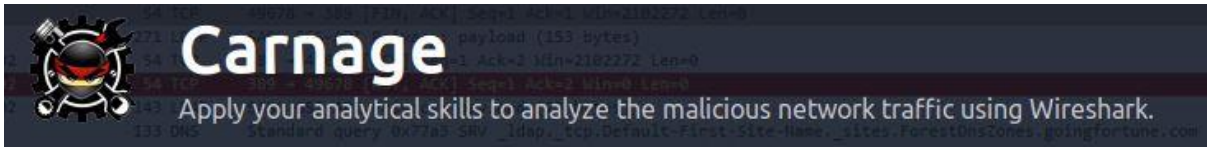
TRY HACK ME: Write-Up Carnage



Task 1 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.

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.

Deploy the machine attached to this task; it will be visible in the split-screen view once it is ready.

If you don't see a virtual machine load, then click the Show Split View button.

Answer to the questions of this section-

No Answer needed

Task 2 Traffic Analysis –

Are you ready for the journey?

Please, load the pcap file in your Analysis folder on the Desktop into Wireshark to answer the questions below.

Answer to the questions of this section-

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

(**answer format**: yyyy-mm-dd hh:mm:ss)

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

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

documents.zip | Correct Answer

What was the domain hosting the malicious zip file?

attirenepal.com | Correct Answer

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

chart-1530076591.xls | Correct Answer

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

LiteSpeed | Correct Answer

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

PHP/7.2.34

Correct Answer

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

jewels.com.au, thietbiagt.com, new.americold.com

Correct Answer

Hint

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)

185.106.96.158, 185.125.204.174

Correct Answer

Hint

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

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

Hint

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

maldivehost.net

Correct

Hint

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

zLIisQRWZI9 Correct Answer

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

281 Correct Answer

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

?.4.49 (cPanel) OpenSSL/1.1.1l mod_bwlimited/1.4 Correct Answer

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)

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

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

api.ipify.org Correct Answer

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

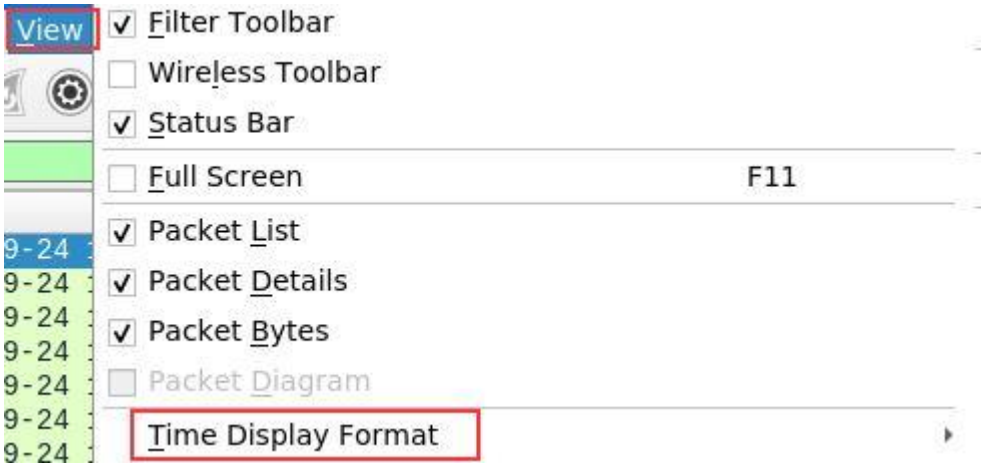
farshin@mailfa.com Correct Answer

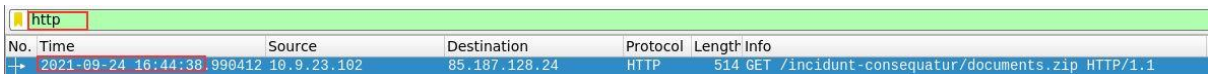
How many packets were observed for the SMTP traffic?

