

Report on Network Traffic Analysis Using Wireshark

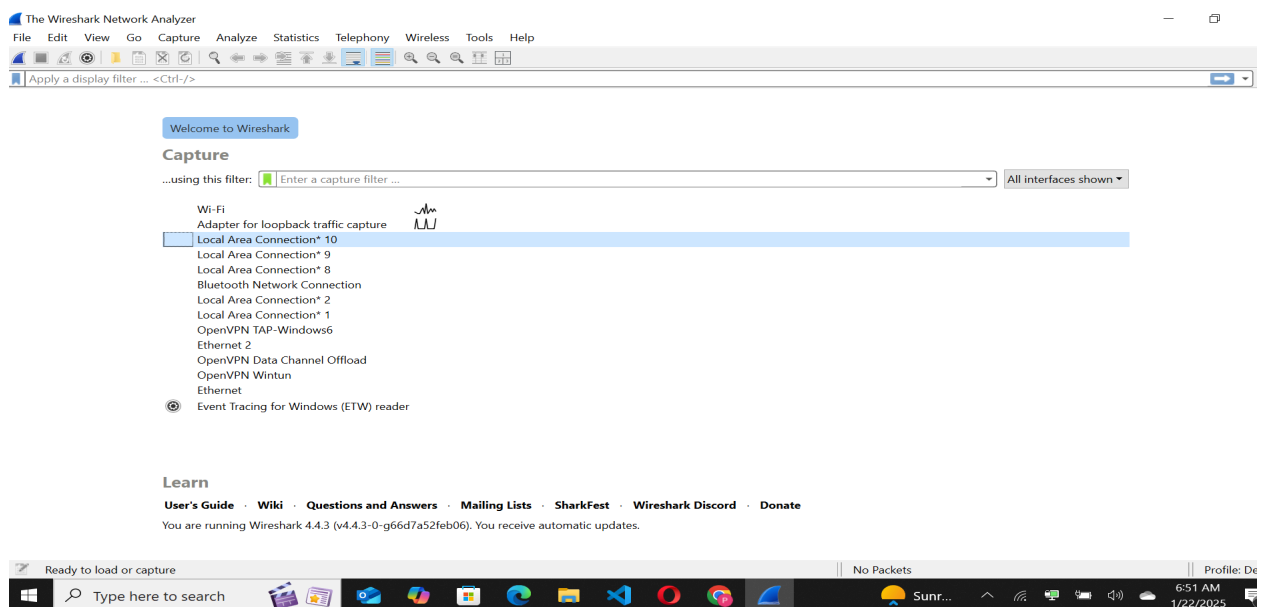
1. Introduction

Network traffic analysis is essential for understanding how data flows within a network, diagnosing performance issues, and identifying potential security vulnerabilities. Wireshark is a powerful and widely used network protocol analyzer that allows for deep inspection of packets traversing a network.

