

STUDENT ID: BSCS2406001

# University of Plymouth

COMP3010

Security Operations & Incident Management

## **Coursework 1: Set Exercises - PCAP Analysis**

Date of Submission: 15 November 2025

Word Count: **1074**

## 1. Introduction

This report investigates a network intrusion incident captured in a packet capture (**COMP3010CW1.pcap**) file. The goal of the analysis is to identify the infected system within the network, analyze how the infection happened, and determine the type of malware or attack used. **Wireshark** was used for packet inspection, while **VirusTotal** was used to verify external threats.

The report includes four sections: Section 1 explains the investigation goals; Section 2 describes the methodology and tools used; Section 3 gives the analysis results together with evidence to support them; and Section 4 concludes with security suggestions to prevent future incidents. This systematic technique matches the standard operational guidelines of a Security Operations Center (SOC) investigation.

## 2. Methodology

This section outlines the tools, analytical process, and evidence utilized to identify the infected system (IP, MAC, hostname, user account) and establish how it was compromised.

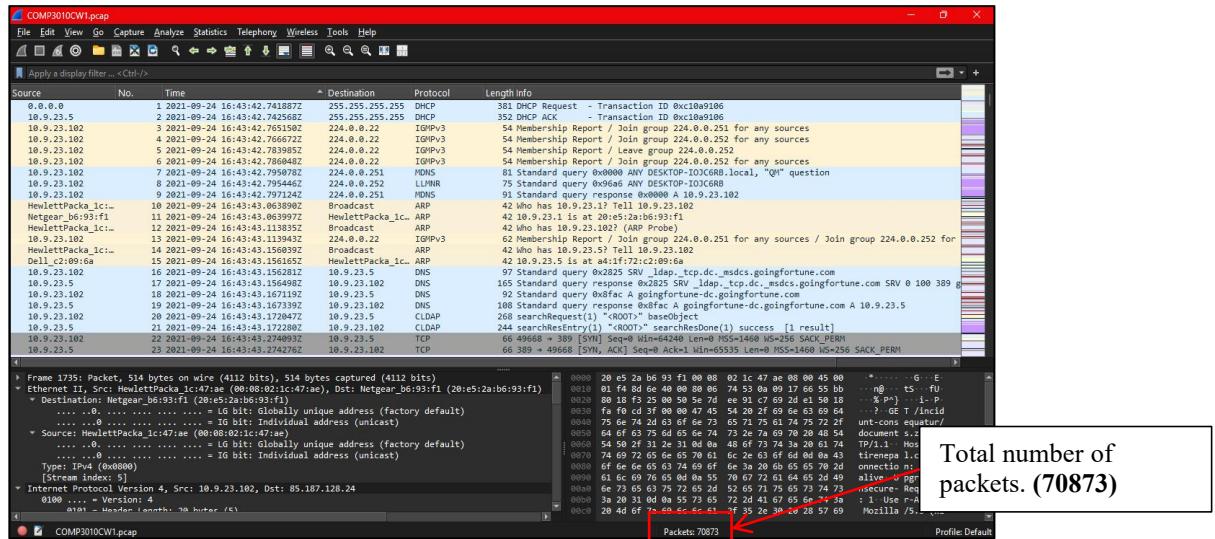
### ➤ 2.1 Tools Used

The investigation used two major tools:

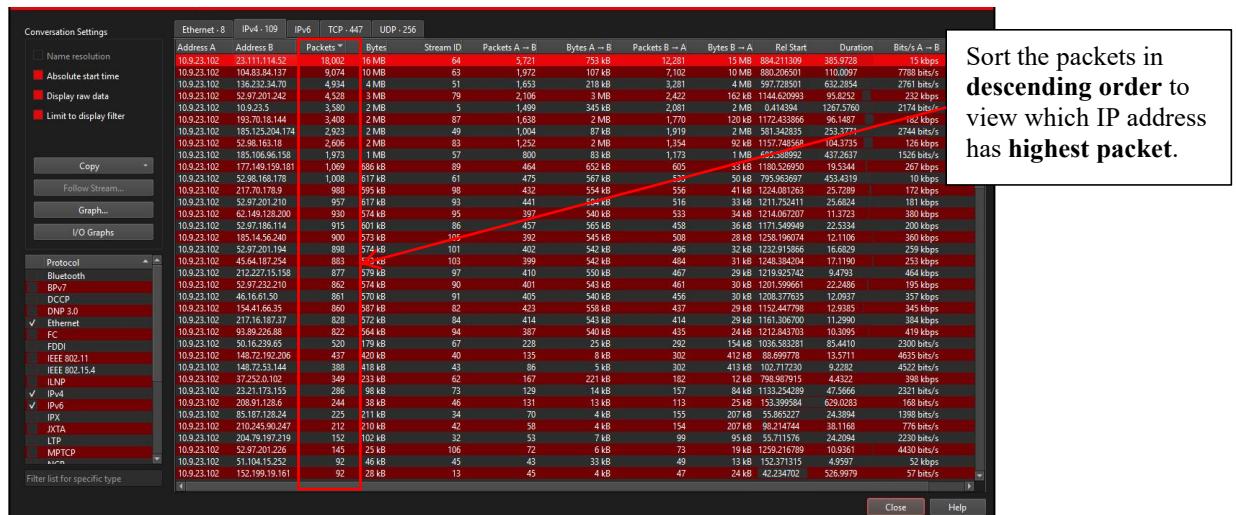
- i. **Wireshark:** Used to investigate packet-level network activity, apply protocol filters, track the infection time frame, and capture indicators of compromise (IoCs) like as IP addresses, domain names, and payload file names.
- ii. **VirusTotal (<https://www.virustotal.com/>):** Used to determine whether the external IP addresses and domains that were captured by Wireshark had previously been flagged as malicious or were associated with Cobalt Strike command-and-control (C2) servers.

## ➤ 2.2 Preparing and Investigating the Capture

1. The provided **COM3010CW1.pcap** file was opened in Wireshark.



2. The initial investigation utilized **Statistics > Conversations > IPv4** to find active endpoints and check the total volume of traffic. This showed that, host **10.9.23.102** engaged in major communication with external servers, indicating an attack.



## ➤ 2.3 Identifying the Infected Host

- The HTTP display filter is used to separate suspicious downloads.

**Type `http` in the filter tab.**

Packets: 7073 - Displayed: 211 (0.3%) Profile: Default

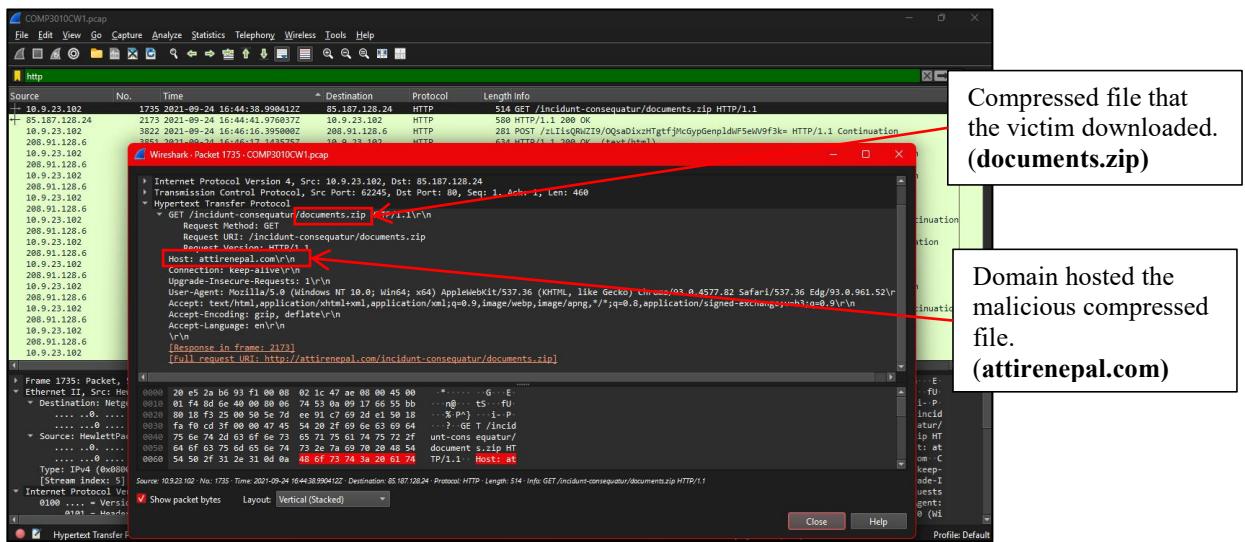
**Double-click on the first packet ,expand the Internet Protocol header to view the IP address of the infected system.**

IP address of the infected system. (10.9.23.102)

**Expand the Ethernet header to view the MAC address of the infected system.**

MAC address of the infected system. (00:08:02:1c:47:ae)

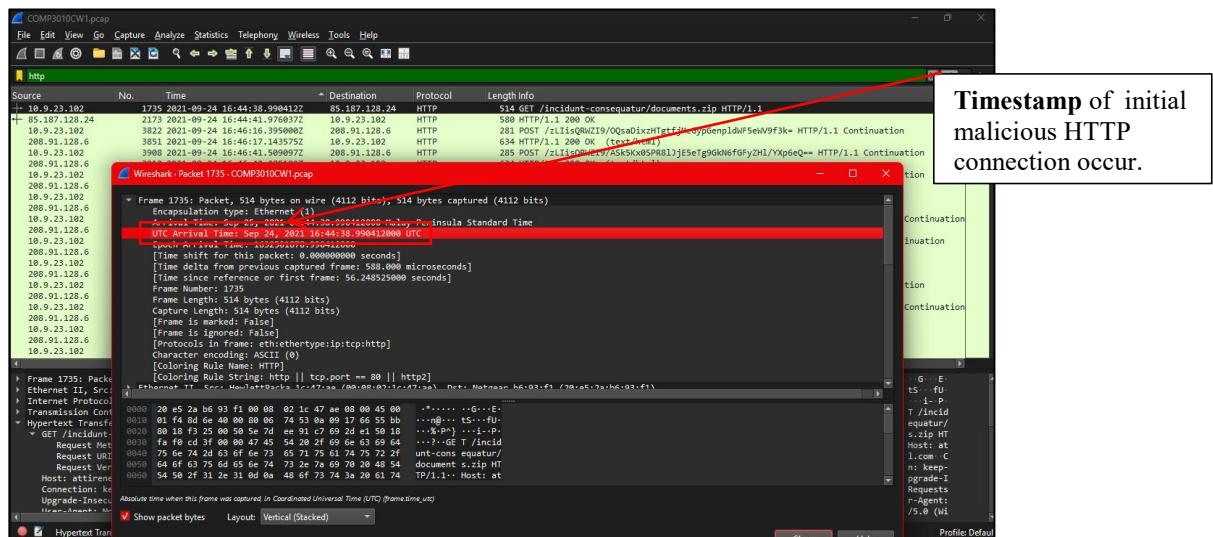
- This showed an outbound HTTP GET request for a compressed file called **documents.zip** hosted at **attirenepal.com**.



