Coursework 1: Set Exercises - PCAP Analysis

Github Link: <https://github.com/Mattrfish/COMP3010-SecOps-and-Incident-Management.git>

Youtube Walkthrough Link:

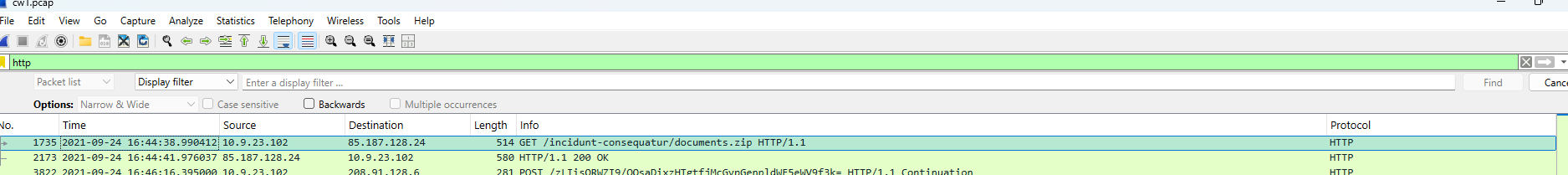
# Introduction

This report presents a detailed analysis of a provided PCAP file to investigate a suspected network intrusion. The primary objective was to reconstruct the cyber kill chain by identifying the infected host, determining the infection vector, classifying the attack, and extracting key Indicators of Compromise (IOCs) to facilitate containment and future prevention.

This report is structured as follows: The methodology section outlines the tools and techniques used and how they were applied to investigate the intrusion. The results section presents the key findings from the PCAP analysis, supported by evidence and screenshots. Finally, the conclusion summarises the findings, discusses prevention strategies to mitigate similar incidents in the future, and reflects on any challenges encountered during the investigation.

# Methodology

The investigation was conducted using Wireshark, as it is one of the most effective open source tools for packet-level network traffic analysis. The analytical process was phased to methodically trace the attack chain. The process began with an initial review of the entire capture to provide context on overall network activity and identify anomalous traffic patterns. For the initial infection analysis, the http display filter was used to isolate and inspect all clear-web HTTP traffic; the "Follow HTTP Stream" function was critical for reconstructing the content of communications between the victim and attacker-controlled servers, allowing for the identification of downloaded files without executing potentially malicious content.

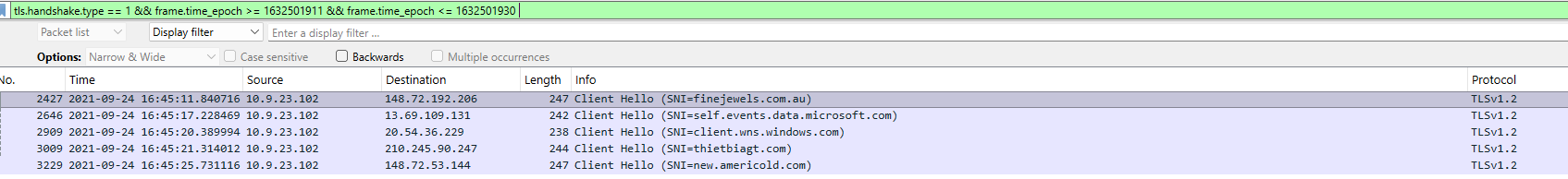


A screenshot of a computer program

AI-generated content may be incorrect. A screenshot of a computer

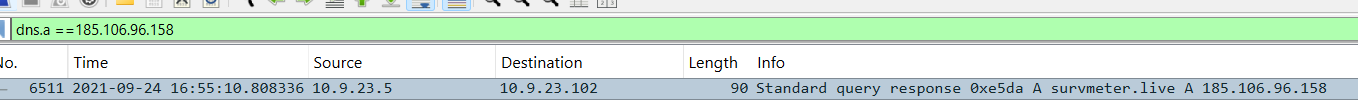
AI-generated content may be incorrect.

To investigate post-infection and C2 activity, filters such as tls.handshake.type == 1 (to find ClientHello packets) and specific time frames (frame.time >= "2021-09-24 16:45:11" && frame.time <= "2021-09-24 16:45:30") were applied to analyse encrypted HTTPS traffic, which allowed me to identify domains involved in the attack even without decrypting the payload. The "Statistics > Conversations" feature was used to identify endpoints with sustained, high-volume communication, a key indicator of Command and Control (C2) beaconing. Finally, filters for specific protocols (e.g., dns and smtp) were used to identify data exfiltration channels and credential harvesting attempts.



