### **CARNAGE — TryHackMe**

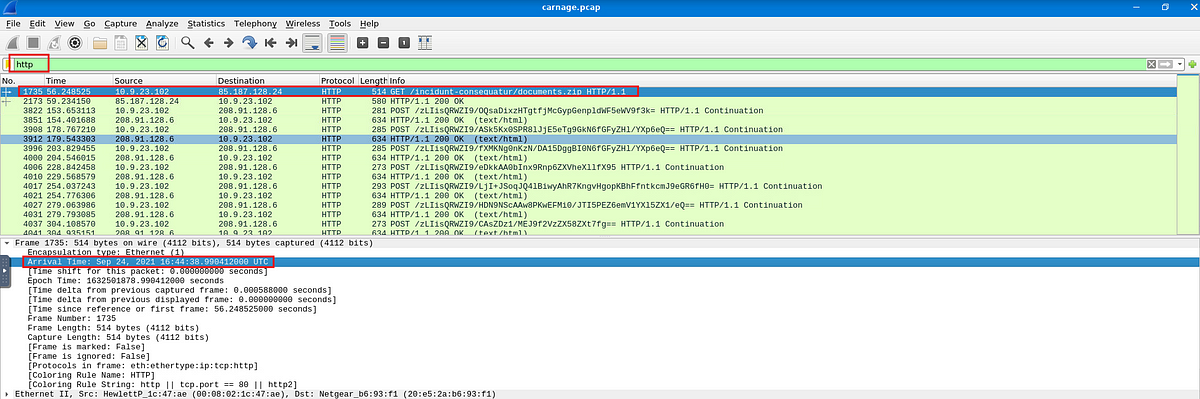
Scenario: Eric Fischer from the Purchasing Department at Bartell Ltd has received an email from a known contact with a Word document attachment. Upon opening the document, he accidentally clicked on “Enable Content.” The SOC Department immediately received an alert from the endpoint agent that Eric’s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

Start the machine, and open the pcap file in wireshark.

Tasks:

1. What was the date and time for the first HTTP connection to the malicious IP?

To find this, we will filter the http traffic and select the first packet and then check the Frame data which contains the exact date and time of the packet.

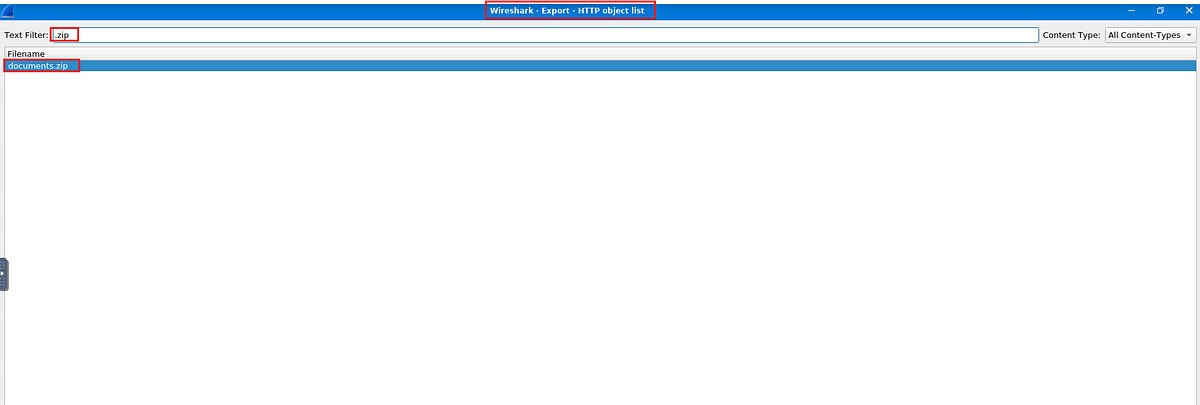


Answer: 2021–09–24 16:44:38

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

To find this we can check for the HTTP objects. Go to File -> Export Objects -> HTTP

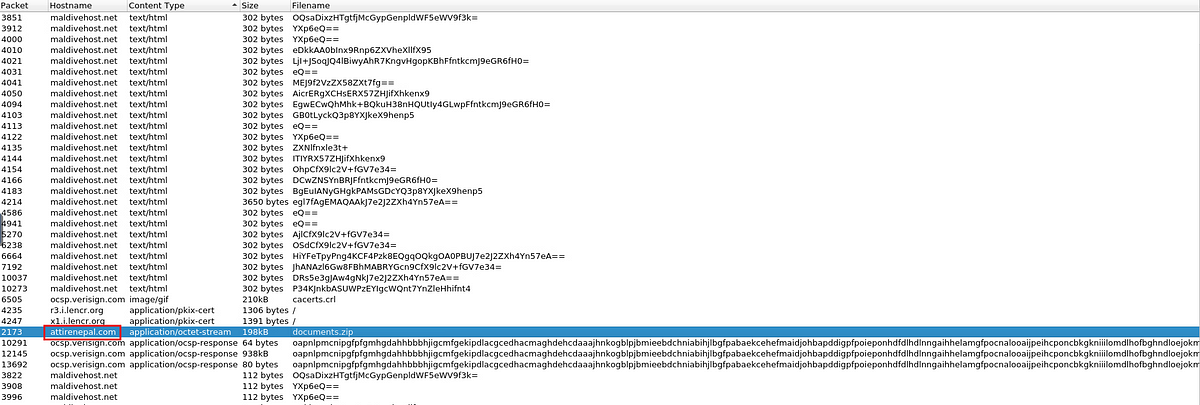
Then in the top filter bar type in “.zip”, we can see the only zip file.