## ➤ 2.4 Identifying Infection Indicators

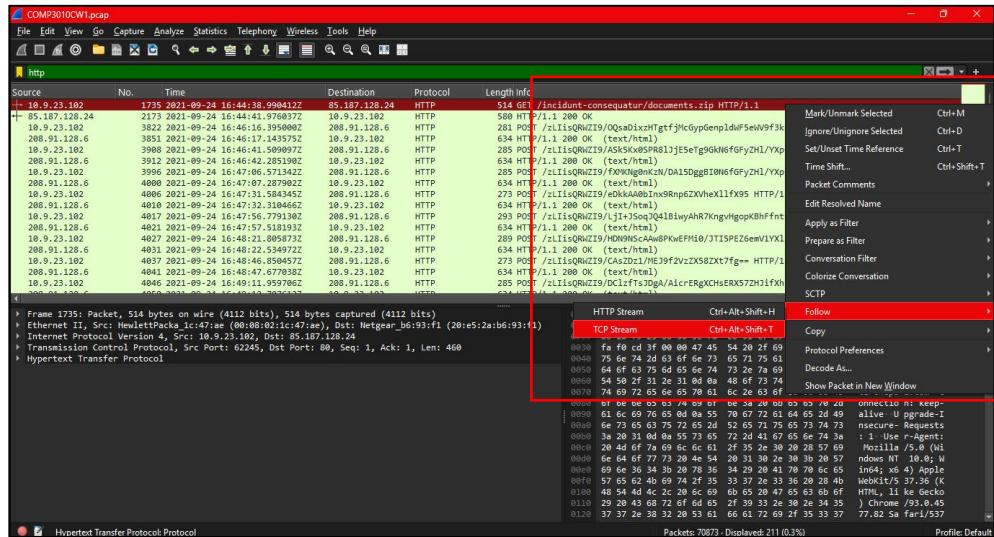
### Indicator 1 - Timestamp of initial malicious activity

- The earliest malicious connection was identified on **2021-09-24 16:44:38 UTC**.



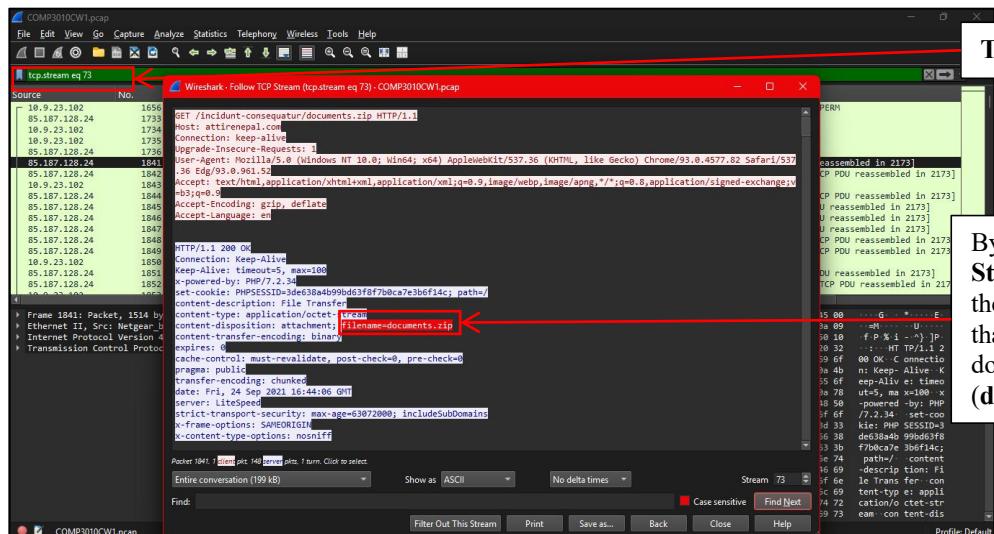
## Indicator 2 - Malicious file downloaded

- The requested resource path from the HTTP GET packet that was chosen above has **documents.zip**. To verify, use **Follow > TCP Stream**.



- Select the initial packet (**Frame 1753**) with a right-click.

- Hover the cursor over **Follow > TCP Stream**.

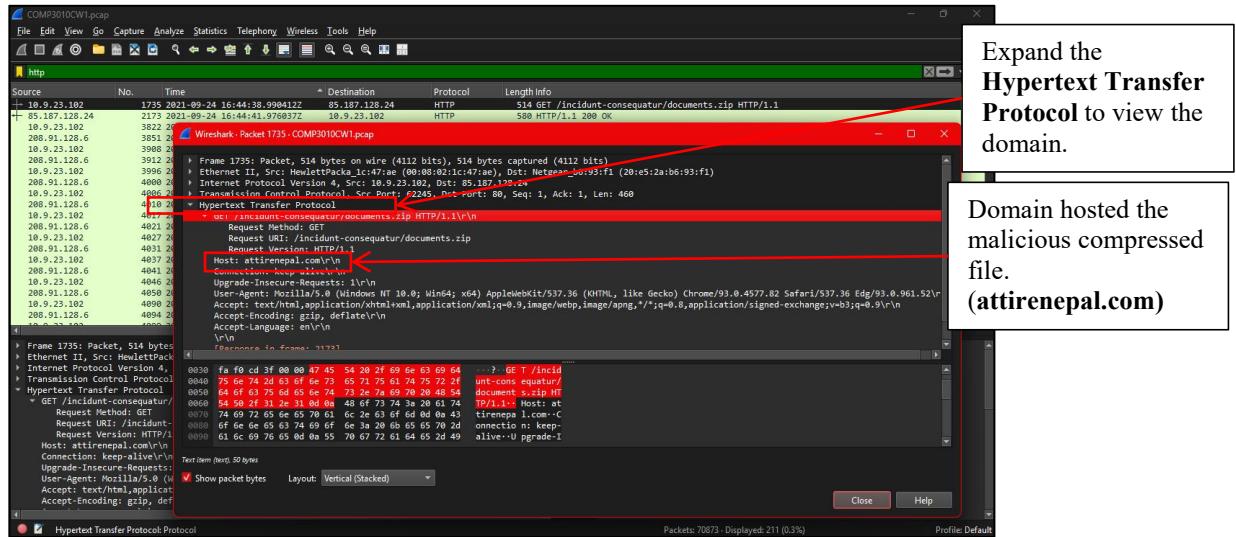


TCP Stream 73,

By following **TCP Stream 73**, can view the compressed file that the victim downloaded. (**documents.zip**)

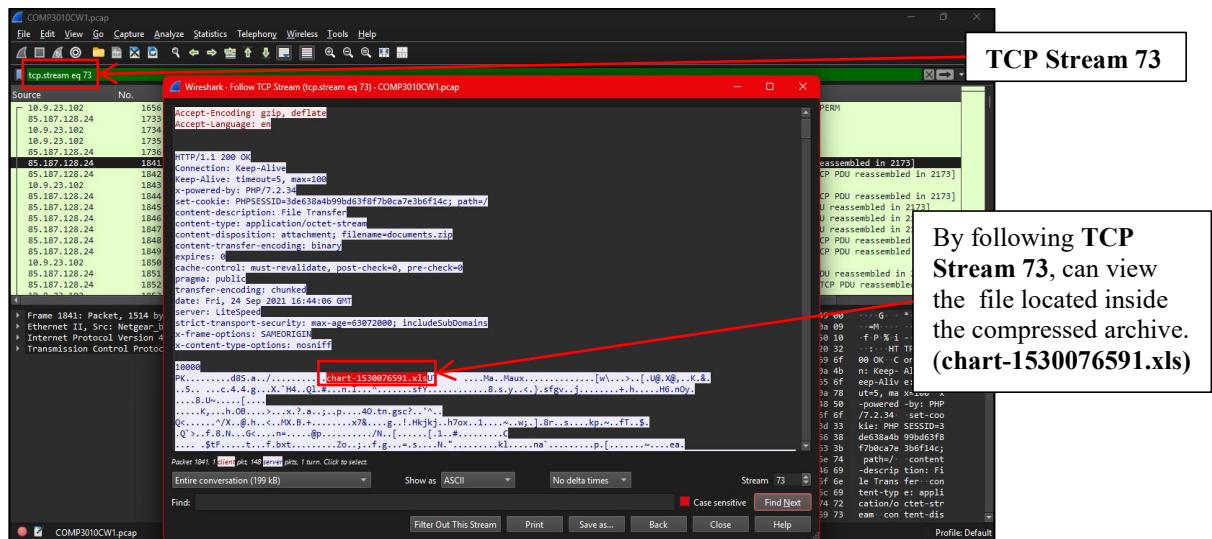
## Indicator 3 - Malicious domain delivering the payload

The domain **attirenepal.com** was found in the **HTTP Host: header** of the GET request. By expanding the **Hypertext Transfer Protocol header**, both the Host and Server fields were collected, proving the domain's role in delivering the malicious data.



