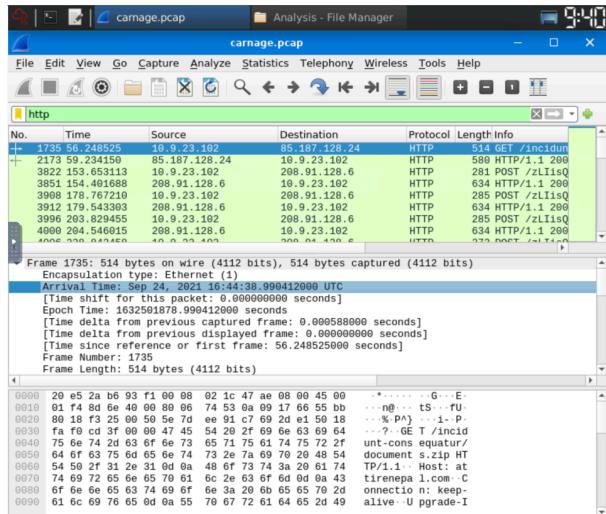


# CARNAGE

>> Deploy the machine

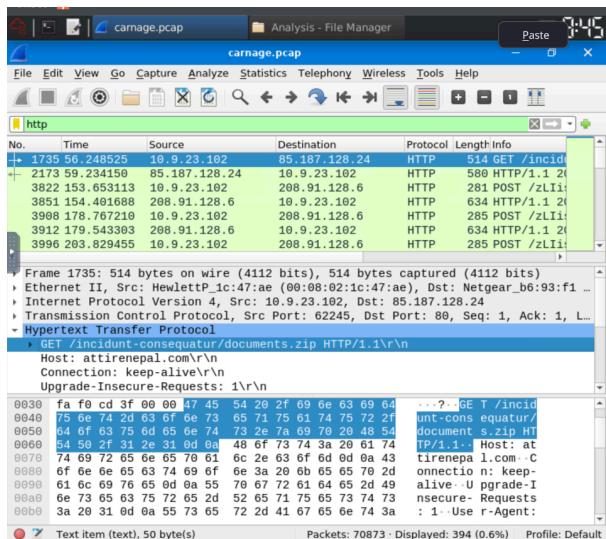
>> Open the analysis file in wireshark

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?

The screenshot shows the Wireshark interface with the packet list pane at the top. A specific HTTP GET request (No. 1735) is selected. The details pane shows the request URI: http://attirenepal.com/incidunt-consequatur/documents.zip. The bytes pane displays the raw hex and ASCII data of the selected packet.

ANS :- attirenepal.com

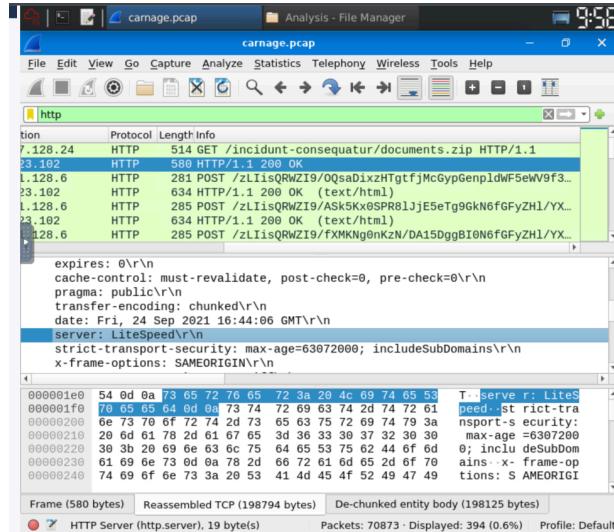
QUE 4; Without downloading the file, what is the name of the file in the zip file?

The screenshot shows the Wireshark interface with the packet list pane at the top. A specific HTTP response (No. 2173) is selected. The details pane shows the request URI: http://attirenepal.com/incidunt-consequatur/documents.zip. The bytes pane displays the raw hex and ASCII data of the selected packet, highlighting the file name -1530076\_591.xlsU.

