TryHackMe: Carnage

Write-Up

Pavel Pecheniuk

1. Introduction

In the Carnage challenge by THM, one is offered to apply the analytical skills to analyse the malicious network traffic using Wireshark, a well-known tool used for network traffic analysis.

2. Scenario

Eric Fischer from the Purchasing Department at Bartell Ltd has received an email from a known contact with a Word document attachment. Upon opening the document, he accidentally clicked on "Enable Content." The SOC Department immediately received an alert from the endpoint agent that Eric's workstation was making suspicious connections outbound. The pcap was retrieved from the network sensor and handed to me for analysis.

Task: Investigate the packet capture and uncover the malicious activities.

*Credit goes to Brad Duncan for capturing the traffic and sharing the pcap packet capture with InfoSec community.

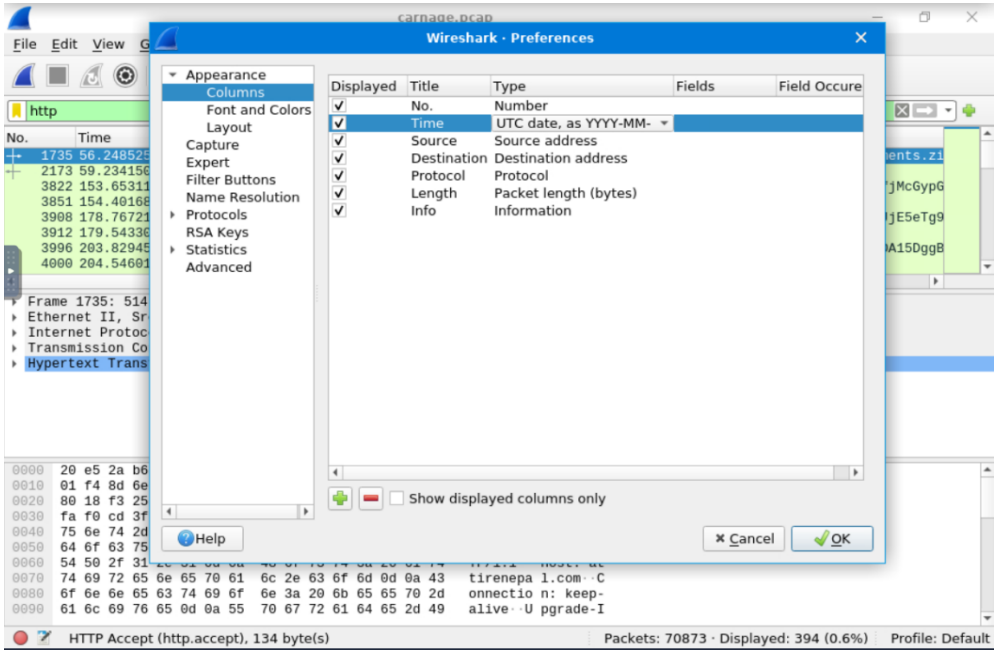
NOTE: DO NOT directly interact with any domains and IP addresses in this challenge.

3. Traffic Analysis

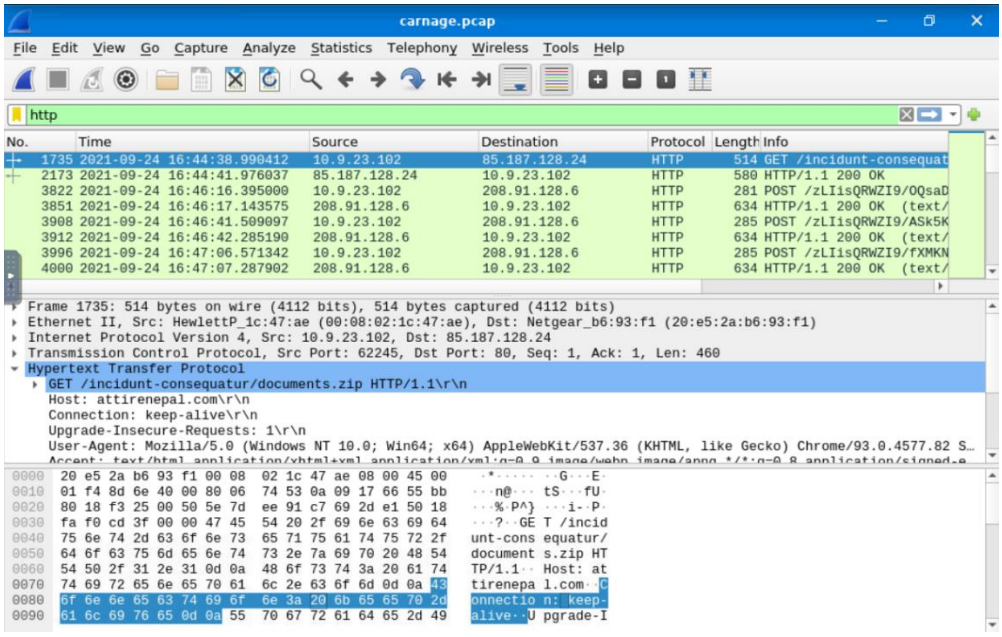
What was the date and time for the first HTTP connection to the malicious IP? (answer format: yyyy-mm-dd hh:mm:ss)

Firstly, HTTP traffic is a traffic of interest, so let's set the filter "http" to print out only HTTP packets.

