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**

STUDENT ID: BSCS2406001

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.

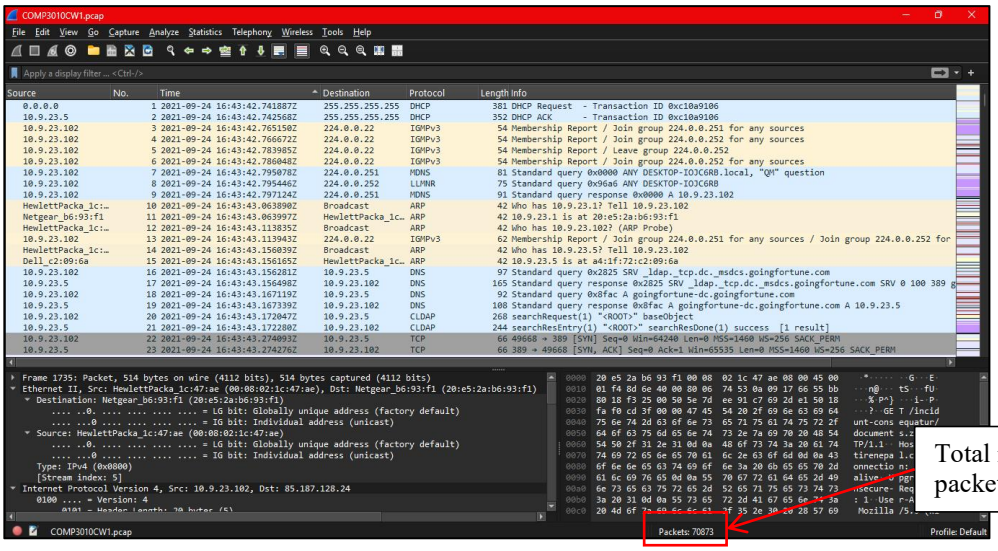
➢ 2.1 Tools Used

The investigation used two major tools:

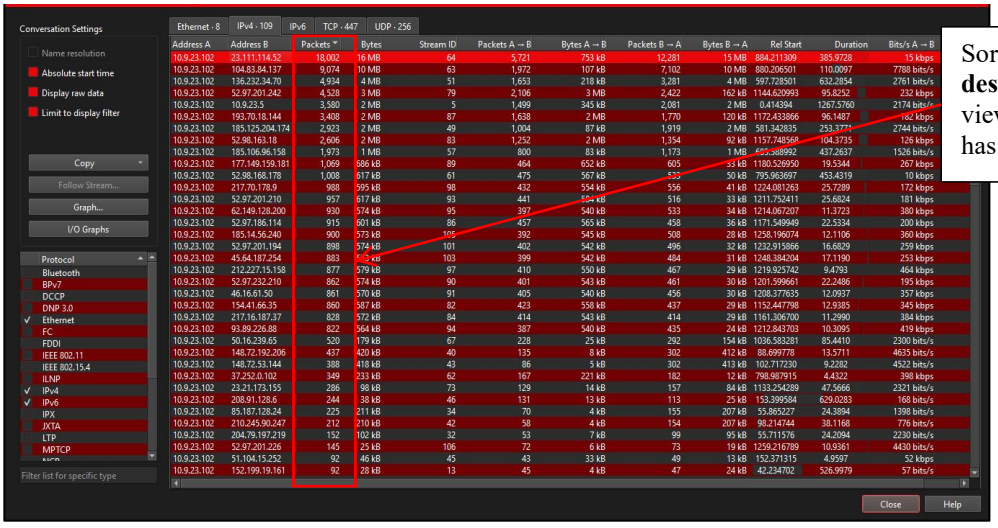
i. **Wireshark:** Used to investigate packet-level network activity, apply protocol filters, track the infection time frame, and capture indicators of compromise (IoCs) like as IP addresses, domain names, and payload file names.
ii. **VirusTotal (https://www.virustotal.com/):** Used to determine whether 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.

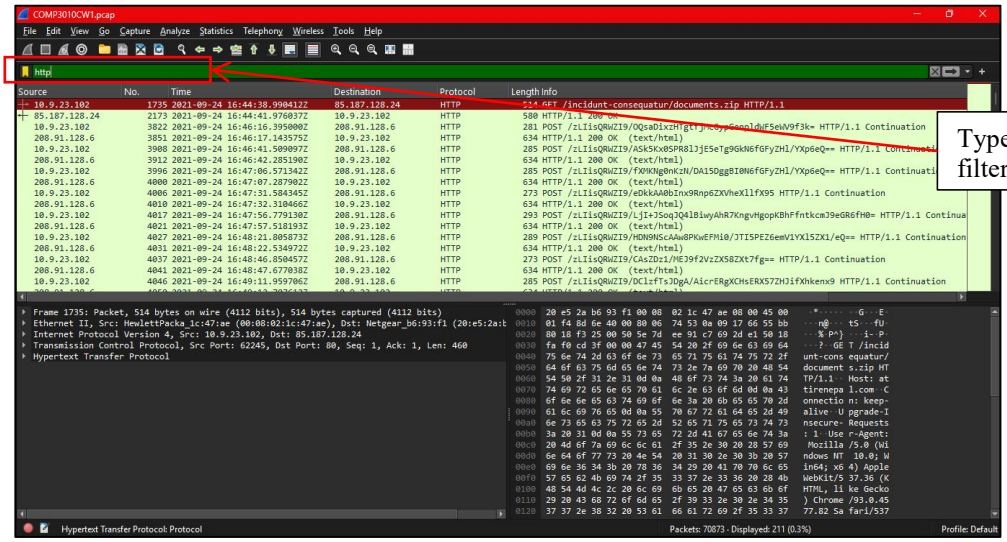


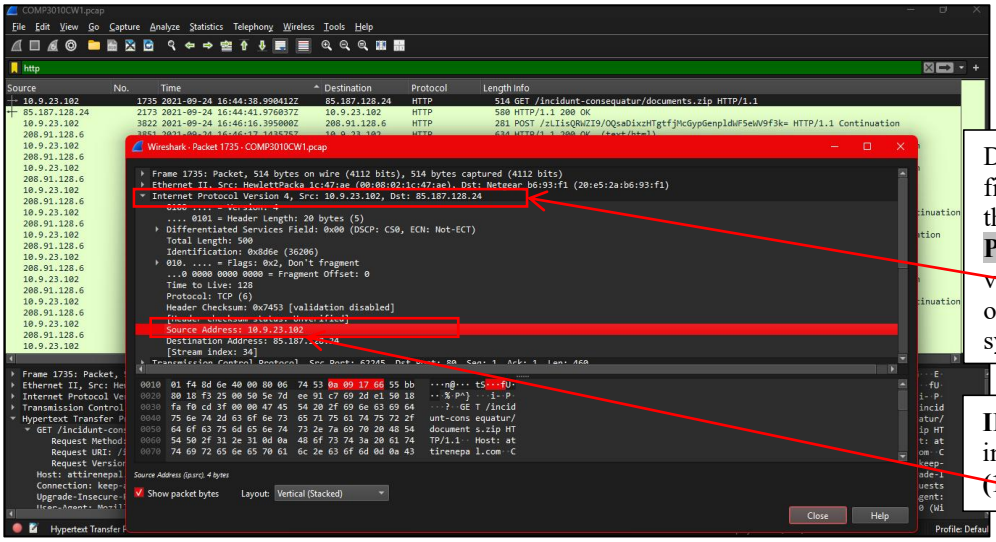
2.The initial investigation utilized **Statistics > Conversations >IPv4** to find active endpoints and check the total volume of traffic.This showed that, host **10.9.23.102** engaged in major communication with external servers, indicating an attack.

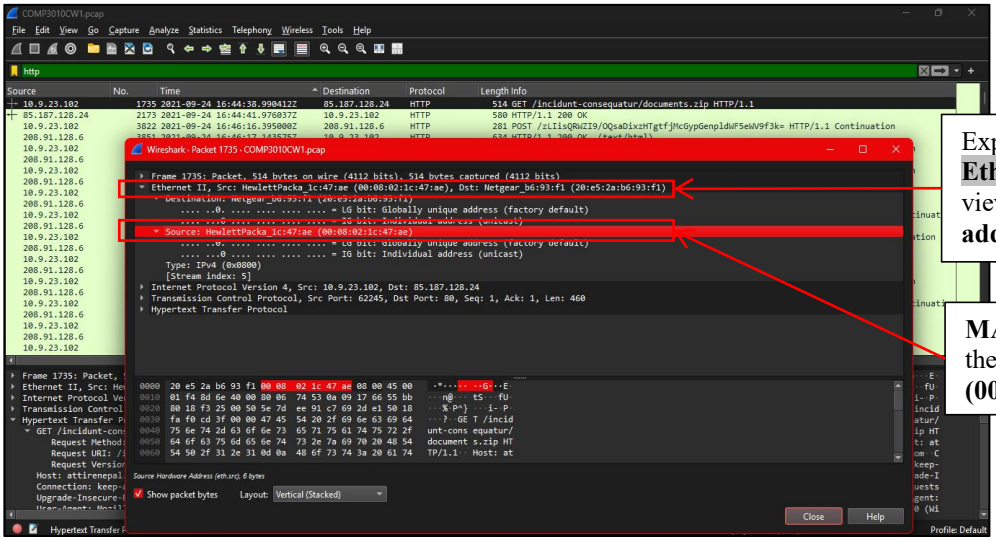


➢ 2.3 Identifying the Infected Host

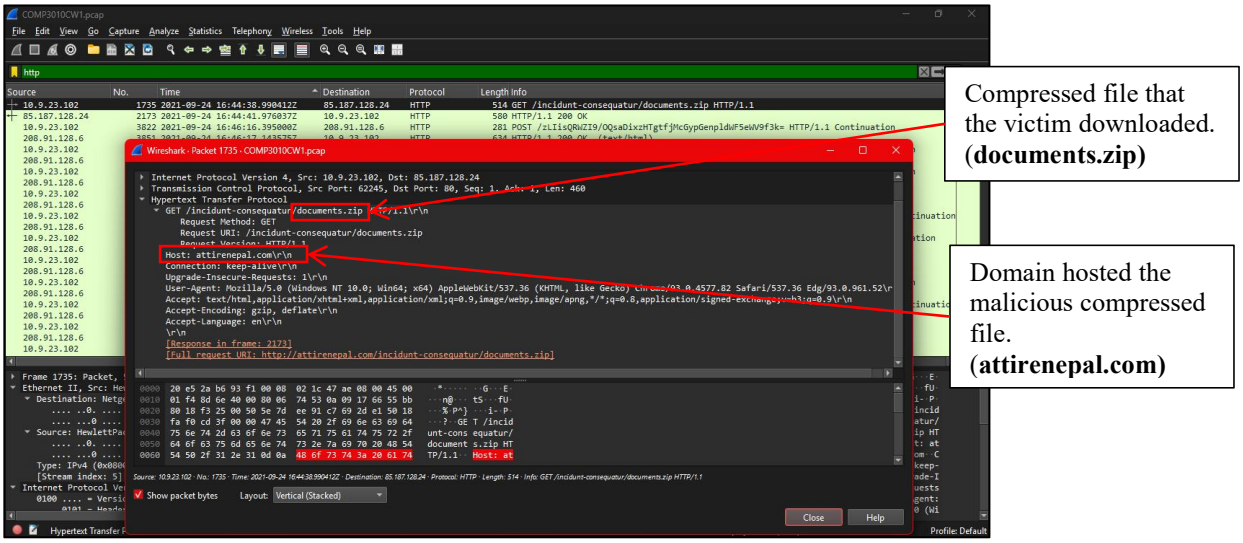
- The HTTP display filter is used to separate suspicious downloads.