Answer: documents.zip

3. What was the domain hosting the malicious zip file?

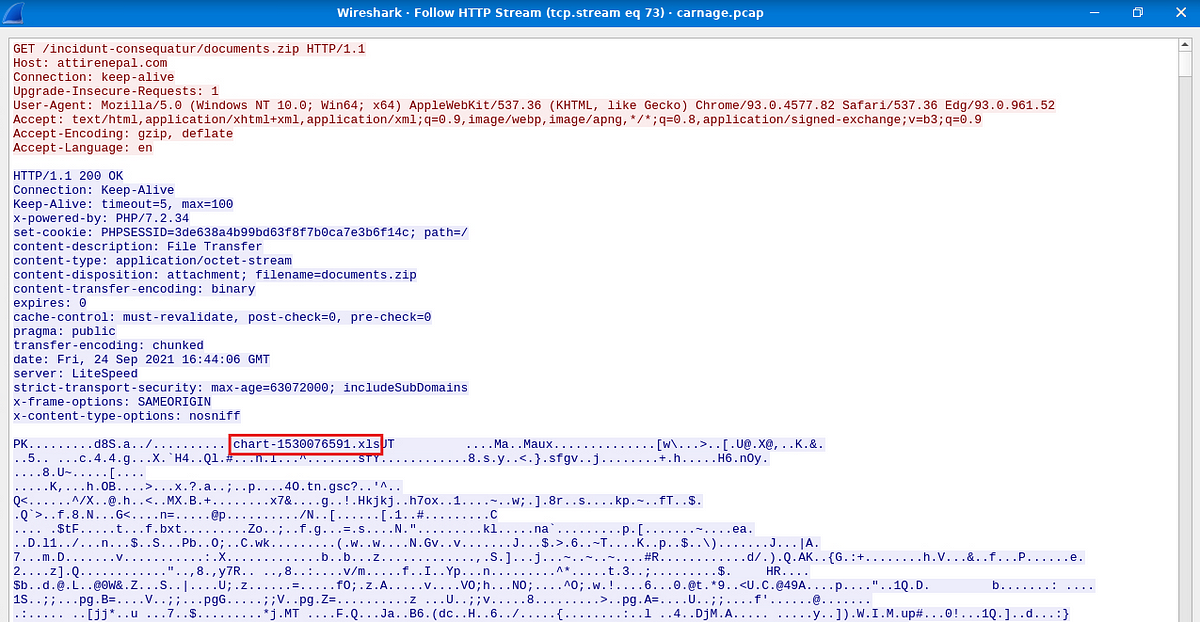
Under the same window, we can see the domain from which this file was downloaded, under the Hostname field.



Answer: attirenepal.com

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

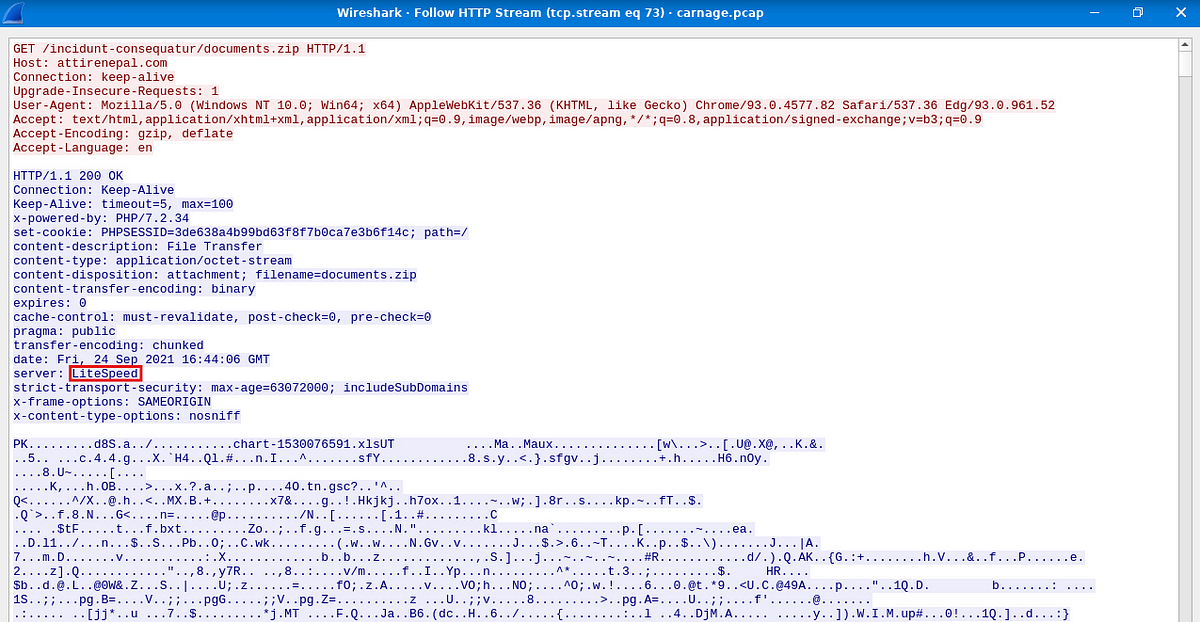
To check the filename inside the zip without downloading the file, we can locate the actual get request from which the zip file was downloaded, and then right click on it and select follow http stream.