Then one can observe inappropriate timing format. Configuration of the right time format is done via *Edit > Preferences > Columns > Time > UTC date, as YYYY-MM-DD, and time > OK*.



Finally, the needed result is obtained.



Answer: 2021-09-24 16:44:38

What is the name of the zip file that was downloaded?

Answer to this question can be found on the second screenshot from the previous task. One can analyse the first HTTP packet and obtain the name of a zip file.

Answer: documents.zip

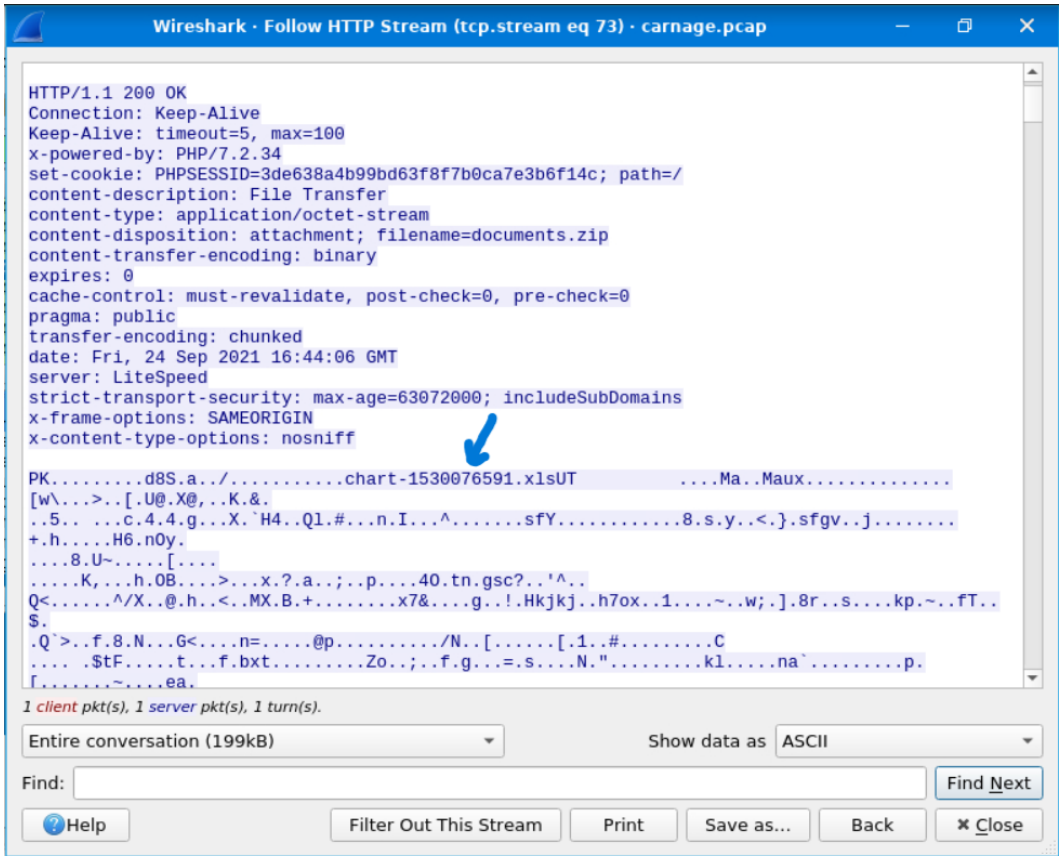
What was the domain hosting the malicious zip file?

Answer can be found again on the second screenshot from the first task. The name of the malicious domain is located under the field “Host”.

Answer: attirenepal.com

Without downloading the file, what is the name of the file in the zip file?

Let’s investigate this HTTP frame to gain the needed information by right-clicking the frame and select *Follow* > *Follow HTTP Stream*. Here is the result containing more useful information, including the needed name.



Answer: chart-1530076591.xls

What is the name of the webserver of the malicious IP from which the zip file was downloaded? What is the version of the webserver from the previous question?