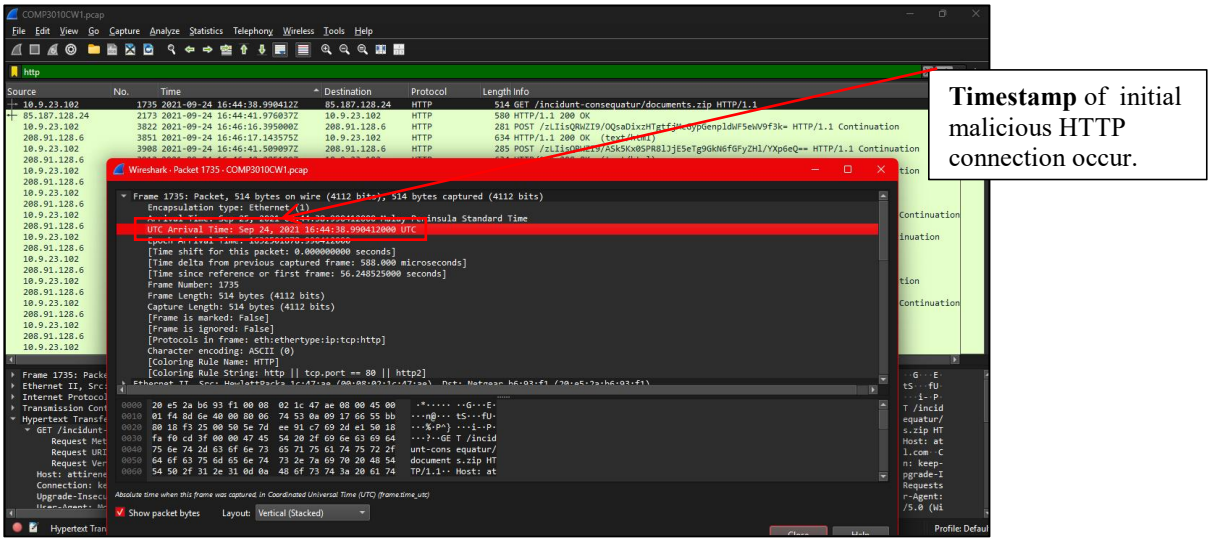
- This showed an outbound HTTP GET request for a compressed file called **documents.zip** hosted at **attirenepal.com**.



➢ 2.4 Identifying Infection Indicators

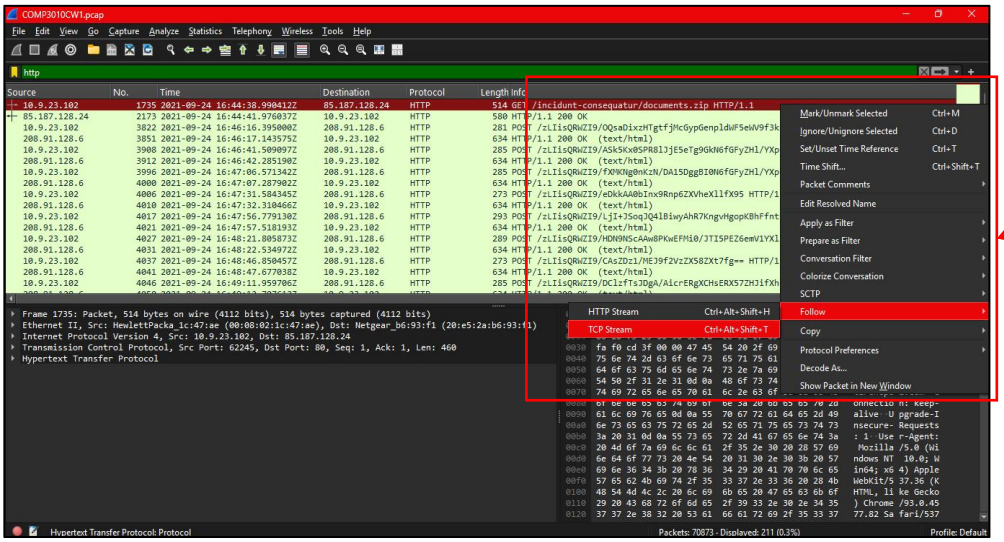
Indicator 1 - Timestamp of initial malicious activity

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



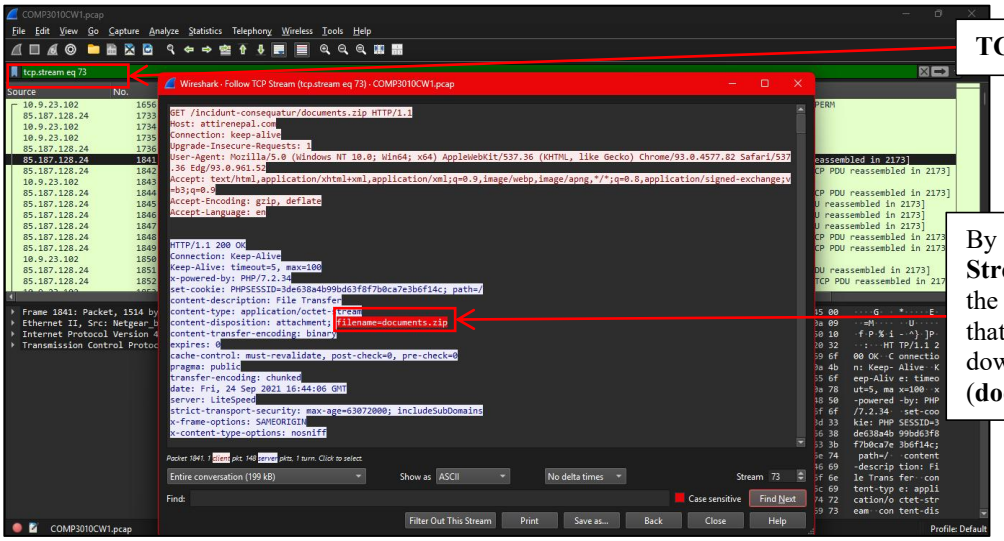
Indicator 2 - Malicious file downloaded

- 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**.

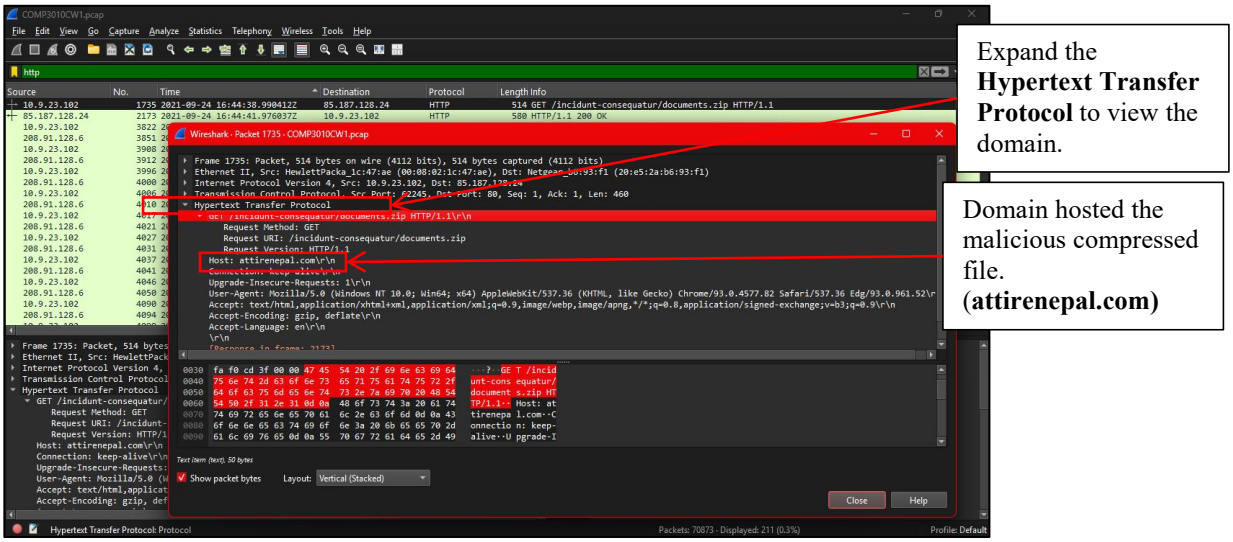


TCP Stream 73,

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

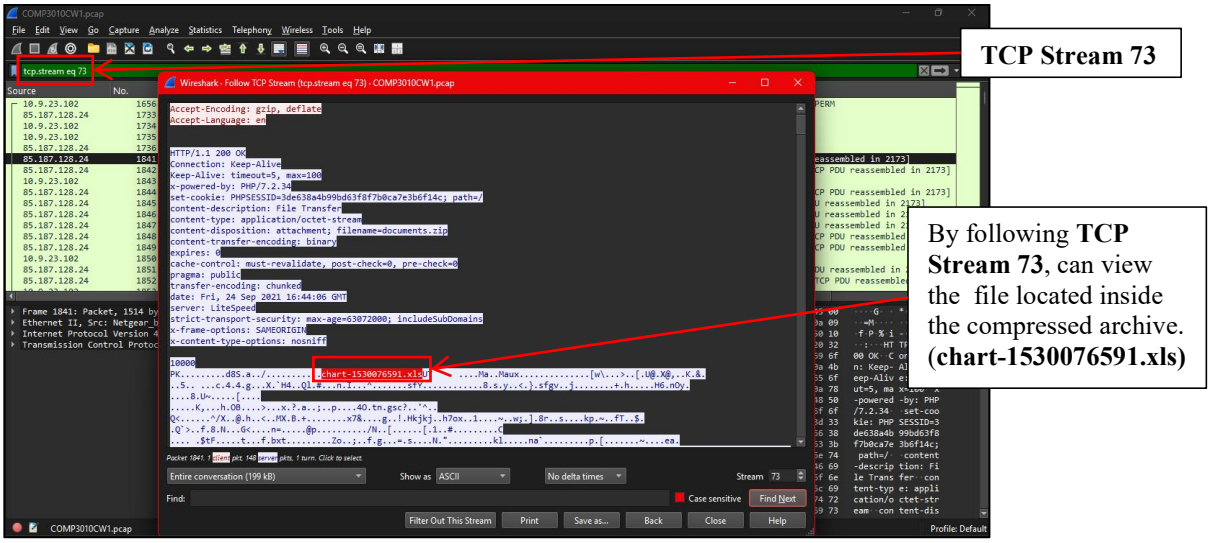
Indicator 3 - Malicious domain delivering the payload

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.



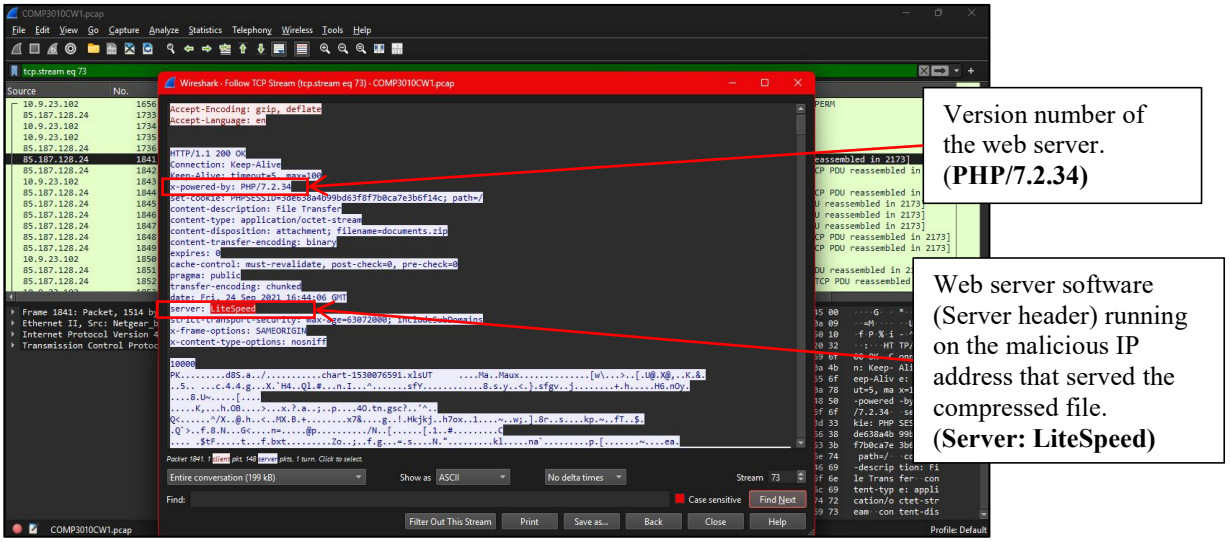
Indicator 4 - Malicious file inside archive

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.