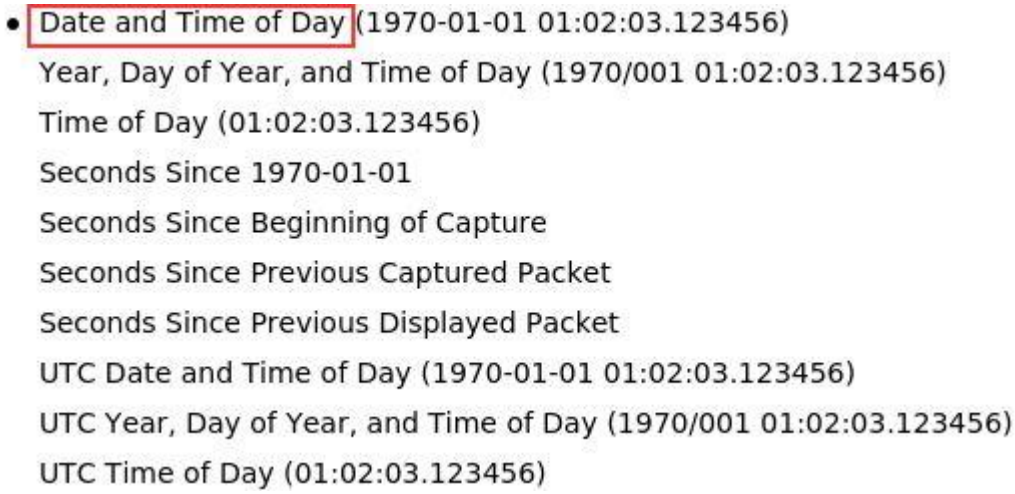
1439 Correct Answer

Answers-

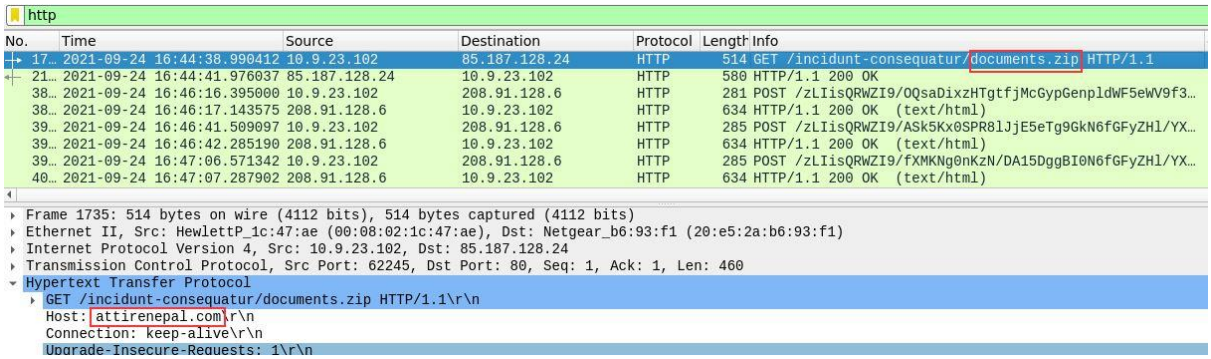
1)


View
Filter Toolbar
Wireless Toolbar
Status Bar
Full Screen F11
Packet List
Packet Details
Packet Bytes
Packet Diagram
Time Display Format

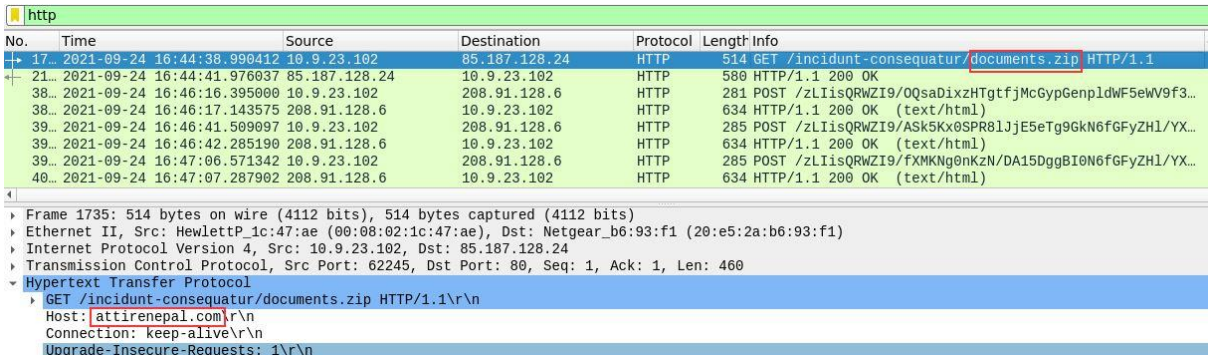

http
No. Time Source Destination Protocol Length Info
2021-09-24 16:44:38.990412 10.9.23.102 85.187.128.24 HTTP 514 GET /incidunt-consequatur/documents.zip HTTP/1.1


Date and Time of Day (1970-01-01 01:02:03.123456)
Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
Time of Day (01:02:03.123456)
Seconds Since 1970-01-01
Seconds Since Beginning of Capture
Seconds Since Previous Captured Packet
Seconds Since Previous Displayed Packet
UTC Date and Time of Day (1970-01-01 01:02:03.123456)
UTC Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
UTC Time of Day (01:02:03.123456)

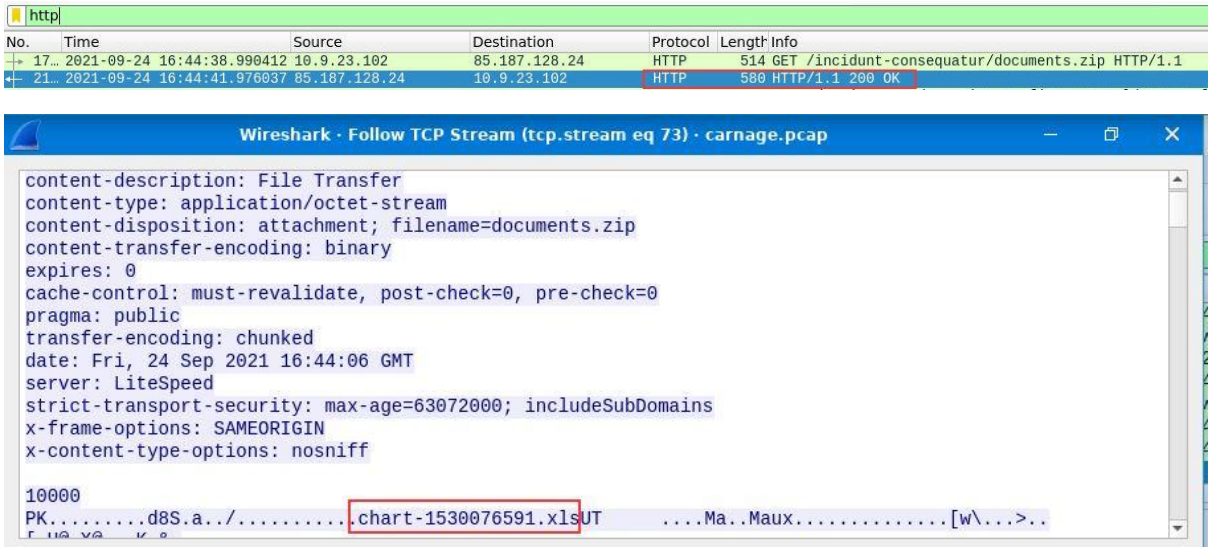
2)