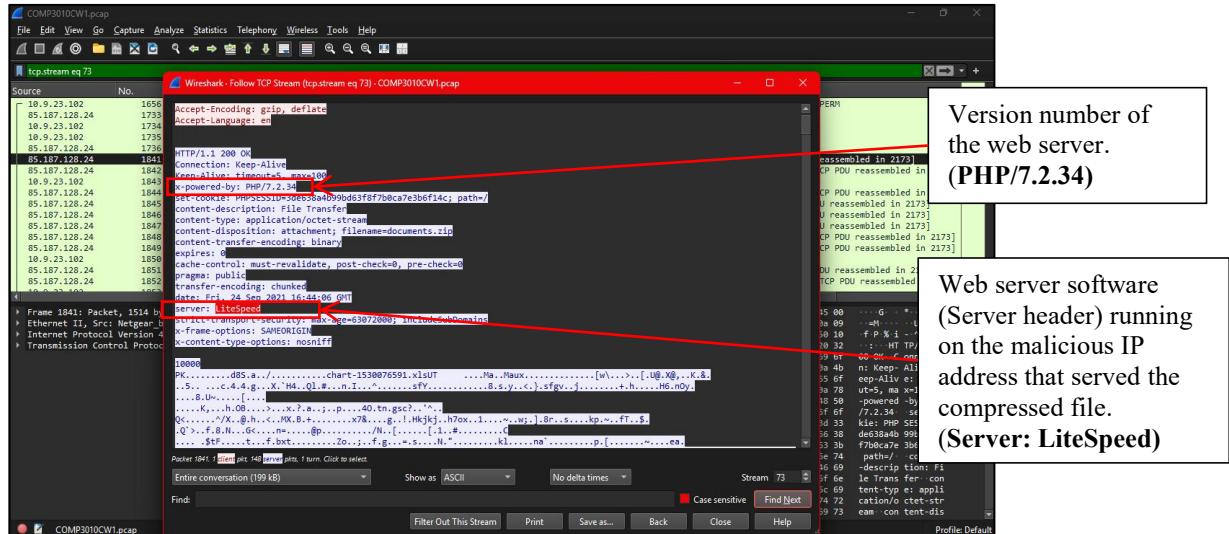
## Indicator 4 - Malicious file inside archive

By inspecting at the **Follow TCP Stream 73**, the file, **chart-1530076591.xls**, was found. The existence of this malicious Excel file was verified by looking at the response data and examining the transferred file's data within the archive content shown in the stream.



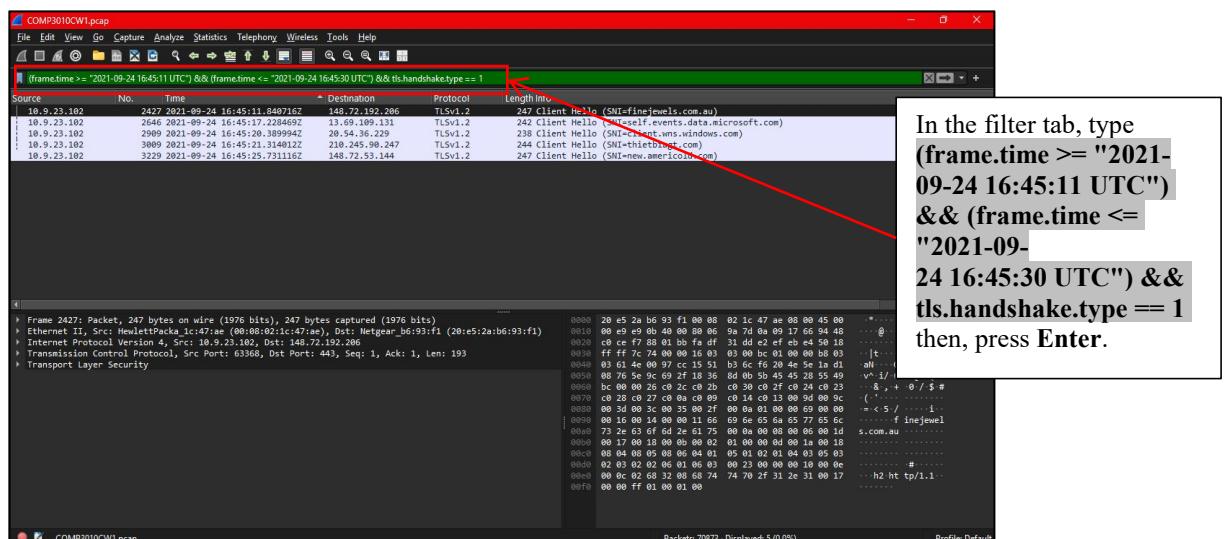
## Indicator 5 - Suspicious server headers

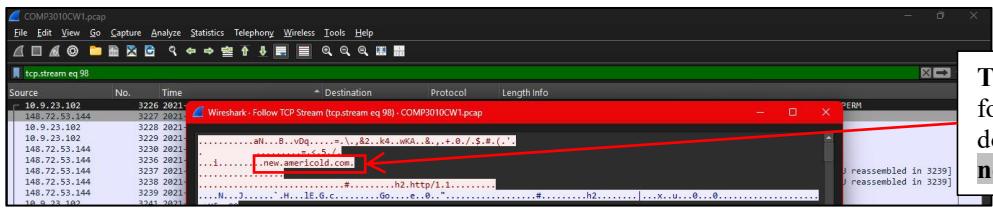
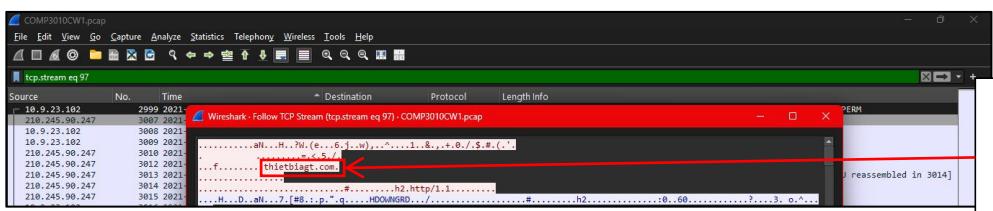
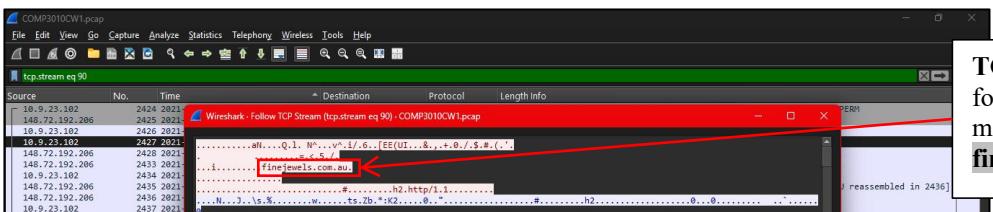
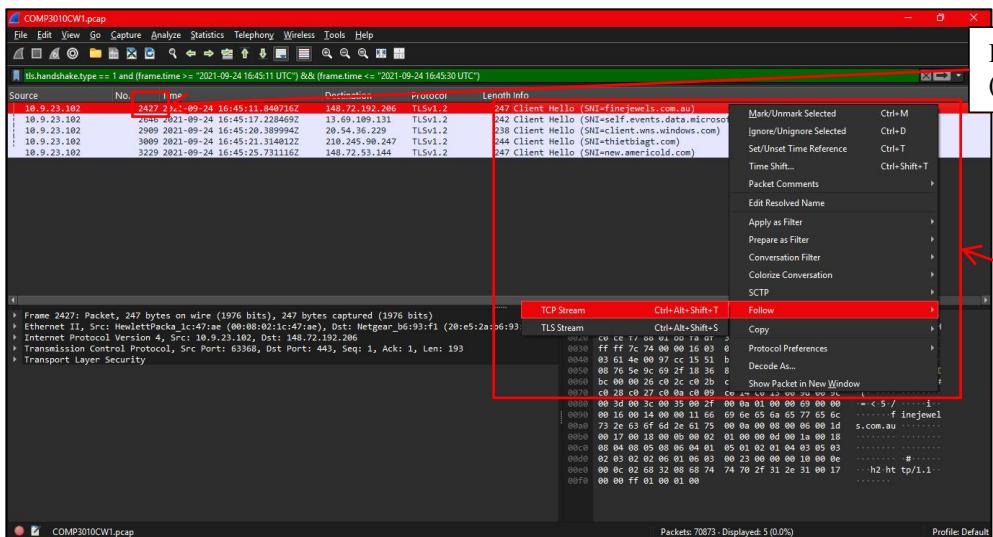
The HTTP response for the download request showed the server information **Server: LiteSpeed** and **PHP/7.2.34**. These details, found by following the **TCP Stream 73**.



## Indicator 6 - Additional suspicious domains accessed immediately after infection

Multiple domains were detected during the investigation of **HTTPS traffic** between **16:45:11** and **16:45:30** UTC, which include **finejewels.com.au**, **thietbiagt.com**, and **new.americold.com**.





## Indicator 7 - Immediate connection to Cobalt Strike C2 IPs

In **Wireshark**, packets were examined. Conversations were sorted by packet count/bytes in descending order by using **Statistics > Conversations > TCP** to find endpoints with high or unusual activity. **VirusTotal** was then used to cross-check potential IP address to find out whether community contributors had previously identified such hosts as connected to **Cobalt Strike**.

Two IP addresses of the Cobalt Strike servers:

- **185.106.96.158**
- **185.125.204.174**

VirusTotal confirmed both addresses as **Cobalt Strike C2 servers**.

