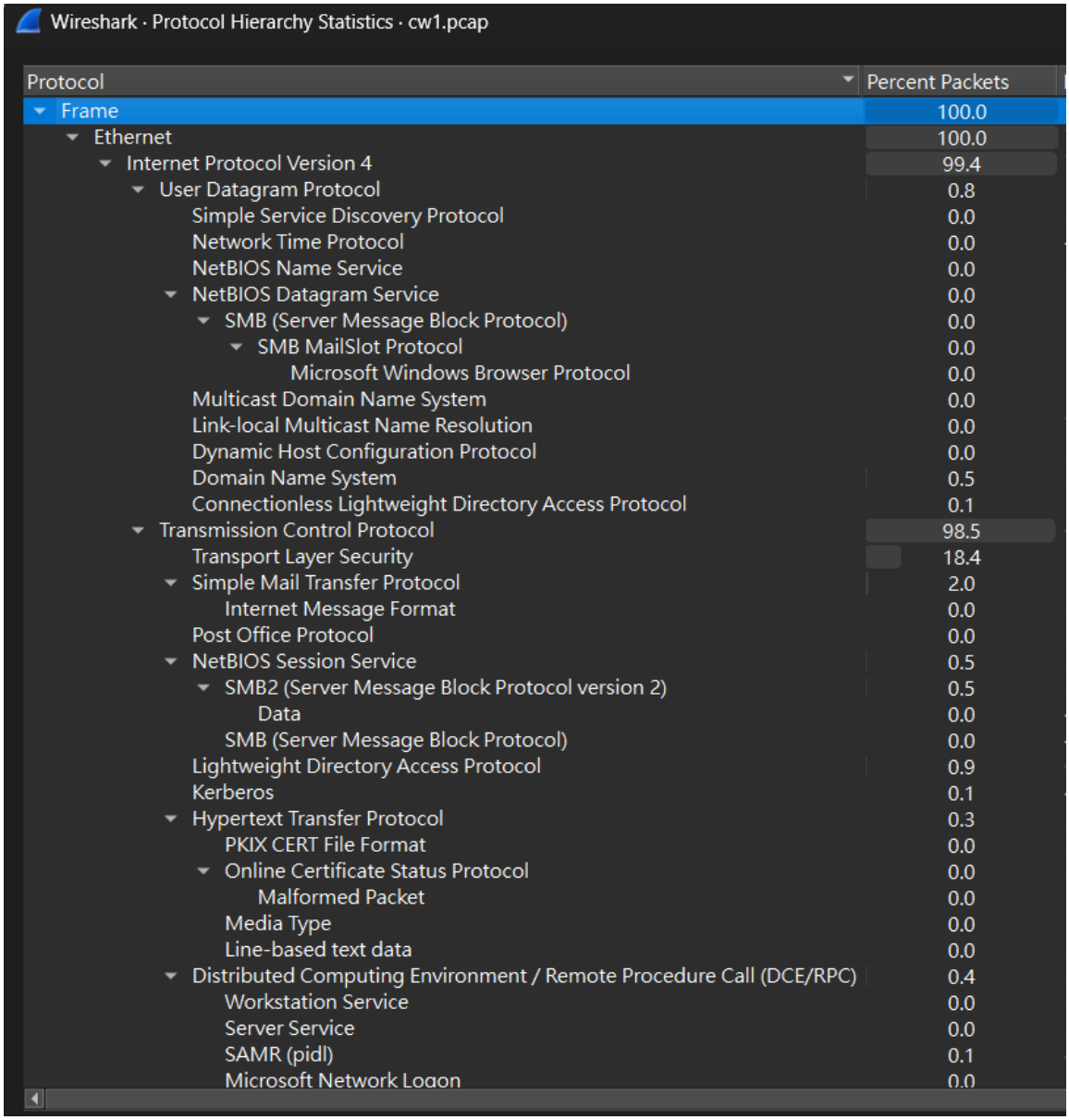
Incident Report: Malicious Network Traffic Analysis

Section 1 – Introduction This incident report documents a comprehensive forensic investigation into suspicious network activity captured in the file cw1.pcap. The analysis was initiated following an endpoint security alert indicating unusual outbound connections from an internal Windows workstation shortly after a user opened an attachment. As a security analyst, the primary objectives were to identify the compromised system, trace the infection vector, classify the malware family, reconstruct the attack chain, and provide actionable recommendations to prevent recurrence.

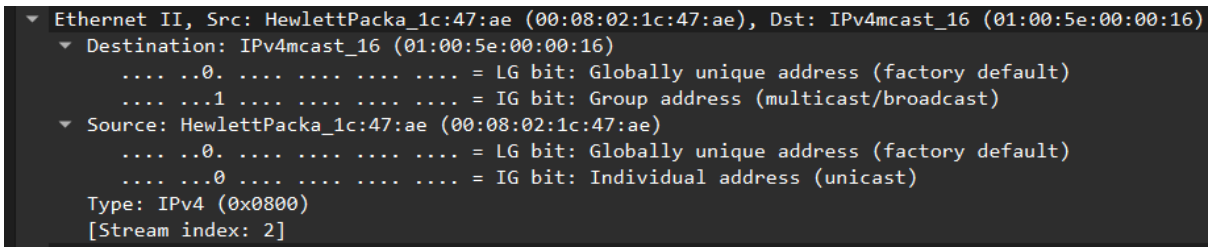
The investigation leveraged 20 targeted quiz questions that systematically guided the discovery of key indicators of compromise (IOCs), including malicious domains, IP addresses, payloads, command-and-control (C2) infrastructure, and exfiltration attempts. Wireshark served as the core analysis platform, supplemented by manual packet dissection, protocol decoding, and external IOC validation via VirusTotal. The report is structured as follows: methodology (tools, techniques, and step-by-step process), results (detailed findings with evidence), and conclusion (lessons learned and prevention strategies). All timestamps are in UTC unless otherwise stated.

Section 2 – Methodology The analysis was performed using **Wireshark** (stable release) as the primary tool due to its powerful filtering engine, protocol dissectors, stream reconstruction, Conversations statistics, and HTTP object export capabilities. No additional commercial tools were required, ensuring reproducibility in resource-constrained environments. The investigative process followed a structured, repeatable approach aligned with NIST SP 800-86 (Guide to Integrating Forensic Techniques into Incident Response):

1. **Initial Triage and Scope Definition** Opened cw1.pcap and reviewed Statistics > Protocol Hierarchy to identify dominant protocols: TCP (majority), HTTP, TLS/HTTPS, DNS, and SMTP. Filtered on the suspected victim IP ip.src == 10.9.23.102 (private 10.0.0.0/8 range) and confirmed the endpoint MAC address 00:08:02:1c:47:ae (Hewlett Packard) as the consistent source of malicious traffic.