2. Methodology

2.1. Setup:

1. Tool Used: Wireshark



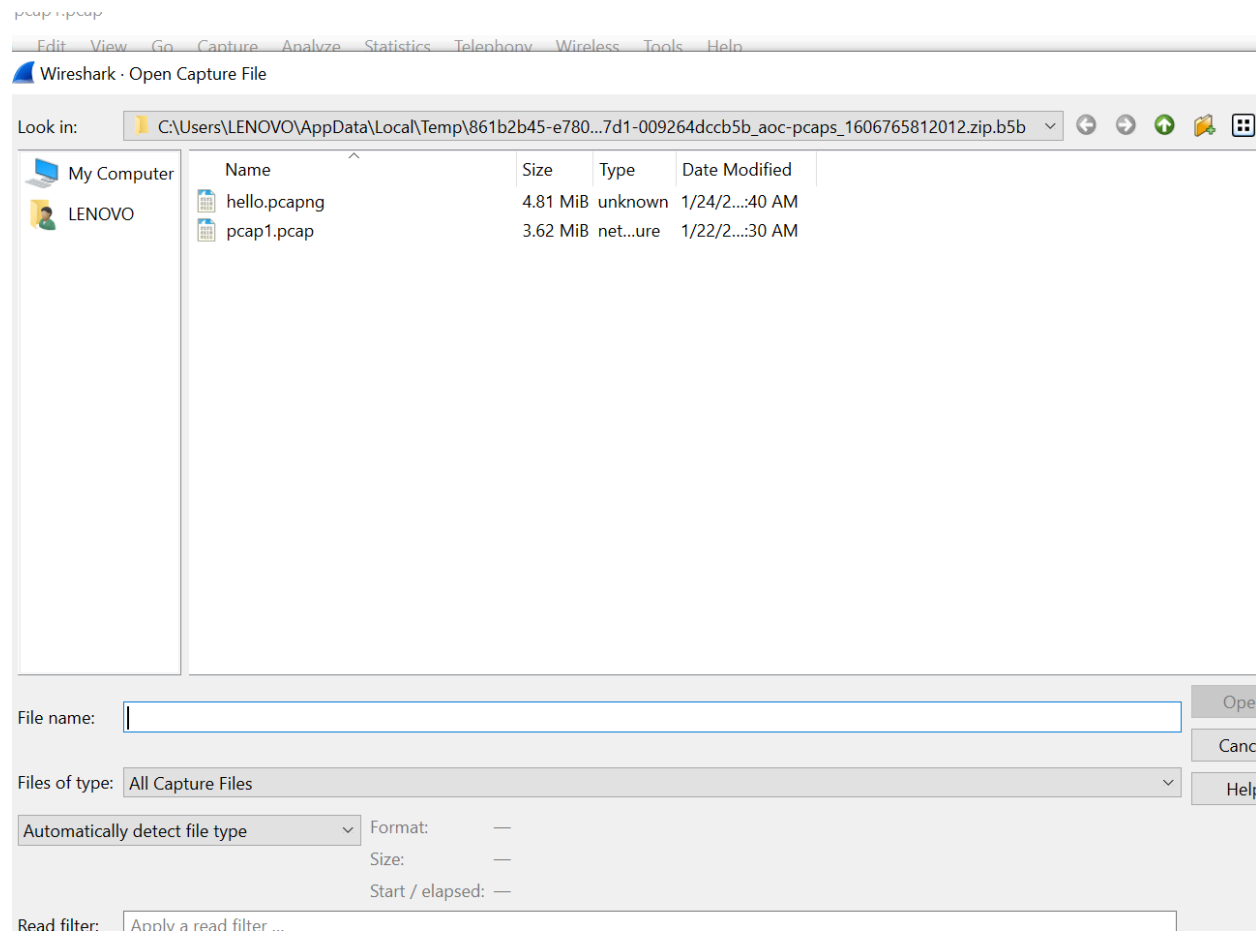
- 2.
3. **Environment:** A standard local area network (LAN) with internet connectivity.
4. **Data Captured:** Network packets over a 10-minute period during regular office hours.
5. **Filters Applied:**
 - Captured traffic from all devices in the network.
 - Focused on TCP, UDP, HTTP, HTTPS, and DNS traffic.

○

2.2. Procedure:

1. Packet Capture:

- Wireshark was started, and a specific network interface wifi was selected for monitoring.
- Captures were saved as hello.pcap and pcap1.pcap files for further analysis.



2. Protocol Filtering:

- Applied filters to identify specific protocols:
 - tcp for Transmission Control Protocol.

- **udp** for User Datagram Protocol.