Address A	Port A Address	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
10.9.23.102	63557.23.111.114.52	65400	18,002	16 MB	267	5,721	753 kB	12,281	15 MB	884.211309	385.9728
10.9.23.102	63555.104.83.84.137	443	9,074	10 MB	265	1,972	107 kB	7,102	10 MB	880.206501	110.0097
10.9.23.102	63465.185.123.204.174	8080	1,375	1 MB	181	408	23 kB	967	1 MB	743.649672	>193
10.9.23.102	63107.185.106.96.158	80	1,074	997 kB	219	379	21 kB	695	976 kB	799.183504	6,6975
10.9.23.102	63459.136.232.34.70	443	1,069	689 kB	412	386	655 kB	605	533 kB	647.865351	193.1441
10.9.23.102	63459.136.232.34.70	443	1,067	689 kB	116	284	16 kB	718	915 kB	647.865351	32.1007
10.9.23.102	63726.52.97.201.242	25	978	827 kB	415	446	593 kB	532	34 kB	1186.875978	35.3396
10.9.23.102	63610.136.232.34.70	443	976	882 kB	320	334	19 kB	642	863 kB	1057.183502	62.8288
10.9.23.102	63732.52.97.201.210	25	957	617 kB	421	441	584 kB	516	33 kB	1211.752411	25.8282
10.9.23.102	63571.136.232.34.70	443	953	911 kB	281	291	57 kB	662	894 kB	932.806205	64.1730
10.9.23.102	63737.21.22.715.158	25	946	884 kB	425	316	56 kB	529	28 kB	1234.081263	25.8091
10.9.23.102	63738.21.70.178.9	25	933	559 kB	427	467	51 kB	538	34 kB	1234.081263	15.8991
10.9.23.102	63734.62.149.128.200	25	930	574 kB	423	397	540 kB	533	34 kB	1214.067207	11.1373
10.9.23.102	63747.52.98.163.18	25	922	579 kB	436	410	544 kB	512	35 kB	1241.902723	20.2193
10.9.23.102	63752.185.14.56.240	25	900	573 kB	441	392	545 kB	508	28 kB	1256.196074	12.1106
10.9.23.102	63744.52.97.201.194	25	898	574 kB	433	402	542 kB	496	32 kB	1232.915866	16.8629
10.9.23.102	63749.45.64.187.124	25	888	574 kB	396	419	546 kB	471	33 kB	1234.081251	12.8778
10.9.23.102	63740.52.98.168.178	25	882	586 kB	429	412	555 kB	470	31 kB	1246.380034	11.1350
10.9.23.102	63725.52.97.201.242	25	878	572 kB	414	411	541 kB	467	31 kB	1236.380031	23.0155
10.9.23.102	63749.45.64.187.124	25	888	574 kB	398	419	542 kB	484	31 kB	1236.380031	33.5240
10.9.23.102	63740.52.98.168.178	25	882	586 kB	429	412	555 kB	470	31 kB	1236.380031	33.5240
10.9.23.102	63725.52.97.201.242	25	878	572 kB	414	411	541 kB	467	31 kB	1236.380031	33.5240
10.9.23.102	63737.21.22.715.158	25	877	579 kB	426	410	550 kB	467	29 kB	1219.925742	9.4793
10.9.23.102	63745.193.70.18.144	25	866	582 kB	434	416	552 kB	450	30 kB	1246.696258	11.0655
10.9.23.102	63729.52.97.201.210	25	861	574 kB	418	400	543 kB	461	30 kB	1201.599661	25.8686
10.9.23.102	63730.52.97.201.210	25	861	574 kB	419	405	545 kB	462	30 kB	1202.599665	12.0937
10.9.23.102	63707.154.41.86.35	25	860	587 kB	397	433	558 kB	377	29 kB	1152.447798	12.5985
10.9.23.102	63741.193.70.18.144	25	860	581 kB	430	403	550 kB	457	31 kB	1229.636491	11.2409
10.9.23.102	63713.52.97.186.114	25	858	591 kB	402	429	563 kB	429	29 kB	1171.549949	15.6778
10.9.23.102	63709.52.98.163.18	25	856	589 kB	398	428	561 kB	428	29 kB	1157.748568	21.2393
10.9.23.102	63750.193.70.18.144	25	854	573 kB	439	407	545 kB	447	30 kB	1257.142067	11.4405
10.9.23.102	63731.52.97.186.114	25	854	573 kB	395	410	546 kB	442	30 kB	1257.142067	11.4405
10.9.23.102	63711.52.98.163.18	25	828	568 kB	400	414	540 kB	414	28 kB	1162.476383	34.2961
10.9.23.102	63711.102.70.19.144	96	870	575 kB	404	415	545 kB	415	28 kB	1173.475962	12.0700

Analyze first IP addresses of the Cobalt Strike servers (**185.106.96.158**) using **VirusTotal**.

18.106.96.158

Wow, I thought that was a CA.

parthmaniar 3 years ago

This IP carried out Apache Log4j RCE attempt(s) (also known as CVE-2021-44228 or Log4Shell). For more information, or to report interesting/incorrect findings, give me a shoutout on @parthmaniar on Twitter.

drb\_ra 4 years ago

Cobalt Strike Server Found C2: https://@185.[106].[96].[158]8888 C2 Server: survmeter[.]live[.]gscp[.]R/[185.[106].[96].[158].gscp[.]R/ POST URL: /supprq/sa/ Country: United States ASN: DeidPath Host Header: oscp[.]verisign[.]com #c2 #cobaltstrike

Analyze IP address: 185.106.96.158 using VirusTotal, to confirm that it is the IP address of Cobalt Strike Server.

- Community contributors had previously identified such hosts as connected to Cobalt Strike.

Analyze second IP addresses of the Cobalt Strike servers (**185.125.204.174**) using VirusTotal.

Analyze IP address:  
**185.125.204.174** using  
VirusTotal, to confirm that  
it is the IP address of Cobalt  
Strike Server.

-Community contributors  
had previously identified  
such hosts as connected to  
**Cobalt Strike**.

### 3. Results

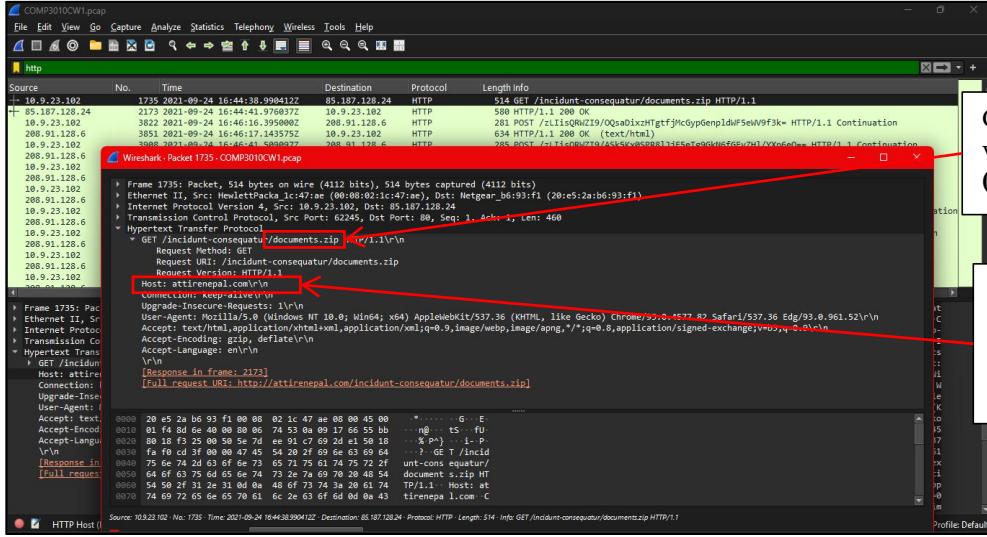
#### 3.1 Initial Infection and Malicious File Delivery

The first malicious action occurs at **2021-09-24 16:44:38 UTC**, when the victim system sends an HTTP GET request to retrieve a compressed file. This timestamp shows the starting point of the intrusion.

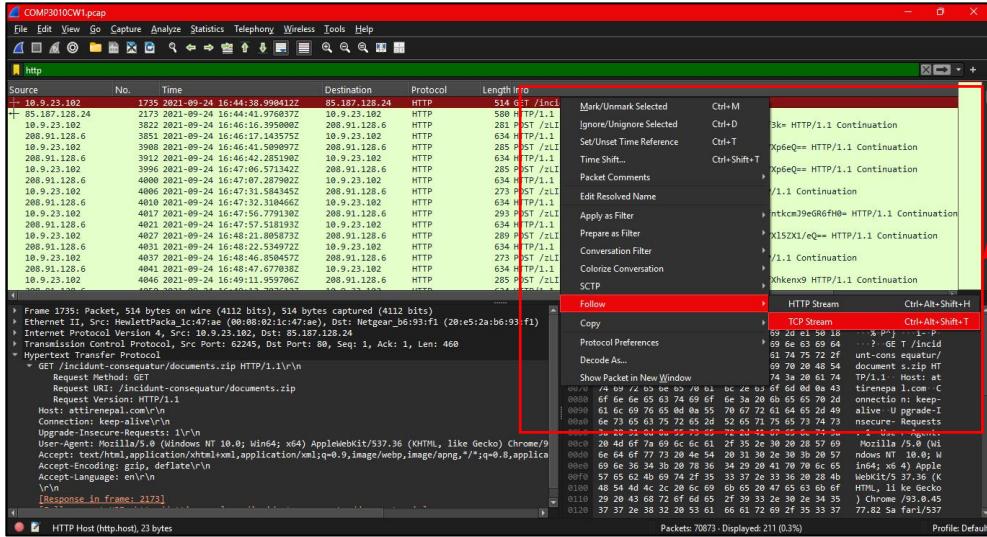
2. Type **http** in the  
filter tab.

1. Timestamp of  
initial malicious HTTP  
connection occur.

The file that was downloaded from the domain **attirenepal.com** is named **documents.zip**. The filename and hosting domain are verified by looking at **frame no. 1735** and expanding its **Hypertext Transfer Protocol** header.



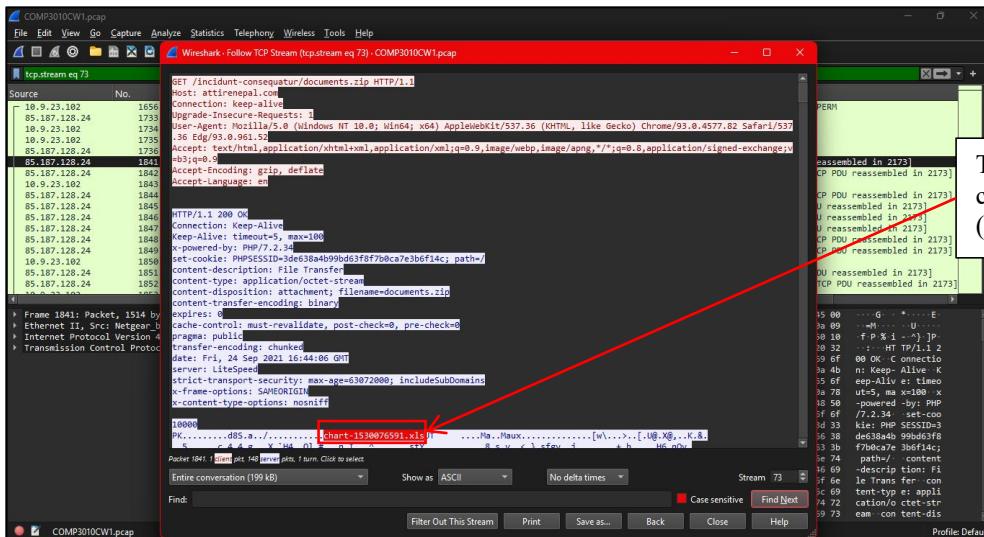
The files inside of the compressed file can be viewed by following the TCP stream (**Stream 73**) without the necessity of extracting it. The malware payload, **chart-1530076591.xls**, is provided inside the archive, showing a malicious spreadsheet that probably contains a macro or exploit execution mechanism.