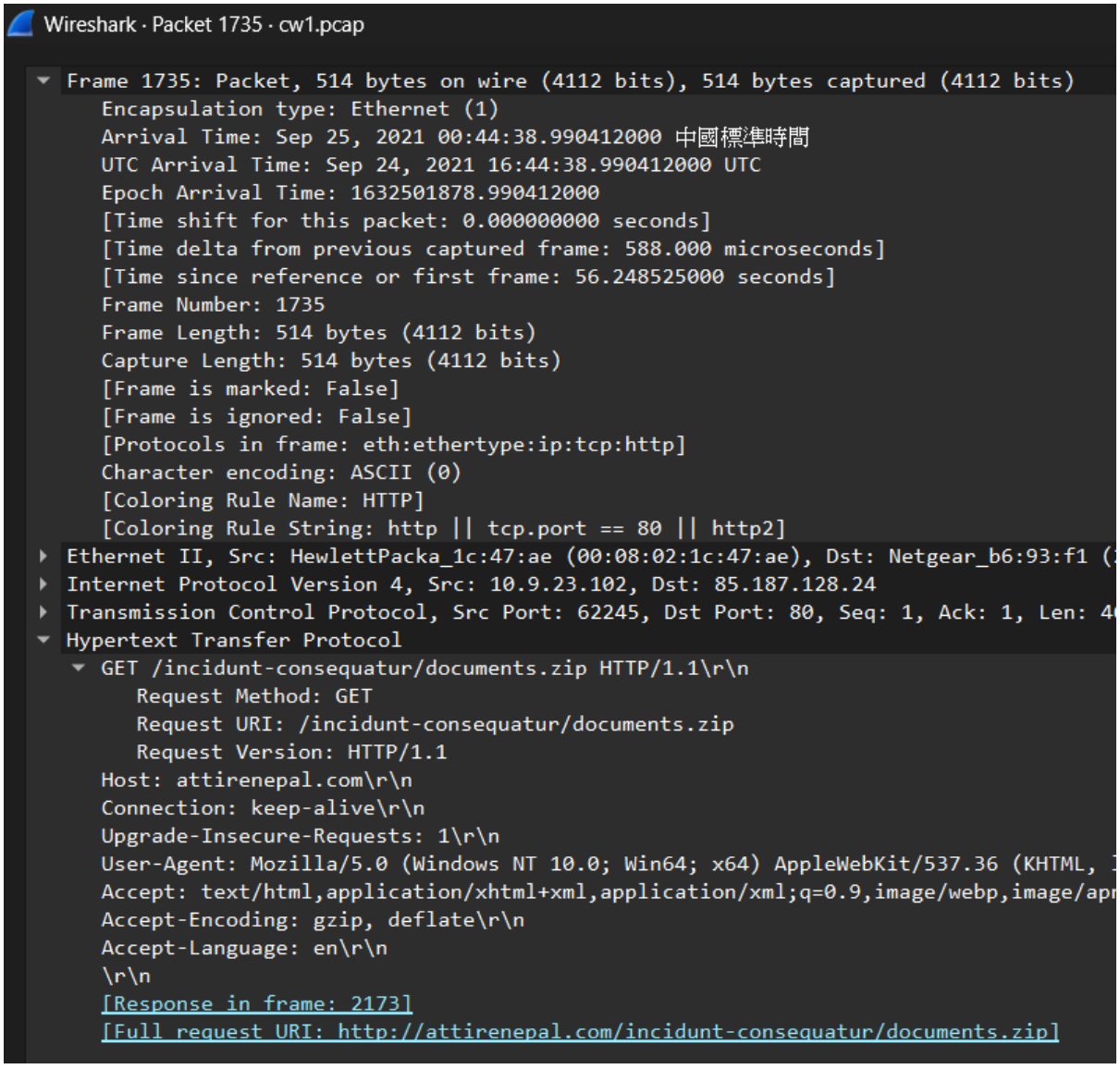
Protocol Hierarchy



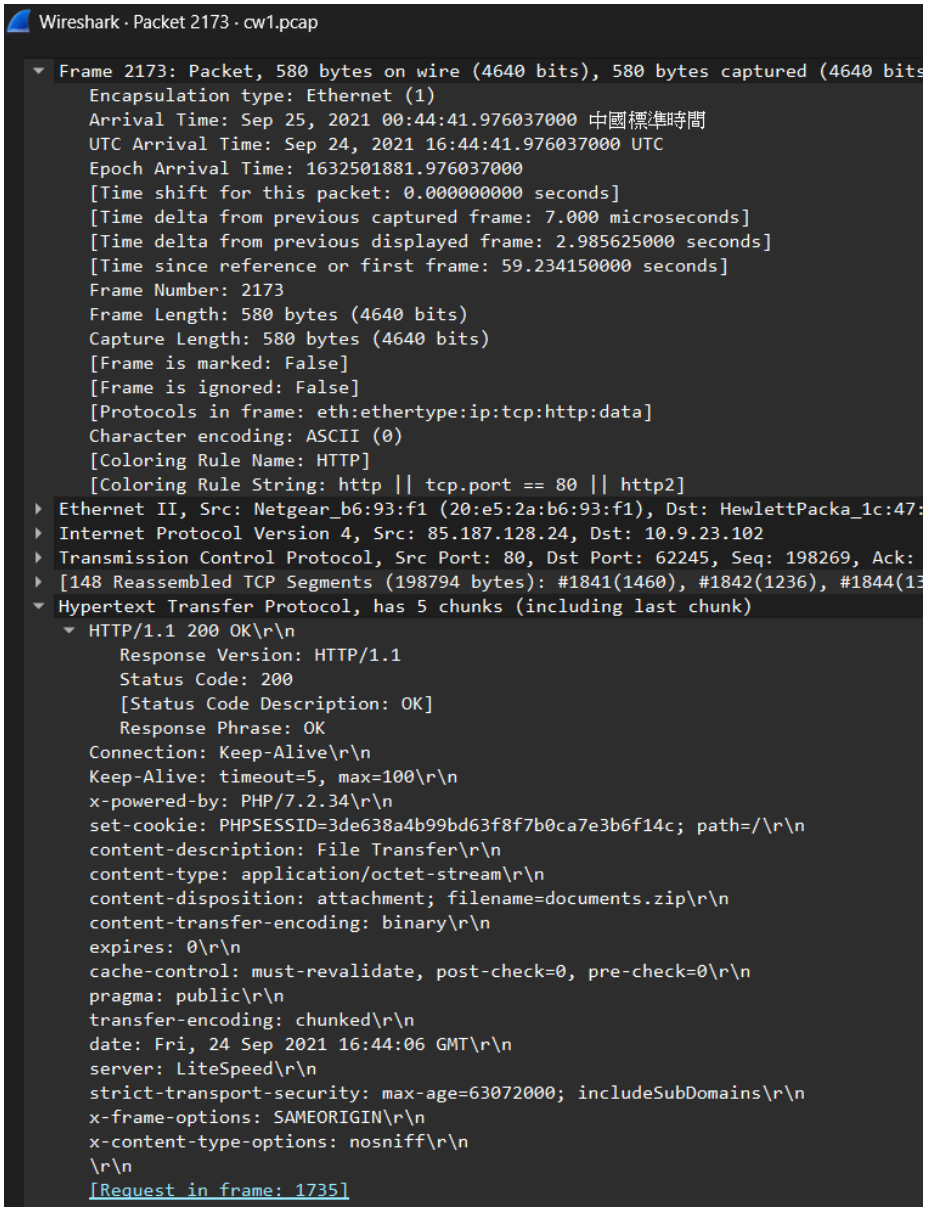
MAC address of infected machine

2. **Reconstruction of Initial Infection Vector** Applied filter http to isolate clear-text web traffic. Identified the first malicious HTTP transaction at **2021-09-24 16:44:38 UTC**:

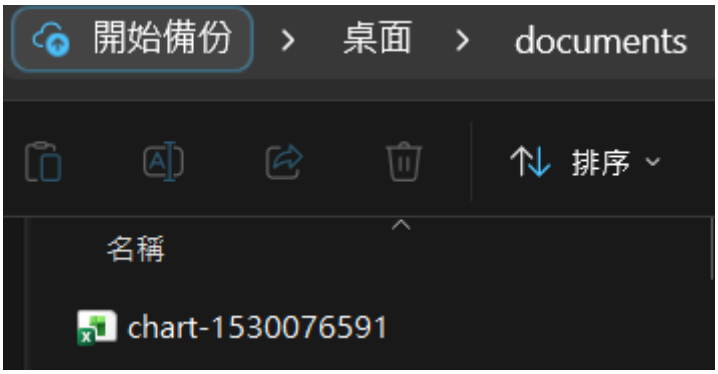
Frame 1735 (GET /incidunt-consequatur/documents.zip HTTP/1.1) to domain **attirenepal.com**. The server response in Frame 2173 returned **documents.zip** (198125 bytes) with headers: Server: **LiteSpeed** (no version disclosed), X-Powered-By: PHP/7.2.34, Content-Disposition: attachment; filename=documents.zip. Exported the file via File > Export Objects > HTTP, decompressed it locally, and discovered the internal file **chart-1530076591.xls** (likely containing malicious VBA macros).



Frame 1735



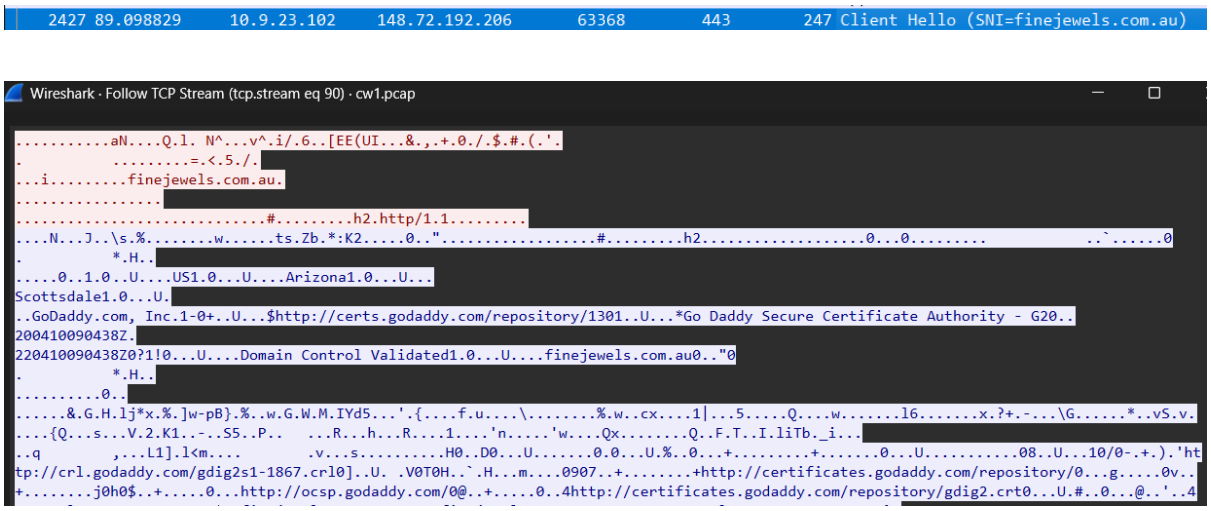
Frame 2173



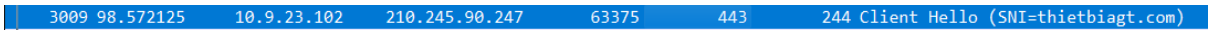
Decompressed documents.zip internal file **chart-1530076591.xls**

3. **Secondary Payload Staging and Lateral Delivery** Narrowed analysis to the critical time window **16:45:11 – 16:45:30 UTC** (quiz hint) using filter tls. Examined Client Hello packets for Server Name Indication (SNI) extension, revealing three additional malicious domains involved in payload delivery:
    a. **finejewels.com.au** (Frame 2427; certificate chain issued by **GoDaddy**)
    b. **Thietbiagt.com (Frame 3009)**
    c. **new.americold.com** (Frame 3229)

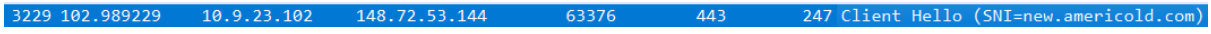
These domains hosted secondary payloads or loaders that facilitated the next stage of compromise.



Frame 2427



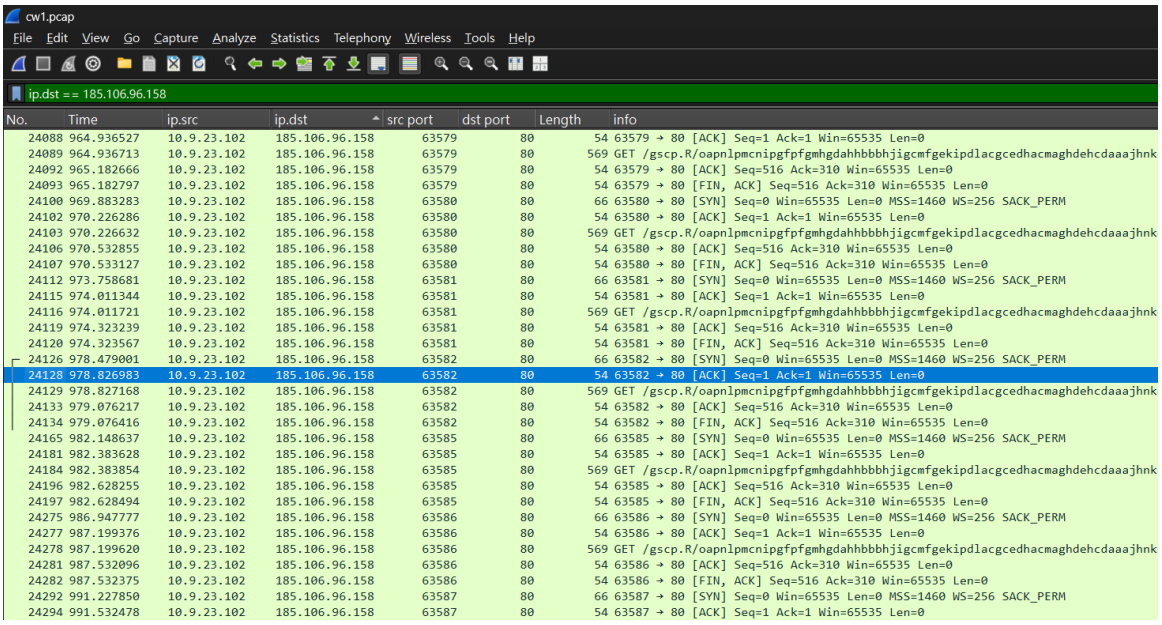
Frame 3009



Frame 3229

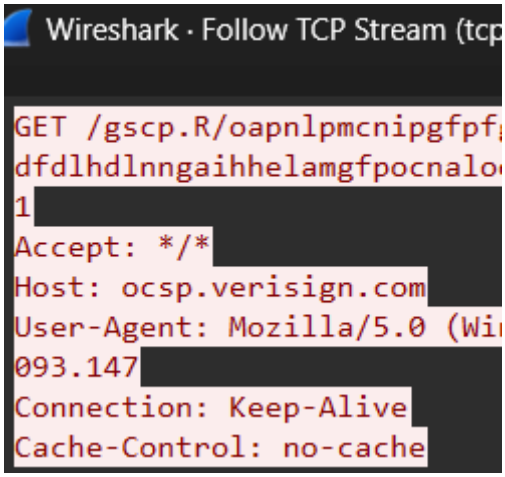
4. **Command-and-Control (C2) Infrastructure Identification** Used Statistics > Conversations > TCP (sorted by packet count and duration) to detect persistent, periodic outbound connections indicative of beaconing. Identified two Cobalt Strike Team Servers:
    a. **185.106.96.158** (port 80/HTTP): Host header **ocsp.verisign.com** (domain fronting technique), associated domain **survmeter.live**

b. **185.125.204.174** (port 443/HTTPS): SNI **securitybusinpuff.com** (Frame 7112 Client Hello)