- **dns** for Domain Name System queries.

hello.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
35	1.412846	172.16.114.121	172.16.112.1	DNS	80	Standard query 0xb82e A beacons.gcp.gvt2.com
36	1.413310	172.16.114.121	172.16.112.1	DNS	80	Standard query 0x4ddd HTTPS beacons.gcp.gvt2.com
37	1.425452	172.16.112.1	172.16.114.121	DNS	130	Standard query response 0xb82e A beacons.gcp.gvt2.com
38	1.439345	172.16.112.1	172.16.114.121	DNS	130	Standard query response 0x4ddd HTTPS beacons.gcp.gvt2.com
319	12.764647	172.16.114.121	172.16.112.1	DNS	86	Standard query 0xd1a9 A waa-pa.clients6.google.com
320	12.764909	172.16.114.121	172.16.112.1	DNS	86	Standard query 0xc9cc HTTPS waa-pa.clients6.google.com
325	12.785754	172.16.112.1	172.16.114.121	DNS	181	Standard query response 0xd1a9 A waa-pa.clients6.google.com
326	12.794920	172.16.112.1	172.16.114.121	DNS	165	Standard query response 0xc9cc HTTPS waa-pa.clients6.google.com
489	16.698508	172.16.114.121	172.16.112.1	DNS	74	Standard query 0xb044 A www.google.com
490	16.699040	172.16.114.121	172.16.112.1	DNS	74	Standard query 0x1246 HTTPS www.google.com
491	16.710631	172.16.112.1	172.16.114.121	DNS	162	Standard query response 0xb044 A www.google.com
492	16.712245	172.16.112.1	172.16.114.121	DNS	171	Standard query response 0x1246 HTTPS www.google.com
580	16.942612	172.16.114.121	172.16.112.1	DNS	74	Standard query 0x32a3 A lh3.google.com
581	16.942925	172.16.114.121	172.16.112.1	DNS	74	Standard query 0x9bf2 HTTPS lh3.google.com
584	16.971507	172.16.112.1	172.16.114.121	DNS	173	Standard query response 0x9bf2 HTTPS lh3.google.com
585	16.971507	172.16.112.1	172.16.114.121	DNS	189	Standard query response 0x32a3 A lh3.google.com
616	17.045071	172.16.114.121	172.16.112.1	DNS	85	Standard query 0xf744 A lh3.googleusercontent.com
617	17.045533	172.16.114.121	172.16.112.1	DNS	85	Standard query 0xddf0 HTTPS lh3.googleusercontent.com
619	17.073254	172.16.112.1	172.16.114.121	DNS	180	Standard query response 0xf744 A lh3.googleusercontent.com
620	17.073254	172.16.112.1	172.16.114.121	DNS	180	Standard query response 0xddf0 HTTPS lh3.googleusercontent.com
627	17.085559	172.16.114.121	172.16.112.1	DNS	88	Standard query 0x26f2 A ogads-pa.clients6.google.com
628	17.085946	172.16.114.121	172.16.112.1	DNS	88	Standard query 0x80ee HTTPS ogads-pa.clients6.google.com
630	17.096911	172.16.112.1	172.16.114.121	DNS	183	Standard query response 0x26f2 A ogads-pa.clients6.google.com

0000 6c 3b 6b ea 0f cf 7a 66 38 17 2d c2 08 00 45 00 l;k...zf 8.....E..

0010 00 42 39 e7 00 00 80 11 c6 28 ac 10 72 79 ac 10 B9.....(..ry..

0020 70 01 f1 8e 00 35 00 2e f7 34 b8 2e 01 00 00 01 p.....5..4.....

0030 00 00 00 00 00 00 07 62 65 61 63 6f 6e 73 03 67b eacons g

0040 63 70 04 67 76 74 32 03 63 6f 6d 00 00 01 00 01 cp gvt2. com.....