Answer: chart-1530076591.xls

5. What is the name of the webserver of the malicious IP from which the zip file was downloaded?

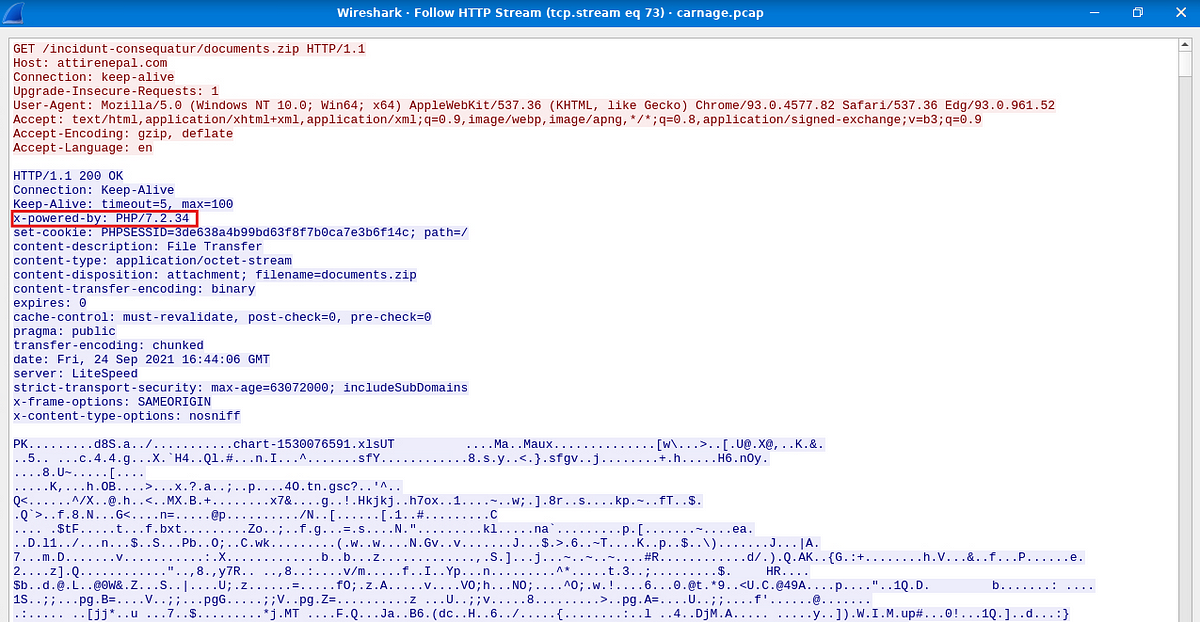
The server name of the IP address can also be found in the HTTP stream, under the http response header.



Answer: LiteSpeed

6. What is the version of the webserver from the previous question?

This also can be found under the http response header in the field x-powered-by.



Answer: PHP/7.2.34

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

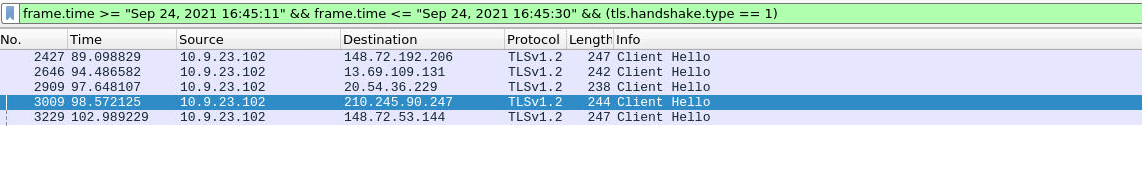
For this, I had to look at the hint. As per the hint, we should be looking at http traffic within a specific time range which is 16:45:11 to 16:45:30.