http
No. Time Source Destination Protocol Length Info
17… 2021-09-24 16:44:38.990412 10.9.23.102 85.187.128.24 HTTP 514 GET /incidunt-consequatur/documents.zip HTTP/1.1
21… 2021-09-24 16:44:41.976037 85.187.128.24 10.9.23.102 HTTP 580 HTTP/1.1 200 OK
38… 2021-09-24 16:46:16.395000 10.9.23.102 208.91.128.6 HTTP 281 POST /zLIisQRWZI9/OQsaDixzHTgtfjMcGypGenpldWF5eWV9f3…
38… 2021-09-24 16:46:17.143575 208.91.128.6 10.9.23.102 HTTP 634 HTTP/1.1 200 OK (text/html)
39… 2021-09-24 16:46:41.509097 10.9.23.102 208.91.128.6 HTTP 285 POST /zLIisQRWZI9/ASk5Kx0SPR8lJjE5eTg9GkN6fGFyZHl/YX…
39… 2021-09-24 16:46:42.285190 208.91.128.6 10.9.23.102 HTTP 634 HTTP/1.1 200 OK (text/html)
39… 2021-09-24 16:47:06.571342 10.9.23.102 208.91.128.6 HTTP 285 POST /zLIisQRWZI9/fXMKNg0nKzN/DA15DggBI0N6fGFyZHl/YX…
40… 2021-09-24 16:47:07.287902 208.91.128.6 10.9.23.102 HTTP 634 HTTP/1.1 200 OK (text/html)
Frame 1735: 514 bytes on wire (4112 bits), 514 bytes captured (4112 bits)
Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
Internet Protocol Version 4, Src: 10.9.23.102, Dst: 85.187.128.24
Transmission Control Protocol, Src Port: 62245, Dst Port: 80, Seq: 1, Ack: 1, Len: 460
Hypertext Transfer Protocol
GET /incidunt-consequatur/documents.zip HTTP/1.1\r\n
Host: attirenepal.com\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n

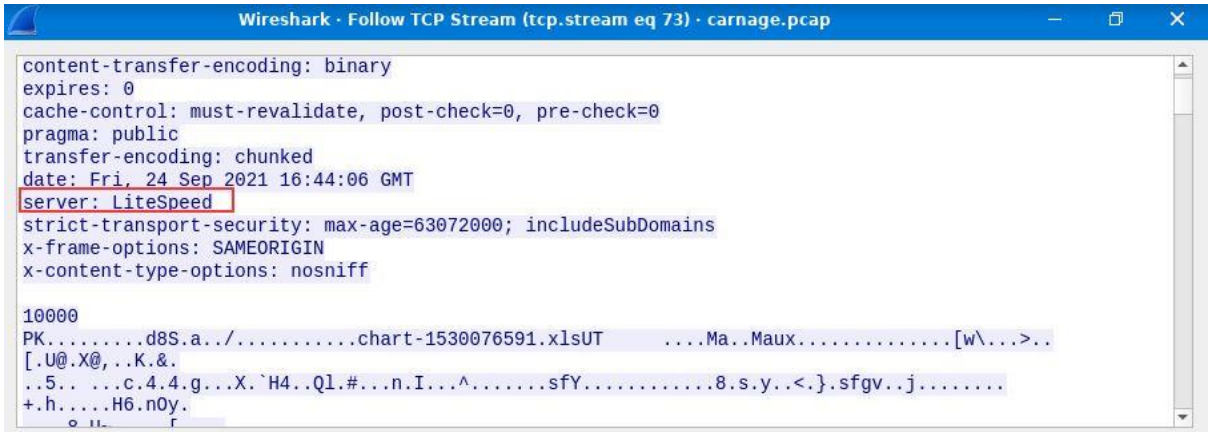
3)



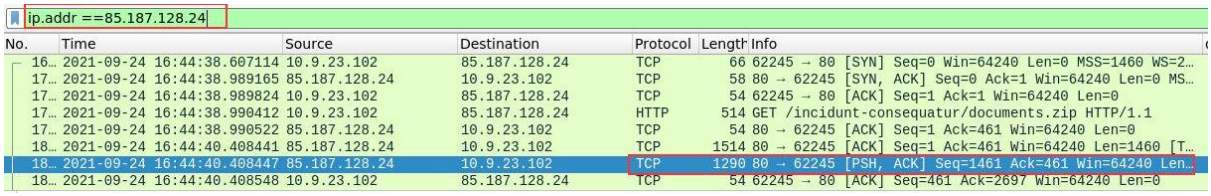
4)



5)