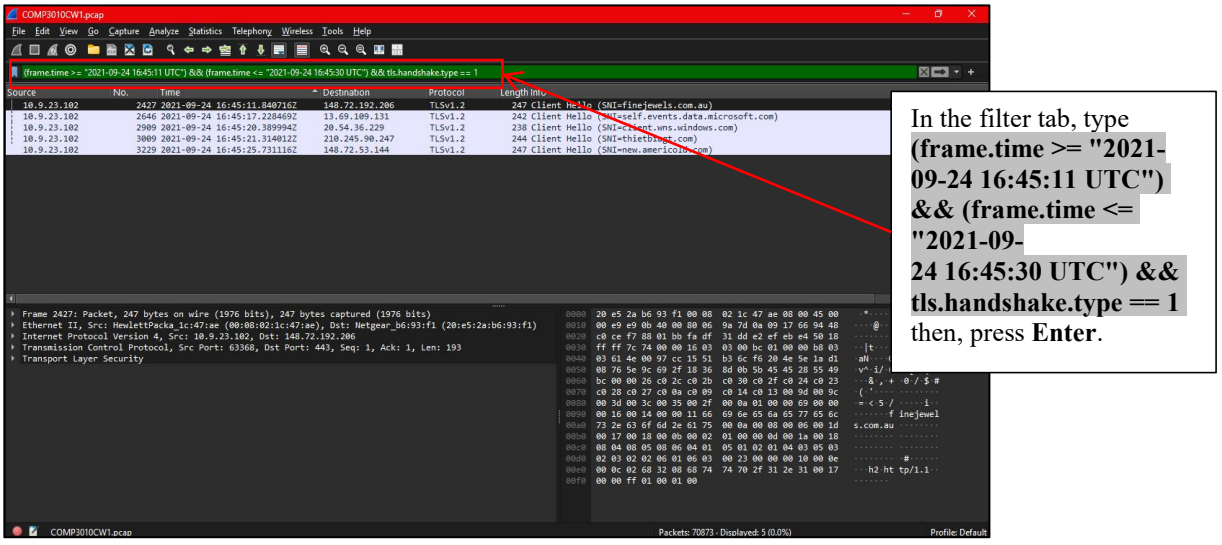
Indicator 5 - Suspicious server headers

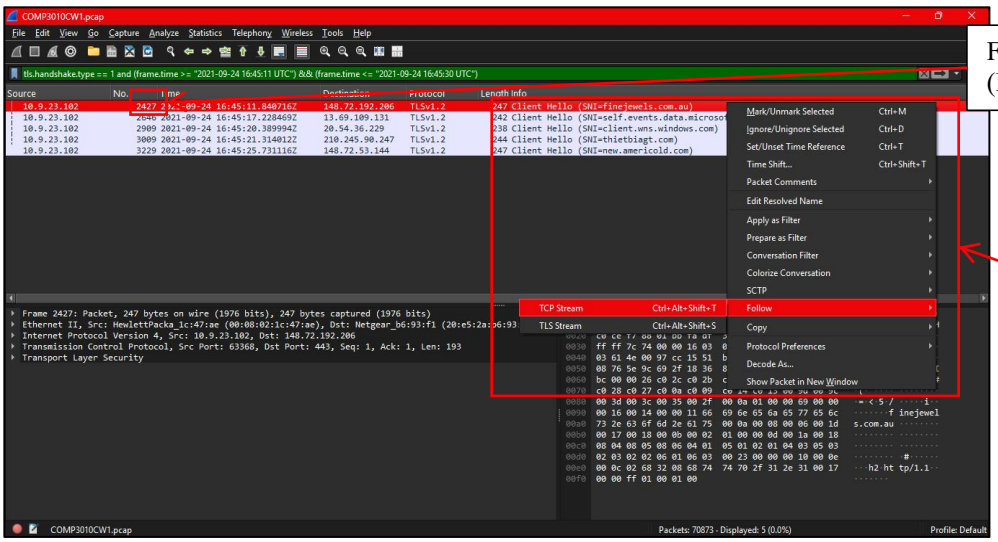
The HTTP response for the download request showed the server information **Server: LiteSpeed** and **PHP/7.2.34**. These details, found by following the **TCP Stream 73**.



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**.

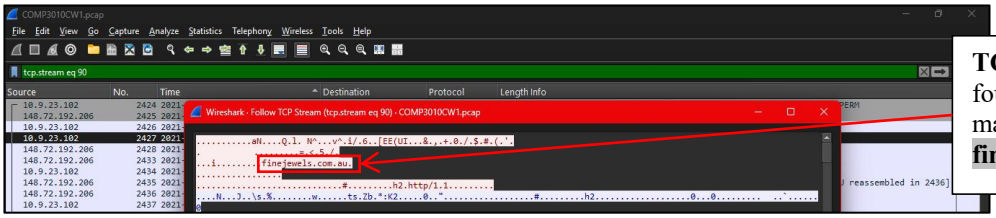




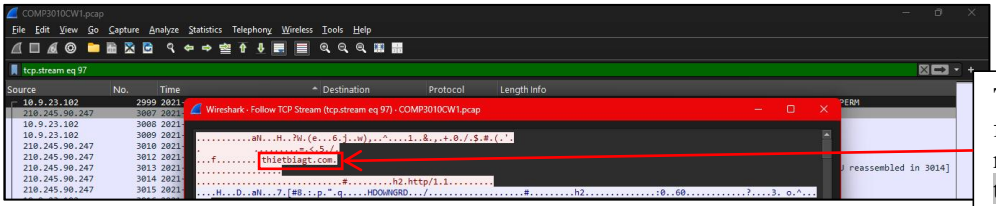
First packet appear is **(Frame no. 2427)**

- Select the packet **(Frame no. 2427)** with a right-click.

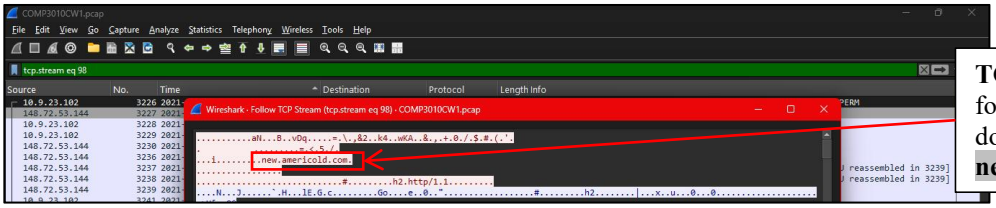
- Hover the cursor over **Follow > TCP Stream**.



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**

STUDENT ID: BSCS2406001

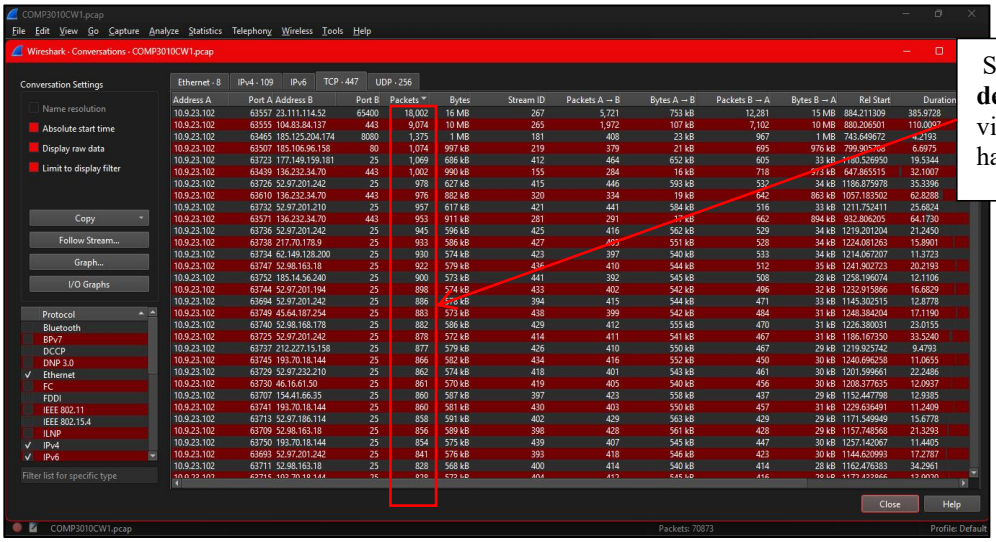
Indicator 7 - Immediate connection to Cobalt Strike C2 IPs

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:

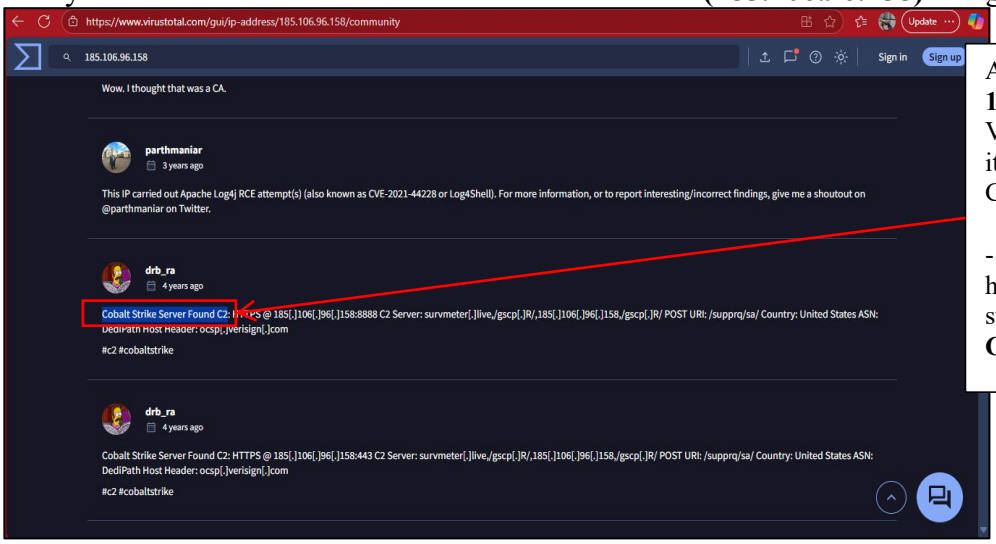
- **185.106.96.158**
- **185.125.204.174**

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



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

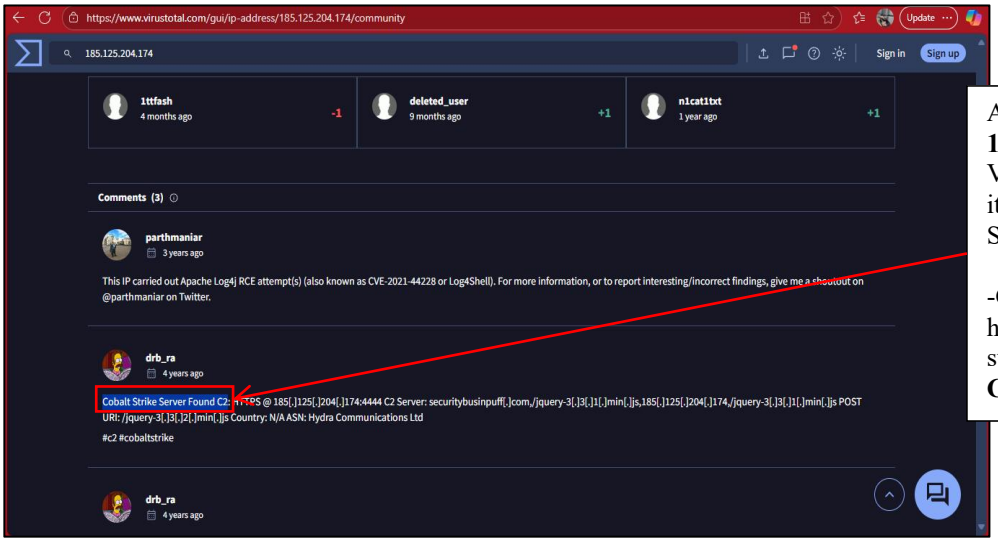
Analyze first IP addresses of the Cobalt Strike servers **(185.106.96.158)** using **VirusTotal.**



