16892	888.207790	192.168.0.105	49.207.34.210	DNS	75	Standard query 0xf3e3 A play.google.com
16894	888.230330	49.207.34.210	192.168.0.105	DNS	131	Standard query response 0x1bd3 HTTPS gemini.google.com SOA ns1.google.com
16895	888.230330	49.207.34.210	192.168.0.105	DNS	97	Standard query response 0xb76d A gemini.google.com A 142.251.43.110
16900	888.241998	49.207.34.210	192.168.0.105	DNS	129	Standard query response 0x489b HTTPS play.google.com SOA ns1.google.com
16901	888.241998	49.207.34.210	192.168.0.105	DNS	95	Standard query response 0xf3e3 A play.google.com A 142.251.223.110
16964	888.691797	192.168.0.105	49.207.34.210	DNS	74	Standard query 0xb19d HTTPS api.github.com
16965	888.692583	192.168.0.105	49.207.34.210	DNS	74	Standard query 0xcda9 A api.github.com
16966	888.704166	192.168.0.105	49.207.34.210	DNS	80	Standard query 0x44b2 HTTPS collector.github.com
16967	888.704956	192.168.0.105	49.207.34.210	DNS	80	Standard query 0xbda3 A collector.github.com
16968	888.720797	49.207.34.210	192.168.0.105	DNS	162	Standard query response 0xb19d HTTPS api.github.com SOA ns-1707.awsdns-21.co.uk
16969	888.720797	49.207.34.210	192.168.0.105	DNS	94	Standard query response 0xcda9 A api.github.com A 20.207.73.85
16972	888.732529	49.207.34.210	192.168.0.105	DNS	201	Standard query response 0x44b2 HTTPS collector.github.com CNAME glb-db52c2cf8be544.github.com SOA ns-1707.awsdns-21.co.uk
16973	888.732529	49.207.34.210	192.168.0.105	DNS	133	Standard query response 0xbda3 A collector.github.com CNAME glb-db52c2cf8be544.github.com A 140.82.114.22
17061	892.874101	192.168.0.105	49.205.171.194	DNS	89	Standard query 0xb962 AAAA v10.events.data.microsoft.com
17062	892.875269	192.168.0.105	49.205.171.194	DNS	89	Standard query 0xb962 AAAA v10.events.data.microsoft.com
17063	892.878212	49.205.171.194	192.168.0.105	DNS	226	Standard query response 0xb962 AAAA v10.events.data.microsoft.com CNAME win-global-asimov-leaves-events-data.trafficmanager.net CNAME ...
17064	892.878212	49.205.171.194	192.168.0.105	DNS	271	Standard query response 0xb962 AAAA v10.events.data.microsoft.com CNAME win-global-asimov-leaves-events-data.trafficmanager.net CNAME ...

Type dns in the bar to get all dns queries.

As we can see there are both standard query and response queries.

3. HTTP vs HTTPS



The image shows a Wireshark packet capture of an HTTP stream. The top pane shows the packet list with packet 1 selected. The middle pane shows the details of the selected packet, which is an HTTP GET request. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.105	192.168.0.105	HTTP	1000	GET / HTTP/1.1

Details of packet 1 (HTTP GET request):

- Host: neverssl.com
- Connection: keep-alive
- Upgrade-Insecure-Requests: 1
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
- Accept-Encoding: gzip, deflate
- Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK

Date: Sun, 01 Feb 2026 06:33:55 GMT

Server: Apache/2.4.62 ()

Upgrade: h2,h2c

Connection: Upgrade, Keep-Alive

Last-Modified: Wed, 29 Jun 2022 00:23:33 GMT

ETag: "f79-5e28b2d38e93-gzip"

Accept-Ranges: bytes

Vary: Accept-Encoding

Content-Encoding: gzip

Content-Length: 1906

Keep-Alive: timeout=5, max=100

Content-Type: text/html; charset=UTF-8

HTML body:

```
<html>
<head>
<title>NeverSSL - Connecting ... </title>
<style>
body {
font-family: Montserrat, helvetica, arial, sans-serif;
font-size: 16v;
color: #444444;
margin: 0;
}
h2 {
font-weight: 700;
font-size: 1.6em;
margin-top: 30px;
}
p {
line-height: 1.6em;
}
```

This is a http file which is not encrypted as we can see the actual html code.

```
Wireshark - Follow TCP Stream (tcp.stream eq 2) - Wi-Fi
.....3.8.....c
.....k...F...M...*
.....s
.....E...V'O.B0d.Q.3
.....N...Q.....H.B...d.D
.....p.....IR:g...z
.....K...mG3.....e...
.....Rkej...DdE...B.I...&
.....Q.....b...h...
.....3...kf...8...8|b
.....MW.NI...g...V1.
.....6...-2
.....ez...F...
.....l.../...$.....0
.....t...2G...j\k@.....
.....b...j...a...et...yf
.....C".K(T...?..*Z.(Z...1.....Uj...:..h...#K.g0).9.....d...L.No.I...-f...e;k.y.U...%...h...0.....u...2.LNx.W.U.y.n...4...d
.....J...Z...&...7.E7...T...(\1.P.2...$...&...:.....qI.....(Eef.T$..ch...:eA.v...
.....U.b...[m\...1...7[...$
.....[...&...J.....)2P1>...).0.....(KX...{z*...-v...5
.....J.../...[...C.t...85...z...EuT.P...g.*M...\.@...^V...qN.hZu..0$.....N.p9...1\1.7.*.....V..7D...:9.....c*...
.....F.....3...-...
.....no...0.%...
.....@z...
.....).....QG.....d...
.....Ag...
.....n,zpk.....:({
.....g).....1.....<...0...
.....].?.....J...c'H5$...
.....E...f...H...E...1
.....P...XK...c)...*...
.....a=h.U
.....9<.....L...I...f...
.....q...q...0
.....?..?..NI...
.....T.....K...p[...
.....m/^.....*]%....&c...
.....a...p.....M...^...Z
.....f...4.....H.T*...1q...
.....>

60 bytes, 60 bytes, 117 bytes
```

This is a https file which is encrypted as we can see unknown language.