6) put filter – ip.addr == 85.187.128.24



No.	Time	Source	Destination	Protocol	Length	Info
16…	2021-09-24 16:44:38.607114	10.9.23.102	85.187.128.24	TCP	66	62245 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=2…
17…	2021-09-24 16:44:38.989165	85.187.128.24	10.9.23.102	TCP	58	80 → 62245 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MS…
17…	2021-09-24 16:44:38.989824	10.9.23.102	85.187.128.24	TCP	54	62245 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
17…	2021-09-24 16:44:38.990412	10.9.23.102	85.187.128.24	HTTP	514	GET /incidunt-consequatur/documents.zip HTTP/1.1
17…	2021-09-24 16:44:38.990522	85.187.128.24	10.9.23.102	TCP	54	80 → 62245 [ACK] Seq=1 Ack=461 Win=64240 Len=0
18…	2021-09-24 16:44:40.408441	85.187.128.24	10.9.23.102	TCP	1514	80 → 62245 [ACK] Seq=1 Ack=461 Win=64240 Len=1460 [T…
18…	2021-09-24 16:44:40.408447	85.187.128.24	10.9.23.102	TCP	1290	80 → 62245 [PSH, ACK] Seq=1461 Ack=461 Win=64240 Len…
18…	2021-09-24 16:44:40.408548	10.9.23.102	85.187.128.24	TCP	54	62245 → 80 [ACK] Seq=461 Ack=2697 Win=64240 Len=0

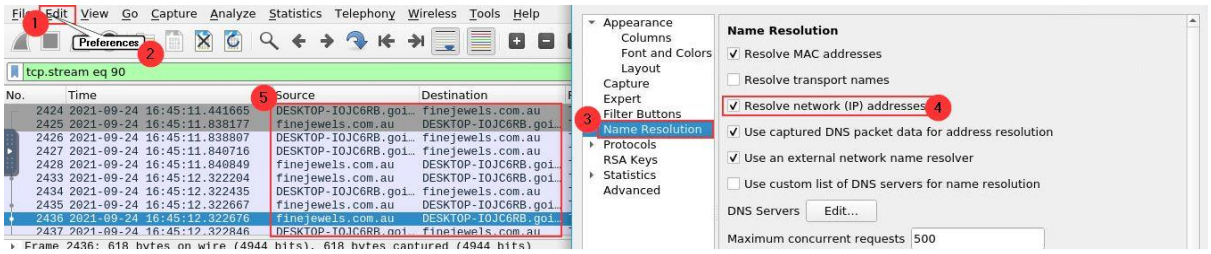
```
GET /incidunt-consequatur/documents.zip HTTP/1.1
Host: attirenepal.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
93.0.4577.82 Safari/537.36 Edg/93.0.961.52
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en

HTTP/1.1 200 OK
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
x-powered-by: PHP/7.2.34
set-cookie: PHPSESSID=3de638a4b99bd63f8f7b0ca7e3b6f14c; path=/
```

7) Hint asks you to check HTTPs traffic means look for SSL/TLS traffic in timeframe 16:45:11 to 16:45:30. Go to Edit -> Preferences -> name resolution -> enable network IP addresses

16:45:12 finejewels.com.au

16:45:25 thietbiagt.com

16:45:27 new.americold.com



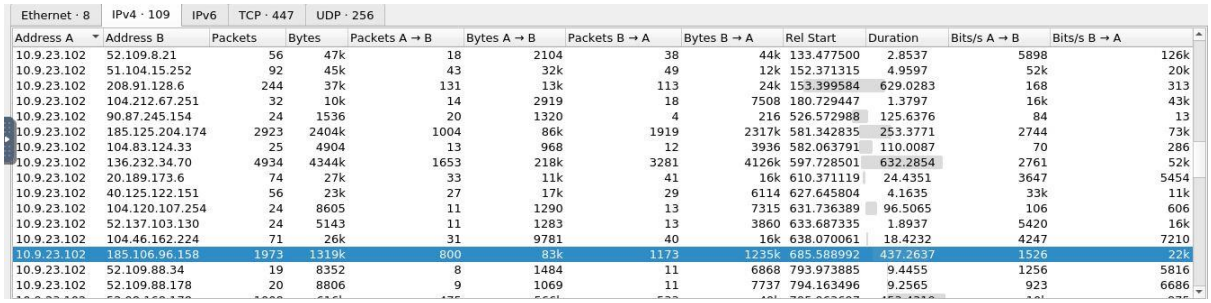
8) CA viewed using - TCP Stream of traffic at 16:45: 12 timeframe for TLS

2436	2021-09-24 16:45:12.322676	finejewels.com.au	DESKTOP-IOJC6RB.goi…	TLSv1.2	618	Certificate, Server Key Exchange, Server Hello Done

SSL certificate

```
..GoDaddy.com, Inc.1-0+..U...$http://certs.godaddy.com/repository/1301..U...*Go Daddy Secure Certificate
Authority - G20..
```