A screenshot of a computer

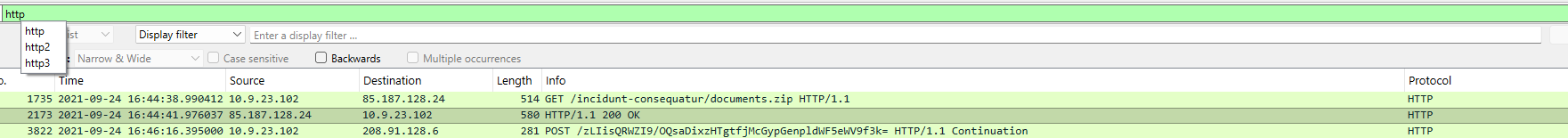
AI-generated content may be incorrect.



# Results

**Initial Infection Analysis**

The analysis successfully reconstructed a multi-stage attack, culminating in the full compromise of an internal host and attempted data exfiltration. The incident began at 2021-09-24 16:44:38 UTC when the internal host 10.9.23.102 initiated an HTTP connection to the malicious IP 85.187.128.24; the host downloaded a file named documents.zip from the domain attirenepal.com. Inside the ZIP archive was a single file, chart-1530076591.xls. This strongly implies the attack relied on a Microsoft Excel Macro as the initial execution mechanism. The serving infrastructure, LiteSpeed/7.2.34, while legitimate, was likely a compromised web server.



A screenshot of a computer program

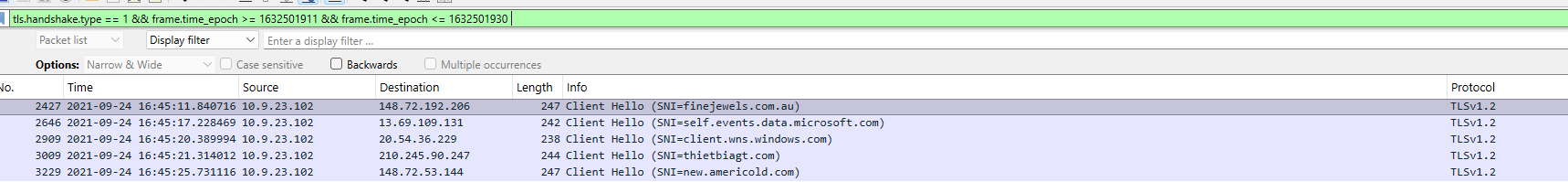
AI-generated content may be incorrect.