■ **http** and **https** for web traffic.

pcap1.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
67	62.185886	10.10.67.199	10.10.15.52	HTTP	394	GET / HTTP/1.1
69	62.186466	10.10.15.52	10.10.67.199	HTTP	1956	HTTP/1.1 200 OK (text/html)
71	62.478663	10.10.67.199	10.10.15.52	HTTP	363	GET /fontawesome/css/all.min.css HTTP/1.1
75	62.479630	10.10.67.199	10.10.15.52	HTTP	348	GET /css/dark.css HTTP/1.1
83	62.480991	10.10.67.199	10.10.15.52	HTTP	333	GET /js/bundle.js HTTP/1.1
85	62.481045	10.10.67.199	10.10.15.52	HTTP	342	GET /js/instantpage.min.js HTTP/1.1
87	62.481475	10.10.15.52	10.10.67.199	HTTP	603	HTTP/1.1 200 OK (text/css)
89	62.482828	10.10.15.52	10.10.67.199	HTTP	1585	HTTP/1.1 200 OK (application/javascript)
91	62.485543	10.10.15.52	10.10.67.199	HTTP	12845	HTTP/1.1 200 OK (text/css)
93	62.486262	10.10.15.52	10.10.67.199	HTTP	20294	HTTP/1.1 200 OK (application/javascript)
95	62.487106	10.10.67.199	10.10.15.52	HTTP	347	GET /images/icon.png HTTP/1.1
102	62.492554	10.10.15.52	10.10.67.199	HTTP	2387	HTTP/1.1 200 OK (PNG)
105	62.516878	10.10.67.199	10.10.15.52	HTTP	336	GET /post/index.json HTTP/1.1
106	62.517081	10.10.15.52	10.10.67.199	HTTP	553	HTTP/1.1 404 Not Found (text/html)
107	62.530696	10.10.67.199	10.10.15.52	HTTP	430	GET /fonts/noto-sans-jp-v25-japanese-regular.woff2 HTTP/1.1
108	62.532591	10.10.67.199	10.10.15.52	HTTP	445	GET /fontawesome/webfonts/fa-solid-900.woff2 HTTP/1.1
114	62.535637	10.10.15.52	10.10.67.199	HTTP	3522	HTTP/1.1 200 OK
117	62.540748	10.10.67.199	10.10.15.52	HTTP	415	GET /fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
118	62.541317	10.10.15.52	10.10.67.199	HTTP	16064	HTTP/1.1 200 OK
202	62.708297	10.10.67.199	10.10.15.52	HTTP	315	GET /favicon.ico HTTP/1.1
203	62.708533	10.10.15.52	10.10.67.199	HTTP	2281	HTTP/1.1 200 OK (PNG)
281	62.761319	10.10.15.52	10.10.67.199	HTTP	641	HTTP/1.1 200 OK
295	63.665611	10.10.67.199	10.10.15.52	HTTP	445	GET / HTTP/1.1

0000 02 89 03 cb f7 6b 02 23 60 d9 6c db 08 00 45 00k.#.....E..

0010 01 7c b2 9f 40 00 40 06 1f ce 0a 0a 43 c7 0a 0a |..@..C.....

0020 0f 34 d9 62 00 50 8c 92 f6 21 d6 c8 17 16 80 18 -4 b P.....!

0030 01 eb 20 65 00 00 01 01 08 0a e9 ca ad 99 05 c0e.....

0040 ec 83 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 ..GET / HTTP/1.1

0050 0d 0a 48 6f 73 74 3a 20 74 62 66 63 2e 62 6c 6f ..Host: tbfc.bio

0060 67 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d g>User-Agent: M

0070 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 31 3b ozilla/5.0 (X11;

3. Analysis:

- Inspected the captured packets for headers, payloads, and communication patterns.

The image displays the Wireshark network protocol analyzer interface. The top window, titled 'Wireshark · Export · HTTP object list', shows a list of objects extracted from the captured packets. The bottom window, titled 'Wireshark · Conversations · Wi-Fi', shows a list of conversations between IP addresses. The bottom-most window shows the details of a selected packet (Frame 3).

