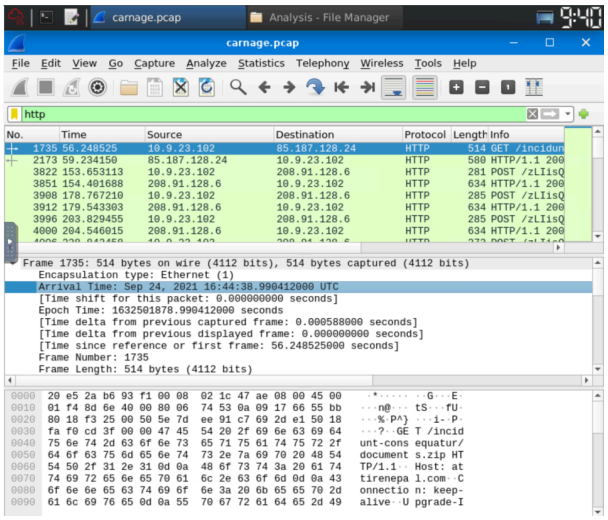
CARNAGE

>> Deploy the machine

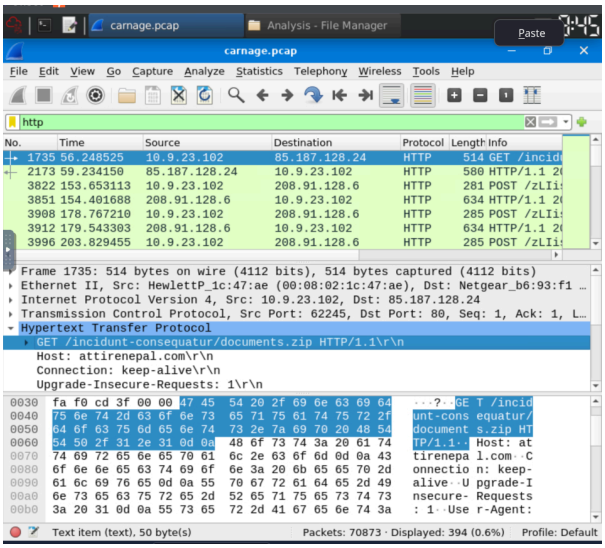
>> Open the analysis file in wireshark

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



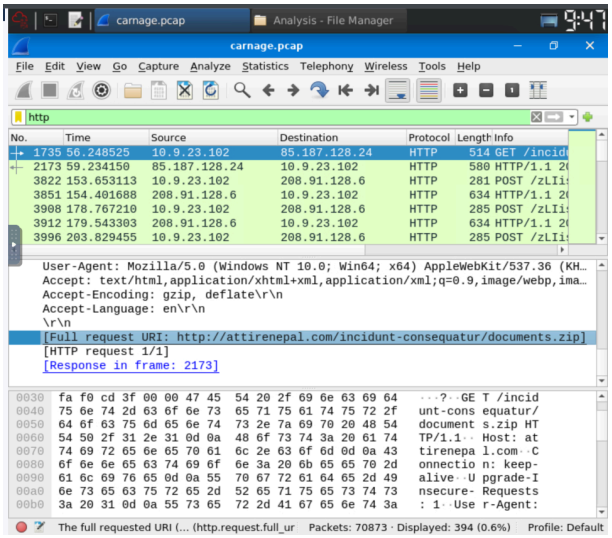
ANS :- 2021-09-24 16:44:38