So I used the following filter

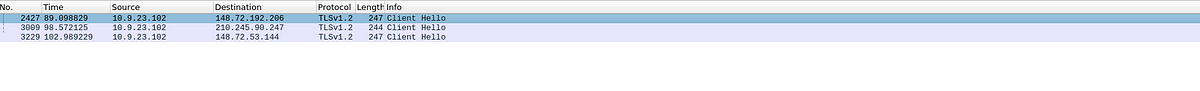
frame.time >= “Sep 24, 2021 16:45:11” && frame.time <= “Sep 24, 2021 16:45:30” && (tls.handshake.type == 1)

**frame.time >= “Sep 24, 2021 16:45:11” && frame.time <= “Sep 24, 2021 16:45:30” :** this part specifies the time range

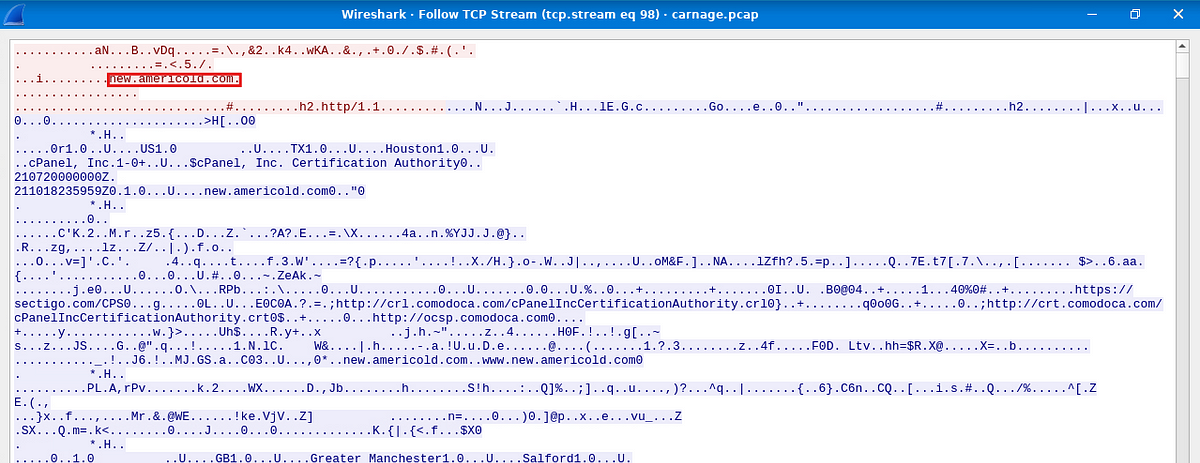
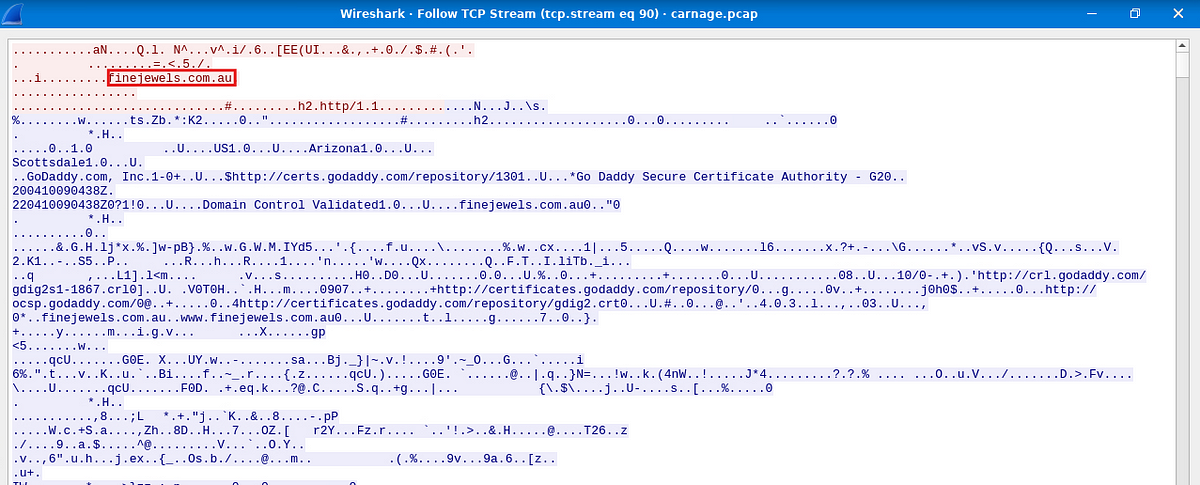
**tls.handshake.type == 1**: This part will specifically display the client hello messages. The client hello message displays the domain name or the host name in plain text.



We got 5 packets, but after examining the packets we can rule out two of these packets as they were legitimate domains belonging to Microsoft. We are now left with three packets.