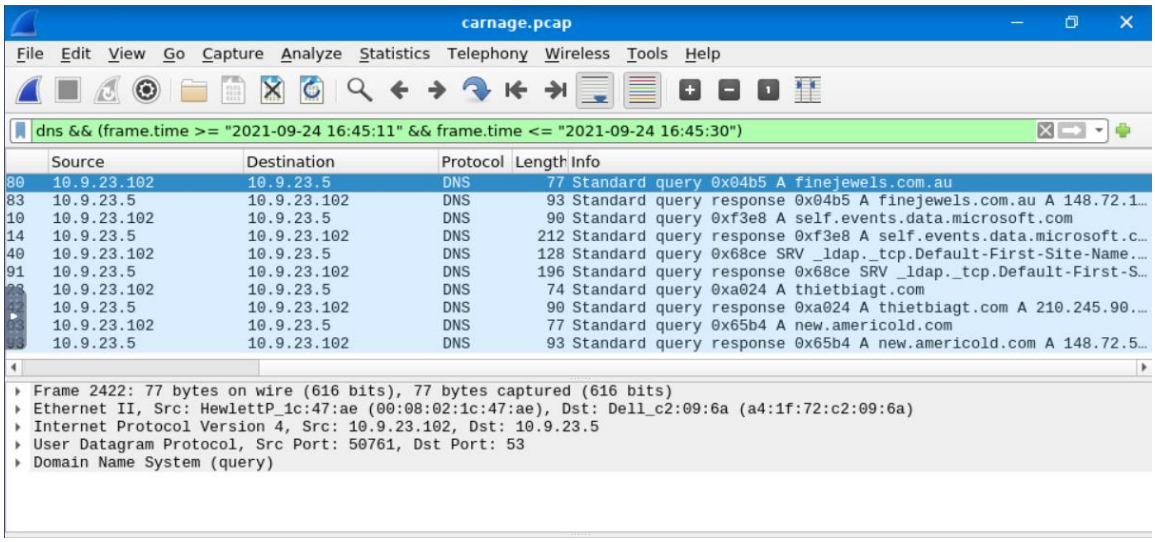
Let's examine the screenshot from the previous task. Answers can be found under the fields "Server" and "x-powered-by" correspondingly.

Answers: LiteSpeed, PHP/7.2.34

Malicious files were downloaded to the victim host from multiple domains. What were the three domains involved with this activity?

Let's examine DNS traffic to solve this task by applying dns as the filtering command. THM provides a query: Narrow down the timeframe from 16:45:11 to 16:45:30. Taking it into account, so the updated filter would be:

dns && (frame.time >= "2021–09–24 16:45:11" && frame.time <= "2021–09–24 16:45:30")

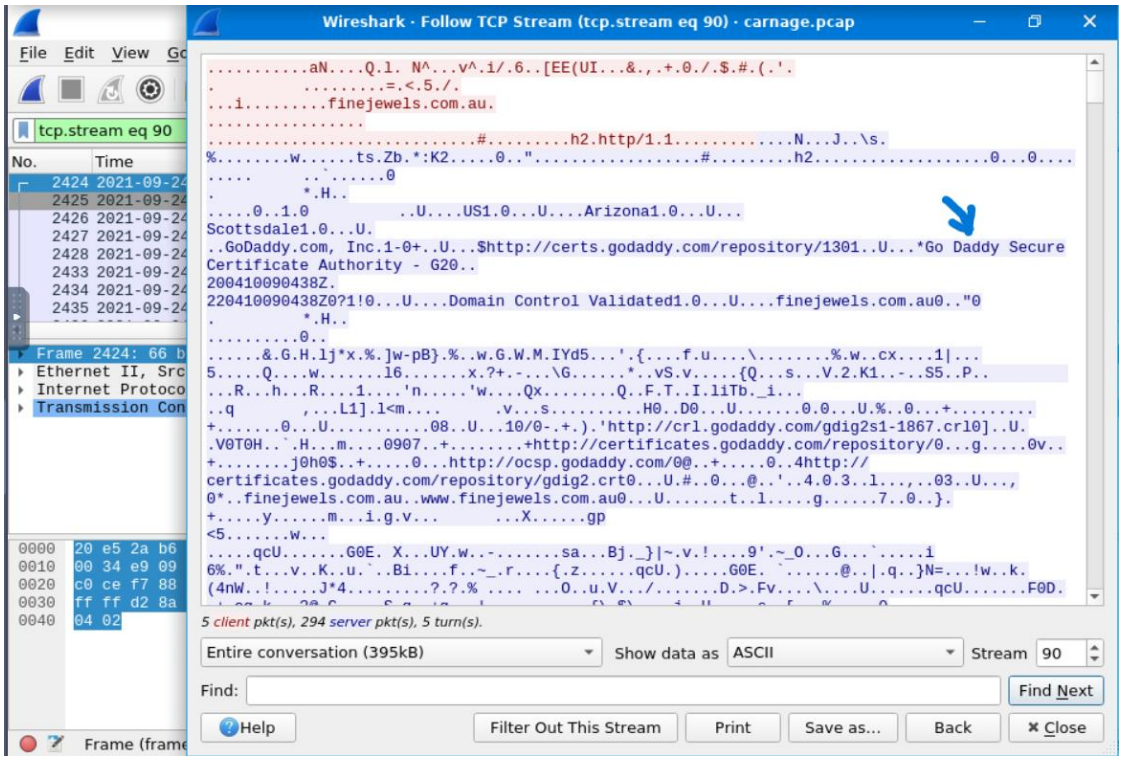


The output provides a list of the malicious domains participated in the files exchange process with the victim host.

Answer: finejewels.com.au, thietbiagt.com, new.americold.com

Which certificate authority issued the SSL certificate to the first domain from the previous question?

Answer to this question can be obtained by following the TCP stream, done via *Follow > Follow TCP Stream*.