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



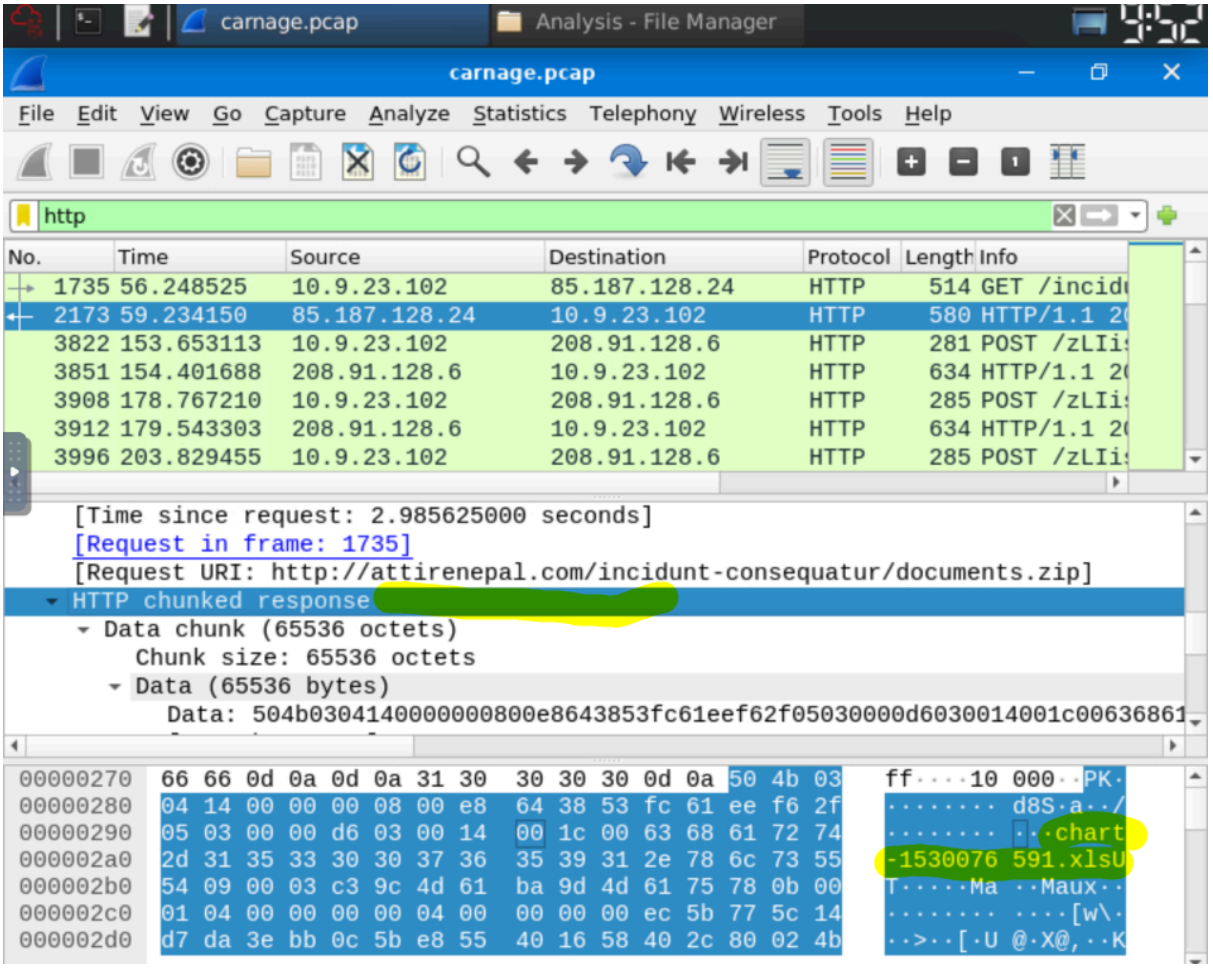
ANS :- document.zip

QUE 3 ; What was the domain hosting the malicious zip file?



ANS :- attirenepal.com

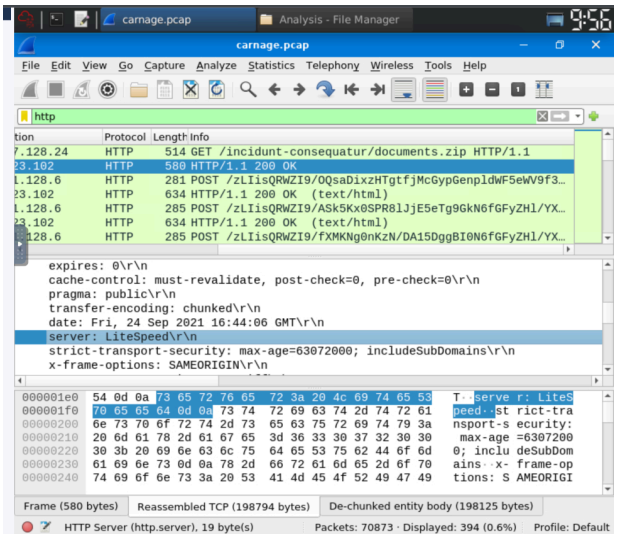
QUE 4; Without downloading the file, what is the name of the file in the zip file?