Analyze IP address: **185.106.96.158** using VirusTotal, to confirm that it is the IP address 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.**



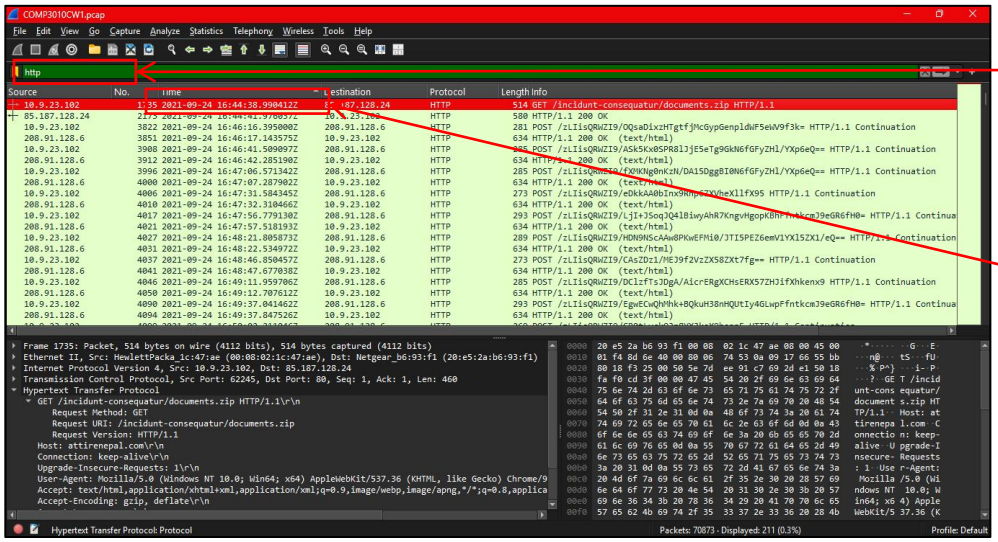
Analyze IP address: **185.125.204.174** using VirusTotal, to confirm that it is the IP address of Cobalt Strike Server.

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

3. Results

3.1 Initial Infection and Malicious File Delivery

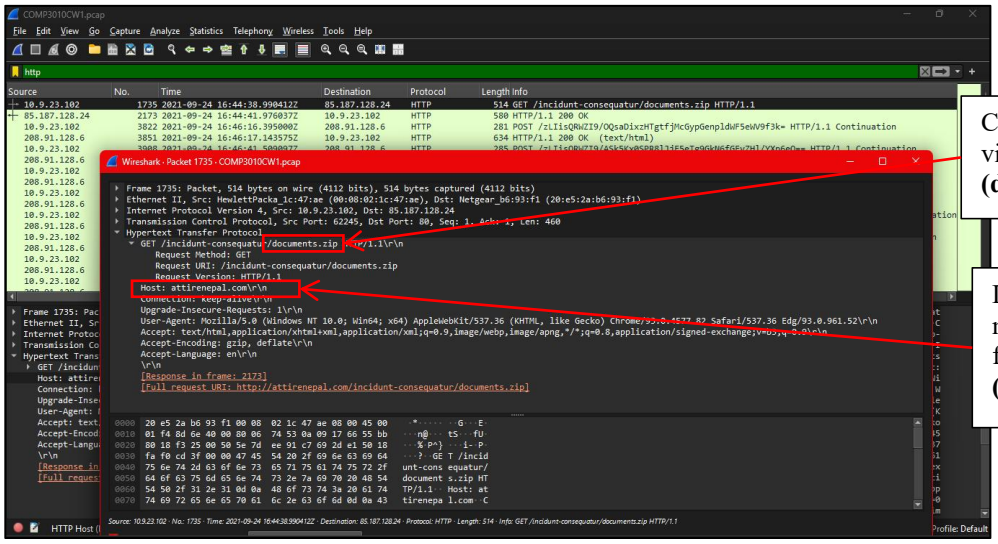
The first malicious action occurs at **2021-09-24 16:44:38 UTC**, when the victim system sends an HTTP GET request to retrieve a compressed file. This timestamp shows the starting point of the intrusion.



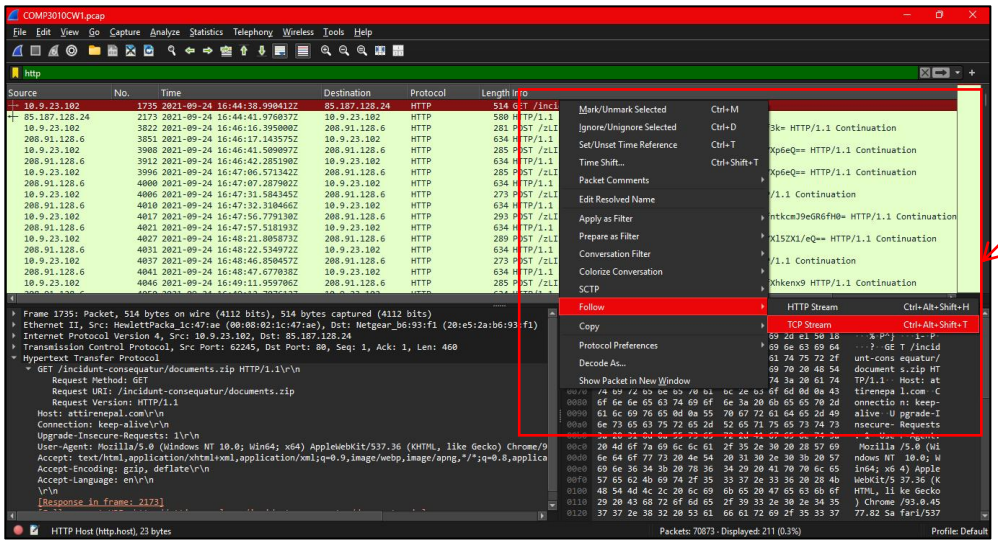
2. Type **http** in the filter tab.

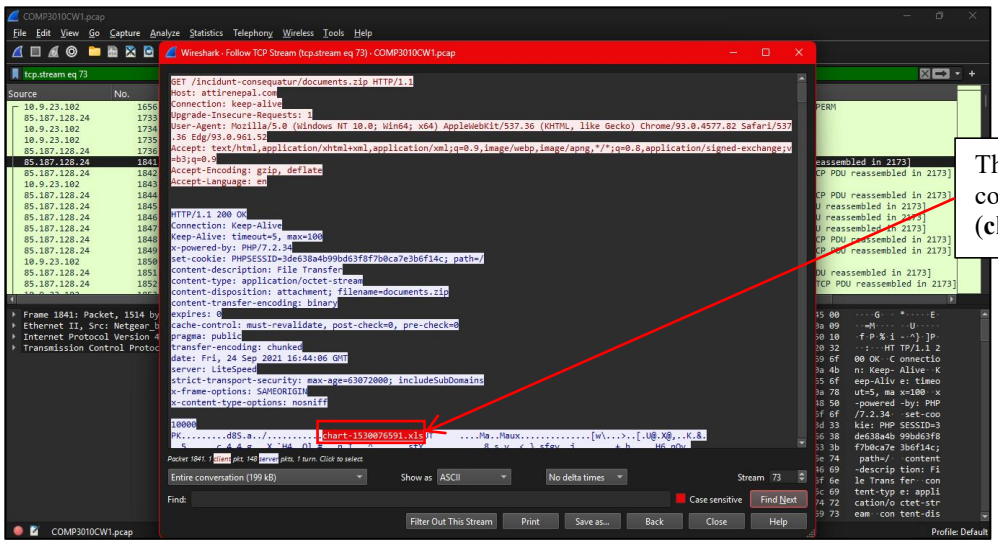
1. **Timestamp** of initial malicious HTTP connection occur.

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.**

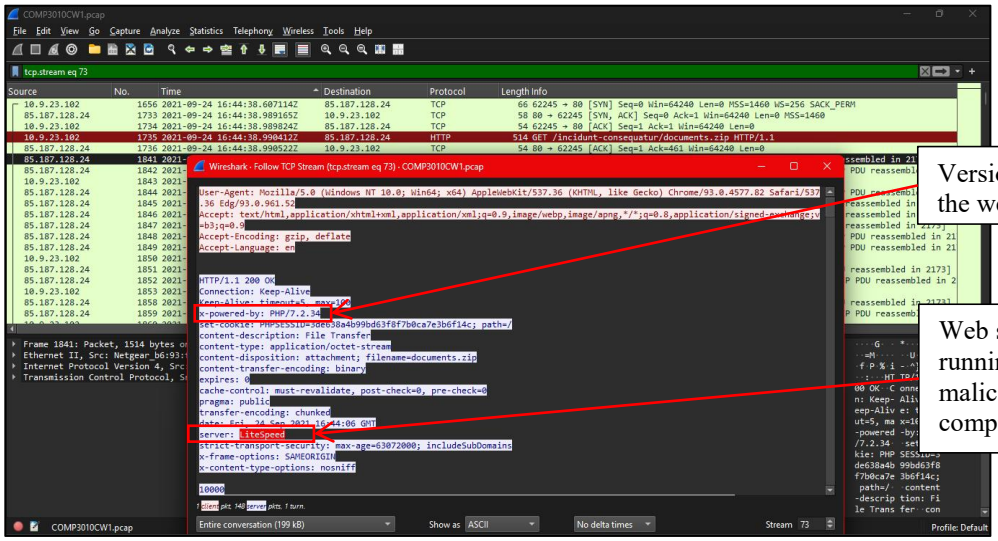


The files inside of the compressed file can be viewed by following the TCP stream **(Stream 73)** without the necessity of extracting it. The malware payload, **chart-1530076591.xls**, is provided inside the archive, showing a malicious spreadsheet that probably contains a macro or exploit execution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



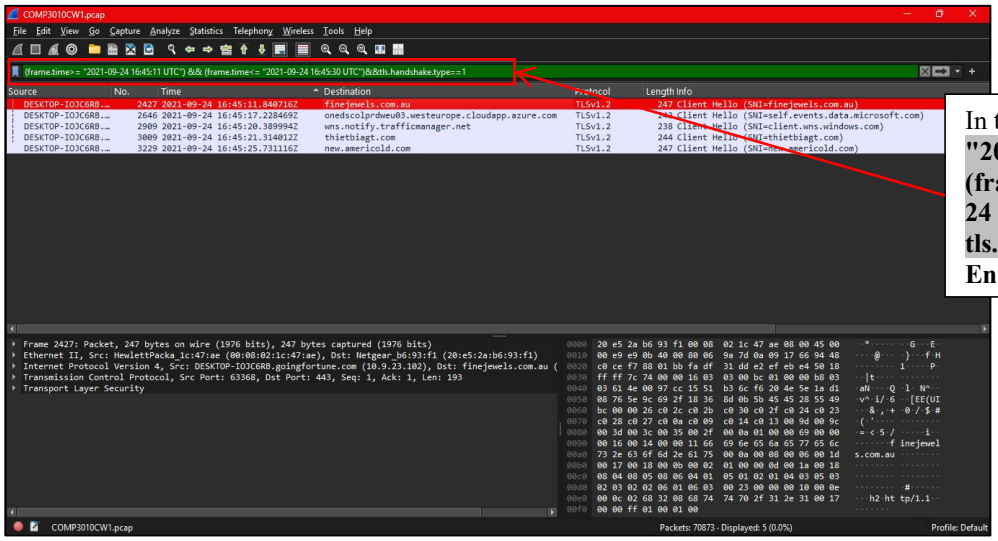


The malicious web server hosting the file identifies itself as **LiteSpeed** and runs **PHP/7.2.34**. This is found in the server response header and shows that the shared hosting environment may be misconfigured or exploited.