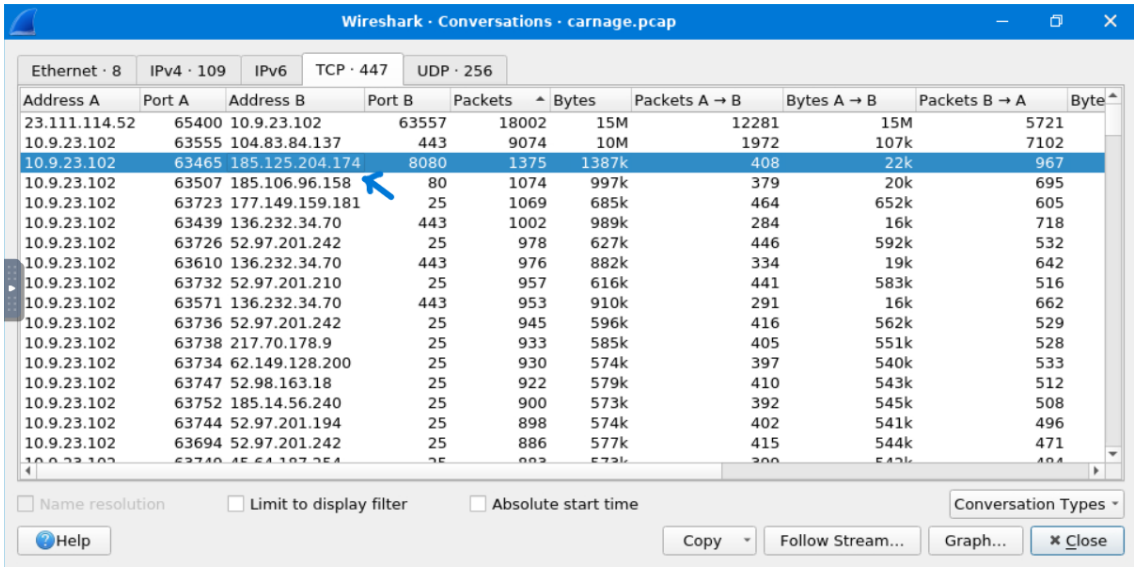


Answer: GoDaddy

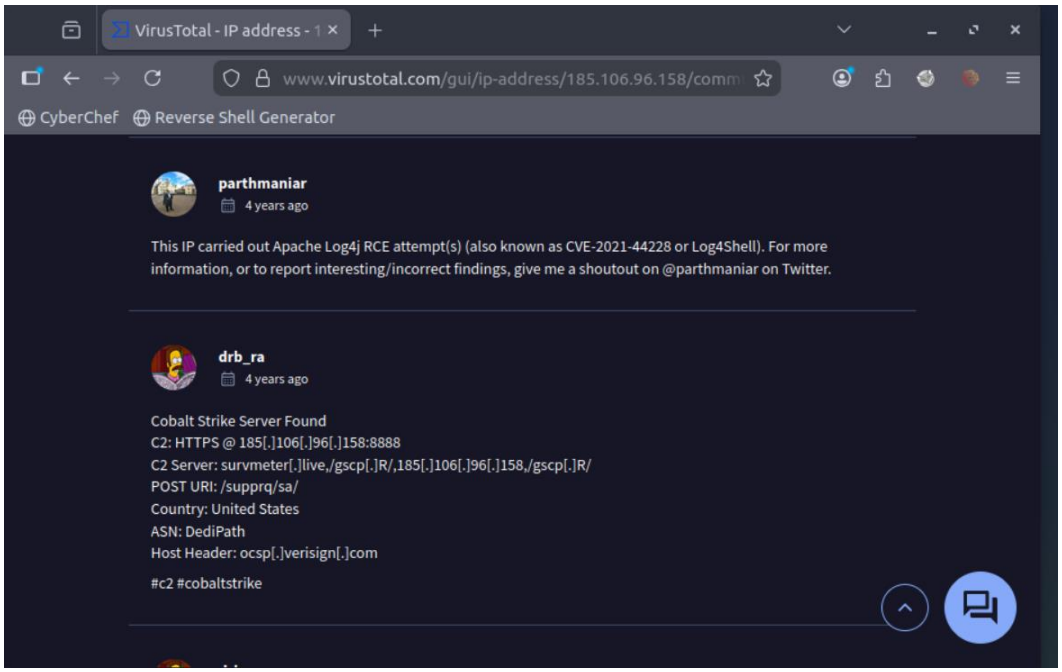
What are the two IP addresses of the Cobalt Strike servers? Use VirusTotal (the Community tab) to confirm if IPs are identified as Cobalt Strike C2 servers.