Wireshark · Export · HTTP object list

No.	Time	Packet	Hostname	Content Type	Size	Filename
1	0.000	69	tbfc.blog	text/html	4532 bytes	\
2	0.000	87	tbfc.blog	text/css	406 bytes	dark.css
3	0.000	89	tbfc.blog	application/javascript	2841 bytes	instantpage.min.js
4	0.000	91	tbfc.blog	text/css	57 kB	all.min.css
5	0.000	93	tbfc.blog	application/javascript	68 kB	bundle.js
6	2.560	102	tbfc.blog	image/png	101 kB	icon.png
7	2.560	106	tbfc.blog	text/html	271 bytes	index.json
8	3.520	114	tbfc.blog	text/html	76 kB	fa-solid-900.woff2
9	3.520	118	tbfc.blog	text/html	15 kB	roboto-v20-latin-regular.woff2
10	3.680	203	tbfc.blog	image/vnd.microsoft.icon	1915 bytes	favicon.ico
11	5.520	281	tbfc.blog	image/vnd.microsoft.icon	1637 kB	noto-sans-jp-v25-japanese_latin-regular.woff2
		297	tbfc.blog	text/html	4532 bytes	\
		305	tbfc.blog	text/css	57 kB	all.min.css
		308	tbfc.blog	text/css	406 bytes	dark.css
		317	tbfc.blog	application/javascript	68 kB	bundle.js
		318	tbfc.blog	application/javascript	2841 bytes	instantpage.min.js
		331	tbfc.blog	image/png	101 kB	icon.png
		336	tbfc.blog	text/html	271 bytes	index.json
		339	tbfc.blog	image/vnd.microsoft.icon	1915 bytes	favicon.ico
		447	tbfc.blog		1637 kB	noto-sans-jp-v25-japanese_latin-regular.woff2
		464	tbfc.blog		76 kB	fa-solid-900.woff2
		468	tbfc.blog		15 kB	roboto-v20-latin-regular.woff2
		472	tbfc.blog	text/html	3210 bytes	reinder-of-the-week

Wireshark · Conversations · Wi-Fi

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
34.211.242.146	443	172.16.114.121	49966	6	387 bytes	13	4	279 bytes	2	108 bytes	18.051843	0.2174	10 kbps	3974 bits/s
172.16.114.121	50254	34.211.242.146	443	26	11 kB	14	12	5 kB	14	7 kB	19.445896	0.9074	40 kbps	57 kbps
172.16.114.121	50252	35.212.16.125	443	32	10 kB	1	17	4 kB	15	6 kB	1.014549	5.9898	5816 bits/s	7726 bits/s
172.16.114.121	50102	40.99.33.146	443	2	121 bytes	2	1	55 bytes	1	66 bytes	2.864594	0.0186	23 kbps	28 kbps
172.16.114.121	49676	92.223.85.162	443	4	242 bytes	3	2	110 bytes	2	132 bytes	4.944584	0.0588	87 bits/s	104 bits/s
172.16.114.121	50228	142.250.199.3	443	2	121 bytes	6	1	55 bytes	1	66 bytes	7.642701	0.0165	26 kbps	32 kbps
172.16.114.121	50227	142.251.222.234	443	2	121 bytes	5	1	55 bytes	1	66 bytes	6.991595	0.0127	34 kbps	41 kbps
172.16.114.121	50229	142.251.222.234	443	2	121 bytes	8	1	55 bytes	1	66 bytes	10.757661	0.0118	37 kbps	44 kbps
172.16.114.121	50230	146.75.45.229	443	2	121 bytes	7	1	55 bytes	1	66 bytes	10.744414	0.0150	29 kbps	35 kbps
172.16.114.121	49862	157.240.236.60	443	4	358 bytes	9	2	178 bytes	2	180 bytes	12.502352	0.2859	4979 bits/s	5035 bits/s
172.16.114.121	49965	172.64.151.4	443	10	965 bytes	11	5	511 bytes	5	454 bytes	14.362058	0.4248	9624 bits/s	8550 bits/s
172.16.114.121	50253	216.58.196.3	443	31	11 kB	12	14	3 kB	17	8 kB	14.423091	0.0806	334 kbps	793 kbps
172.16.114.121	50226	216.58.196.14	443	2	121 bytes	4	1	55 bytes	1	66 bytes	6.940765	0.0142	31 kbps	37 kbps
172.16.114.121	50238	216.58.221.202	443	2	121 bytes	10	1	55 bytes	1	66 bytes	13.089597	0.0117	37 kbps	45 kbps
204.79.197.222	443	172.16.114.121	50220	1	54 bytes	0	1	54 bytes	0	0 bytes	0.067167	0.0000		