Look at the 2nd http packet for the response.

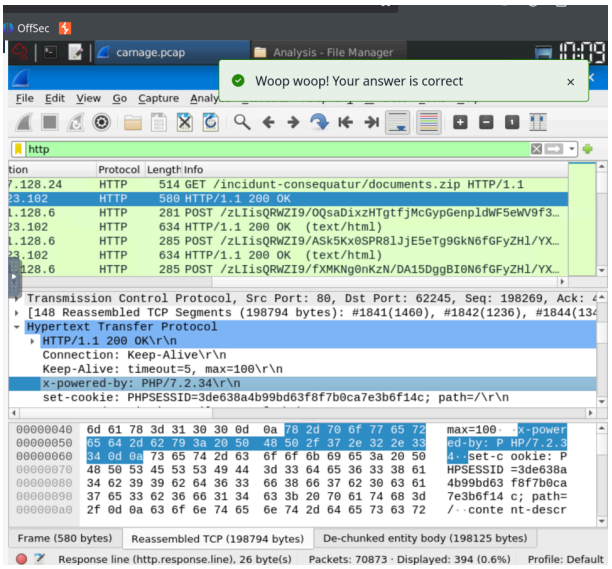
ANS :- chart-1530076591.xls

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



ANS :- LiteSpeed

QUE 6; What is the version of the webserver from the previous question?