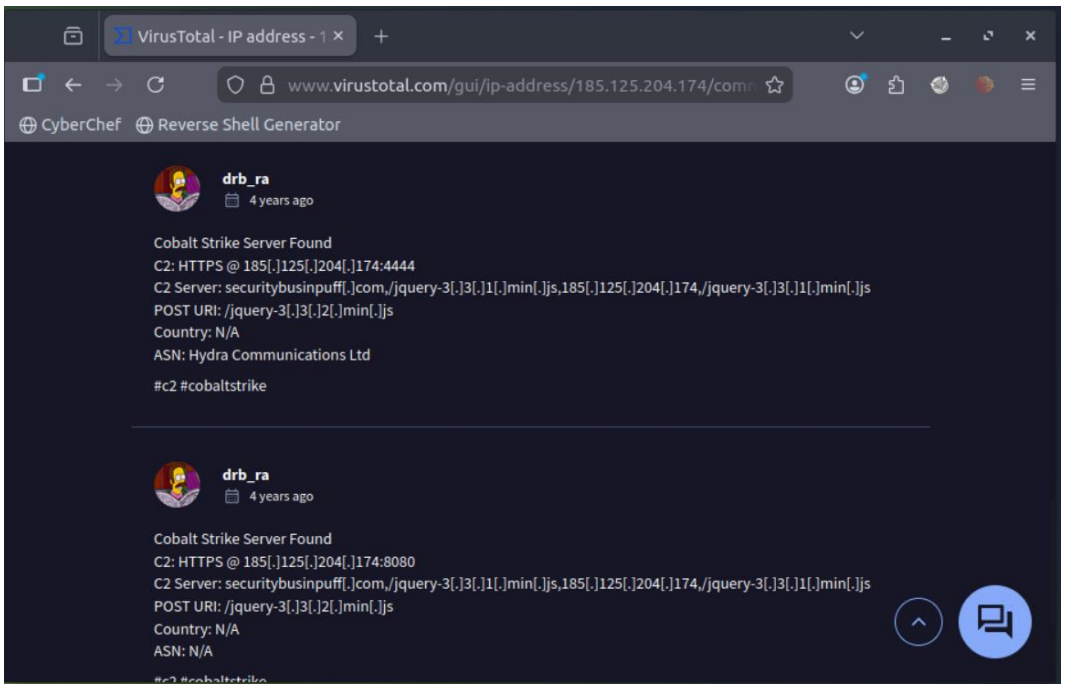
Solving this task requires some statistics collection and analysis. To conduct it, one clicks the tab *Statistics* found in the menu bar, then selects *Conversations*. Let's filter these addresses list by *TCP* and order results by column *Packets*.

After a research, one obtains the needed IP addresses.



VirusTotal and the Community tab confirm these are Cobalt Strike C2 servers' addresses:

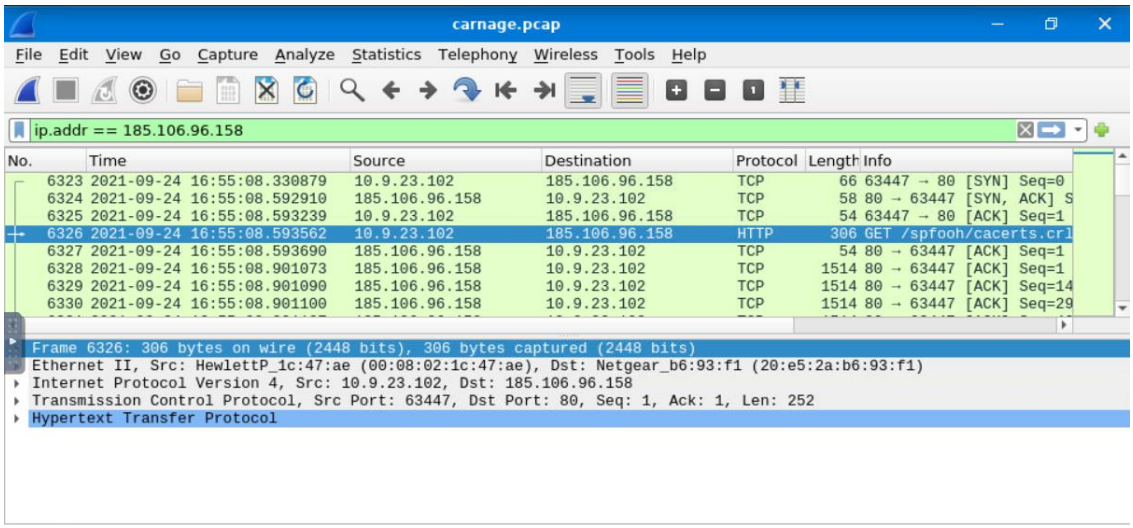




Answer: 185.106.96.158, 185.125.204.174

What is the Host header for the first Cobalt Strike IP address from the previous question?

Now the IP address 185.106.96.158 is known. Let's find the address-related traffic by entering a filtering query *ip.addr == 185.106.96.158*. One is interested in GET methods.