9) Go to Statistics -> conversations -> look inside IPv4 tab



Ethernet · 8 | IPv4 · 109 | IPv6 | TCP · 447 | UDP · 256

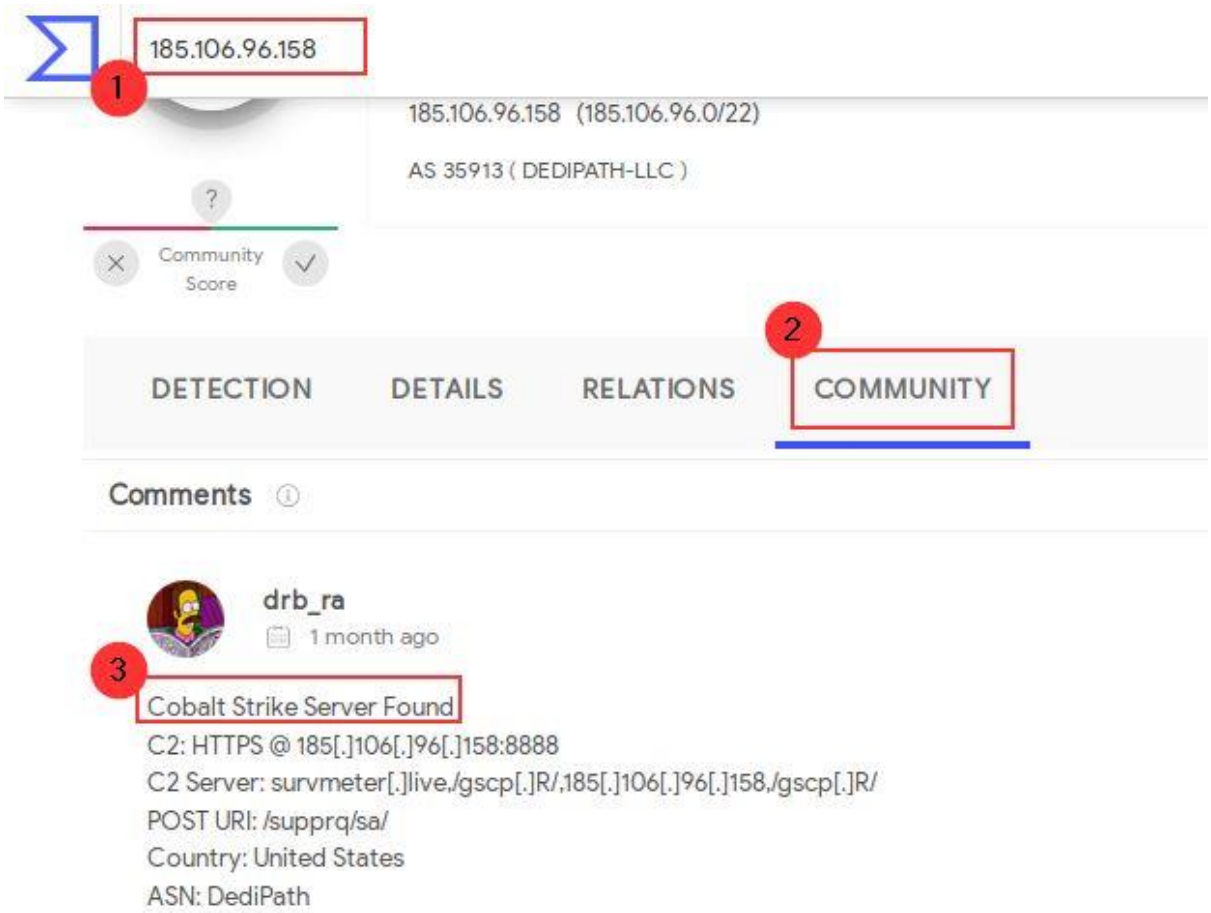
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
10.9.23.102	52.109.8.21	56	47k	18	2104	38	44k	133.477500	2.8537	5898	126k
10.9.23.102	51.104.15.252	92	45k	43	32k	49	12k	152.371315	4.9597	52k	20k
10.9.23.102	208.91.128.6	244	37k	131	13k	113	24k	153.399584	629.0283	168	313
10.9.23.102	104.212.67.251	32	10k	14	2919	18	7508	180.729447	1.3797	16k	43k
10.9.23.102	90.87.245.154	24	1536	20	1320	4	216	526.572988	125.6376	84	13
10.9.23.102	185.125.204.174	2923	2404k	1004	86k	1919	2317k	581.342835	253.3771	2744	73k
10.9.23.102	104.83.124.33	25	4904	13	968	12	3936	582.063791	110.0087	70	286
10.9.23.102	136.232.34.70	4934	4344k	1653	218k	3281	4126k	597.728501	632.2854	2761	52k
10.9.23.102	20.189.173.6	74	27k	33	11k	41	16k	610.371119	24.4351	3647	5454
10.9.23.102	40.125.122.151	56	23k	27	17k	29	6114	627.645804	4.1635	33k	11k
10.9.23.102	104.120.107.254	24	8605	11	1290	13	7315	631.736389	96.5065	106	606
10.9.23.102	52.137.103.130	24	5143	11	1283	13	3860	633.687335	1.8937	5420	16k
10.9.23.102	104.46.162.224	71	26k	31	9781	40	16k	638.070061	18.4232	4247	7210
10.9.23.102	185.106.96.158	1973	1319k	800	83k	1173	1235k	685.588992	437.2637	1526	22k
10.9.23.102	52.109.88.34	19	8352	8	1484	11	6868	793.973885	9.4455	1256	5816
10.9.23.102	52.109.88.178	20	8806	9	1069	11	7737	794.163496	9.2565	923	6686

Default port for Cobalt Strike is PORT 8080, look for IP addresses using this port

IP address 1- 185.106.96.158 at port 80

10.9.23.102	63561	185.106.96.158	80	10	1379	5	797	5	582	900.632453	0.7770	8205
10.9.23.102	63564	185.106.96.158	80	9	1325	5	797	4	528	904.897152	0.6108	10k