Look at the 2nd http packet for the response.

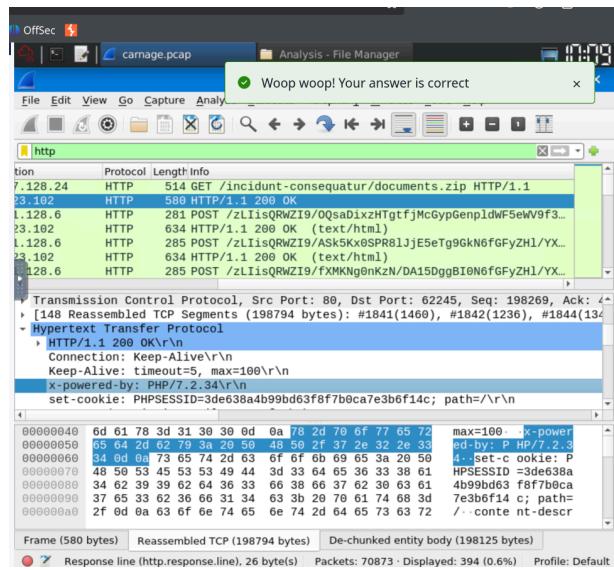
ANS :- chart-1530076591.xls

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

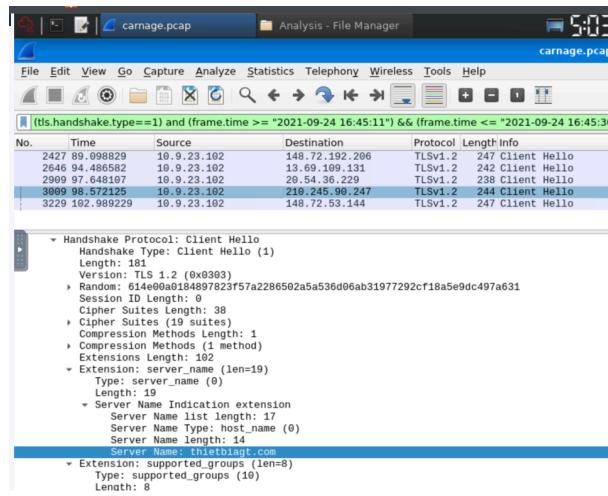
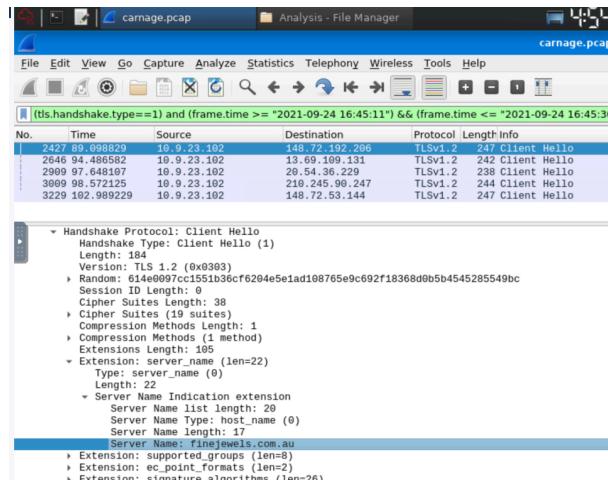
QUE 7; Malicious files were downloaded to the victim host from multiple domains. What were the three domains involved with this activity?