No.	Time	ip.src	ip.dst	src port	dst port	Length	info
24088	964.936527	10.9.23.102	185.106.96.158	63579	80	54	63579 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
24089	964.936713	10.9.23.102	185.106.96.158	63579	80	569	GET /gscp.R/oapnlpmcnipgfpfgmhgdahhbbbhjigcmfgekipdlacgcedhacmaghdehcdaaajhnk
24092	965.182666	10.9.23.102	185.106.96.158	63579	80	54	63579 → 80 [ACK] Seq=516 Ack=310 Win=65535 Len=0
24093	965.182797	10.9.23.102	185.106.96.158	63579	80	54	63579 → 80 [FIN, ACK] Seq=516 Ack=310 Win=65535 Len=0
24100	969.883283	10.9.23.102	185.106.96.158	63580	80	66	63580 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
24102	970.226286	10.9.23.102	185.106.96.158	63580	80	54	63580 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
24103	970.226632	10.9.23.102	185.106.96.158	63580	80	569	GET /gscp.R/oapnlpmcnipgfpfgmhgdahhbbbhjigcmfgekipdlacgcedhacmaghdehcdaaajhnk
24106	970.532855	10.9.23.102	185.106.96.158	63580	80	54	63580 → 80 [ACK] Seq=516 Ack=310 Win=65535 Len=0
24107	970.533127	10.9.23.102	185.106.96.158	63580	80	54	63580 → 80 [FIN, ACK] Seq=516 Ack=310 Win=65535 Len=0
24112	973.758681	10.9.23.102	185.106.96.158	63581	80	66	63581 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
24115	974.011344	10.9.23.102	185.106.96.158	63581	80	54	63581 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
24116	974.011721	10.9.23.102	185.106.96.158	63581	80	569	GET /gscp.R/oapnlpmcnipgfpfgmhgdahhbbbhjigcmfgekipdlacgcedhacmaghdehcdaaajhnk
24119	974.323239	10.9.23.102	185.106.96.158	63581	80	54	63581 → 80 [ACK] Seq=516 Ack=310 Win=65535 Len=0
24120	974.323567	10.9.23.102	185.106.96.158	63581	80	54	63581 → 80 [FIN, ACK] Seq=516 Ack=310 Win=65535 Len=0
24126	978.479001	10.9.23.102	185.106.96.158	63582	80	66	63582 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
24128	978.826983	10.9.23.102	185.106.96.158	63582	80	54	63582 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
24129	978.827168	10.9.23.102	185.106.96.158	63582	80	569	GET /gscp.R/oapnlpmcnipgfpfgmhgdahhbbbhjigcmfgekipdlacgcedhacmaghdehcdaaajhnk
24133	979.076217	10.9.23.102	185.106.96.158	63582	80	54	63582 → 80 [ACK] Seq=516 Ack=310 Win=65535 Len=0
24134	979.076416	10.9.23.102	185.106.96.158	63582	80	54	63582 → 80 [FIN, ACK] Seq=516 Ack=310 Win=65535 Len=0
24165	982.148637	10.9.23.102	185.106.96.158	63585	80	66	63585 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
24181	982.383628	10.9.23.102	185.106.96.158	63585	80	54	63585 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
24184	982.383854	10.9.23.102	185.106.96.158	63585	80	569	GET /gscp.R/oapnlpmcnipgfpfgmhgdahhbbbhjigcmfgekipdlacgcedhacmaghdehcdaaajhnk
24196	982.628255	10.9.23.102	185.106.96.158	63585	80	54	63585 → 80 [ACK] Seq=516 Ack=310 Win=65535 Len=0
24197	982.628494	10.9.23.102	185.106.96.158	63585	80	54	63585 → 80 [FIN, ACK] Seq=516 Ack=310 Win=65535 Len=0
24275	986.947777	10.9.23.102	185.106.96.158	63586	80	66	63586 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
24277	987.199376	10.9.23.102	185.106.96.158	63586	80	54	63586 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
24278	987.199620	10.9.23.102	185.106.96.158	63586	80	569	GET /gscp.R/oapnlpmcnipgfpfgmhgdahhbbbhjigcmfgekipdlacgcedhacmaghdehcdaaajhnk
24281	987.532096	10.9.23.102	185.106.96.158	63586	80	54	63586 → 80 [ACK] Seq=516 Ack=310 Win=65535 Len=0
24282	987.532375	10.9.23.102	185.106.96.158	63586	80	54	63586 → 80 [FIN, ACK] Seq=516 Ack=310 Win=65535 Len=0
24292	991.227850	10.9.23.102	185.106.96.158	63587	80	66	63587 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
24294	991.532478	10.9.23.102	185.106.96.158	63587	80	54	63587 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0