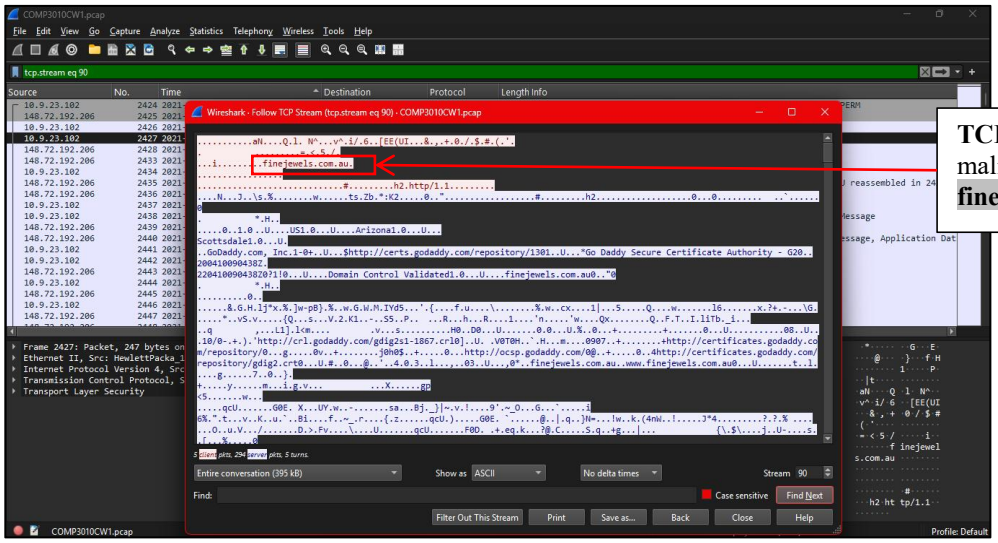


Together, these results verify that the malicious file download via insecure HTTP was the infection vector, allowing the attacker to send the victim an Excel-based payload that was hidden.

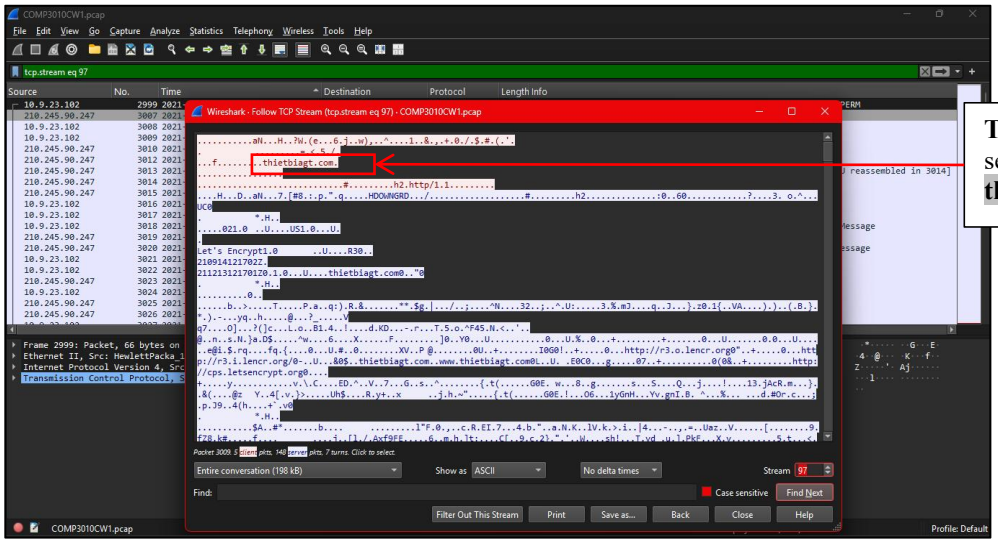
After the initial file download, the victim host quickly established encrypted connections to three additional domains which is **finejewels.com.au**, **thietbiagt.com**, and **new.americold.com** during the window **16:45:11 to 16:45:30 UTC**.



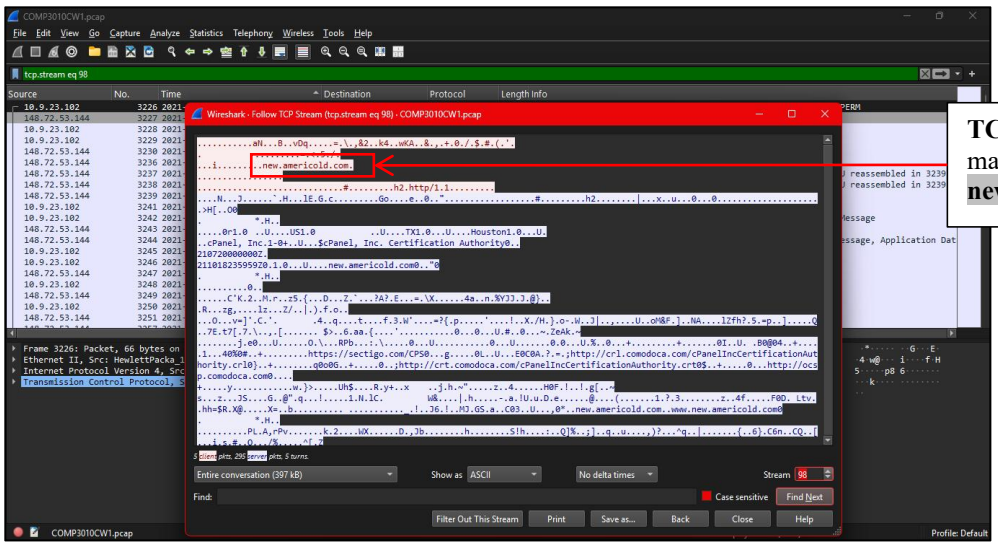
In the filter tab, type **(frame.time >= "2021-09-24 16:45:11 UTC") && (frame.time <= "2021-09-24 16:45:30 UTC") && tls.handshake.type == 1** then, press **Enter**.



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



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

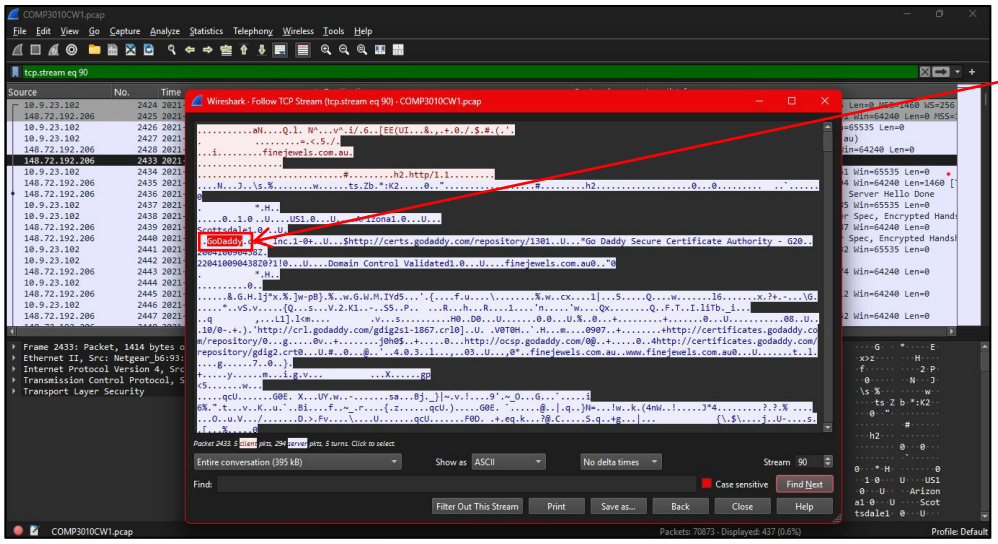


TCP Stream 98, found third malicious domain: **new.americold.com**

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

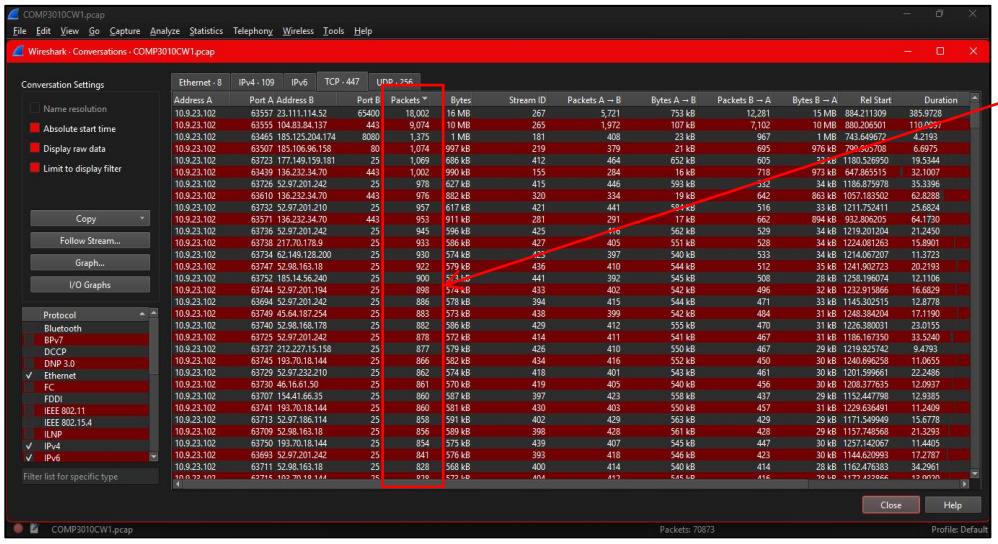
GoDaddy issued the certificate that was used during the TLS exchange with the first domain which is **finejewels.com.au**, showing that the domain used a valid **Certificate Authority (CA)** and was probably able to bypass detection by security appliances.



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

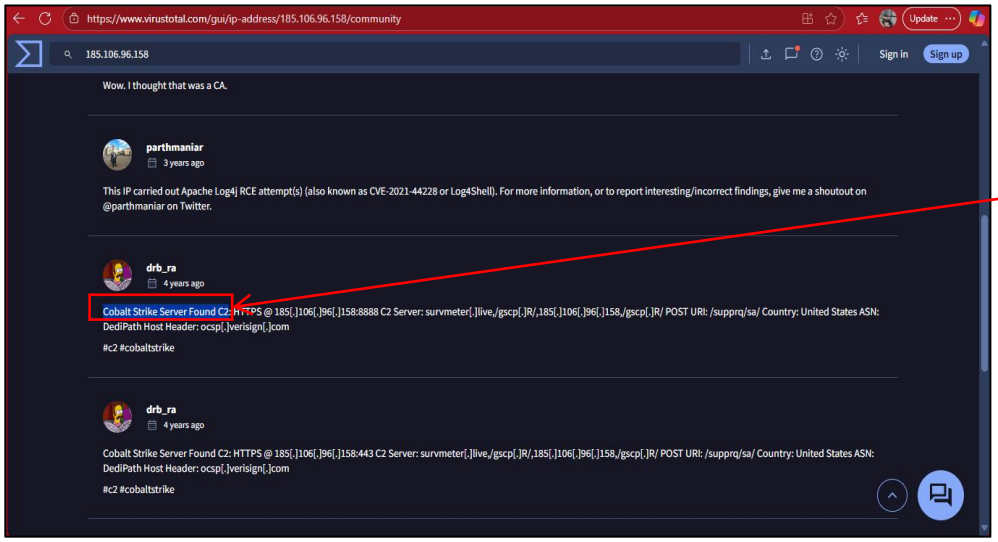
To identify potential command-and-control (C2) servers, firstly investigated ongoing TCP traffic from the infected computer.To find the most active external endpoints, use Wireshark's **Statistics > Conversations > TCP** to sort the list by bytes in **descending order**. Each potential IP address was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



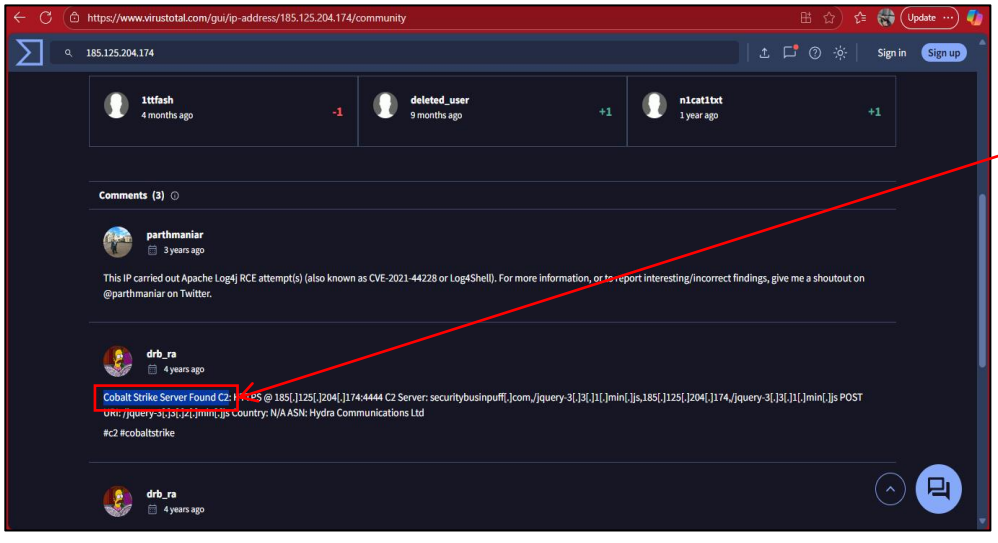
Sort the packets in **descending order** to view which IP address has **highest packet**.