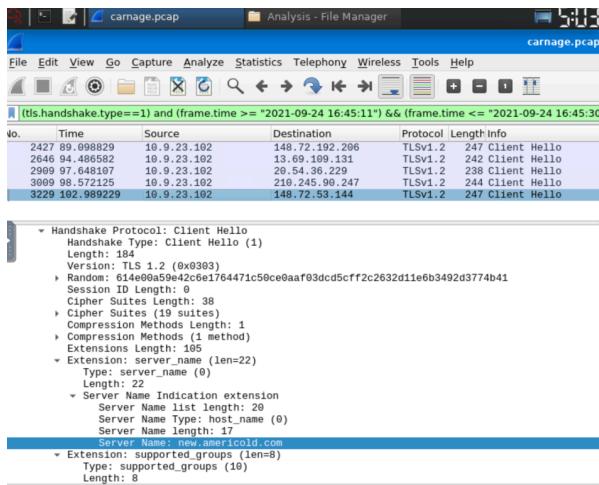
**http.request.method** ( too much packets)  
**tls** (as the encryption is done through tls)  
**tls.handshake.type == 1** (to look for client hello reqs)  
**(tls.handshake.type) and (frame.time >= 2021-09-24 16:45:11) &&(frame.time <= 2021-09-24 16:45:30)**

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



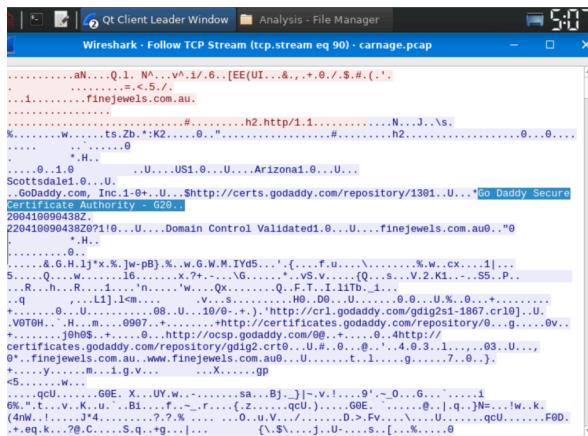


ANS :- finejewels.com.au, thietbiagt.com, new.americold.com

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.

Qt Client Leader Window Analysis - File Manager

Wireshark - Conversations : carnage.pcap

5:30

Ethernet · 1	IPv4 · 3	IPv6	TCP · 77	UDP			
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B
10.9.23.102	63532	185.106.96.158	80	1	569	1	
10.9.23.102	63534	185.106.96.158	80	1	569	1	
10.9.23.102	63535	185.106.96.158	80	1	569	1	
10.9.23.102	63536	185.106.96.158	80	1	569	1	
10.9.23.102	63542	185.106.96.158	80	1	569	1	
10.9.23.102	63544	185.106.96.158	80	1	569	1	
10.9.23.102	63545	185.106.96.158	80	1	569	1	
10.9.23.102	63546	185.106.96.158	80	1	569	1	
10.9.23.102	63547	185.106.96.158	80	1	569	1	
10.9.23.102	63548	185.106.96.158	80	1	569	1	
10.9.23.102	63549	185.106.96.158	80	1	569	1	
10.9.23.102	63550	185.106.96.158	80	1	569	1	
10.9.23.102	63552	185.106.96.158	80	1	569	1	
10.9.23.102	63553	185.106.96.158	80	1	569	1	
10.9.23.102	63556	185.106.96.158	80	1	569	1	
10.9.23.102	63558	185.106.96.158	80	1	569	1	
10.9.23.102	63559	185.106.96.158	80	1	569	1	
10.9.23.102	63560	185.106.96.158	80	1	569	1	
10.9.23.102	63561	185.106.96.158	80	1	569	1	
10.9.23.102	63564	185.106.96.158	80	1	569	1	
10.9.23.102	63565	185.106.96.158	80	1	569	1	
10.9.23.102	63566	185.106.96.158	80	1	569	1	
10.9.23.102	63567	185.106.96.158	80	1	569	1	
10.9.23.102	63568	185.106.96.158	80	1	569	1	
10.9.23.102	63569	185.106.96.158	80	1	569	1	
10.9.23.102	63570	185.106.96.158	80	1	569	1	