Traffic of **185.106.96.158**



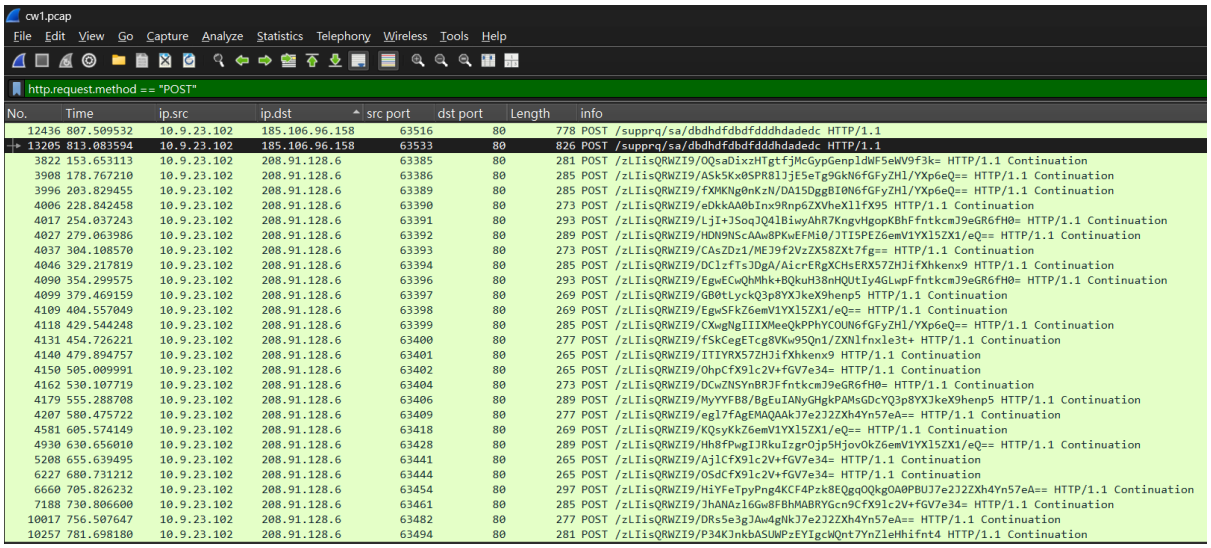
Host header **ocsp.verisign.com**

No.	Time	ip.src	ip.dst	src port	dst port	Length	info
4216	581.342835	10.9.23.102	185.125.204.174	63410	8080	66	63410 → 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SAC
4217	581.504598	185.125.204.1…	10.9.23.102	8080	63410	58	8080 → 63410 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
4218	581.504879	10.9.23.102	185.125.204.174	63410	8080	54	63410 → 8080 [ACK] Seq=1 Ack=1 Win=65535 Len=0
4219	581.509907	10.9.23.102	185.125.204.174	63410	8080	203	63410 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=149
4220	581.510000	185.125.204.1…	10.9.23.102	8080	63410	54	8080 → 63410 [ACK] Seq=1 Ack=150 Win=64240 Len=0
4221	581.683263	185.125.204.1…	10.9.23.102	8080	63410	144	8080 → 63410 [PSH, ACK] Seq=1 Ack=150 Win=64240 Len=90
4222	581.683508	10.9.23.102	185.125.204.174	63410	8080	54	63410 → 8080 [ACK] Seq=150 Ack=91 Win=65535 Len=0
4223	581.685014	185.125.204.1…	10.9.23.102	8080	63410	1402	8080 → 63410 [PSH, ACK] Seq=91 Ack=150 Win=64240 Len=1348
4224	581.685191	10.9.23.102	185.125.204.174	63410	8080	54	63410 → 8080 [ACK] Seq=150 Ack=1439 Win=65535 Len=0
4225	581.844256	185.125.204.1…	10.9.23.102	8080	63410	367	8080 → 63410 [PSH, ACK] Seq=1439 Ack=150 Win=64240 Len=313
4226	581.844480	10.9.23.102	185.125.204.174	63410	8080	54	63410 → 8080 [ACK] Seq=150 Ack=1752 Win=65535 Len=0
4249	583.867600	10.9.23.102	185.125.204.174	63410	8080	147	63410 → 8080 [PSH, ACK] Seq=150 Ack=1752 Win=65535 Len=93
4250	583.867693	185.125.204.1…	10.9.23.102	8080	63410	54	8080 → 63410 [ACK] Seq=1752 Ack=243 Win=64240 Len=0
4251	584.039040	185.125.204.1…	10.9.23.102	8080	63410	60	8080 → 63410 [PSH, ACK] Seq=1752 Ack=243 Win=64240 Len=6
4252	584.039292	10.9.23.102	185.125.204.174	63410	8080	54	63410 → 8080 [ACK] Seq=243 Ack=1758 Win=65535 Len=0
4253	584.208411	185.125.204.1…	10.9.23.102	8080	63410	99	8080 → 63410 [PSH, ACK] Seq=1758 Ack=243 Win=64240 Len=45
4254	584.208634	10.9.23.102	185.125.204.174	63410	8080	54	63410 → 8080 [ACK] Seq=243 Ack=1803 Win=65535 Len=0
4255	584.210999	10.9.23.102	185.125.204.174	63410	8080	449	63410 → 8080 [PSH, ACK] Seq=243 Ack=1803 Win=65535 Len=395
4256	584.211071	185.125.204.1…	10.9.23.102	8080	63410	54	8080 → 63410 [ACK] Seq=1803 Ack=638 Win=64240 Len=0
4257	584.384719	185.125.204.1…	10.9.23.102	8080	63410	353	8080 → 63410 [PSH, ACK] Seq=1803 Ack=638 Win=64240 Len=299
4258	584.384985	10.9.23.102	185.125.204.174	63410	8080	54	63410 → 8080 [ACK] Seq=638 Ack=2102 Win=65535 Len=0
4259	584.385882	185.125.204.1…	10.9.23.102	8080	63410	1514	8080 → 63410 [ACK] Seq=2102 Ack=638 Win=64240 Len=1460
4260	584.385893	185.125.204.1…	10.9.23.102	8080	63410	1290	8080 → 63410 [PSH, ACK] Seq=3562 Ack=638 Win=64240 Len=1236
4261	584.386284	10.9.23.102	185.125.204.174	63410	8080	54	63410 → 8080 [ACK] Seq=638 Ack=4798 Win=65535 Len=0
4262	584.386321	185.125.204.1…	10.9.23.102	8080	63410	1402	8080 → 63410 [PSH, ACK] Seq=4798 Ack=638 Win=64240 Len=1348
4263	584.386423	10.9.23.102	185.125.204.174	63410	8080	54	63410 → 8080 [ACK] Seq=638 Ack=6146 Win=65535 Len=0
4264	584.386635	185.125.204.1…	10.9.23.102	8080	63410	1514	8080 → 63410 [ACK] Seq=6146 Ack=638 Win=64240 Len=1460
4265	584.386667	185.125.204.1…	10.9.23.102	8080	63410	1514	8080 → 63410 [ACK] Seq=7606 Ack=638 Win=64240 Len=1460
4266	584.386698	185.125.204.1…	10.9.23.102	8080	63410	1178	8080 → 63410 [PSH, ACK] Seq=9066 Ack=638 Win=64240 Len=1124
4267	584.386741	185.125.204.1…	10.9.23.102	8080	63410	1402	8080 → 63410 [PSH, ACK] Seq=10190 Ack=638 Win=64240 Len=1348