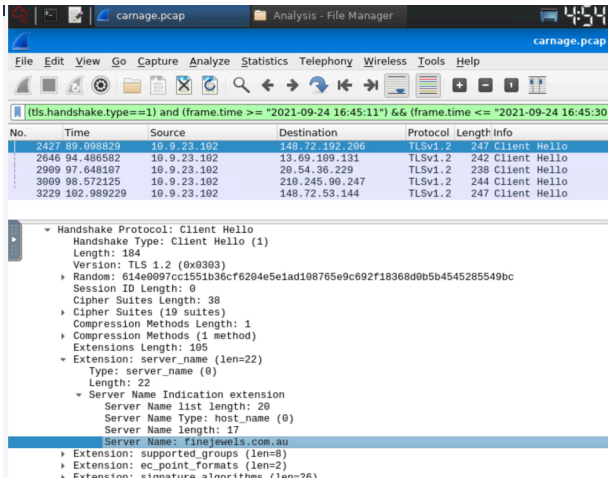


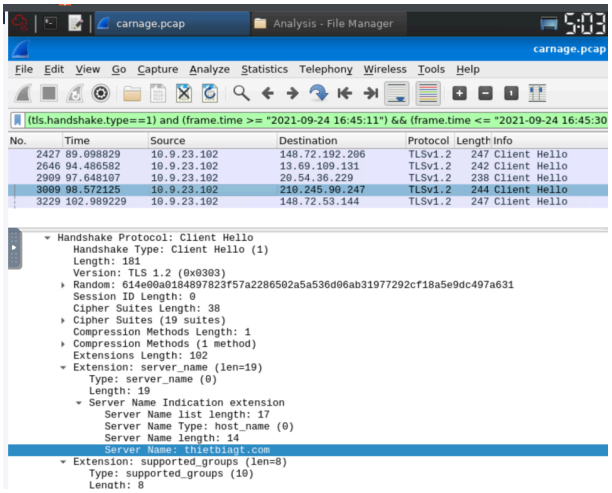
ANS :- PHP/7.2.34

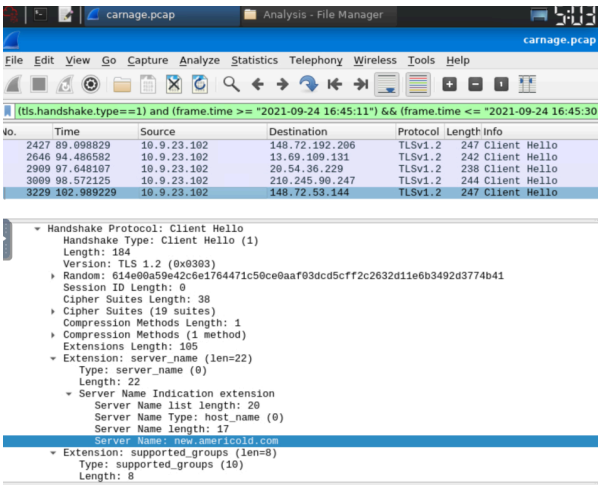
QUE 7; Malicious files were downloaded to the victim host from multiple domains. What were the three domains involved with this activity?

http.request.method (too much packets)
tls (as the encryption is done through tls)
tls.handshake.type == 1 (to look for client hello reqs)
(tls.handshake,type) and (frame.time >= 2021-09-24 16:45:11) &&(frame.time <= 2021-09-24 16:45:30)

This filters the packets to only 5
The time period is found in the hint by THM itself.
Click on the 1st packet and search for server name ,we got the first server name



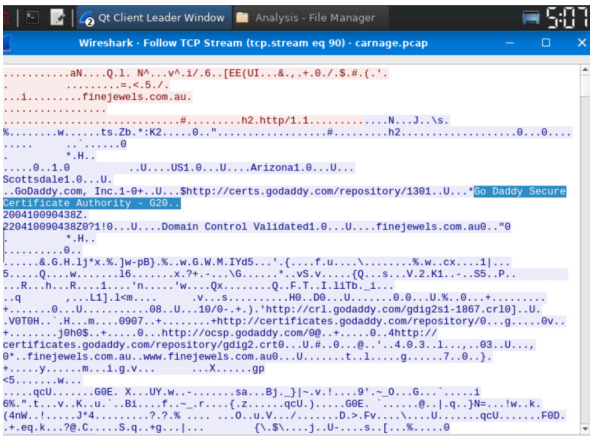




ANS :- finejewels.com.au, thietbiagt.com, new.americold.com

QUE 8; Which certificate authority issued the SSL certificate to the first domain from the previous question?

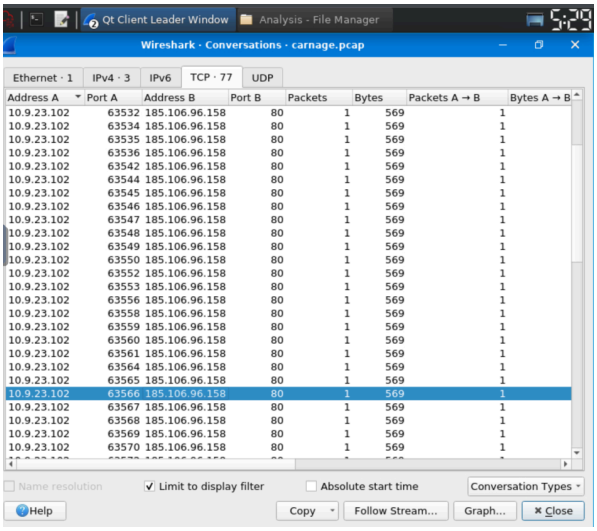
Right click on the packet —> follow —> tcp stream
There you will get the SSL certificate details.