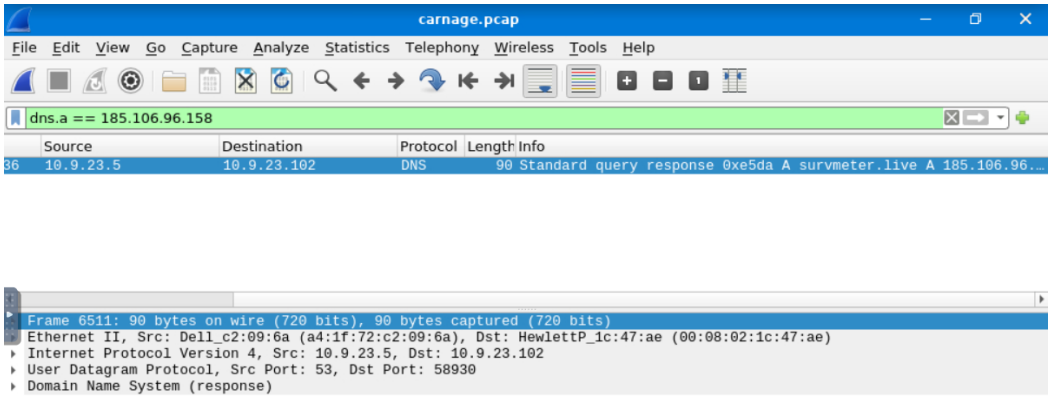


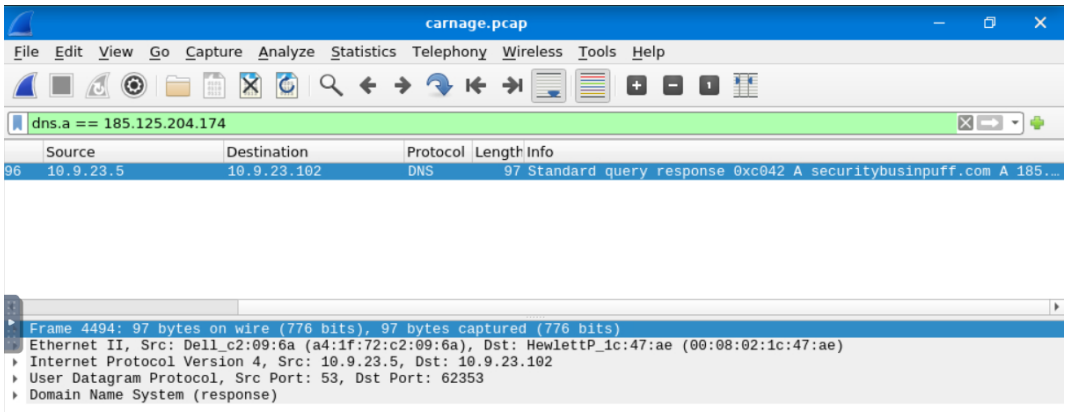
Let's follow its HTTP Stream. The host header is found under the respective field.

Answer: ocsp.verisign.com

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). What is the domain name of the second Cobalt Strike server IP?

There is a hint by THM: Filter out the DNS queries. Let's print out DNS queries for the given addresses by applying the command *dns.a == 185.106.96.158* and *dns.a == 185.125.204.174*:



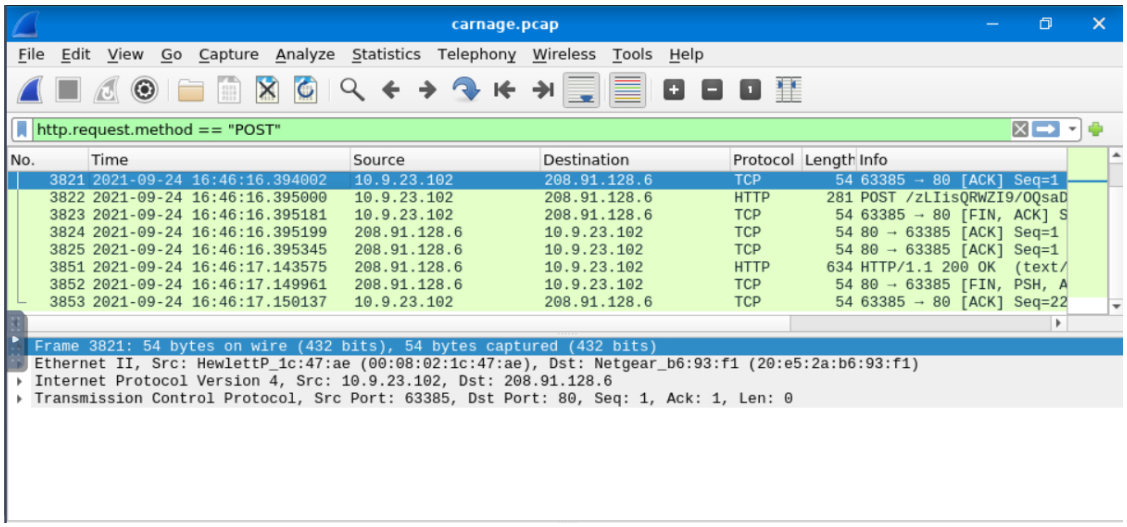


The Info tab discloses the domain names. Taking a look on the re-used screenshots from VirusTotal confirms the findings.

Answers: survmeter.live, securitybusinpuff.com

What is the domain name of the post-infection traffic?