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



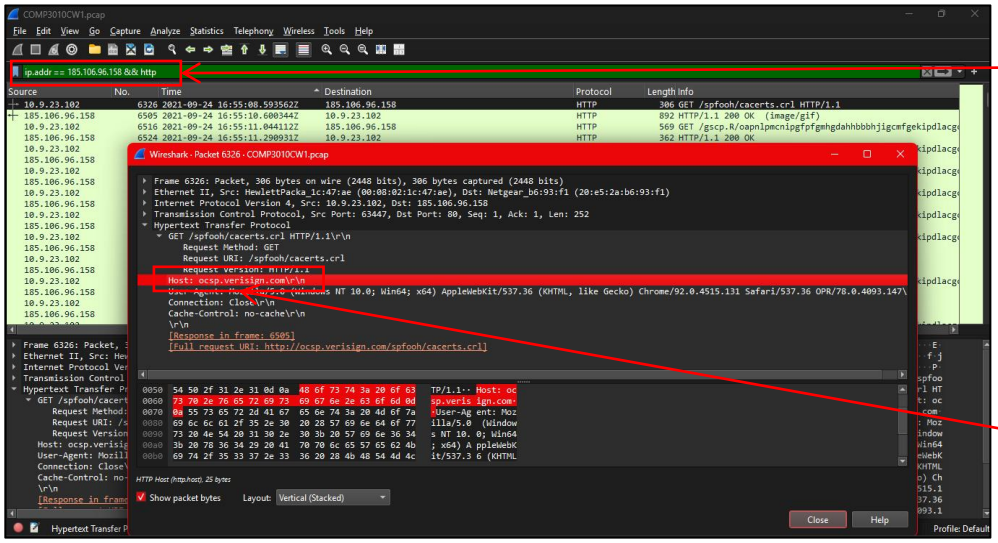
Analyze IP address: **185.106.96.158** using VirusTotal, to confirm that it is the IP address is flagged as **Cobalt Strike servers** in VirusTotal's Community section.

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

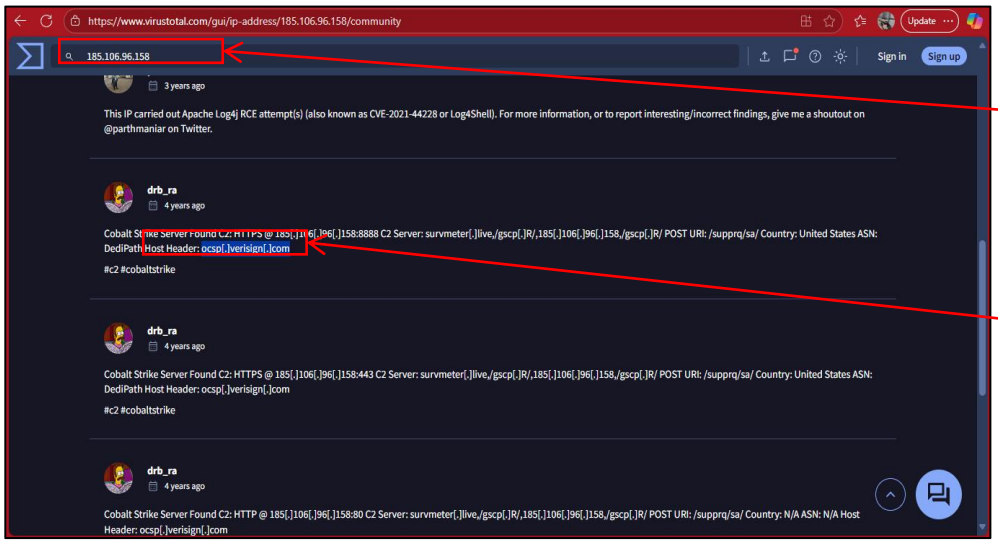


Analyze IP address: **185.125.204.174** using VirusTotal, to confirm that it is the IP address is flagged as **Cobalt Strike servers** in VirusTotal's Community section.

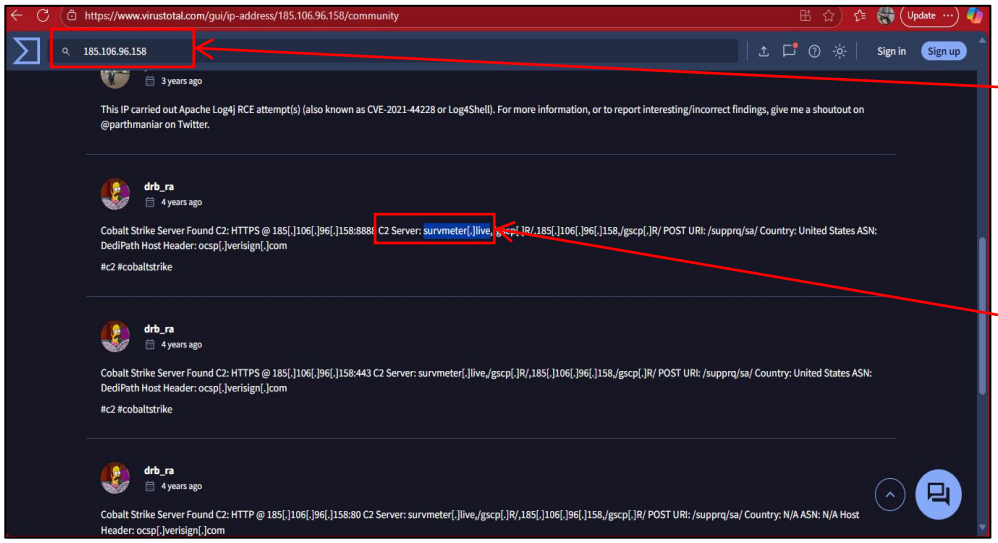
Analysis of HTTP traffic to the first C2 server shows the Host header used for communication is **ocsp.verisign.com**, which is an intentional imitation of a legitimate OCSP domain.



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

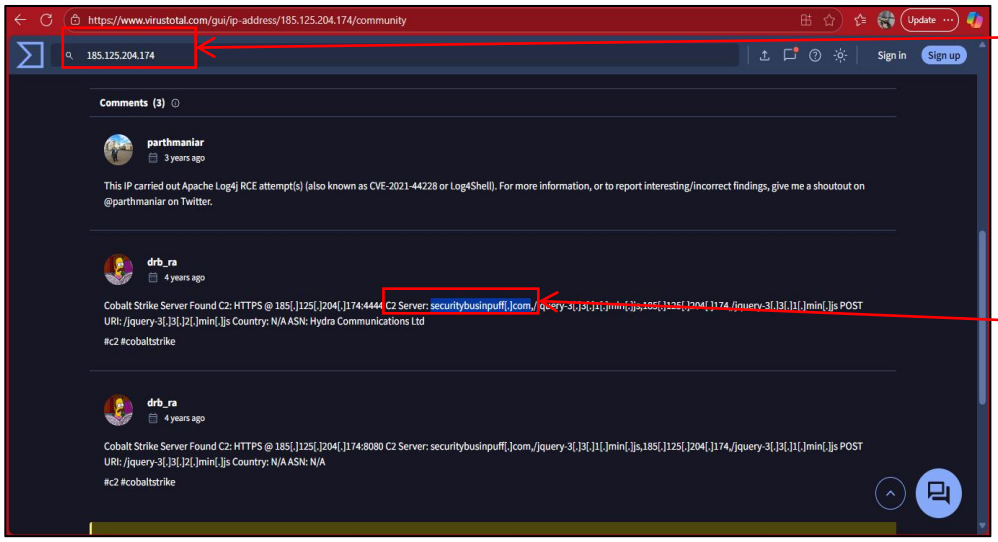


The domain **survmeter.live**, which is associated with the first C2 IP **185.106.96.158**, was verified by VirusTotal while the second C2 domain, **securitybusinpuff.com**, associated with **185.125.204.174**, was identified on **VirusTotal**.



First Cobalt Strike IP address.

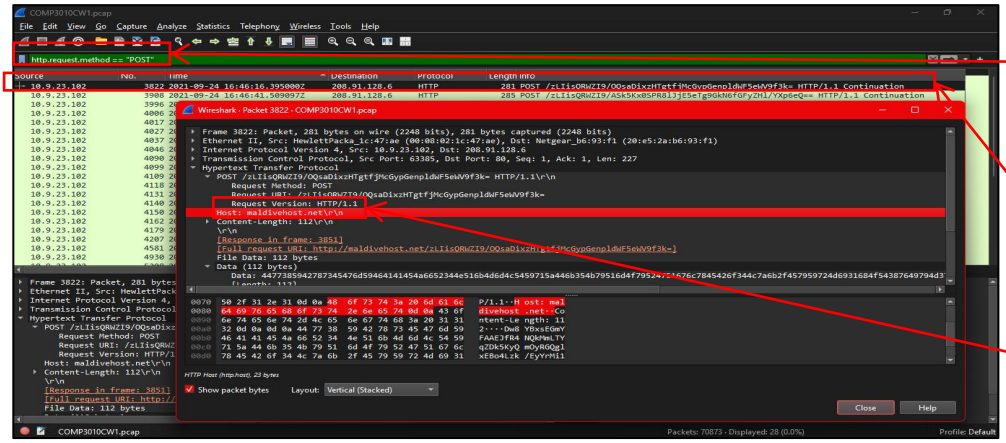
Domain name associated with the **first Cobalt Strike IP address.**



Second Cobalt Strike IP address.