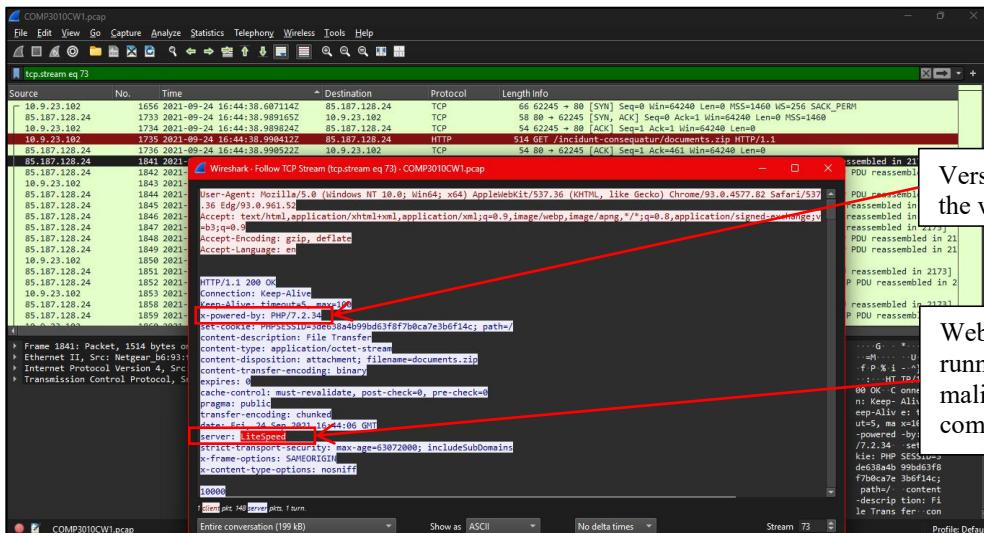
Compressed file that the victim downloaded.  
(**documents.zip**)

Domain hosted the malicious compressed file.  
(**attirenepal.com**)

- Select the initial packet (**Frame 1735**) with a right-click.
- Hover the cursor over **Follow > TCP Stream**.

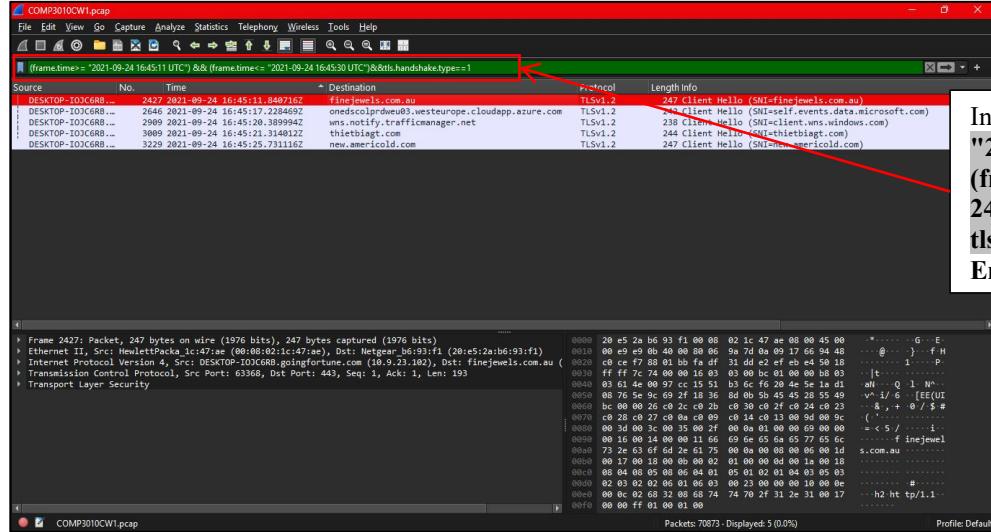


The malicious web server hosting the file identifies itself as **LiteSpeed** and runs **PHP/7.2.34**. This is found in the server response header and shows that the shared hosting environment may be misconfigured or exploited.

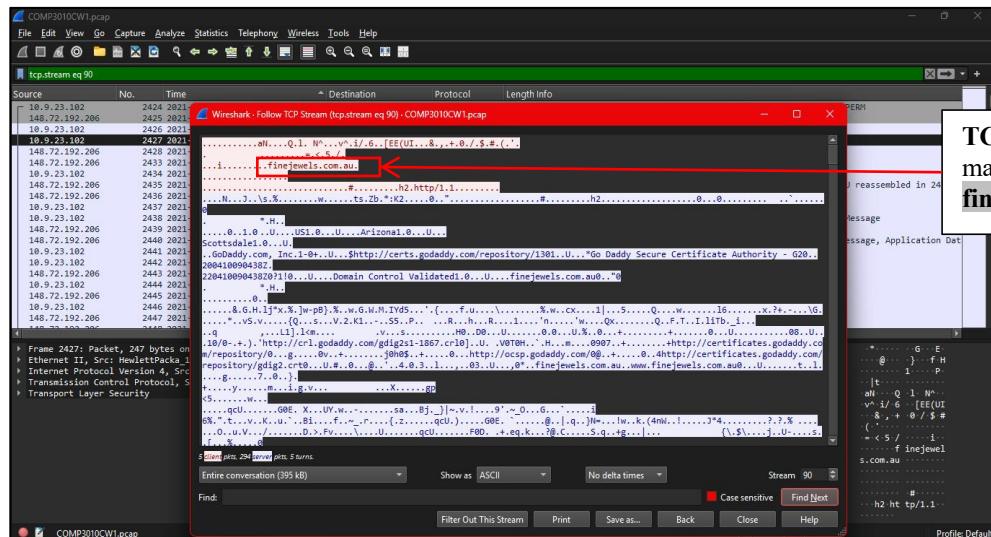


Together, these results verify that the malicious file download via insecure HTTP was the infection vector, allowing the attacker to send the victim an Excel-based payload that was hidden.

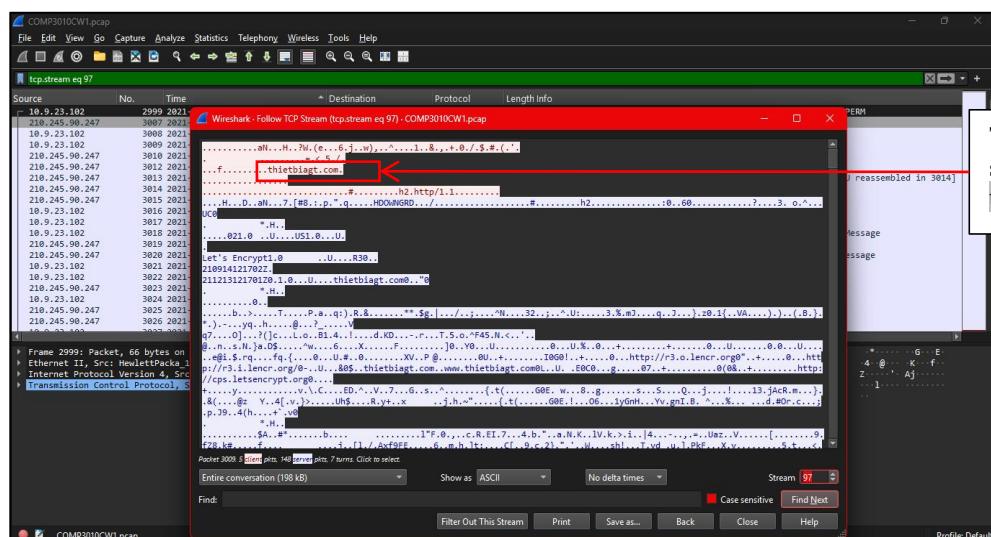
After the initial file download, the victim host quickly established encrypted connections to three additional domains which is **finejewels.com.au**, **thietbiagt.com**, and **new.americold.com** during the window **16:45:11 to 16:45:30 UTC**.



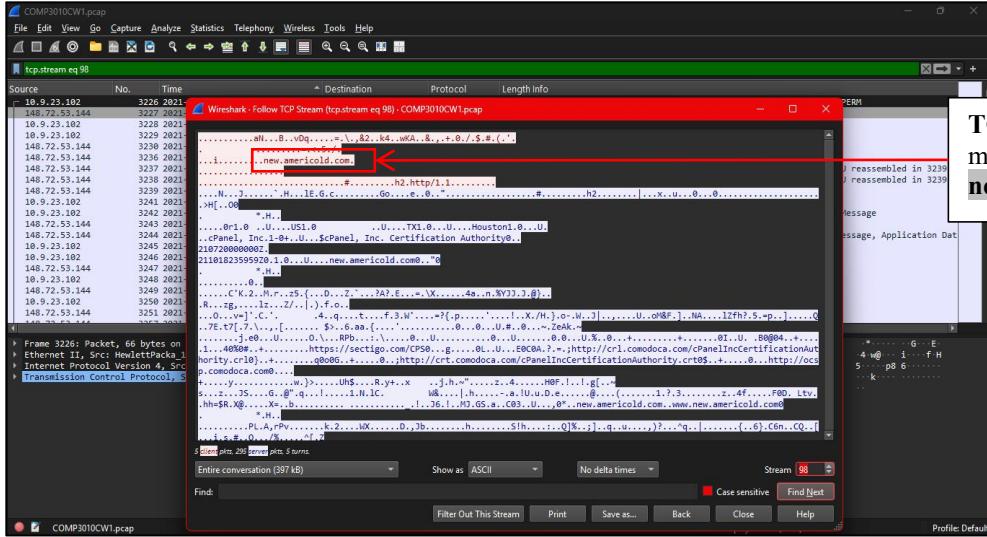
In the filter tab, type **(frame.time >= "2021-09-24 16:45:11 UTC") && (frame.time <= "2021-09-24 16:45:30 UTC") && tls.handshake.type == 1** then, press Enter.