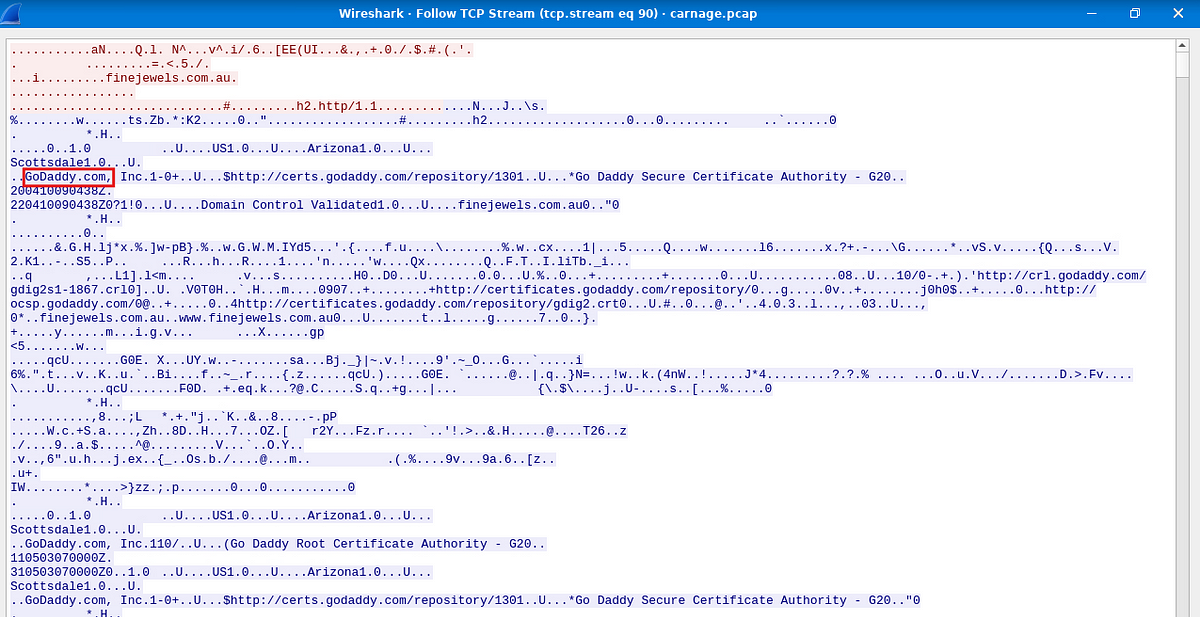
If we follow the tcp stream on these packets, we can see our required domains.



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

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

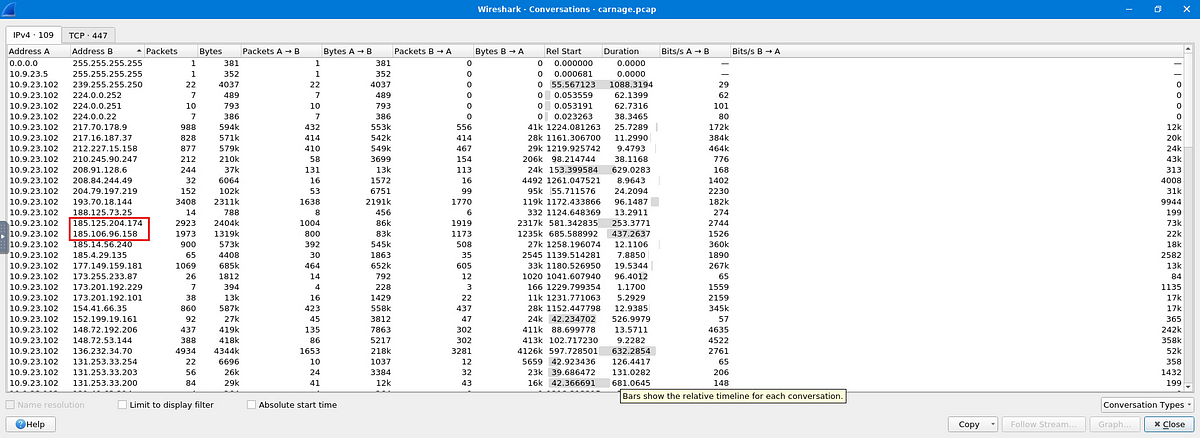
The answer to this is visible in the domain-1 screenshot provided above



Answer: Godaddy.com

8. 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)

I had no idea how to find this out, the hint says to look at the conversations filter, so I had to look at each of the IP and at last I found the 2 IP’s