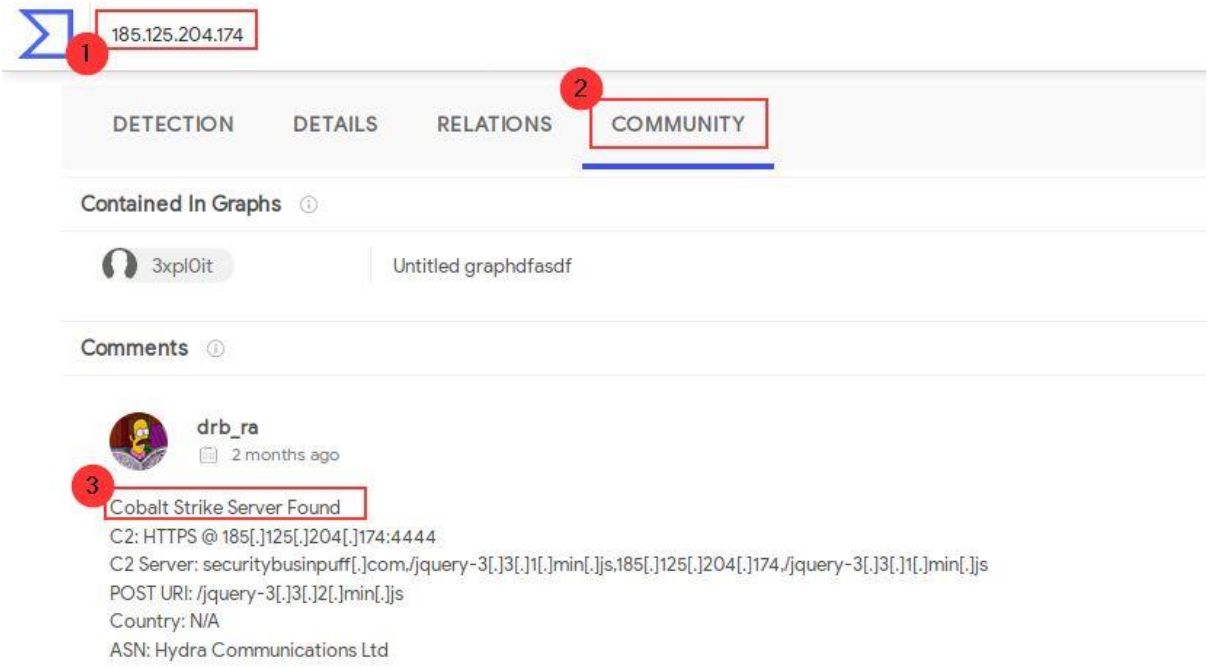
Proof by Virus Total-



IP address 2- 185.125.204.174 at port 8080

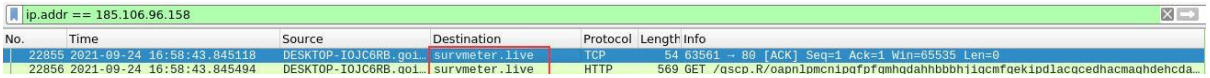
10.9.23.102	63413	185.125.204.174	8080	29	10k	13	1539	16	8734	585.265235	1.0495	11k
10.9.23.102	63423	185.125.204.174	8080	27	8501	14	1547	13	6954	614.911448	0.8403	14k
10.9.23.102	63438	185.125.204.174	8080	23	8236	10	1367	13	6869	645.707867	0.8662	12k

Proof by Virus Total-

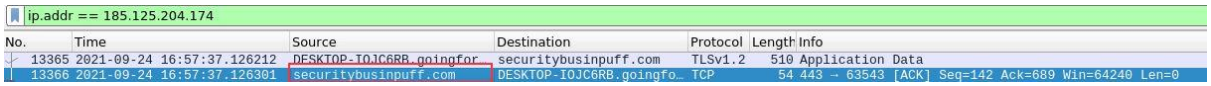


10) Apply ip.addr == 185.106.96.158 as filter and follow TCP stream for HOST header value

11) using ip.addr == 185.106.96.158 find the domain name, also by enabling network IP addresses filter in name resolution of preferences by edit tab



12) Do same as mentioned in point 11



13) Apply http.request.method == POST as filter in wireshark

14) zLIisQRWZI9

http.request.method == POST

No.	Time	Source	Destination	Protocol	Length	Info
4930	2021-09-24 16:54:13.397897	DESKTOP-IOJC6RB.goingfor…	maldivehost.net	HTTP	289	POST /zLIisQRWZI9/
5208	2021-09-24 16:54:38.381382	DESKTOP-IOJC6RB.goingfor…	maldivehost.net	HTTP	265	POST /zLIisQRWZI9/
6227	2021-09-24 16:55:03.473099	DESKTOP-IOJC6RB.goingfor…	maldivehost.net	HTTP	265	POST /zLIisQRWZI9/

15) 281 first packet length sent to C2 Server

http.request.method == POST

No.	Time	Source	Destination	Protocol	Length	Info
3822	2021-09-24 16:46:16.395000	DESKTOP-IOJC6RB.goingfor…	maldivehost.net	HTTP	281	POST /zLIisQRWZI9/(
3908	2021-09-24 16:46:41.509097	DESKTOP-IOJC6RB.goingfor…	maldivehost.net	HTTP	285	POST /zLIisQRWZI9/A