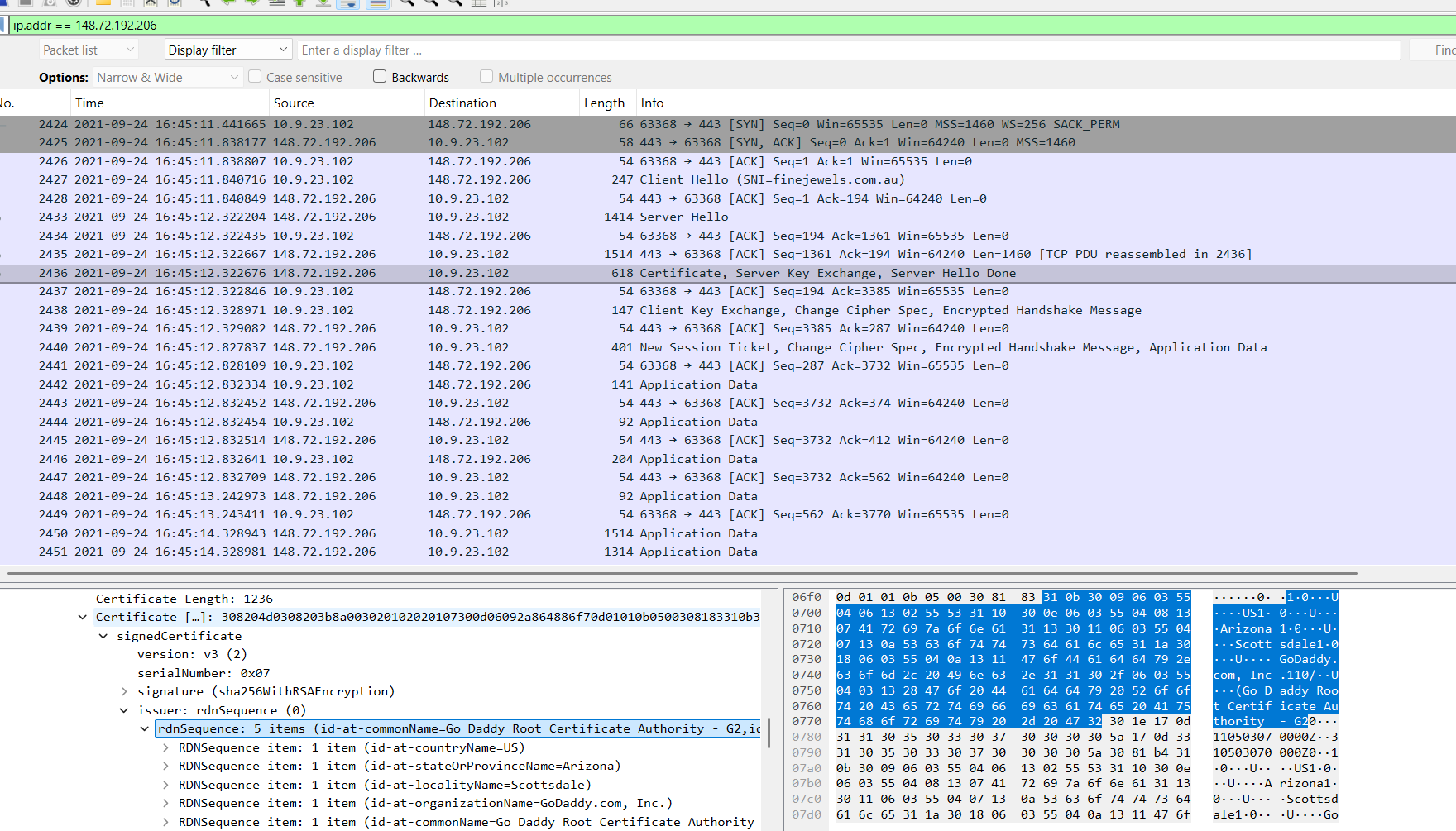


Following the initial download, the victim host immediately began communicating with other suspicious domains over HTTPS. Analysis of TLS handshakes between 16:45:11 and 16:45:30 UTC revealed connections to three additional domains: finejewels.com.au, thietbiagt.com, and new.americold.com; the SSL certificate for finejewels.com.au was issued by the GoDaddy Root Certificate Authority to evade detection by making malicious traffic appear legitimate.

A screenshot of a computer

AI-generated content may be incorrect.





**Post-Infection & C2 Beaconing Analysis**

Post-infection analysis revealed persistent beaconing to a suspicious domain. The "Statistics > Conversations" view revealed two additional external IPs, 185.106.96.158 and 185.125.204.174, exhibiting high, sustained packet counts with the victim indicating C2. The regularity of these requests, occurring at consistent intervals, is a classic sign of automated malware like Cobalt Strike Beacon, which uses these callbacks to await further instructions.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.



A screenshot of a computer

AI-generated content may be incorrect.

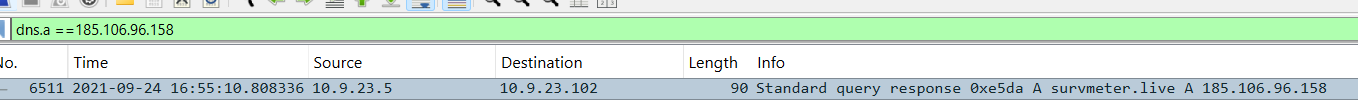
A screenshot of a computer

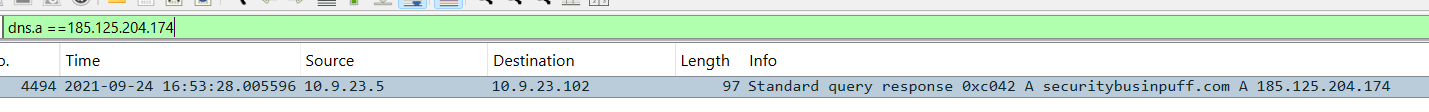
AI-generated content may be incorrect.

Traffic to the first C2 server (185.106.96.158) used the HTTP Host header ocsp.verisign.com\r\n. This is a clear attempt at domain impersonation, designed to disguise malicious C2 traffic as legitimate communication, thereby bypassing simple security controls that whitelist trusted domains. DNS analysis mapped these IPs to their domains: survmeter.live and securitybusinpuff.com.

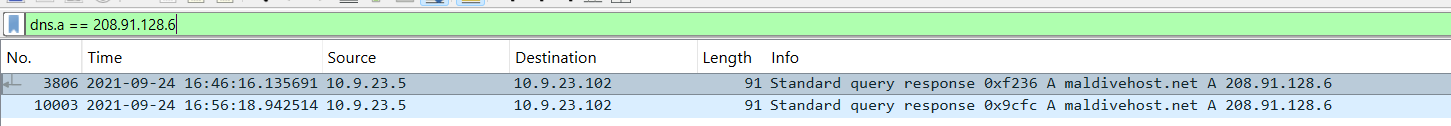
A screenshot of a computer

AI-generated content may be incorrect.