Domain name associated with the **second Cobalt Strike IP address.**

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

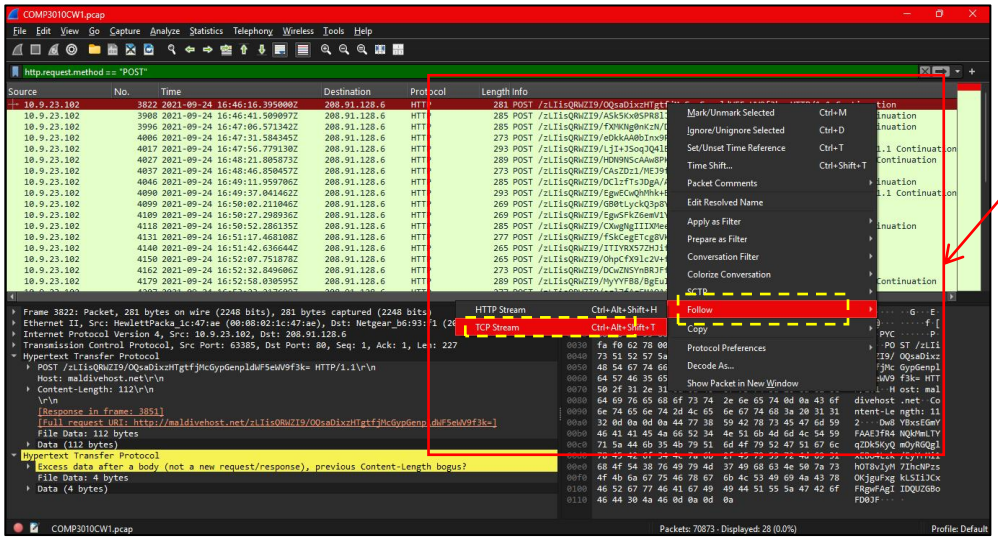


2. Use filter : **http.request.method == "POST"** to shows only the HTTP packets that are being sent to a server by the client (victim).

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

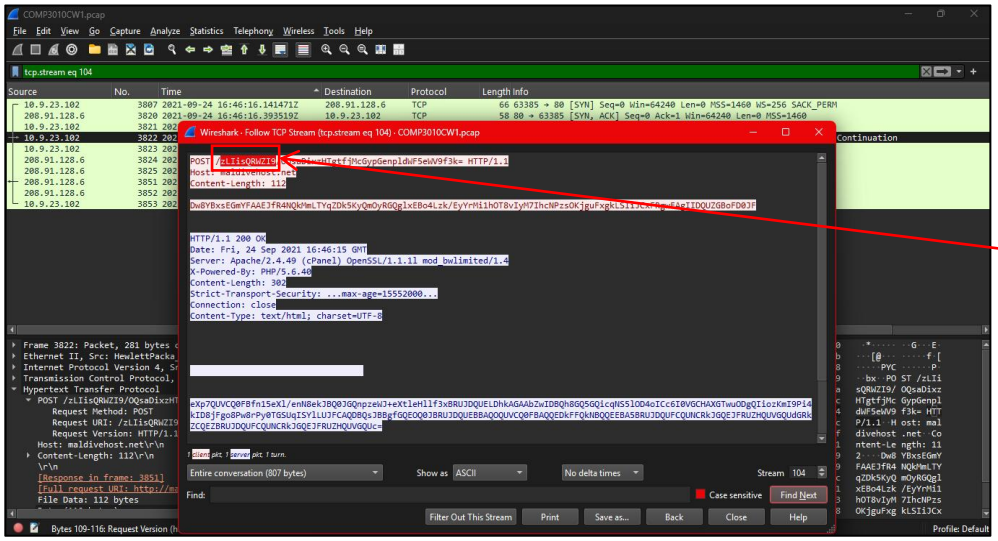
Domain name used for the **post-infection traffic.**

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



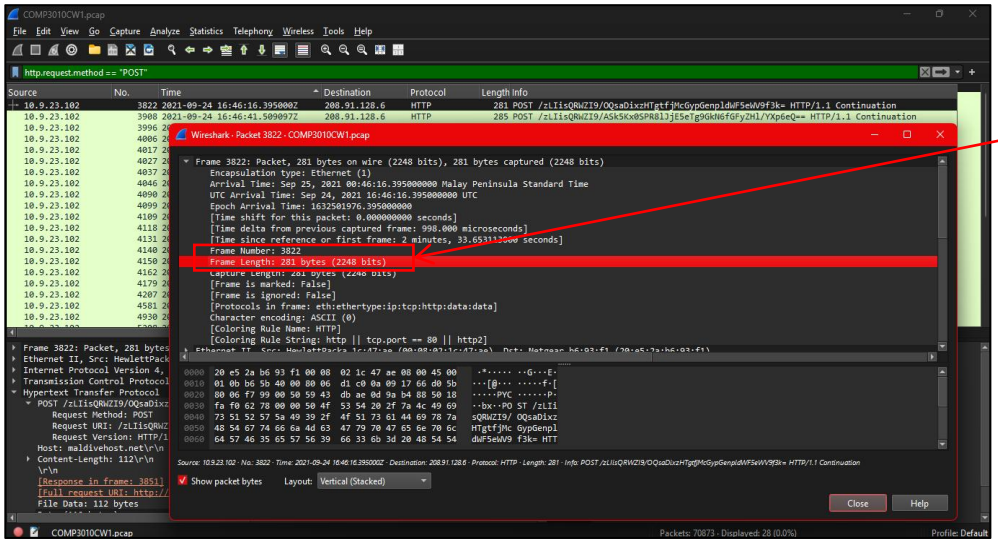
- Select the packet **(Frame no. 3822)** with a right-click.

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



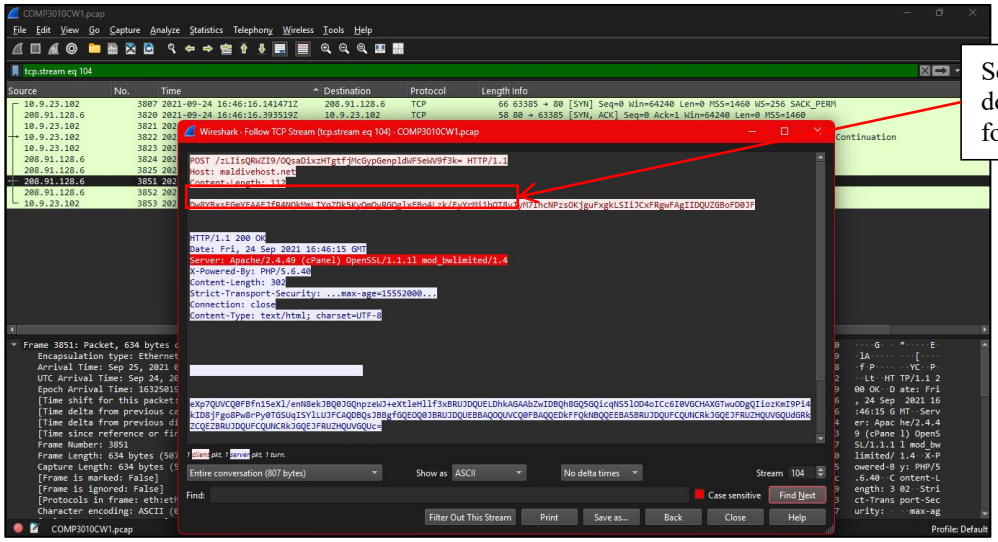
The **first eleven characters** of the data the victim host sends to the malicious domain: **maldivehost.net**

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.



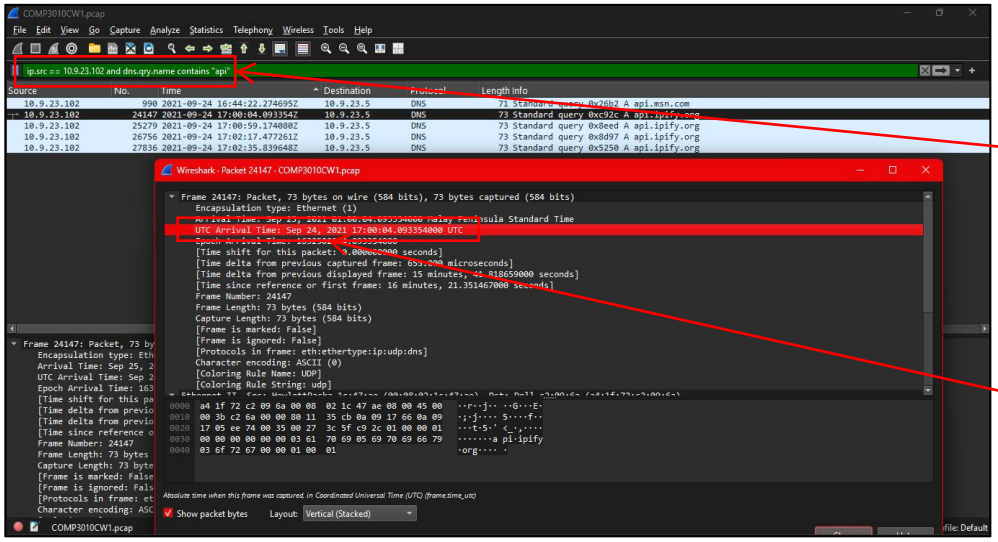
Length of the first packet the victim sent to the C2 server.

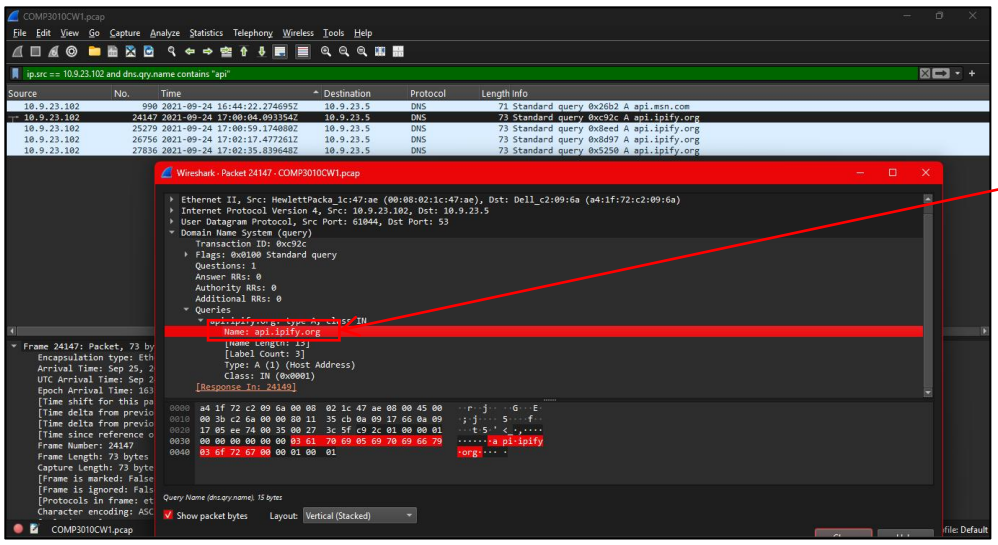
Maldivehost.net's server header includes **Apache/2.4.49 (cPanel) OpenSSL/1.1.1l mod_bwlimited/1.4**, showing an outdated and vulnerable web hosting stack often used for C2 operations.



➢ 3.3 Final Exfiltration/Check-in

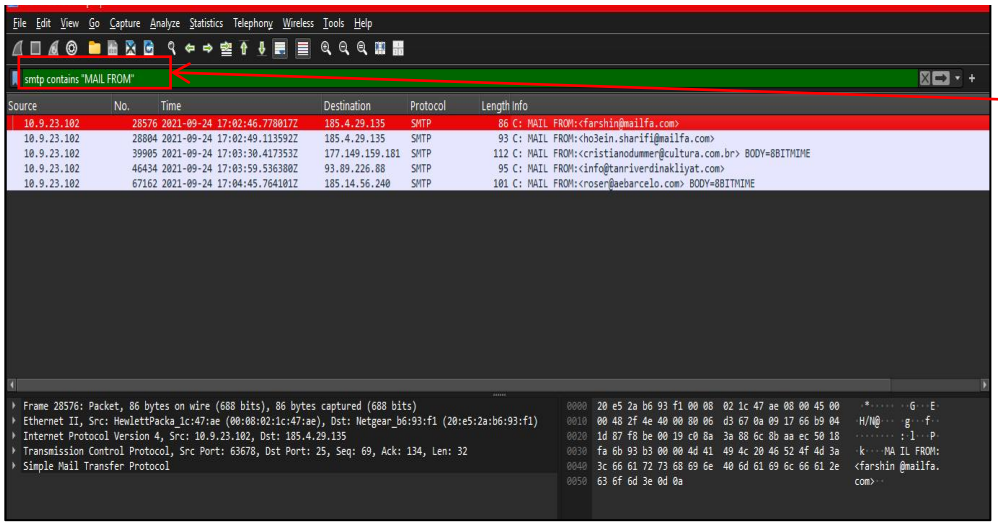
At **2021-09-24 17:00:04 UTC**, the attacker tried to find the victim's public IP address by sending a DNS query to **api.ipify.org**.