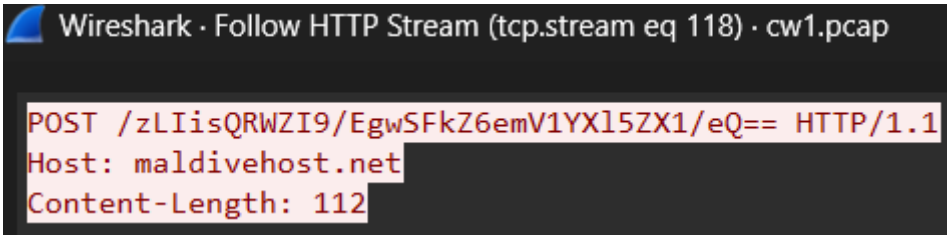
Traffic of **185.125.204.174**

SNI **securitybusinpuff.com**

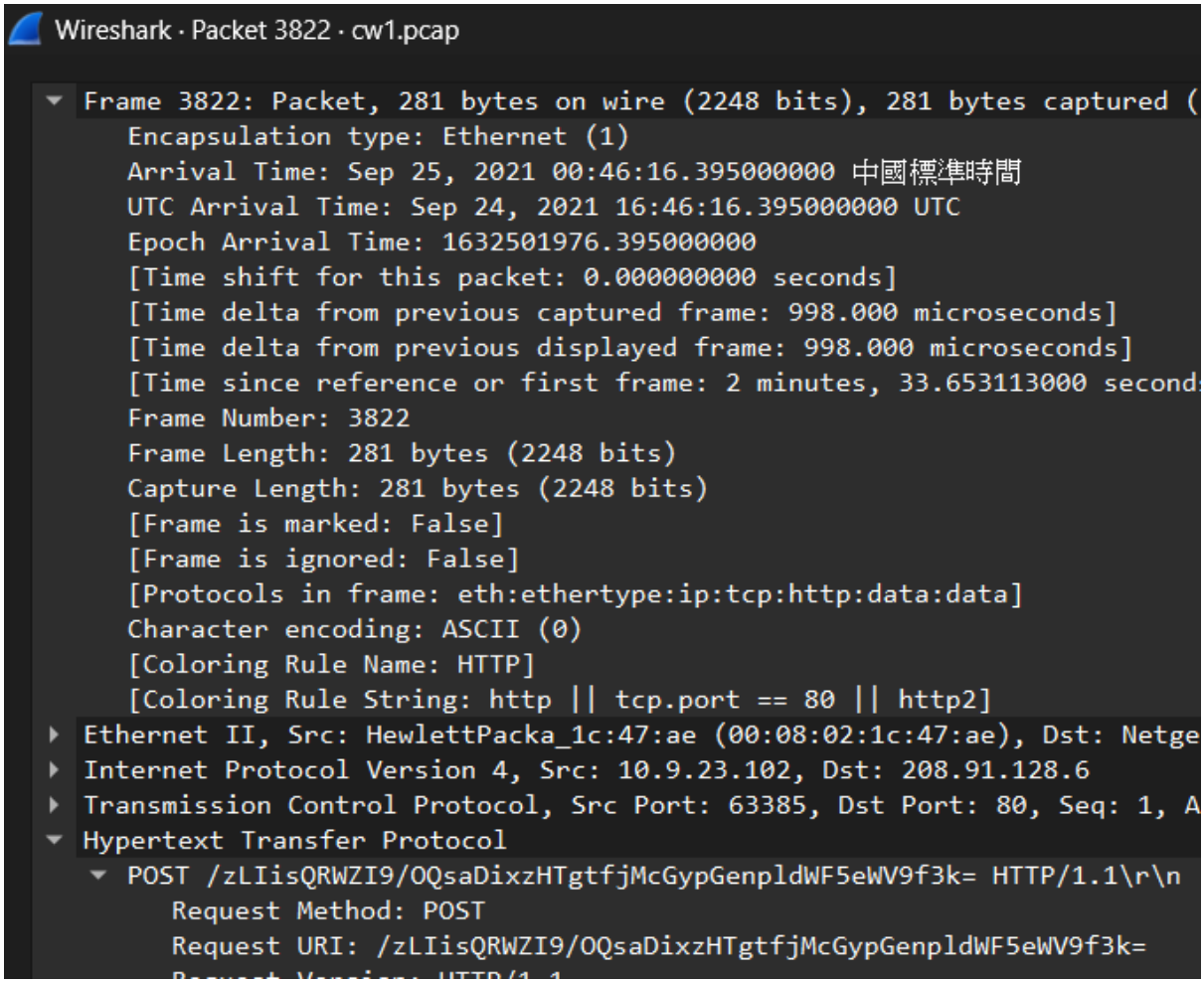
5. **Post-Infection C2 and Beacon Activity** Filtered http.request.method == "POST" to locate active C2 channels. Discovered POST requests to **maldivehost.net** (Frame 3822, 281-byte payload starting **zLIisQRWZI9**). Server response (Frame 3851) revealed **Apache/2.4.49 (cPanel) OpenSSL/1.1.1l mod_bwlimited/1.4**.