Name resolution Limit to display filter Absolute start time Conversation Types

Help Copy Follow Stream... Graph... Close

Q 185.106.96.158

This IP carried out Apache Log4j RCE attempt(s) (also known as CVE-2021-44228 or Log4Shell). For more information, or to report interesting/incorrect findings, give me a shoutout on @parthmaniar on Twitter.

drb\_ra 3 years ago

Cobalt Strike Server Found  
C2: HTTPS @ 185[.]106[.]96[.]158:8888  
C2 Server: surveymeter[.]live./gscpl[.]R/[185[.]106[.]96[.]158]/gscpl[.]R/  
POST URI: /supprq[sa]  
Country: United States  
ASN: DediPath  
Host Header: oscp[.]verisign[.]com  
#c2 #cobaltstrike

drb\_ra 3 years ago

Cobalt Strike Server Found  
C2: HTTPS @ 185[.]106[.]96[.]158:443  
C2 Server: surveymeter[.]live./gscpl[.]R/[185[.]106[.]96[.]158]/gscpl[.]R/  
POST URI: /supprq[sa]  
Country: United States  
ASN: DediPath  
Host Header: oscp[.]verisign[.]com  
#c2 #cobaltstrike

Sign in Sign up

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.

Qt Client Leader Window Analysis - File Manager

Wireshark - Conversations : carnage.pcap

5:30

Ethernet · 8	IPv4 · 109	IPv6	TCP · 447	UDP · 256			
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B
10.9.23.102	63388	104.212.67.251	443	32	10k	14	
10.9.23.102	63389	208.91.128.6	80	10	1367	5	
10.9.23.102	63390	208.91.128.6	80	9	1301	5	
10.9.23.102	63391	208.91.128.6	80	10	1375	5	
10.9.23.102	63392	208.91.128.6	80	10	1371	5	
10.9.23.102	63393	208.91.128.6	80	9	1301	5	
10.9.23.102	63394	208.91.128.6	80	10	1367	5	
10.9.23.102	63395	13.69.116.104	443	38	15k	19	
10.9.23.102	63396	208.91.128.6	80	9	1321	5	
10.9.23.102	63397	208.91.128.6	80	10	1351	5	
10.9.23.102	63398	208.91.128.6	80	9	1297	5	
10.9.23.102	63399	208.91.128.6	80	9	1313	5	
10.9.23.102	63400	208.91.128.6	80	9	1305	5	
10.9.23.102	63401	208.91.128.6	80	9	1293	5	
10.9.23.102	63402	208.91.128.6	80	9	1293	5	
10.9.23.102	63403	90.87.245.154	2222	6	384	5	
10.9.23.102	63404	208.91.128.6	80	9	1301	5	
10.9.23.102	63405	90.87.245.154	2222	6	384	5	
10.9.23.102	63406	208.91.128.6	80	9	1317	5	
10.9.23.102	63407	90.87.245.154	2222	6	384	5	
10.9.23.102	63408	90.87.245.154	2222	6	384	5	
10.9.23.102	63409	208.91.128.6	80	12	4816	6	
10.9.23.102	63410	185.125.204.174	8080	255	235k	81	
10.9.23.102	63411	104.83.124.33	80	12	2376	6	
10.9.23.102	63412	104.83.124.33	80	13	2528	7	
10.9.23.102	63413	185.125.204.174	8080	29	10k	13	

This IP carried out Apache Log4j RCE attempt(s) (also known as CVE-2021-44228 or Log4Shell). For more information, or to report interesting/incorrect findings, give me a shoutout on @parthmaniar on Twitter.