16) Viewed TCP stream for below packet having 281 length

3822 2021-09-24 16:46:16.395000 DESKTOP-IOJC6RB.goingfor… maldivehost.net HTTP 281 POST /zLIisQRWZI9/OQsaDixzHTgtfjMcGypGenpldWF5eWV9f3k= HTTP/1.1 Continua…

Server Header-

Wireshark · Follow HTTP Stream (tcp.stream eq 104) · carnage.pcap

```
POST /zLIisQRWZI9/OQsaDixzHTgtfjMcGypGenpldWF5eWV9f3k= HTTP/1.1
Host: maldivehost.net
Content-Length: 112

Dw8YBxsEGmYFAAEJfR4NQkMmLTYqZDk5KyQmOyRGQglxEBo4Lzk/
EyYrMi1hOT8vIyM7IhcNPzsOKjguFxgkLSIiJCxFRgwFAgIIDQUZGBoFD0JFHTTP/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/5.6.40
Content-Length: 302
Strict-Transport-Security: ...max-age=15552000...
Connection: close
Content-Type: text/html; charset=UTF-8
```

17) Apply frame contains “api” filter in wireshark

frame contains "api"

No.	Time	Source	Destination	Protocol	Length	Info
1474	2021-09-24 16:44:26.385162	20.190.159.135	10.9.23.102	TCP	1414	443 → 49738 [PSH, ACK] Seq=1361 Ack=200 Win=64240 Len=1360 [T…
2179	2021-09-24 16:44:42.718430	13.107.22.200	10.9.23.102	TCP	1514	443 → 63360 [ACK] Seq=1361 Ack=518 Win=64240 Len=1460 [TCP se…
3925	2021-09-24 16:46:43.104811	131.253.33.200	10.9.23.102	TCP	1514	443 → 63387 [ACK] Seq=1361 Ack=189 Win=64240 Len=1460 [TCP se…
5757	2021-09-24 16:54:47.706743	136.232.34.70	10.9.23.102	TCP	1514	443 → 63439 [ACK] Seq=549492 Ack=1125 Win=64240 Len=1460 [TCP…
10519	2021-09-24 16:56:57.243661	52.109.88.178	10.9.23.102	TCP	1514	443 → 63502 [ACK] Seq=1361 Ack=191 Win=64240 Len=1460 [TCP se…
24146	2021-09-24 17:00:04.092699	23.111.114.52	10.9.23.102	TLSv1.2	114	Ignored Unknown Record
24147	2021-09-24 17:00:04.093354	10.9.23.102	10.9.23.5	DNS	73	Standard query 0xc92c A api.ipify.org
24149	2021-09-24 17:00:04.233864	10.9.23.5	10.9.23.102	DNS	299	Standard query response 0xc92c A api.ipify.org CNAME nagano-1…
24161	2021-09-24 17:00:04.791170	23.111.114.52	10.9.23.102	TLSv1.2	329	Ignored Unknown Record
24162	2021-09-24 17:00:04.791435	10.9.23.102	54.243.45.255	TLSv1.2	319	Client Hello
24166	2021-09-24 17:00:04.995747	23.111.114.52	10.9.23.102	TLSv1.2	329	Ignored Unknown Record
24167	2021-09-24 17:00:04.996060	10.9.23.102	54.243.45.255	TLSv1.2	319	Client Hello

18) api.ipify.org

frame contains "api"

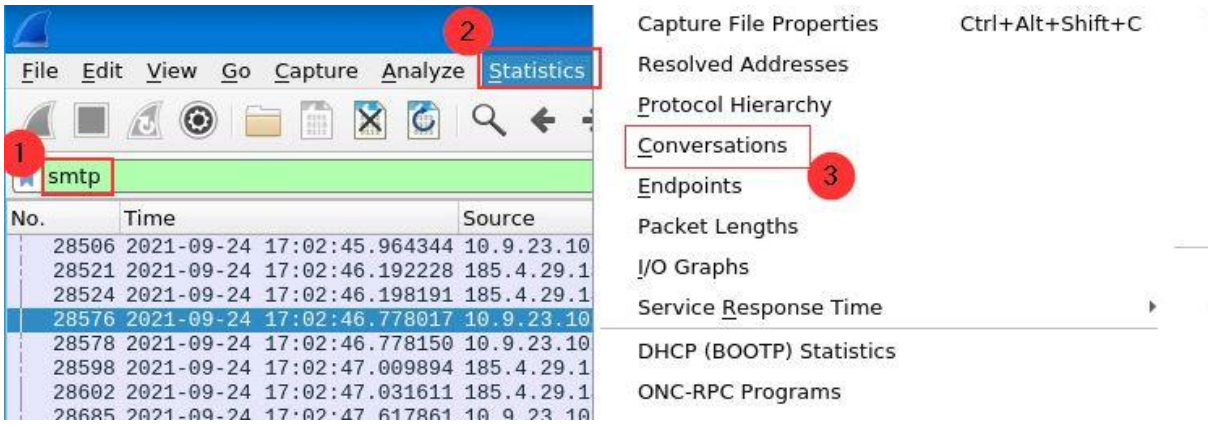
No.	Time	Source	Destination	Protocol	Length	Info
1474	2021-09-24 16:44:26.385162	20.190.159.135	10.9.23.102	TCP	1414	443 → 49738 [PSH, ACK] Seq=1361 Ack=200 Win=64240 Len=1360 [T…
2179	2021-09-24 16:44:42.718430	13.107.22.200	10.9.23.102	TCP	1514	443 → 63360 [ACK] Seq=1361 Ack=518 Win=64240 Len=1460 [TCP se…
3925	2021-09-24 16:46:43.104811	131.253.33.200	10.9.23.102	TCP	1514	443 → 63387 [ACK] Seq=1361 Ack=189 Win=64240 Len=1460 [TCP se…
5757	2021-09-24 16:54:47.706743	136.232.34.70	10.9.23.102	TCP	1514	443 → 63439 [ACK] Seq=549492 Ack=1125 Win=64240 Len=1460 [TCP…
10519	2021-09-24 16:56:57.243661	52.109.88.178	10.9.23.102	TCP	1514	443 → 63502 [ACK] Seq=1361 Ack=191 Win=64240 Len=1460 [TCP se…
24146	2021-09-24 17:00:04.092699	23.111.114.52	10.9.23.102	TLSv1.2	114	Ignored Unknown Record
24147	2021-09-24 17:00:04.093354	10.9.23.102	10.9.23.5	DNS	73	Standard query 0xc92c A api.ipify.org
24149	2021-09-24 17:00:04.233864	10.9.23.5	10.9.23.102	DNS	299	Standard query response 0xc92c A api.ipify.org CNAME nagano-1…
24161	2021-09-24 17:00:04.791170	23.111.114.52	10.9.23.102	TLSv1.2	329	Ignored Unknown Record
24162	2021-09-24 17:00:04.791435	10.9.23.102	54.243.45.255	TLSv1.2	319	Client Hello
24166	2021-09-24 17:00:04.995747	23.111.114.52	10.9.23.102	TLSv1.2	329	Ignored Unknown Record
24167	2021-09-24 17:00:04.996060	10.9.23.102	54.243.45.255	TLSv1.2	319	Client Hello