**Data Exfiltration and Reconnaissance**  
A third domain, maldivehost.net, was identified for thefrequent HTTP POST requests from the victim. This activity is characteristic of data exfiltration. The first packet sent to this server contained a 281-byte payload beginning with the unique identifier zLIisQRWZI9. This string likely represents a victim identifier or session token, allowing the attacker to correlate exfiltrated data with a specific machine. The server was running Apache/2.4.49 (cPanel), a common web hosting configuration, suggesting the attacker may have compromised a legitimate server for their exfiltration.



A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

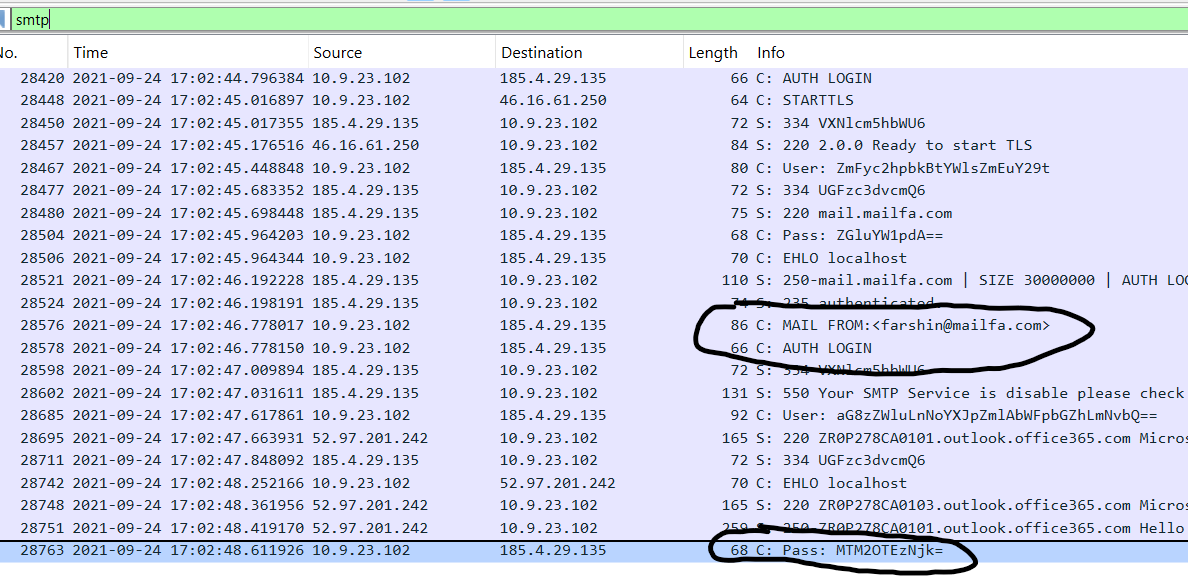
AI-generated content may be incorrect.

Further investigation revealed two critical post-compromise actions. Firstly, a DNS query to api.ipify.org was made at 2021-09-24 17:00:04. This service returns the public IP address of the requester, indicating the malware was performing environmental reconnaissance to determine the victim's external network profile, which can inform the attacker's next steps.

A screenshot of a computer

AI-generated content may be incorrect.

Secondly, SMTP traffic analysis uncovered exfiltration attempts. The attacker sent data from farshin@mailfa.com, with authentication attempts for ho3ein.sharifi@mailfa.com using the encoded password MTM2OTEzNjk= (which decodes from Base64 to 13691369). The transmission of credentials over the network suggests the malware had harvested them from the victim system and was attempting to exfiltrate them to an attacker-controlled mailbox.



A screenshot of a computer

AI-generated content may be incorrect.

# Conclusion

The investigation confirmed a multi-stage intrusion initiated when a user executed a malicious macro within chart-1530076591.xls, delivered from the compromised attirenepal.com. This characteristic Advanced Persistent Threat campaign progressed through an orchestrated sequence: retrieving secondary payloads from domains like finejewels.com.au and thietbiagt.com, establishing encrypted C2 channels with infrastructure at survmeter.live and securitybusinpuff.com, and culminating in data exfiltration via maldivehost.net and SMTP.

One of the main challenges encountered during the analysis was examining HTTPs- encrypted data, which concealed the full contents of the secondary payloads and limited visibility of certain indicators within the traffic. This necessitated a heavy reliance on behavioural analysis, including beaconing timing, TLS handshake sequences, and protocol anomalies.

To prevent recurrence, immediate measures should include user training on macro threats and blocking internet-sourced macros by default. Deploying advanced endpoint protection and network monitoring systems is also crucial to detect such behavioural patterns and block the identified IOCs, thereby containing threats before full compromise occurs.

The wider implications for an organisation include potential data breach consequences, significant operational disruption, and severe reputational damage, making proactive investment in security measures both operationally and financially imperative.

# Appendix