**drb\_ra** 3 years ago

Cobalt Strike Server Found  
C2: HTTPS @ 185[.]125[.]204[.]1174:4444  
C2 Server: securitybusinpuff[.]com./jquery-3[.]3[.]1[.]min[.]js,185[.]125[.]204[.]1174./jquery-3[.]3[.]1[.]min[.]js  
POST URL: /jquery-3[.]3[.]2[.]min[.]js  
Country: N/A  
ASN: Hydra Communications Ltd  
#c2 #cobaltstrike

**drb\_ra** 3 years ago

Cobalt Strike Server Found  
C2: HTTPS @ 185[.]125[.]204[.]1174:8080  
C2 Server: securitybusinpuff[.]com./jquery-3[.]3[.]1[.]min[.]js,185[.]125[.]204[.]1174./jquery-3[.]3[.]1[.]min[.]js  
POST URL: /jquery-3[.]3[.]2[.]min[.]js  
Country: N/A  
ASN: N/A  
#c2 #cobaltstrike

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;

File Edt View Go Capture Analyze Statistics Telephony Wireless Tools Help

Analysis - File Manager carnage.pcap

File Manager

ip.dst==185.106.96.158

No.	Time	Source	Destination	Protocol	Length	Info
6323	685.588992	10.9.23.102	185.106.96.158	TCP	66	63447 → 80 [SYN] Seq: 1
6324	685.589075	10.9.23.102	185.106.96.158	TCP	36	63447 → 80 [ACK] Seq: 2
6327	686.159477	10.9.23.102	185.106.96.158	TCP	54	63447 → 80 [ACK] Seq: 3
6343	686.466971	10.9.23.102	185.106.96.158	TCP	54	63447 → 80 [ACK] Seq: 4
6344	686.466210	10.9.23.102	185.106.96.158	TCP	54	63447 → 80 [ACK] Seq: 5
6351	686.467658	10.9.23.102	185.106.96.158	TCP	54	63447 → 80 [ACK] Seq: 6

Frame 6326: 306 bytes on wire (2448 bits), 306 bytes captured (2448 bits)  
Ethernet II, Src: Carnage (08:00:27:b6:93:1f), Dst: Internet\_Botnet (08:00:27:b6:93:1f) (20:e5:2a:b6:93:  
Internet Protocol Version 4, Src: 10.9.23.102, Dst: 185.106.96.158  
Transmission Control Protocol, Src Port: 63447, Dst Port: 80, Seq: 1, Ack: 1, Len: 252  
HyperText Transfer Protocol  
GET /spfooh/cacerts.crl HTTP/1.1\r\nHost: ocsp.verisign.com\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Connection: Close\r\nCache-Control: no-cache\r\n\r\n[Full request URL: http://ocsp.verisign.com/spfooh/cacerts.crl]  
[HTTP request 1/1]  
[Response in frame: 6505]

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).

**drb\_ra** 3 years ago

Cobalt Strike Server Found  
C2: HTTPS @ 185[.]106[.]96[.]158:443  
C2 Server: survmeter[.]live./gscp[.]R/185[.]106[.]96[.]158/gscp[.]R/  
POST URL: /supprq/sa/  
Country: United States  
ASN: DediPath  
Host Header: ocsp[.]verisign[.]com  
#c2 #cobaltstrike

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).

Cobalt Strike Server Found  
C2: HTTPS @ 185[.]112[.]204[.]1174:8080  
[IC2 Server securitybusinpuff.com /jquery-3[.]3[.]1[.]min[.]js,185[.]125[.]204[.]174[.]jquery-3[.]3[.]1[.]min[.]js  
POST URI: /jquery-3[.]3[.]2[.]min[.]js  
Country: N/A  
ASN: N/A  
IC2 #cobaltstrike

ANS :- securitybusinpuff.com

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

Frame 3822: 281 bytes on wire (2248 bits), 281 bytes captured (2248 bits)  
Ethernet II, Src: Hewlett\_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear\_b6:93:f1 (20:e5:2a:b6:93:  
Internet Protocol Version 4, Src: 10.9.23.102, Dst: 208.91.128.6  
...  
HTTP Request / [Content-Length: 112]  
Host: malidivehost.net\r\n\r\n

ANS :- malidivehost.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?