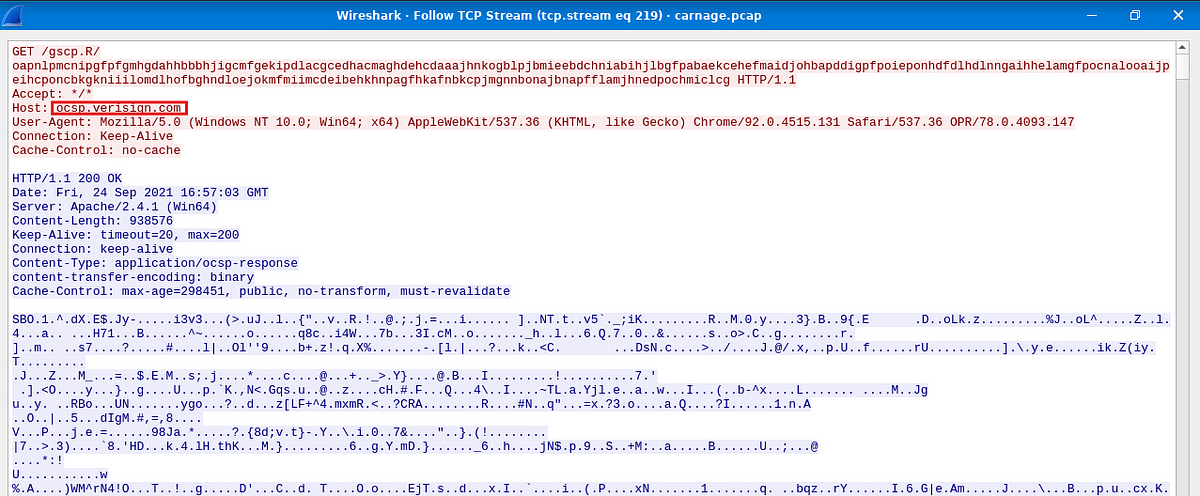
Answer: 185.106.96.158, 185.125.204.174

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

Check for the traffic belonging to the Ip address using the filter

ip.addr ==185.106.96.158

Then follow stream on any packet and we can find the host.

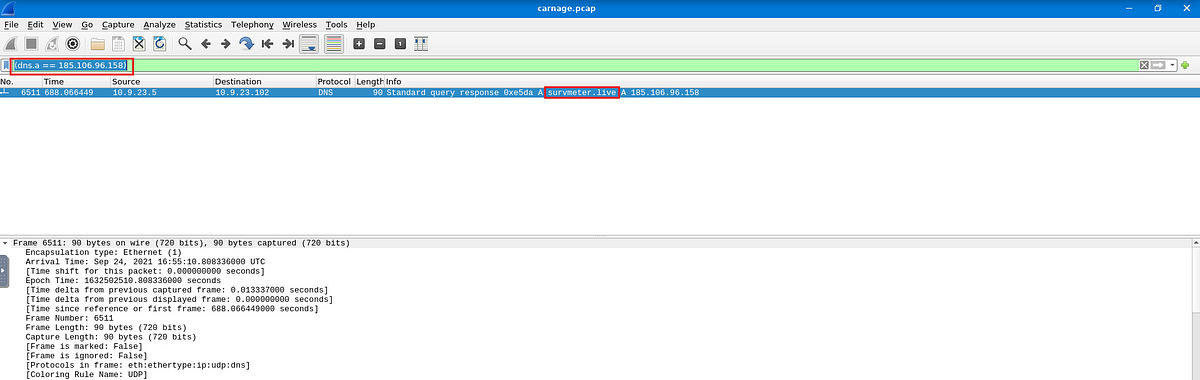


Answer: ocsp.verisign.com

10. 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).

I filtered out the dns records using the given IP address, and found out the domain.

Filter: dns.a == 185.106.96.158



Answer: survmeter.live

10. 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).

The same can be used to find the answer for this.

Answer: securitybusinpuff.com

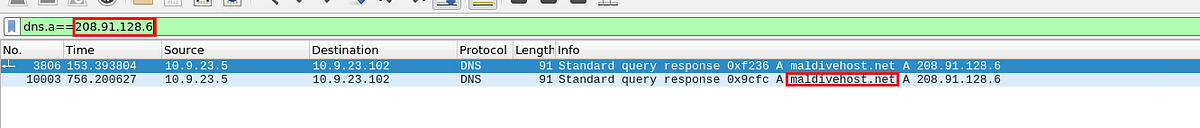
11. What is the domain name of the post-infection traffic?

I filtered out the http POST requests and there was only one other IP present other than the two C2 server IP’s.

Filter: http.request.method == POST



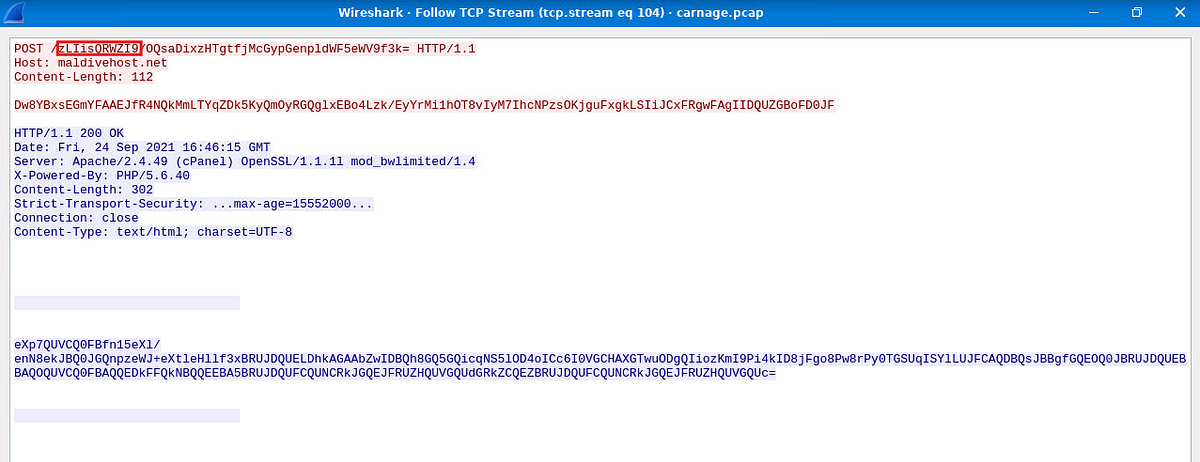
Then I checked the DNS record of the IP address similar to the previous two questions.