Here THM gives a hint to filter Post HTTP traffic. Applying the filter *http.request.method = "POST"* allows to achieve it.



Following HTTP Stream on the HTTP Post frame 3822 and finding the needed domain name under "Host" field:

Answer: maldivehost.net

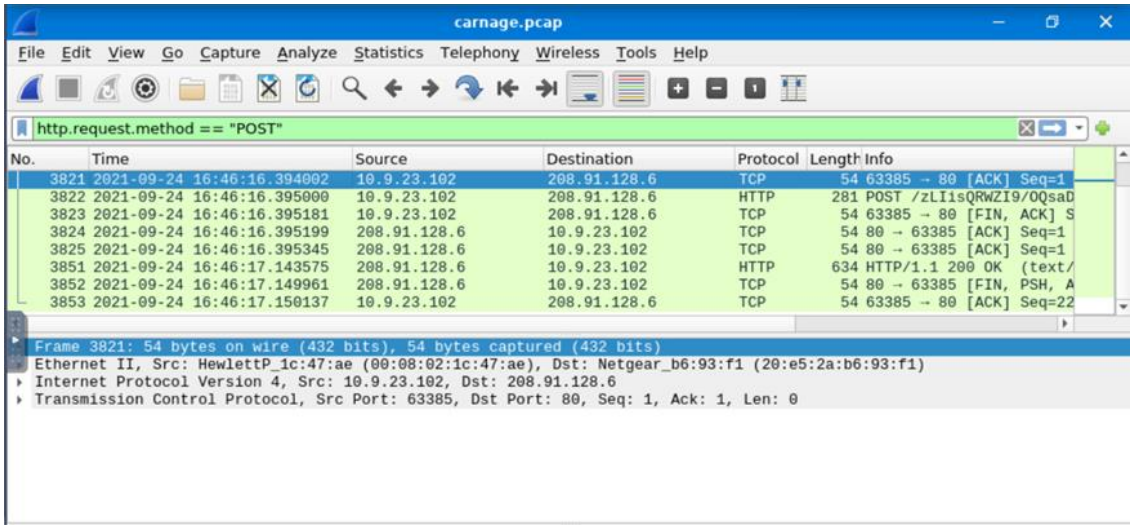
What are the first eleven characters that the victim host sends out to the malicious domain involved in the post-infection traffic?

Here one can filter traffic by the malicious domain maldivehost.net from the previous task and reliably obtain the sent characters. Another approach is to simply analyse the sequence of characters which one finds in the followed HTTP Stream for the same frame (the previous screenshot), and subtract the first eleven symbols. It worked for this task.

Answer: zLIisQRWZI9

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

Let's get back to the screenshot with the filtered HTTP Post traffic. Take another look at the first POST packet and observe the value under the column "Length", which is the answer to the question.



Answer: 281

What was the Server header for the malicious domain from the previous question?

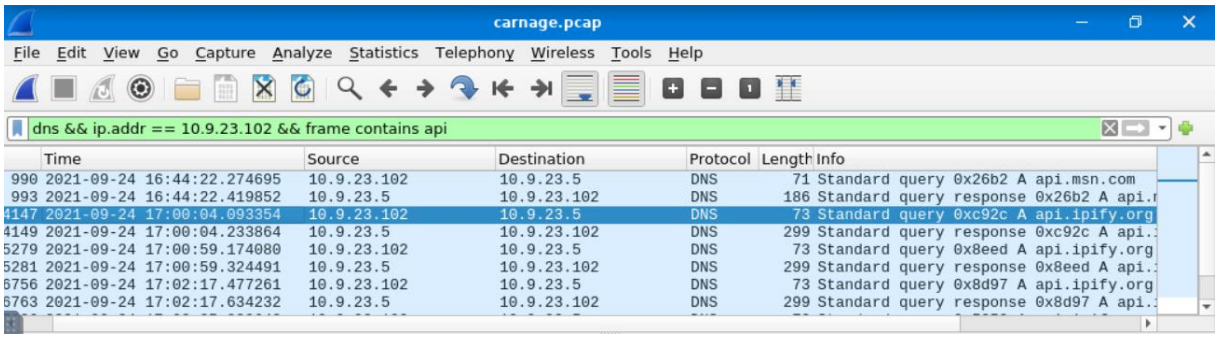
The answer is located under the "Server" field.