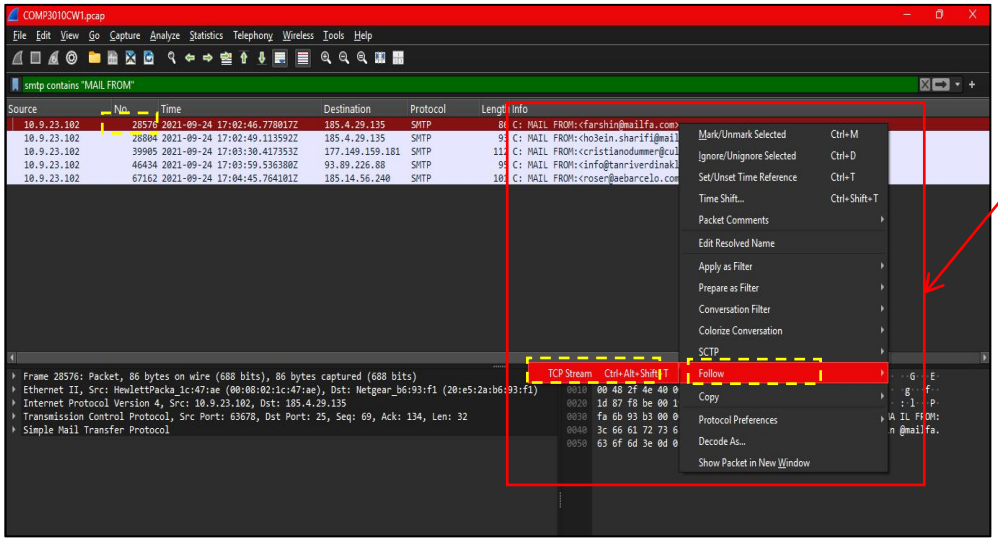


Domain name in the DNS query found by expanding the **Domain Name System (query) header.**

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.

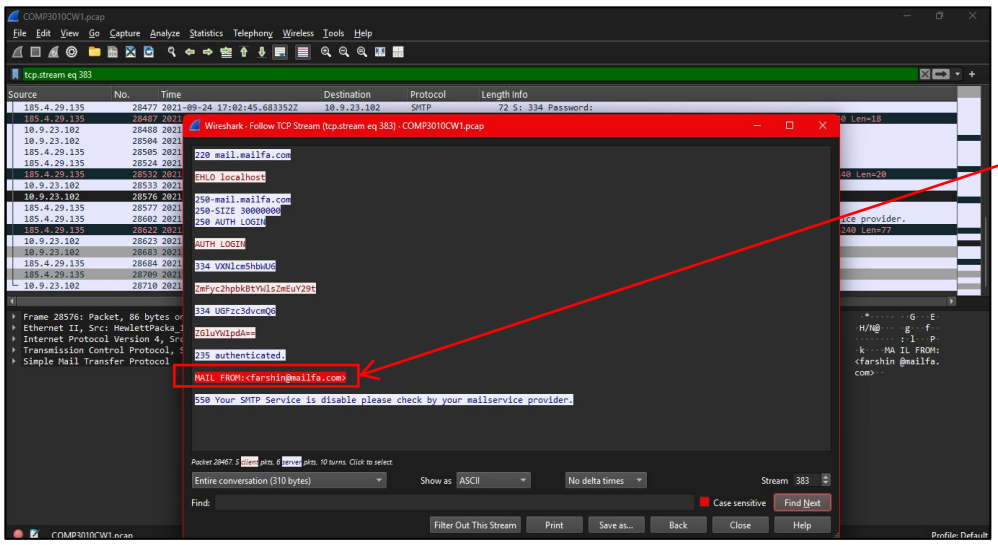


Use filter: **smtp contains "MAIL FROM"** to show me only the SMTP packets that have the word **MAIL FROM** in them.



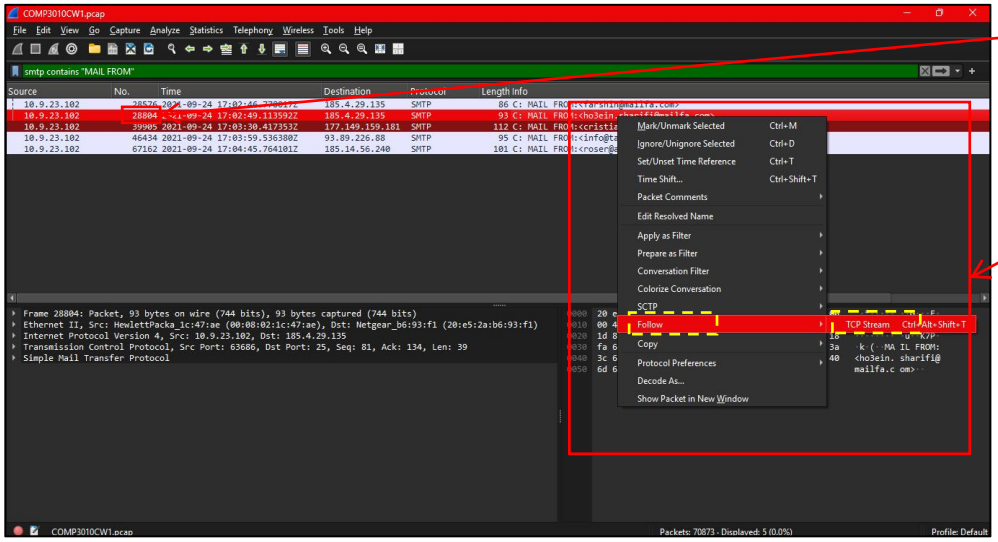
- Select the packet **(Frame no. 28576)** with a right-click.

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



First email address observed in the SMTP traffic is found by following the **TCP stream 383.**

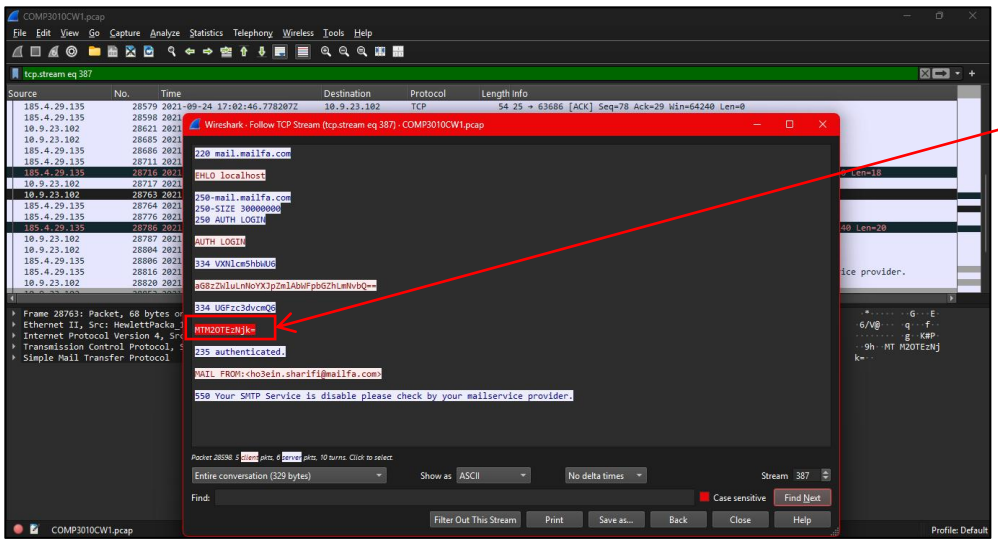
Following **TCP Stream 387**, credentials for **ho3ein.sharifi** are encoded in **Base64** as **MTM2OTEzNjk=**, which decodes to **13691369**.



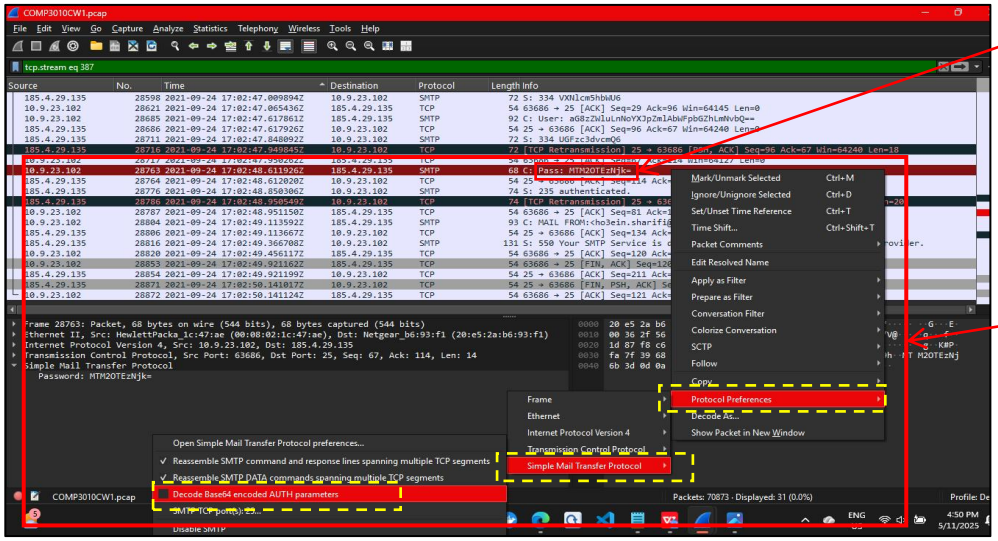
Frame No. 28804

- Select the second packet **(Frame no. 28804)** with a right-click .

- Hover the cursor over **Follow > TCP Stream** to view the details for **ho3ein.sharifi.**



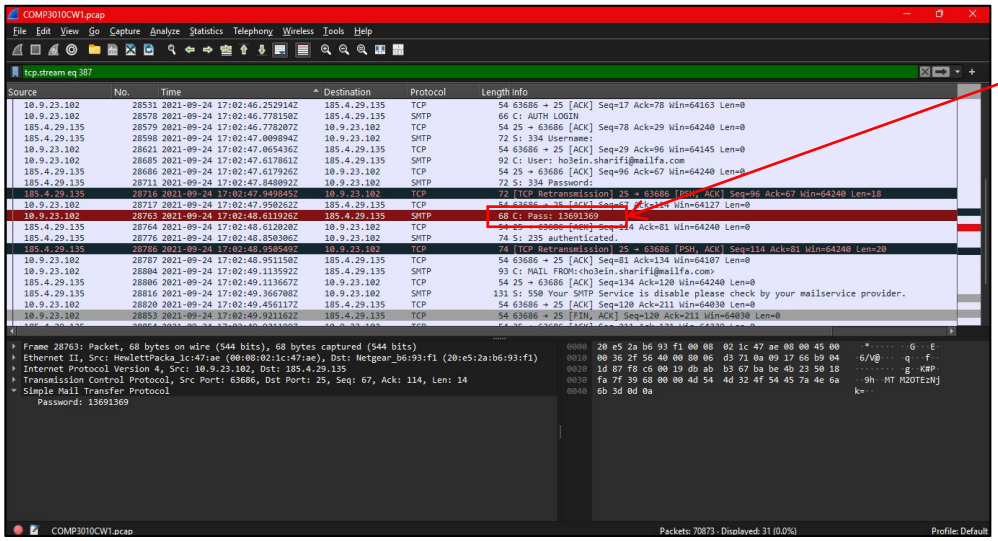
ho3ein.sharifi's password but it is **encoded** in Base64.



Encoded Password: **MTM2OTEzNjk=**

- Right-click on packet **(frame no. 28763)** where it shows the password for **ho3ein.sharifi**

- Hover the cursor over **Protocol Preferences > Simple Mail Transfer Protocol > check the Decode Base64 encoded AUTH parameters** to decode the Base64 fields in the packet information to view the password and username in plain text.



The password is decoded: **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