Answer: maldivehost.net

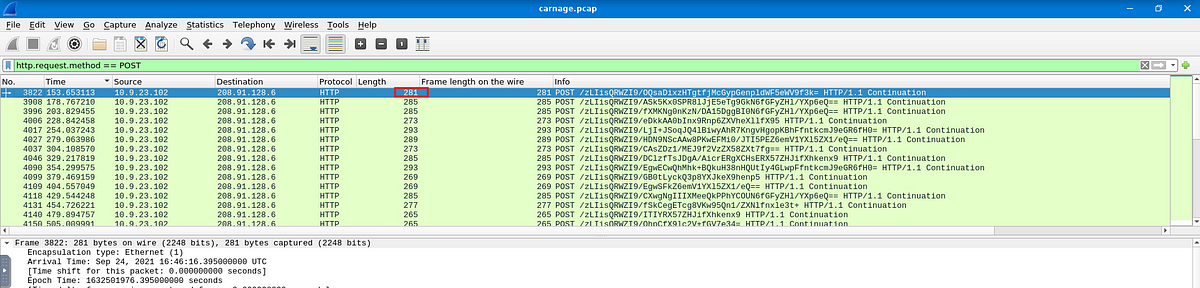
12. What are the first eleven characters that the victim host sends out to the malicious domain involved in the post-infection traffic?

Follow stream on any packet to the 208.91.128.6 Ip address, and copy the first 11 characters of the http request.



Answer: zLIisQRWZI9

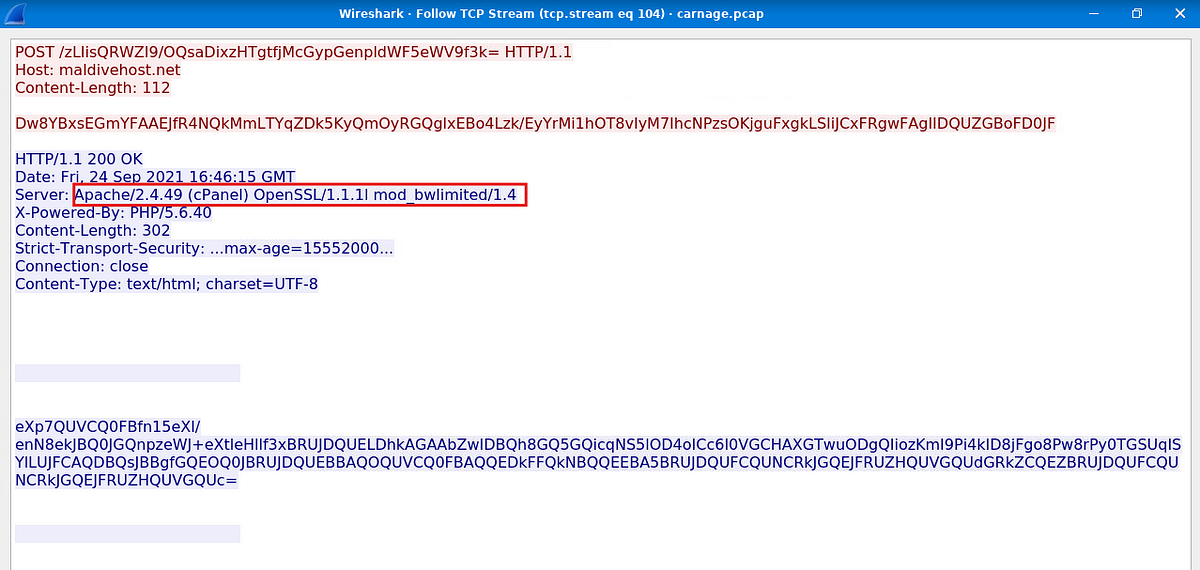
13: What was the length for the first packet sent out to the C2 server?



Answer: 281

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

Again, follow TCP stream on the packet and we can find the server header in the http response.