Answer: Apache/2.4.49 (cPanel) OpenSSL/1.1.1l mod_bwlimited/1.4

The malware used an API to check for the IP address of the victim's machine. What was the date and time when the DNS query for the IP check domain occurred? (answer format: yyyy-mm-dd hh:mm:ss UTC)

The IP address of the victim's machine is 10.9.23.102. Let's search for the DNS queries related to the given IP address and find the traffic that includes the usage of API. Applied filter is:

dns && ip.addr = = 10.9.23.102 && frame contains api



Answer: 2021-09-24 17:00:04

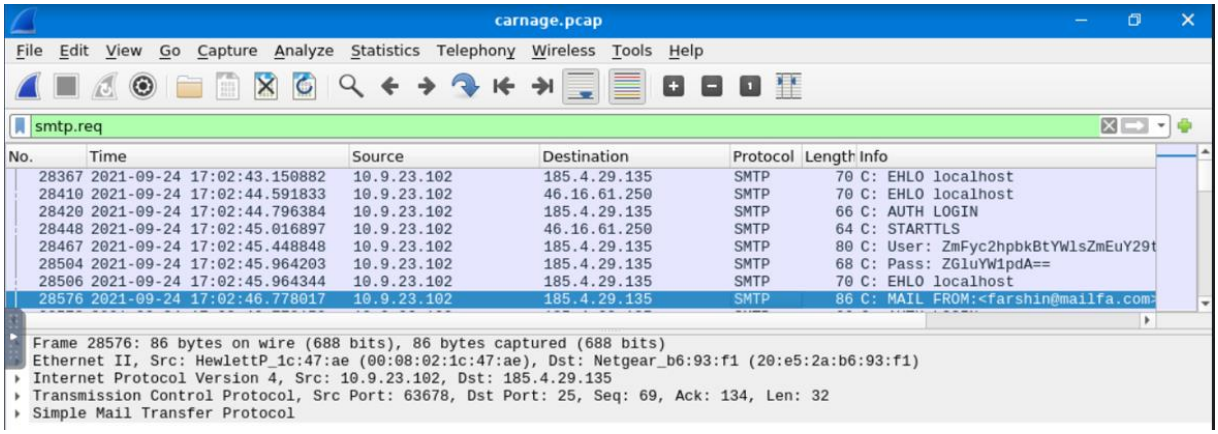
What was the domain in the DNS query from the previous question?

The Info tab discloses the needed domain in the query.

Answer: api.ipify.org

Looks like there was some malicious spam (malspam) activity going on. What was the first MAIL FROM address observed in the traffic?

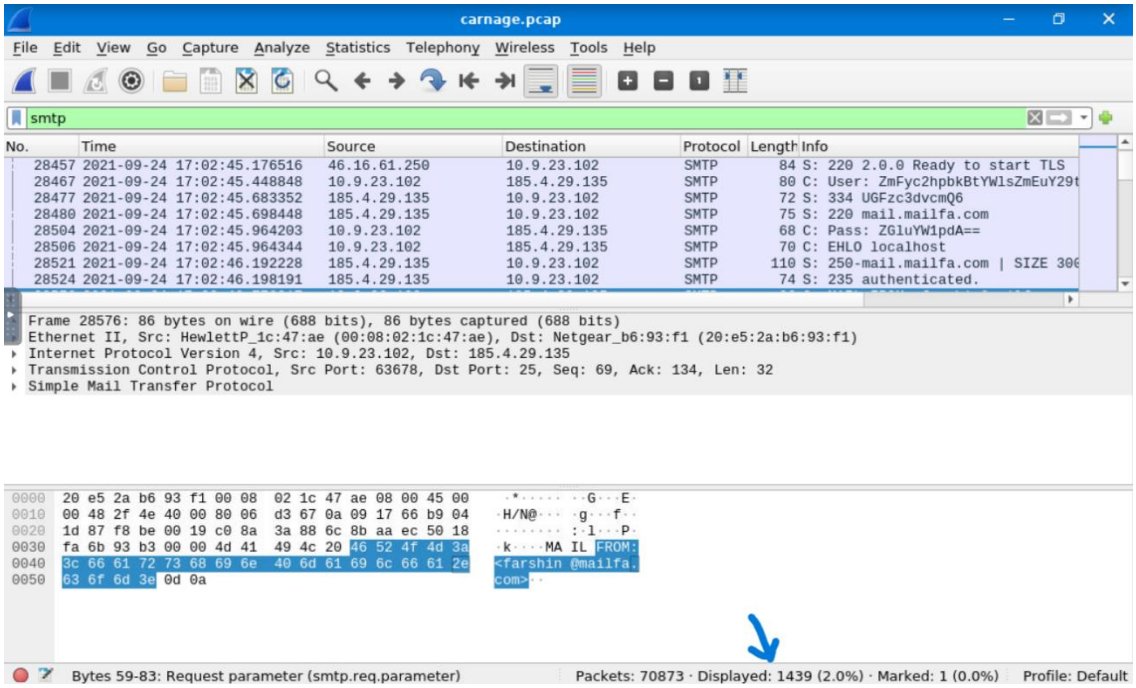
The MAIL FROM parameter implies the outgoing traffic, so let's analyse traffic related to the requests and email transfer protocol SMTP by applying filter *smtp.req* and observe the first address containing MAIL FROM:



Answer: farshin@mailfa.com

How many packets were observed for the SMTP traffic?

Let's filter out only SMTP traffic and make use of the built-in functionality of Wireshark, specifically the displayed packets' counter located at the very down:



Answer: 1439

4. Summary

This write-up documents the completion of the Carnage room from TryHackMe. During this challenge I practiced my analytical skills, explored the functionality and usefulness of Wireshark for the network traffic analysis, and put myself into shoes of a network security analyst.

Thank you for your attention!