**TCP Stream 90**, found first malicious domain:  
**finejewels.com.au**



**TCP Stream 97**, found second malicious domain:  
**thietbiagt.com**

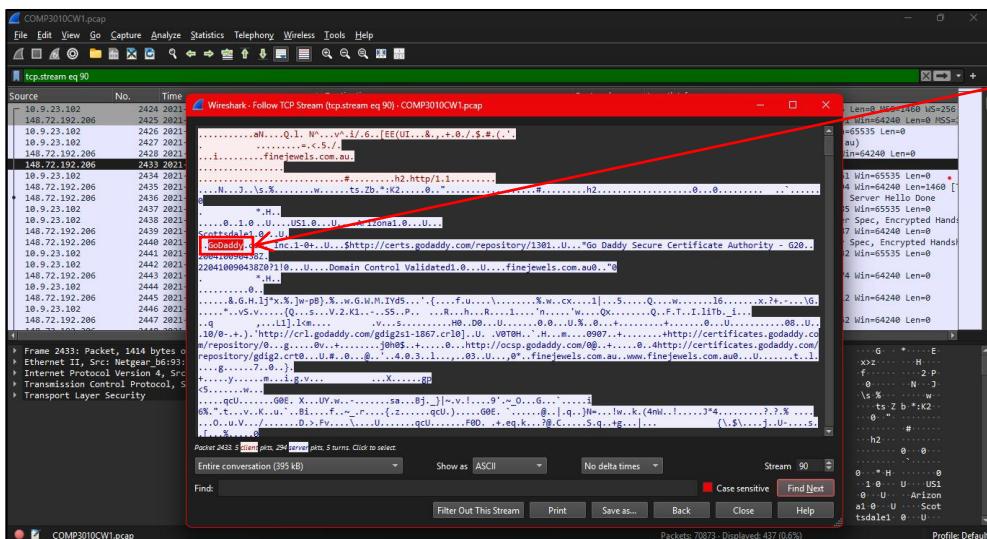


TCP Stream 98, found third malicious domain:  
new.americold.com

This multi-domain activity shows that additional modules or configuration files were retrieved after the initial compromise, indicating that the infection involved staged payload delivery.

## ➤ 3.2 Command and Control (C2) Activity

**GoDaddy** issued the certificate that was used during the TLS exchange with the first domain which is **finejewels.com.au**, showing that the domain used a valid **Certificate Authority (CA)** and was probably able to bypass detection by security appliances.



The Certificate Authority (CA) issued the SSL certificate for the first Domain which is finejewels.com.au

To identify potential command-and-control (C2) servers, firstly investigated ongoing TCP traffic from the infected computer. To find the most active external endpoints, use Wireshark's **Statistics > Conversations > TCP** to sort the list by bytes in **descending order**. Each potential IP address was then carefully reviewed and validated using **VirusTotal**.

In the capture, two IP addresses, **185.106.96.158** (port 80) and **185.125.204.174** (port 8080), showed persistent TCP sessions and were specifically flagged as **Cobalt Strike servers** in VirusTotal's Community section.

Sort the packets in descending order to view which IP address has highest packet.

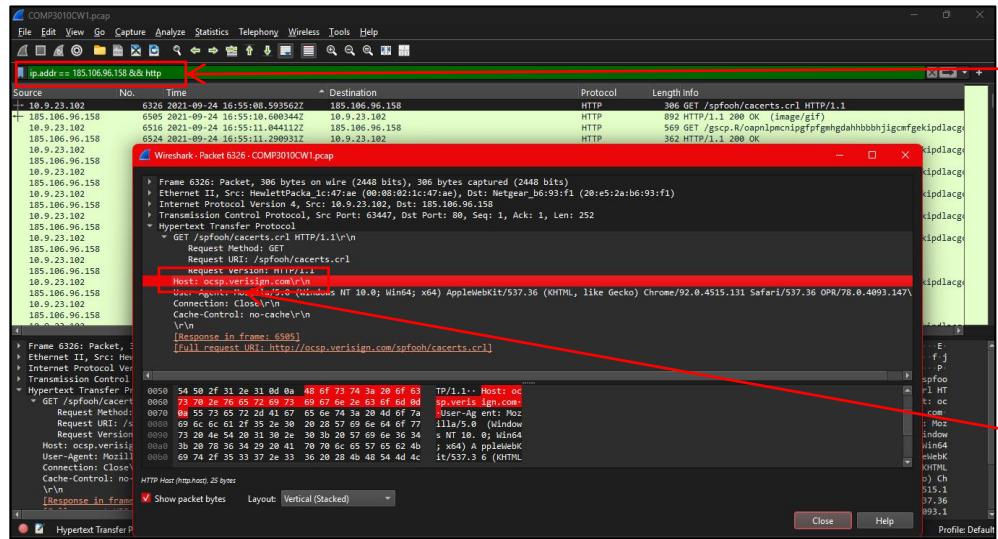
Analyze first IP addresses of the Cobalt Strike servers (**185.106.96.158**) using VirusTotal.

Analyze IP address: **185.106.96.158** using VirusTotal, to confirm that it is the IP address is flagged as **Cobalt Strike servers** in VirusTotal's Community section.

Analyze second IP addresses of the Cobalt Strike servers (**185.125.204.174**) using VirusTotal.

Analyze IP address: **185.125.204.174** using VirusTotal, to confirm that it is the IP address is flagged as **Cobalt Strike servers** in VirusTotal's Community section.

Analysis of HTTP traffic to the first C2 server shows the Host header used for communication is **ocsp.verisign.com**, which is an intentional imitation of a legitimate OCSP domain.



Use filter :  
**ip.addr == 185.106.96.158  
&& http** to show only  
HTTP packets.

Host header for the first Cobalt Strike IP address.

Use Virustotal, to verify the Host Header for the IP address: **185.106.96.158**.

First Cobalt Strike IP address.

Host header for the first Cobalt Strike IP address.

The domain **survmeter.live**, which is associated with the first C2 IP **185.106.96.158**, was verified by VirusTotal while the second C2 domain, **securitybusinpuff.com**, associated with **185.125.204.174**, was identified on VirusTotal.

**First Cobalt Strike IP address.**

This IP carried out Apache Log4j RCE attempt(s) (also known as CVE-2021-44228 or Log4Shell). For more information, or to report interesting/incorrect findings, give me a shoutout on @parthmaniar on Twitter.

Cobalt Strike Server Found C2: HTTPS @ 185[.]106[.]96[.]158:8888 C2 Server: survmeter[.]live, https://185[.]106[.]96[.]158[.]gscpl[.]R/ POST URl: /supprq/sa/ Country: United States ASN: DediPath Host Header: oscp[.]verisign[.]com #c2 #cobaltstrike

Cobalt Strike Server Found C2: HTTPS @ 185[.]106[.]96[.]158:443 C2 Server: survmeter[.]live, https://185[.]106[.]96[.]158[.]gscpl[.]R/ POST URl: /supprq/sa/ Country: United States ASN: DediPath Host Header: oscp[.]verisign[.]com #c2 #cobaltstrike

Cobalt Strike Server Found C2: HTTP @ 185[.]106[.]96[.]158:80 C2 Server: survmeter[.]live, https://185[.]106[.]96[.]158[.]gscpl[.]R/ POST URl: /supprq/sa/ Country: N/A ASN: N/A Host Header: oscp[.]verisign[.]com

**Second Cobalt Strike IP address.**

This IP carried out Apache Log4j RCE attempt(s) (also known as CVE-2021-44228 or Log4Shell). For more information, or to report interesting/incorrect findings, give me a shoutout on @parthmaniar on Twitter.

Cobalt Strike Server Found C2: HTTPS @ 185[.]125[.]204[.]174:4444 C2 Server: securitybusinpuff[.]com, https://185[.]125[.]204[.]174[.]jquery-3[.]3[.]1[.]min[.]js POST URl: /jquery-3[.]3[.]1[.]min[.]js Country: N/A ASN: Hydra Communications Ltd #c2 #cobaltstrike

Cobalt Strike Server Found C2: HTTPS @ 185[.]125[.]204[.]174:8080 C2 Server: securitybusinpuff[.]com, https://185[.]125[.]204[.]174[.]jquery-3[.]3[.]1[.]min[.]js POST URl: /jquery-3[.]3[.]1[.]min[.]js Country: N/A ASN: N/A #c2 #cobaltstrike

The domain used for post-infection communications is **maldivethost.net**, which was found through analysis of HTTP POST requests.

**2. Use filter :**  
**http.request.method == "POST"** to shows only the HTTP packets that are being sent to a server by the client (victim).

**1. Double-click on the first packet to view the packet details.**

**Domain name used for the post-infection traffic.**

Following **TCP Stream 104** shows the initial beacon payload, in which the victim sends the first 11 bytes of exfiltrated data which is **zLIisQRWZI9**.

Selected packet (Frame no. 3822) with a right-click.