Frame 3: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0

Ethernet II, Src: Sa:cc:66:2e:69:3b (Sa:cc:66:2e:69:3b), Dst: 172.16.114.121

Internet Protocol Version 4, Src: 172.16.114.121, Dst: 172.16.114.121

TCP, Src Port: 50220, Dst Port: 443

Application/javascript

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 02

0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f

Instantpage.min.js

0000 01 00 5e 00 00 fb 5a cc 66 2e 69 3b 08 00 45 00

0010 00 56 9c b2 00 00 ff 11 17 37 ac 10 7a a1 e0 00

0020 00 fb 14 e9 14 e9 00 42 a0 60 00 00 00 00 00 0

- Noted anomalies such as repeated failed connection attempts or irregular DNS queries.

3. Findings

3.1. Common Protocols Identified

1. TCP (Transmission Control Protocol):

- Accounts for the majority of traffic.
- Observed as the backbone for web browsing (HTTP/HTTPS), file transfers, and email communication.
- Reliable, connection-oriented communication was evident through SYN, SYN-ACK, and ACK handshakes.

2. UDP (User Datagram Protocol):

- Primarily associated with DNS and some streaming traffic.
- Notable for its low latency but lack of reliability (e.g., no acknowledgment mechanisms).

3. DNS (Domain Name System):

- Used for hostname-to-IP resolution.
- Frequent DNS queries, including standard A (IPv4) and AAAA (IPv6) records.

4. HTTP/HTTPS:

- Predominant for web browsing.
- HTTPS traffic was encrypted, making payloads inaccessible, but metadata such as SNI (Server Name Indication) and server IPs were available.

5. ICMP (Internet Control Message Protocol):

- Observed occasional pings for network diagnostics.

3.2. Traffic Patterns

1. High Peak Traffic:

- During specific hours, there was a surge in HTTP/HTTPS traffic, likely due to employees accessing web-based applications.

2. DNS Queries:

- Consistent DNS traffic with occasional spikes during browsing sessions or application launches.
 - 3. **TCP Retransmissions and Latency:**
 - A small percentage of packets exhibited retransmissions, indicating potential congestion or packet loss.
 - 4. **Unusual Activity:**
 - Repeated connection attempts to unresponsive servers were flagged for potential investigation.
-

4. Insights and Recommendations

4.1. Insights

1. HTTPS encryption ensures privacy for web traffic but limits visibility into payloads for analysis.
2. The network exhibited a mix of standard office traffic with no immediate signs of malicious activity.
3. DNS servers responded quickly, ensuring smooth hostname resolution.

4.2. Recommendations

1. **Optimize Network Performance:**
 - Identify and reduce retransmission occurrences by addressing congestion points.
 - Ensure adequate bandwidth for peak usage times.
2. **Enhance Security:**
 - Monitor for anomalies like excessive DNS queries or connection attempts to unknown servers.
 - Deploy intrusion detection systems (IDS) to complement packet analysis.
3. **Regular Monitoring:**
 - Schedule periodic network traffic analysis to identify evolving patterns or threats.
 - Analyze logs from multiple points in the network for comprehensive insights.

5. Conclusion

The analysis revealed a healthy mix of standard network traffic with no critical anomalies. Wireshark proved to be an invaluable tool for capturing and analyzing network packets, offering insights into protocol usage and traffic patterns. Continuous monitoring and proactive measures are recommended to maintain network performance and security.