Frame 3822: 281 bytes on wire (2248 bits), 281 bytes captured (2248 bits)  
Ethernet II, Src: Hewlett\_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear\_b6:93:f1 (20:e5:2a:b6:93:  
Internet Protocol Version 4, Src: 10.9.23.102, Dst: 208.91.128.6  
...  
HTTP Request / [Content-Length: 112]  
Host: malidivehost.net\r\n\r\n

ANS :- zLlisQRWZl9

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?

```
POST /zLlisQRWZl9/QosadixzHTgjfjMcGypGenpldWF5eWVf3k= HTTP/1.1
Host: mailivehost.net
Content-Length: 112

HTTP/1.1 200 OK
Date: Fri, 24 Sep 2021 16:46:15 GMT
Server: Apache/2.4.49 (cPanel) OpenSSL/1.1.1l mod_bwlimited/1.4
X-Powered-By: PHP/5.6.48
Content-Length: 308
Strict-Transport-Security: ...max-age=15552000...
Connection: close
Content-Type: text/html; charset=UTF-8
```

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”

No.	Time	Source	Destination	Protocol	Length	Info
998	09:39:53.8888	10.9.23.182	10.9.23.5	DNS	71	Standard query 0x26
999	09:39:57.7965	10.9.23.182	10.9.23.102	DNS	186	Standard query response 0x86
24147	981.351467	10.9.23.102	10.9.23.5	DNS	73	Standard query 0x86
24149	981.491977	10.9.23.5	10.9.23.102	DNS	299	Standard query response 0x86
25279	1036.432193	10.9.23.102	10.9.23.5	DNS	73	Standard query 0x86
25281	1036.582604	10.9.23.5	10.9.23.102	DNS	299	Standard query response 0x86
26756	1114.735374	10.9.23.102	10.9.23.5	DNS	73	Standard query response 0x86

No.	Time	Source	Destination	Protocol	Length	Info
998	09:39:53.8888	10.9.23.182	10.9.23.5	DNS	71	Standard query 0x26
999	09:39:57.7965	10.9.23.182	10.9.23.102	DNS	186	Standard query response 0x86
24147	981.351467	10.9.23.102	10.9.23.5	DNS	73	Standard query 0x86
24149	981.491977	10.9.23.5	10.9.23.102	DNS	299	Standard query response 0x86
25279	1036.432193	10.9.23.102	10.9.23.5	DNS	73	Standard query 0x86
25281	1036.582604	10.9.23.5	10.9.23.102	DNS	299	Standard query response 0x86
26756	1114.735374	10.9.23.102	10.9.23.5	DNS	73	Standard query response 0x86

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

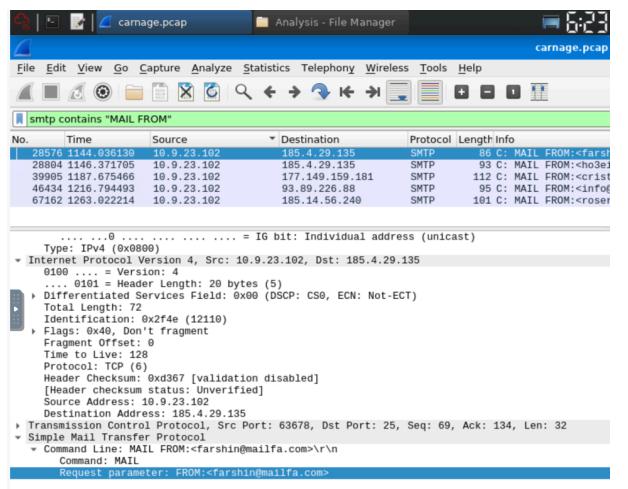
QUE 18; What was the domain in the DNS query from the previous question?  
follow —> dns stream



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