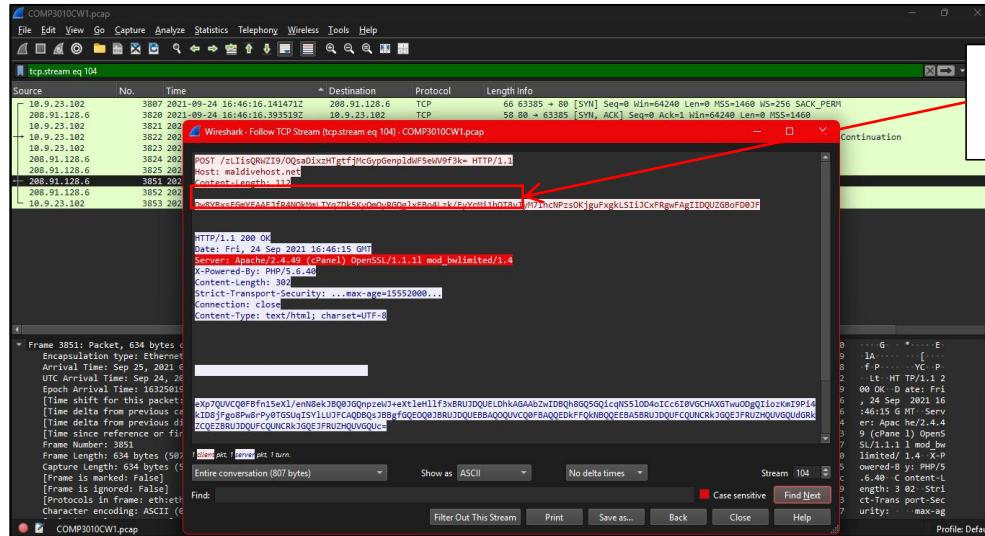
- Hover the cursor over Follow > TCP Stream.

The first eleven characters of the data the victim host sends to the malicious domain: **maldiverhost.net**

The length of first packet transmitted to the C2 is **281 bytes (2248 bits)**, which is common for beacon registration packets that carry host and callback information.

Length of the first packet the victim sent to the C2 server.

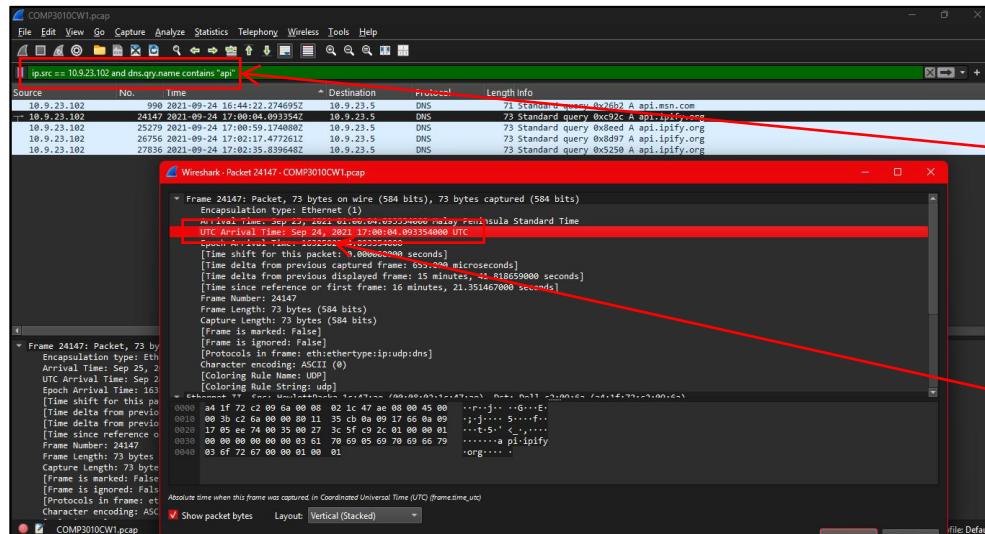
Maldiverhost.net's server header includes **Apache/2.4.49 (cPanel) OpenSSL/1.1.1l** **mod\_bwlimited/1.4**, showing an outdated and vulnerable web hosting stack often used for C2 operations.



Server header value for the malicious domain:**maldiverhost.net** found by following the **TCP stream 104**.

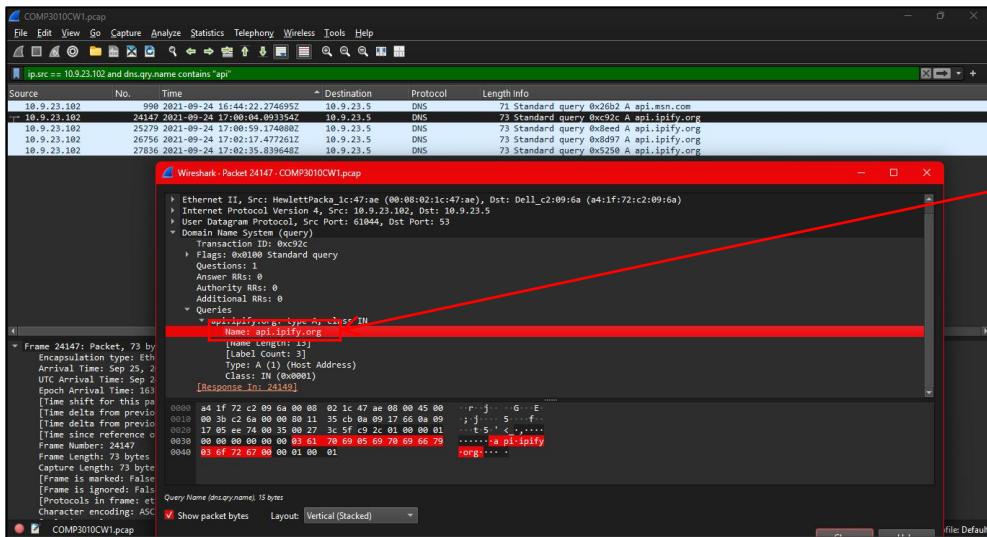
### ➤ 3.3 Final Exfiltration/Check-in

At **2021-09-24 17:00:04 UTC**, the attacker tried to find the victim's public IP address by sending a DNS query to **api.ipify.org**.

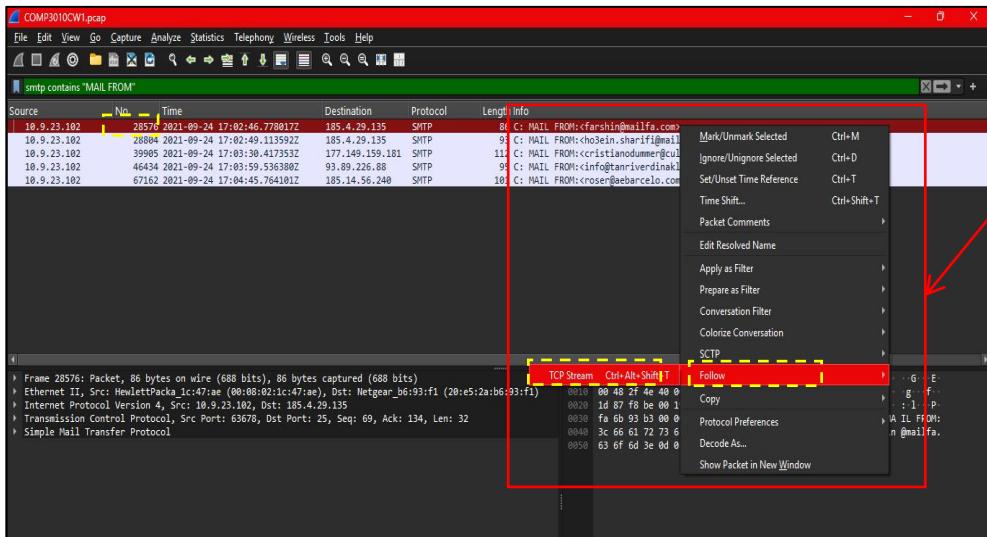
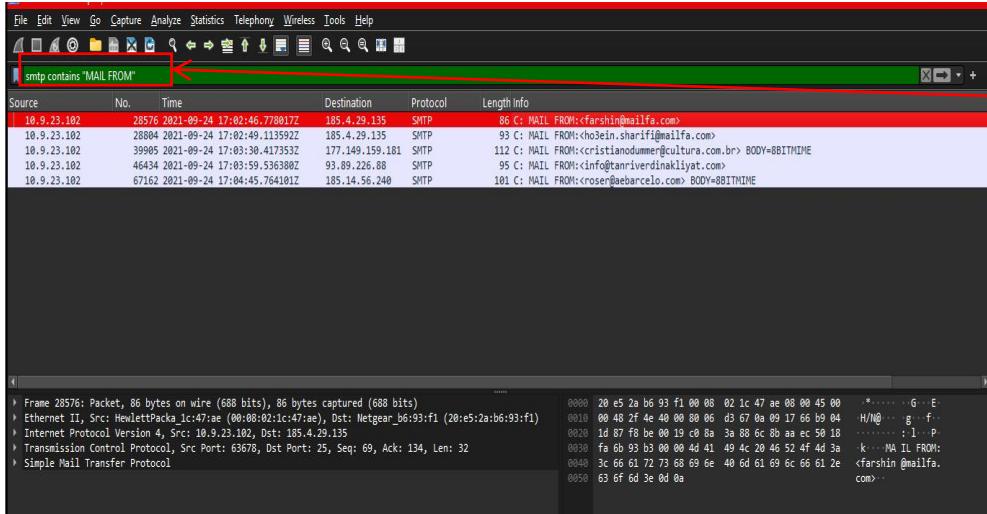


Use filter: **ip.src == 10.9.23.102 and dns.qry.name contains "api"** which will be showing only the DNS query packets that the IP address 10.9.23.102 host sent.

Date and time when the DNS query occurred for the domain used by the malware to check the victim's external IP address.



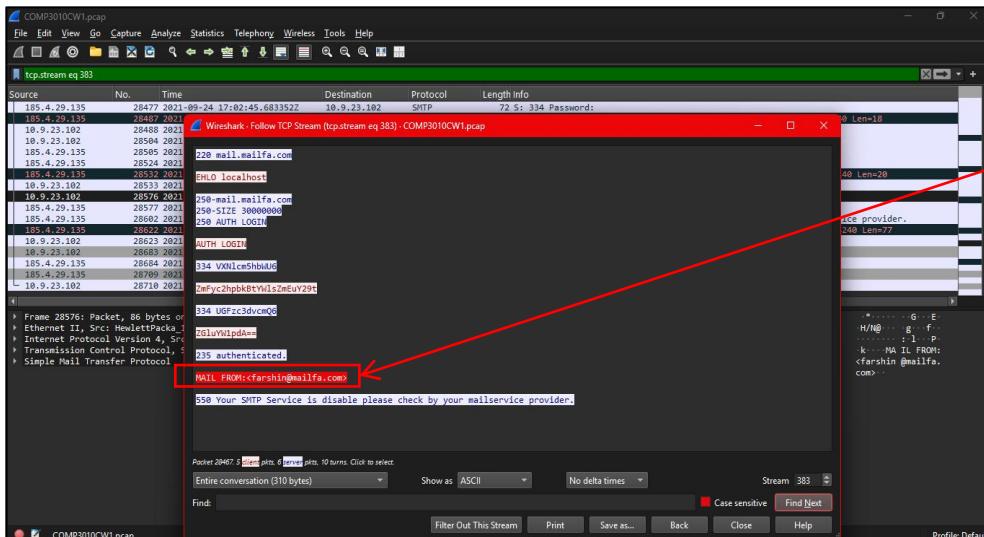
Additionally, the PCAP includes SMTP traffic that shows proof of compromised email credentials being used for command forwarding or spam. When filtering SMTP, **farshin@mailfa.com** appears as the first MAIL FROM address.