19) Apply smtp filter or we can also use frame contains “MAIL FROM”

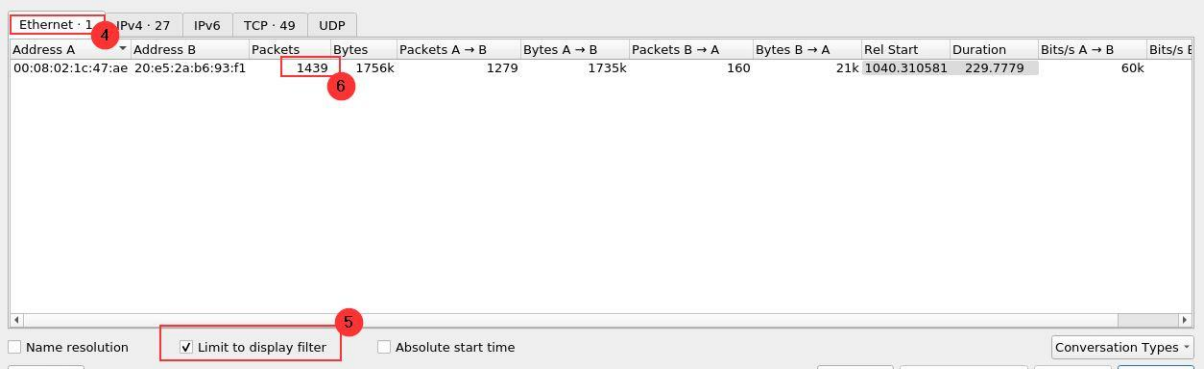
smtp

No.	Time	Source	Destination	Protocol	Length	Info
28506	2021-09-24 17:02:45.964344	10.9.23.102	185.4.29.135	SMTP	70	C: EHLO localhost
28521	2021-09-24 17:02:46.192228	185.4.29.135	10.9.23.102	SMTP	110	S: 250-mail.mailfa.com | SIZE 30000000 | AUTH LOGIN
28524	2021-09-24 17:02:46.198191	185.4.29.135	10.9.23.102	SMTP	74	S: 235 authenticated.
28576	2021-09-24 17:02:46.778017	10.9.23.102	185.4.29.135	SMTP	86	C: MAIL FROM:<farshin@mailfa.com>
28578	2021-09-24 17:02:46.778150	10.9.23.102	185.4.29.135	SMTP	66	C: AUTH LOGIN
28598	2021-09-24 17:02:47.009894	185.4.29.135	10.9.23.102	SMTP	72	S: 334 VXNlcm5hbWU6
28602	2021-09-24 17:02:47.031611	185.4.29.135	10.9.23.102	SMTP	131	S: 550 Your SMTP Service is disable please check by your mail…
28685	2021-09-24 17:02:47.617861	10.9.23.102	185.4.29.135	SMTP	92	C: User: aG8zZWluLnNoYXJpZmlAbWFpbGZhLmNvbQ==
28695	2021-09-24 17:02:47.663931	52.97.201.242	10.9.23.102	SMTP	165	S: 220 ZR0P278CA0101.outlook.office365.com Microsoft ESMTP MA…
28711	2021-09-24 17:02:47.848092	185.4.29.135	10.9.23.102	SMTP	72	S: 334 UGFzc3dvcmQ6
28742	2021-09-24 17:02:48.252166	10.9.23.102	52.97.201.242	SMTP	70	C: EHLO localhost

20) Apply smtp as filter and then go to Statistics -> Conversations -> Etherent tab



Ethernet tab, then do enable Limit to display filter checkbox



That is all for this Write-up, hoping this will help you in solving the challenges of Carnage.

Have Fun and Enjoy Hacking!

Do visit other rooms and modules on TryHackMe for more learning.

-by Shefali Kumai