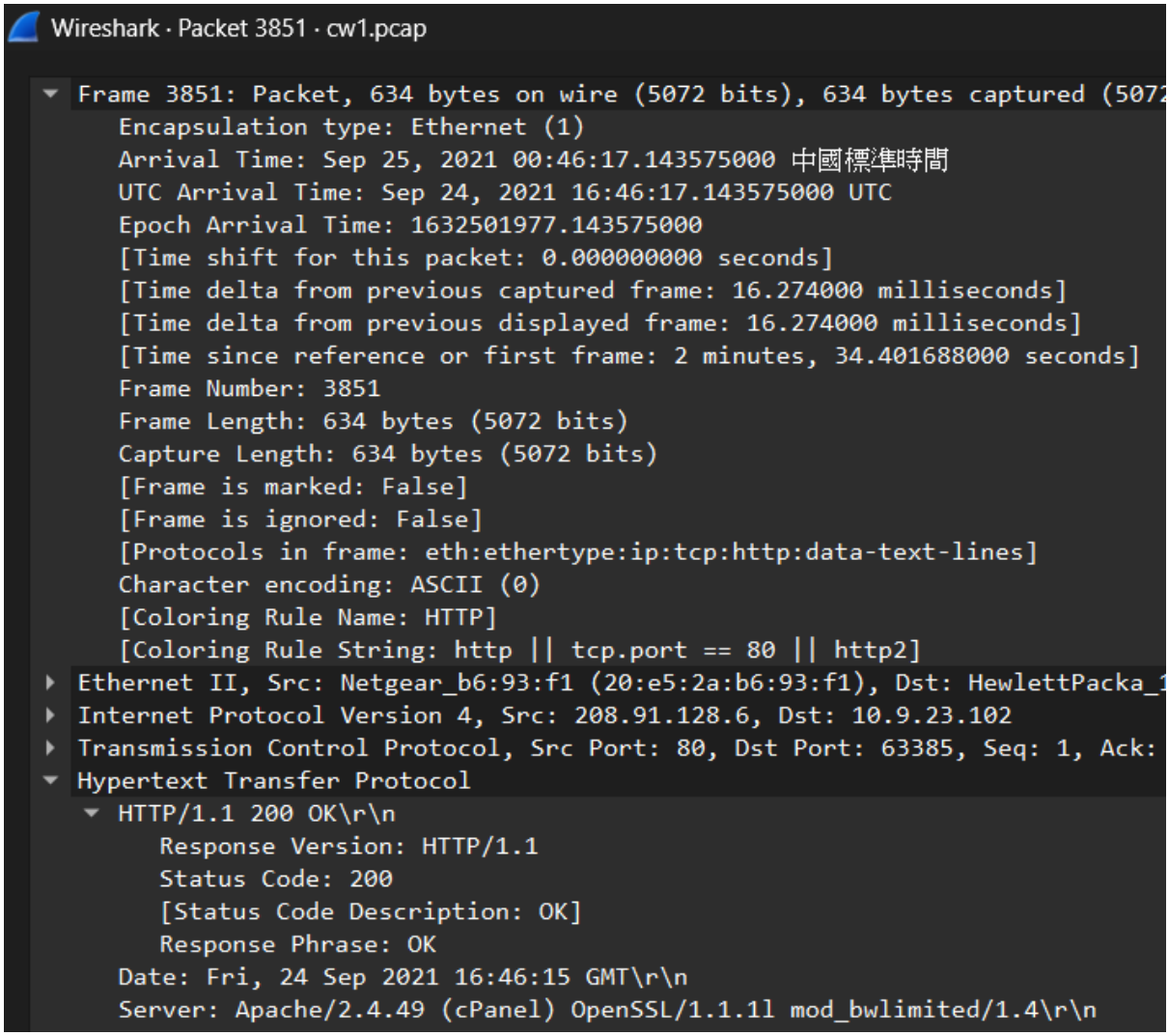
active C2 channels



POST requests to **maldivehost.net**

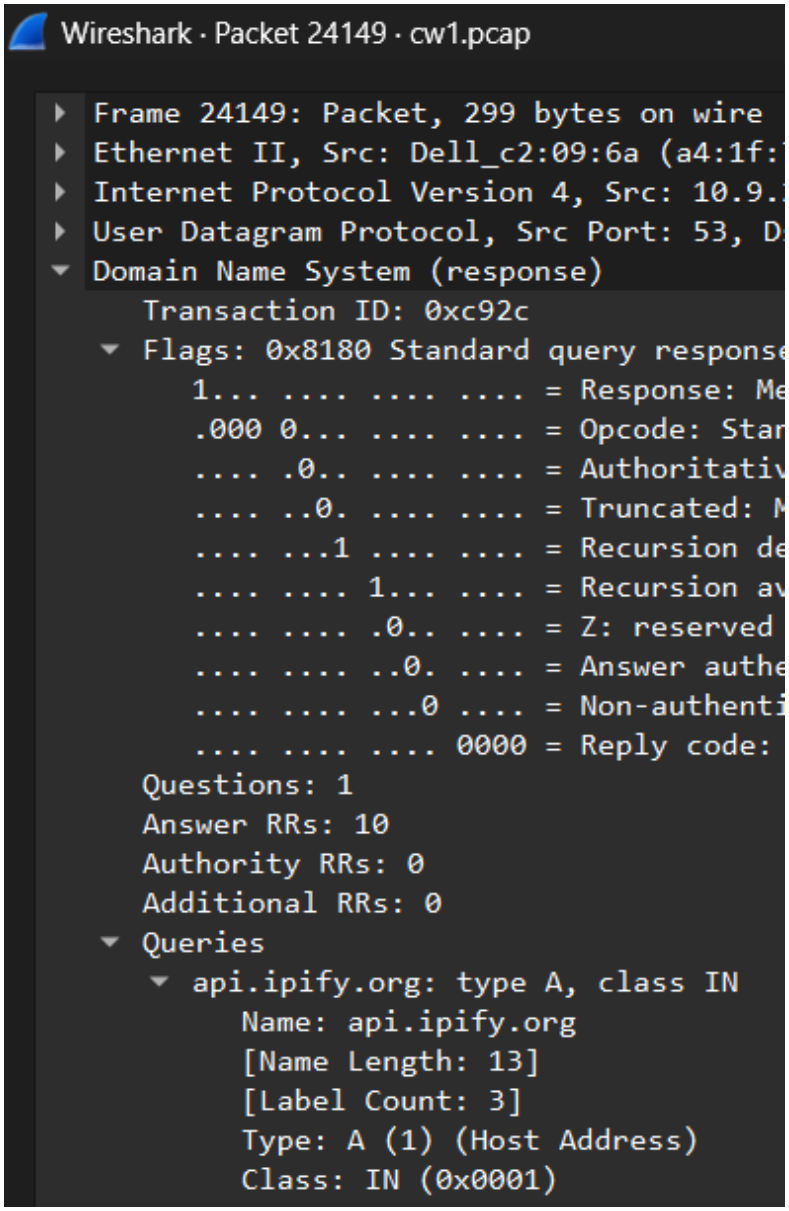

Wireshark · Packet 3822 · cw1.pcap
Frame 3822: Packet, 281 bytes on wire (2248 bits), 281 bytes captured (
Encapsulation type: Ethernet (1)
Arrival Time: Sep 25, 2021 00:46:16.395000000 中國標準時間
UTC Arrival Time: Sep 24, 2021 16:46:16.395000000 UTC
Epoch Arrival Time: 1632501976.395000000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 998.000 microseconds]
[Time delta from previous displayed frame: 998.000 microseconds]
[Time since reference or first frame: 2 minutes, 33.653113000 second
Frame Number: 3822
Frame Length: 281 bytes (2248 bits)
Capture Length: 281 bytes (2248 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http:data:data]
Character encoding: ASCII (0)
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae), Dst: Netge
Internet Protocol Version 4, Src: 10.9.23.102, Dst: 208.91.128.6
Transmission Control Protocol, Src Port: 63385, Dst Port: 80, Seq: 1, A
Hypertext Transfer Protocol
POST /zLIisQRWZI9/OQsaDixzHTgtfjMcGypGenpldWF5eWV9f3k= HTTP/1.1\r\n
Request Method: POST
Request URI: /zLIisQRWZI9/OQsaDixzHTgtfjMcGypGenpldWF5eWV9f3k=

Frame 3822

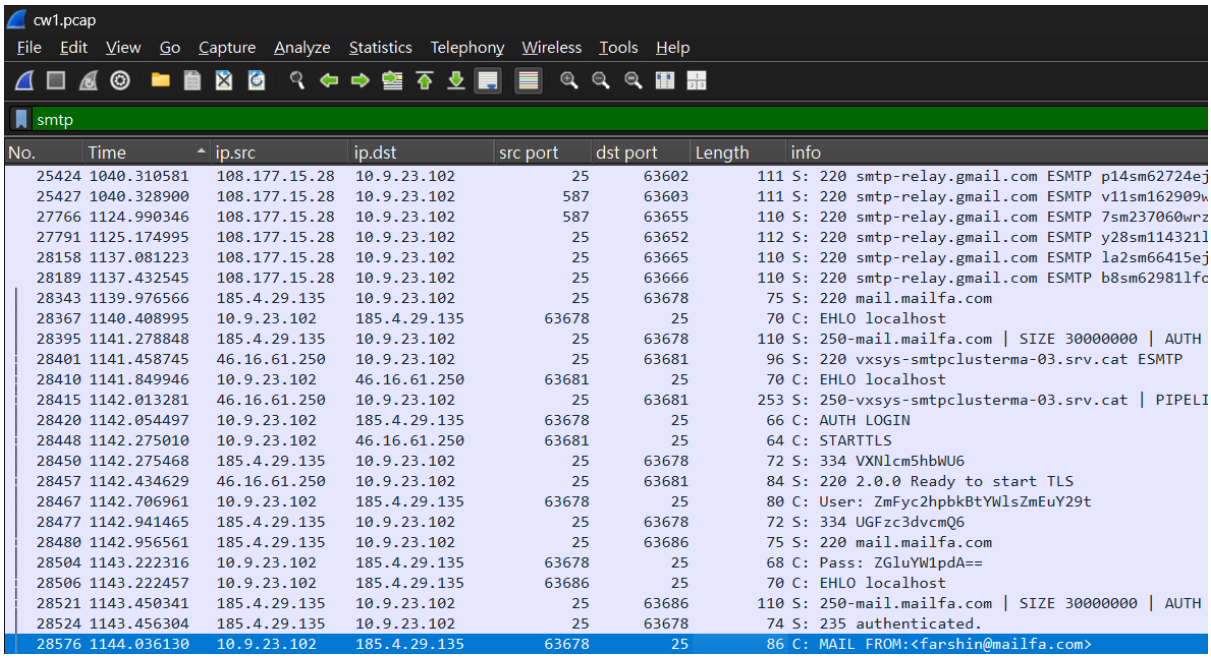


Frame 3851

6. **Reconnaissance and Exfiltration** Filtered dns and identified an A query to **api.ipify.org** at **2021-09-24 17:00:04 UTC** (Frame 24149), used by the malware to determine the victim's public IP. Filtered smtp to detect exfiltration attempts. The first MAIL FROM observed was farshin@mailfa.com. Following the TCP stream revealed AUTH LOGIN credentials for ho3ein.sharifi@mailfa.com (password decoded from base64: **13691369**).