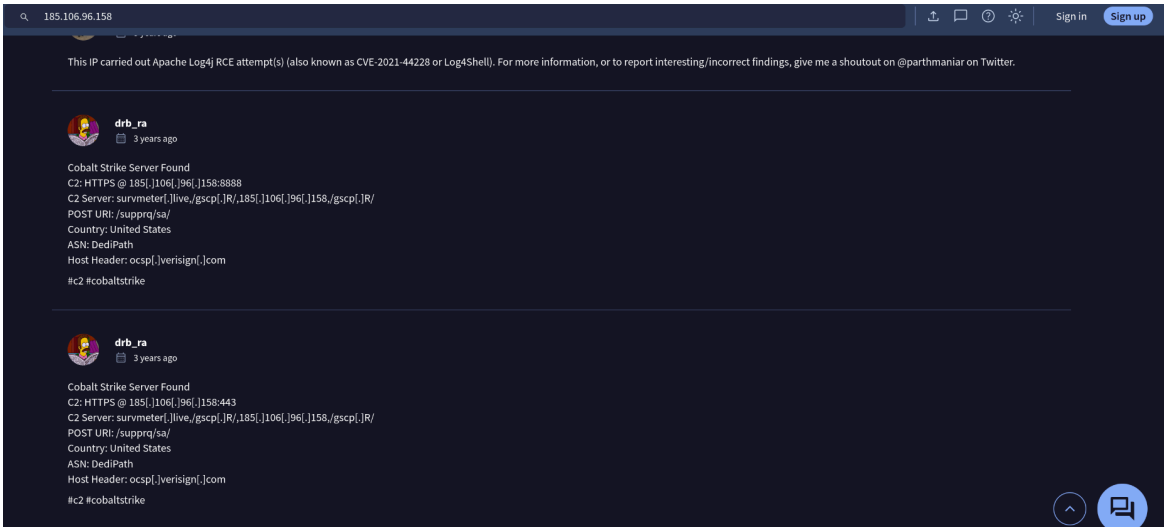


ANS :- godaddy

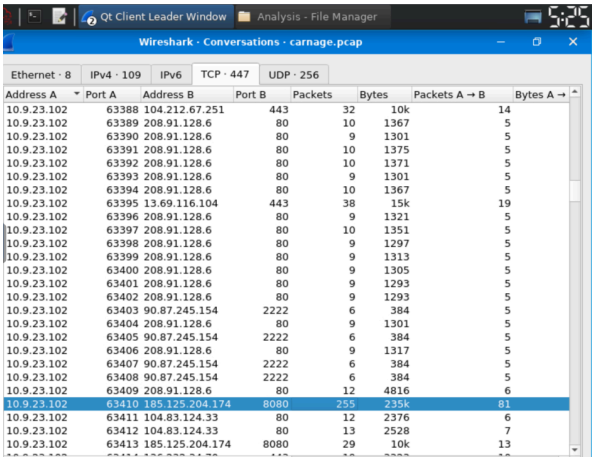
QUE 9; What are the two IP addresses of the Cobalt Strike servers? Use VirusTotal (the Community tab) to confirm if IPs are identified as Cobalt Strike C2 servers. (answer format: enter the IP addresses in sequential order)

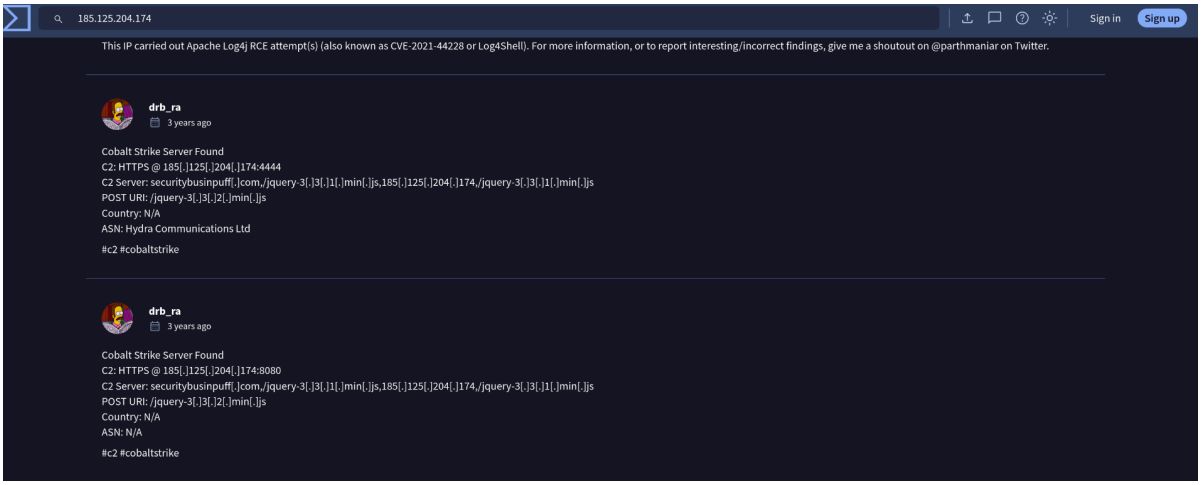
http.request.method==get
On the top bar go to statistics —> conversations menu —> TCP —> Limit to display filter
There we can see the same IP and out of curiosity I checked it in virus total and finds out it is malicious and using C2 server.



