EX.NO: 4 Analyze the Malicious Network Traffic using Wireshark

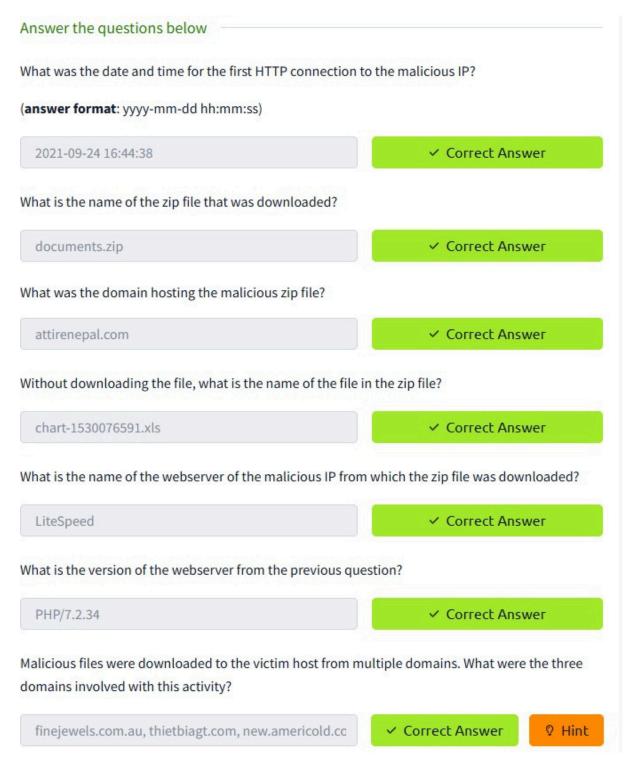
DATE: 05.03.2025

## AIM:

Applying analytical skill to analyze the malicious network traffic using wireshark.

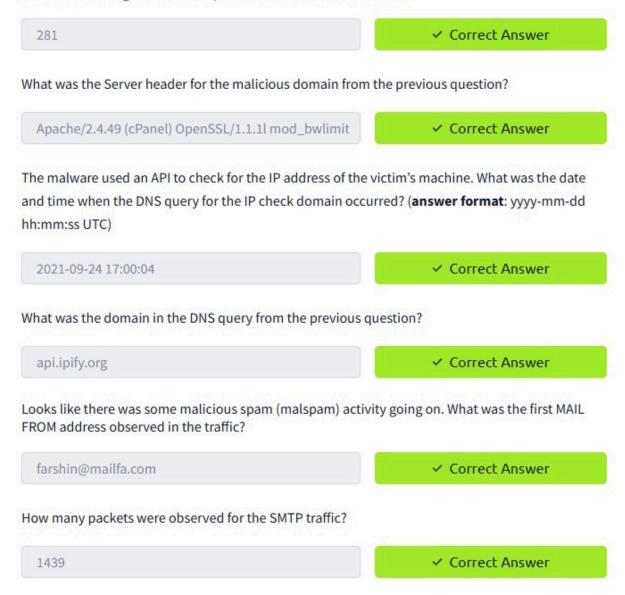


TASK 2: TRAFFIC ANALYSIS



Which certificate authority issued the SSL certificate to the first domain from the previous question? GoDaddy ✓ Correct Answer What are the two IP addresses of the Cobalt Strike servers? Use VirusTotal (the Community tab) to confirm if IPs are identified as Cobalt Strike C2 servers. (answer format: enter the IP addresses in sequential order) ∩ Hint ✓ Correct Answer 185.106.96.158, 185.125.204.174 What is the Host header for the first Cobalt Strike IP address from the previous question? ocsp.verisign.com ✓ Correct Answer What is the domain name for the first IP address of the Cobalt Strike server? You may use VirusTotal to confirm if it's the Cobalt Strike server (check the Community tab). survmeter.live ✓ Correct Answer 9 Hint What is the domain name of the second Cobalt Strike server IP? You may use VirusTotal to confirm if it's the Cobalt Strike server (check the Community tab). securitybusinpuff.com ✓ Correct Answer 9 Hint What is the domain name of the post-infection traffic? ✓ Correct Answer maldivehost.net What are the first eleven characters that the victim host sends out to the malicious domain involved in the post-infection traffic? zLlisQRWZI9 ✓ Correct Answer

What was the length for the first packet sent out to the C2 server?



## CONCLUSION:

Tryhackme platform Analyze the Malicious Network Traffic using Wireshark task is successfully completed.