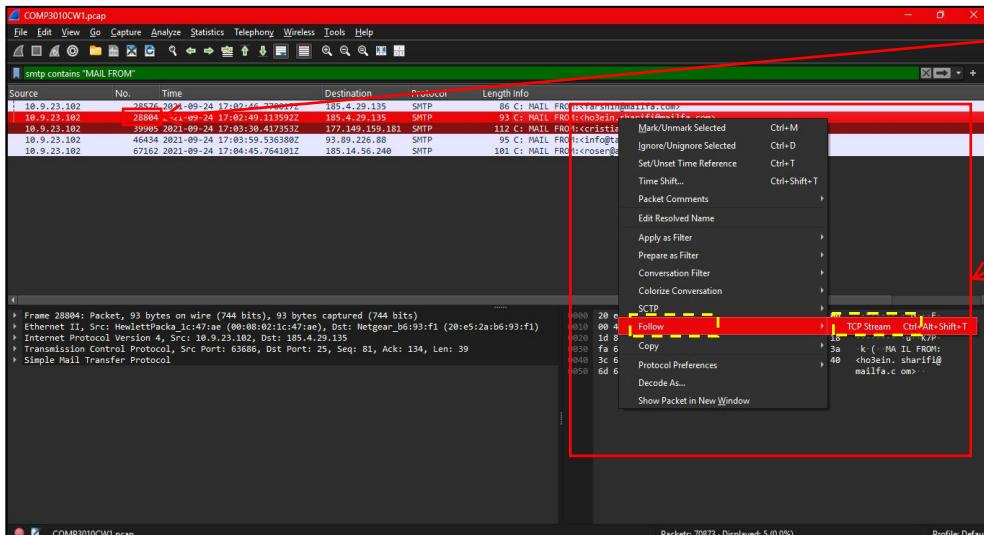
**Domain name in the DNS query** found by expanding the Domain Name System (query) header.

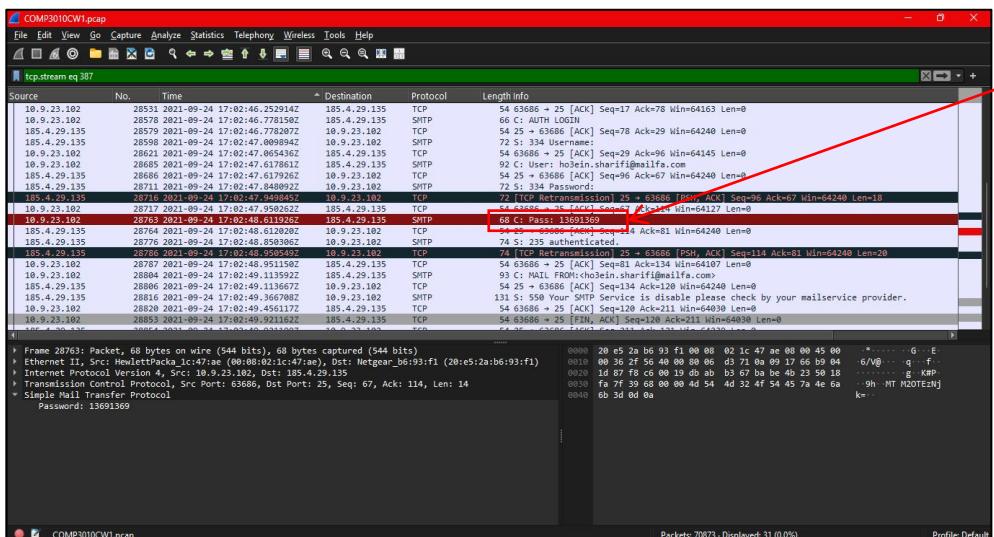
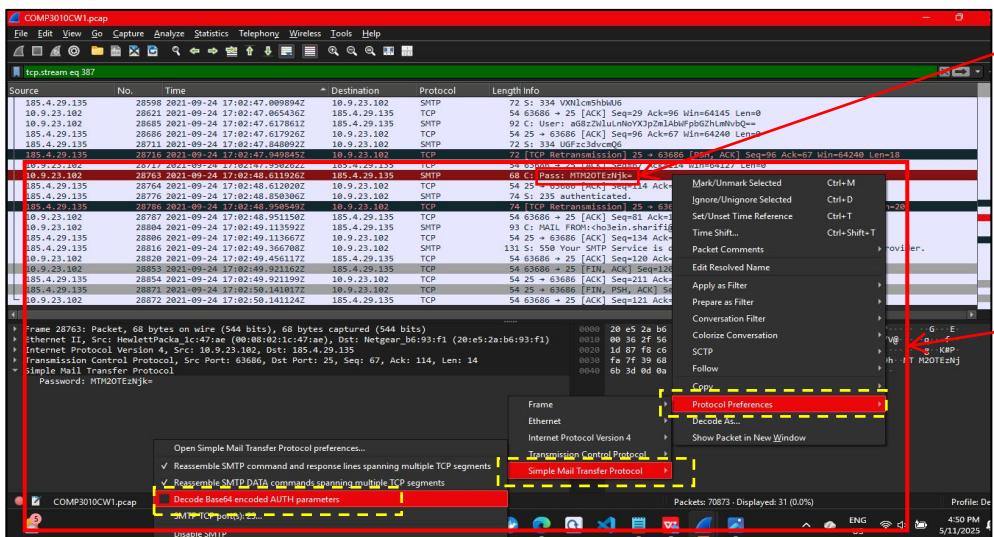
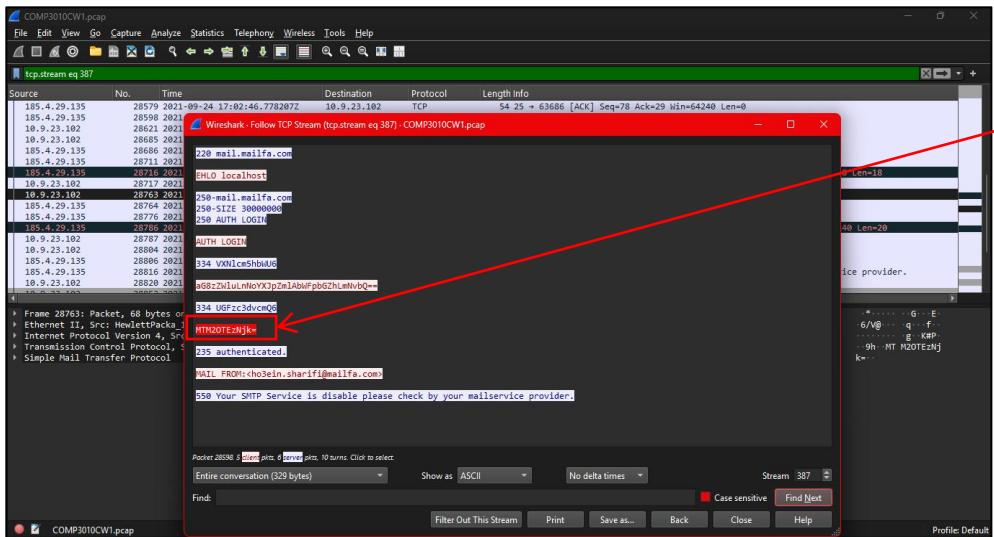
Use filter: **smtp contains "MAIL FROM"** to show me only the SMTP packets that have the word **MAIL FROM** in them.

- Select the packet (**Frame no. 28576**) with a right-click.  
- Hover the cursor over **Follow > TCP Stream**.



Following TCP Stream 387, credentials for **ho3ein.sharifi** are encoded in **Base64** as **MTM2OTEzNjk=**, which decodes to **13691369**.





## 4. Conclusion and References

### Conclusion

The investigation revealed a complete infection chain, including a malicious HTTP download, many staging domains, and two verified Cobalt Strike C2 servers. Following POST traffic to maldivehost.net, DNS queries to api.ipify.org, and SMTP credential theft demonstrate clear post-exploitation and exfiltration activity. This analysis showed that integrating Wireshark packet analysis with VirusTotal intelligence may reliably identify Indicators of Compromise (IoCs) and attacker behavior.

#### 4.1 Prevention and Mitigation

To reduce the possibility of such incidents:

- **Block suspicious downloads and attachments-** Block Office and ZIP files from unreliable websites.
- **Limit Office macros-** Disable signed macros.
- **Use network monitoring and Endpoint Detection and Response (EDR)-** Identify the patterns of Cobalt Strike beacons.
- **Regularly update servers-** Update PHP, Apache, and LiteSpeed.
- **Include threat intelligence streams-** Automatically mark known C2 IPs and domains.
- **Educate and train the users-** Boost awareness of the risks of phishing scams.

#### 4.2 Open Challenges

Modern malware limits visibility and reduces the dependability of static IoCs by using encryption (TLS 1.3), fast domain rotation, and temporary infrastructure. **VirusTotal** community data helps with attribution, but accuracy needs to be double-checked. In order to enhance manual packet inspection, future research should concentrate on behavior-based detection and automated correlation methods.

## **4.4 References**

1. Wireshark Foundation (2024). Wireshark User Guide. <https://www.wireshark.org/docs>
2. VirusTotal (2024). VirusTotal Intelligence Platform. <https://www.virustotal.com>

**Github Link:** <https://github.com/taarsinii/COMP3010-Security-Operations-Incident-Management>

**YouTube Link:** <https://youtu.be/ra4YI9RCxUo>