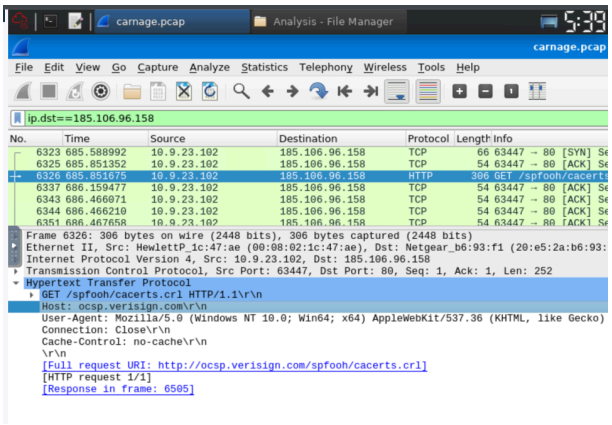


Now untick the filter and search through various other IPs also,I checked mostly IPs starting from 185.X.X.X and found 1 and when checked ,it is malicious and using c2 server.





QUE 10; What is the Host header for the first Cobalt Strike IP address from the previous question?
This ans can be found in the virustotal community tab otherwise;



ANS :- ocsp.verisign.com

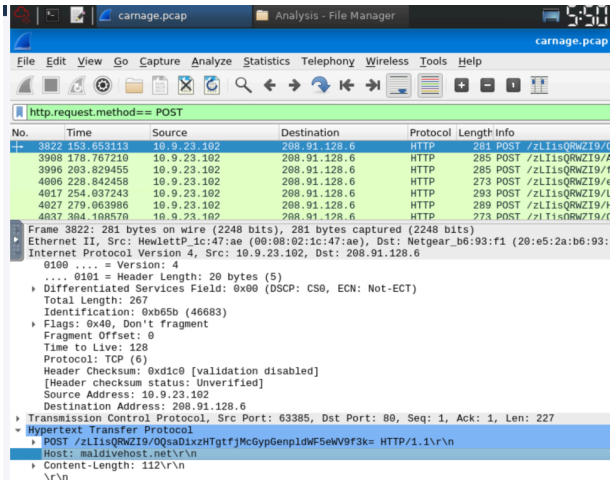
QUE 11; What is the domain name for the first IP address of the Cobalt Strike server? You may use VirusTotal to confirm if it's the Cobalt Strike server (check the Community tab).

ANS :- survmeter.live

QUE 12; 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).

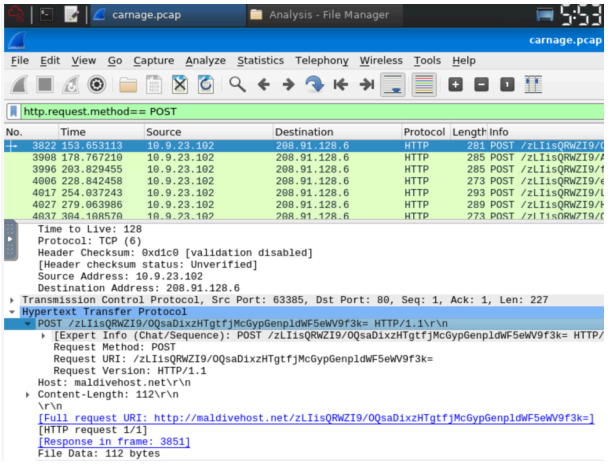
ANS :- securitybusinpuff.com

QUE 13; What is the domain name of the post-infection traffic?