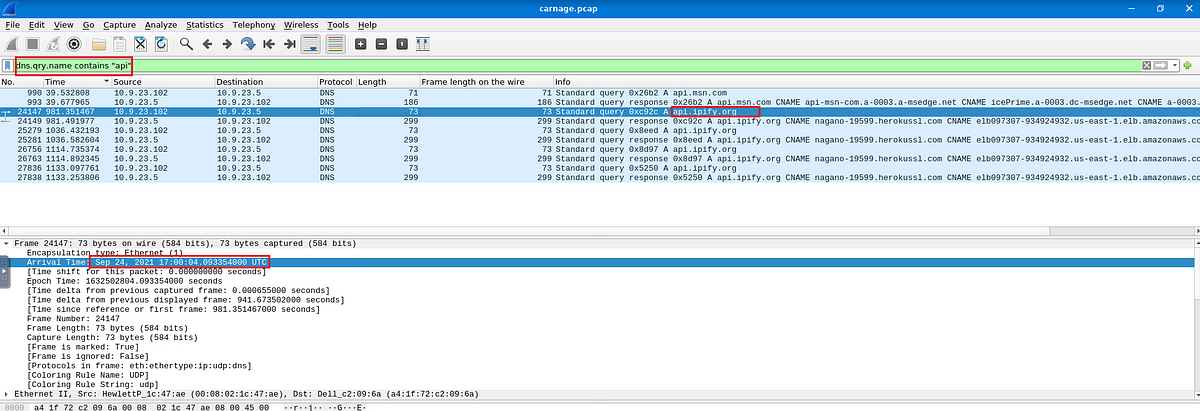


Answer: Apache/2.4.49 (cPanel) OpenSSL/1.1.1l mod\_bwlimited/1.4

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

For this, we will check for the dns records which contain api in their query.

Filter: dns.qry.name contains “api”



Answer: 2021–09–24 17:00:04

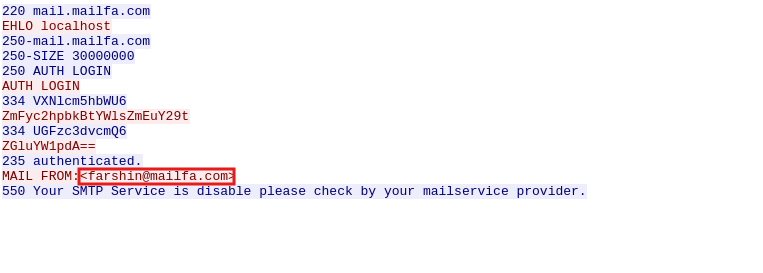
16. What was the domain in the DNS query from the previous question?

This is also visible in the above screenshot.

Answer: api.ipify.org

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

Let us check the smtp traffic, specifically directed towards the victim machine. If we check out the packets we can see a message saying “Your SMTP Service is disable please check by your mailservice provider”. If we check the sender of this mail we can see it is farshin@mailfa.com.



But, the domain used by the victim is different, hence this is the mail address responsible for spam.

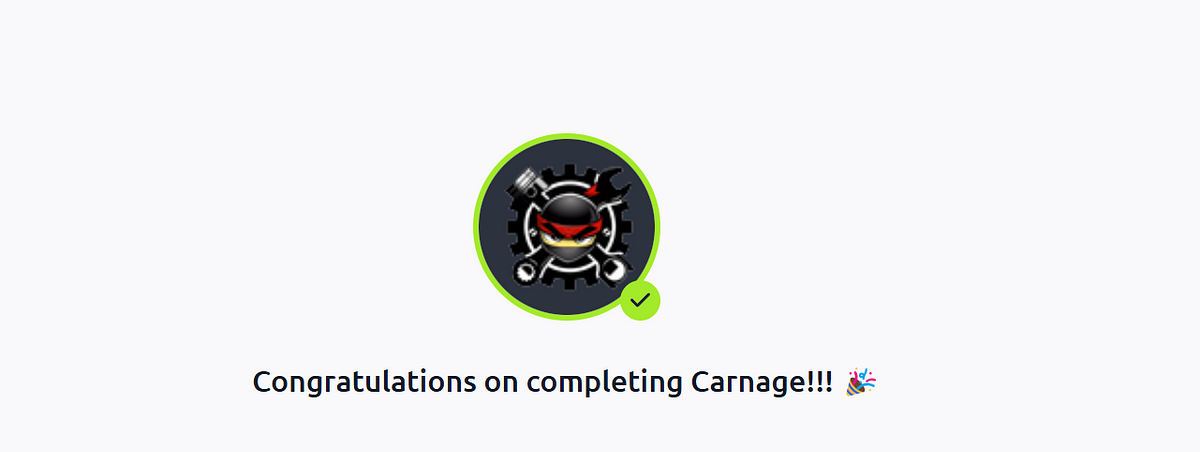
Answer: farshin@mailfa.com

How many packets were observed for the SMTPtraffic?

We can check the statistics -> Protocol Hierarchy for the answer to this question.



Answer: 1439



This is the end of the walkthrough.