Wireshark · Packet 24149 · cw1.pcap
Frame 24149: Packet, 299 bytes on wire
Ethernet II, Src: Dell_c2:09:6a (a4:1f:
Internet Protocol Version 4, Src: 10.9.
User Datagram Protocol, Src Port: 53, D
Domain Name System (response)
Transaction ID: 0xc92c
Flags: 0x8180 Standard query response
1... .... = Response: Me
.000 0... .... = Opcode: Star
.... .0.. .... = Authoritativ
.... ..0. .... = Truncated: N
....1 .... = Recursion de
.... 1... .... = Recursion av
.... .0.. .... = Z: reserved
....0. .... = Answer authe
....0 .... = Non-authenti
.... 0000 = Reply code:
Questions: 1
Answer RRs: 10
Authority RRs: 0
Additional RRs: 0
Queries
api.ipify.org: type A, class IN
Name: api.ipify.org
[Name Length: 13]
[Label Count: 3]
Type: A (1) (Host Address)
Class: IN (0x0001)

Frame 24149



No.	Time	ip.src	ip.dst	src port	dst port	Length	info
25424	1040.310581	108.177.15.28	10.9.23.102	25	63602	111	S: 220 smtp-relay.gmail.com ESMTP p14sm62724ej
25427	1040.328900	108.177.15.28	10.9.23.102	587	63603	111	S: 220 smtp-relay.gmail.com ESMTP v11sm162909w
27766	1124.990346	108.177.15.28	10.9.23.102	587	63655	110	S: 220 smtp-relay.gmail.com ESMTP 7sm237060wrz
27791	1125.174995	108.177.15.28	10.9.23.102	25	63652	112	S: 220 smtp-relay.gmail.com ESMTP y28sm114321l
28158	1137.081223	108.177.15.28	10.9.23.102	25	63665	110	S: 220 smtp-relay.gmail.com ESMTP la2sm66415ej
28189	1137.432545	108.177.15.28	10.9.23.102	25	63666	110	S: 220 smtp-relay.gmail.com ESMTP b8sm62981lfc
28343	1139.976566	185.4.29.135	10.9.23.102	25	63678	75	S: 220 mail.mailfa.com
28367	1140.408995	10.9.23.102	185.4.29.135	63678	25	70	C: EHLO localhost
28395	1141.278848	185.4.29.135	10.9.23.102	25	63678	110	S: 250-mail.mailfa.com | SIZE 30000000 | AUTH
28401	1141.458745	46.16.61.250	10.9.23.102	25	63681	96	S: 220 vxsys-smtpclusterma-03.srv.cat ESMTP
28410	1141.849946	10.9.23.102	46.16.61.250	63681	25	70	C: EHLO localhost
28415	1142.013281	46.16.61.250	10.9.23.102	25	63681	253	S: 250-vxsys-smtpclusterma-03.srv.cat | PIPELI
28420	1142.054497	10.9.23.102	185.4.29.135	63678	25	66	C: AUTH LOGIN
28448	1142.275010	10.9.23.102	46.16.61.250	63681	25	64	C: STARTTLS
28450	1142.275468	185.4.29.135	10.9.23.102	25	63678	72	S: 334 VXNlcm5hbWU6
28457	1142.434629	46.16.61.250	10.9.23.102	25	63681	84	S: 220 2.0.0 Ready to start TLS
28467	1142.706961	10.9.23.102	185.4.29.135	63678	25	80	C: User: ZmFyc2hpbkBtYWlsZmEuY29t
28477	1142.941465	185.4.29.135	10.9.23.102	25	63678	72	S: 334 UGFzc3dvcmQ6
28480	1142.956561	185.4.29.135	10.9.23.102	25	63686	75	S: 220 mail.mailfa.com
28504	1143.222316	10.9.23.102	185.4.29.135	63678	25	68	C: Pass: ZGluYW1pdA==
28506	1143.222457	10.9.23.102	185.4.29.135	63686	25	70	C: EHLO localhost
28521	1143.450341	185.4.29.135	10.9.23.102	25	63686	110	S: 250-mail.mailfa.com | SIZE 30000000 | AUTH
28524	1143.456304	185.4.29.135	10.9.23.102	25	63678	74	S: 235 authenticated.
28576	1144.036130	10.9.23.102	185.4.29.135	63678	25	86	C: MAIL FROM:<farshin@mailfa.com>

First mail received farshin@mailfa.com

TCP stream of first mail

Section 3 – Results The compromised endpoint is workstation 10.9.23.102 (MAC 00:08:02:1c:47:ae). Initial compromise occurred at 2021-09-24 16:44:38 UTC via a drive-by download of documents.zip from attirenepal.com (LiteSpeed server). The archive contained chart-1530076591.xls, which, upon execution, likely triggered malicious VBA macros or shellcode.

Secondary payloads were delivered over HTTPS (16:45:11 – 16:45:30 UTC) from finejewels.com.au (GoDaddy-issued certificate), thietbiagt.com, and new.americold.com.

Persistent C2 was established using Cobalt Strike beacons to 185.106.96.158 (port 80, Host: ocsp.verisign.com, domain: survmeter.live) and 185.125.204.174 (port 443, SNI: securitybusinpuff.com). Post-infection command-and-control occurred over maldivehost.net (Apache/2.4.49 response), with beacon data beginning zLIisQRWZI9 (first packet to C2: 281 bytes).

The malware performed external IP reconnaissance via DNS query to api.ipify.org at 2021-09-24 17:00:04 UTC. Exfiltration was attempted via SMTP using farshin@mailfa.com (first MAIL FROM); credentials for ho3ein.sharifi@mailfa.com were exposed as 13691369.

Type of Infection — Cobalt Strike beaconing (commercial adversary emulation tool abused for persistence, C2 over HTTP/HTTPS with domain fronting, obfuscated URIs, and credential exfiltration).

Section 4 – Conclusion & Recommendations This incident demonstrates a classic multi-stage attack: phishing-driven file download → user execution of macro-enabled document → staged payloads → deployment of Cobalt Strike → persistent C2 and attempted SMTP exfiltration. The use of domain fronting (ocsp.verisign.com) and legitimate-looking infrastructure delayed detection.

Prevention & Mitigation

- Endpoint Hardening — Disable Office macros by default; enforce Protected View and block external content (Group Policy). Deploy EDR with macro/script scanning and Cobalt Strike behavioral detection.
- Network Controls — Implement web filtering/proxy to block known C2 domains/IPs (attirenepal.com, maldivehost.net, survmeter.live, securitybusinpuff.com). Monitor DNS for anomalous queries (api.ipify.org, dynamic update patterns).

- **Email & Attachment Security** — Enhance phishing filters; quarantine ZIP/XLS with macros; enforce strict SMTP relay policies and monitor AUTH attempts.
- **User Awareness** — Conduct regular phishing simulations and training on suspicious attachments and macro prompts.
- **Monitoring & Response** — Enable network packet capture with automated IOC matching; use JA3 fingerprinting for Cobalt Strike detection; maintain updated blocklists.

Remaining challenges include encrypted beacon traffic and legitimate domain abuse — requiring advanced behavioral analytics and continuous threat hunting.

References

- Wireshark Documentation (filters, Follow Stream, Export Objects)
- MITRE ATT&CK: T1204.002, T1071.001, T1566.001
- VirusTotal IOC reports

My Github link: https://github.com/Patrick-cybersec/COMP3010HK-Security-Operations-Incident-Management/issues