ANS :- maldivehost.net

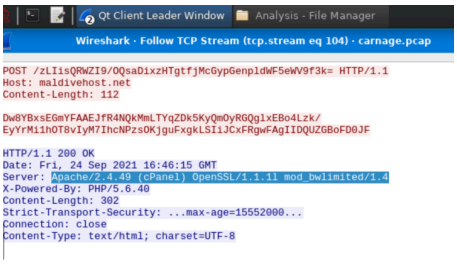
QUE 14 ; What are the first eleven characters that the victim host sends out to the malicious domain involved in the post-infection traffic?



ANS :- zLlisQRWZI9

QUE 15 ; What was the length for the first packet sent out to the C2 server?
ANS :- 281 (Length is found at the first glance itself)

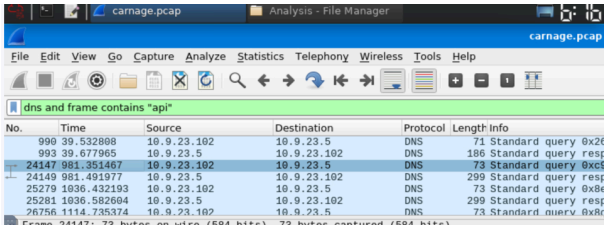
QUE 16; What was the Server header for the malicious domain from the previous question?

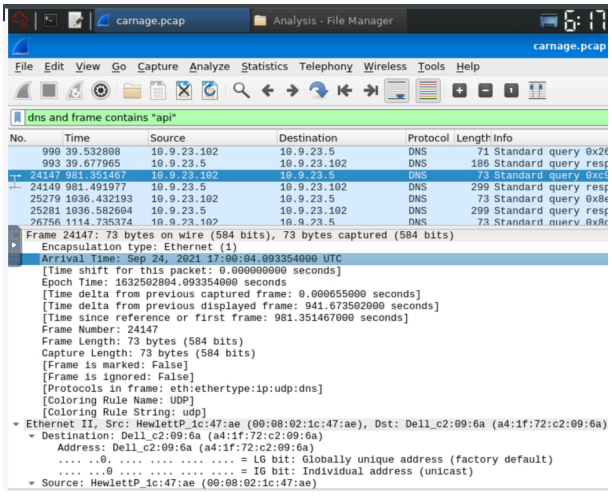


ANS :- Apache/2.4.49 (cPanel) OpenSSL/1.1.1l mod_bwlimited/1.4

QUE 17; 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)

dns and frame contains "api"



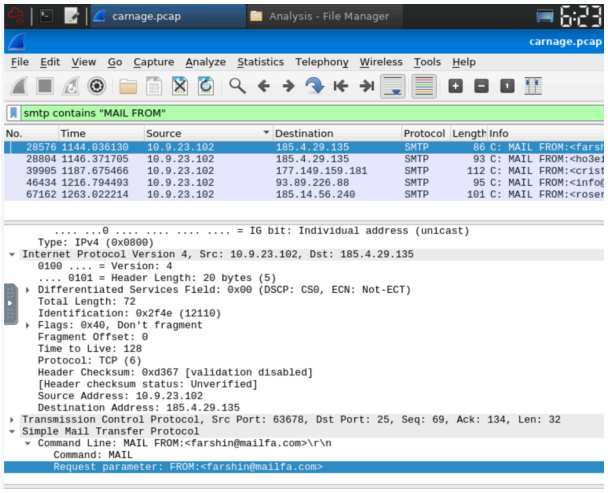


ANS :- 2021-09-24 17:00:04

QUE 18; What was the domain in the DNS query from the previous question?
follow —> dns stream

ANS ; api.ipify.org

QUE 19; Looks like there was some malicious spam (malspam) activity going on. What was the first MAIL FROM address observed in the traffic?
smtp contains “MAIL FROM” (smtp is used for mail transfer ,and check which contains “MAIL FROM”)



QUE 20; How many packets were observed for the SMTP traffic?
smtp (to filter out smtp traffic)

ANS :- 1439

HURRAY!!!! ROOM COMPLETED