

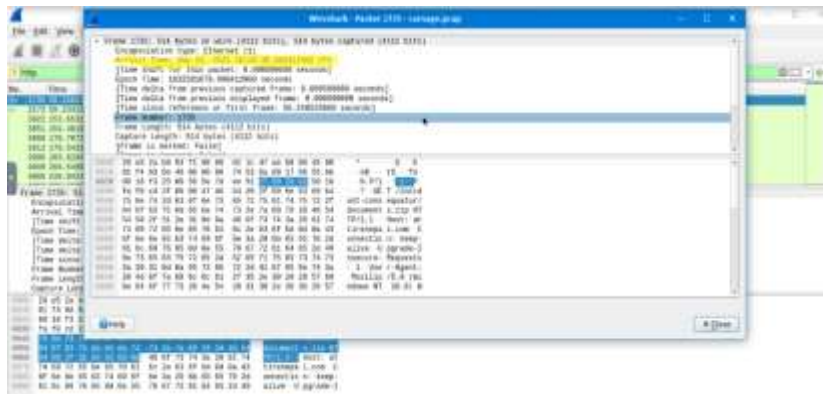
A walkthrough on the TryHackMe Carnage Room for pcap traffic analysis using Wireshark.

First, I opened the file on the Analysis Folder in the Virtual Machine using Wireshark attempted the questions as follows:

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

The packet info on the first packet revealed the required date and time of the first HTTP connection to the malicious IP. The time is indicated as Sep 24, 2021 16:44:38 but you can manually change it to fit the format specified in the question. Ans: **2021-09-24 16:44:38**

Note that you can also change the time format by selecting the “View” tab then navigating to “Time Display Format” and selecting the format you prefer.

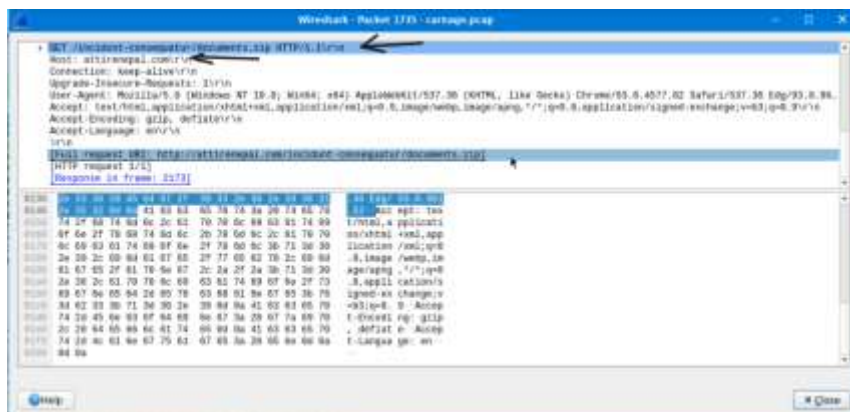


2. What is the name of the zip file that was downloaded?

On further investigation of the displayed information of the packet we see a GET request of the downloaded file as well as the domain hosting the malicious file. Ans: **documents.zip**

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

The domain hosting the malicious file is also displayed on the same window. Ans: **attirenepal.com**

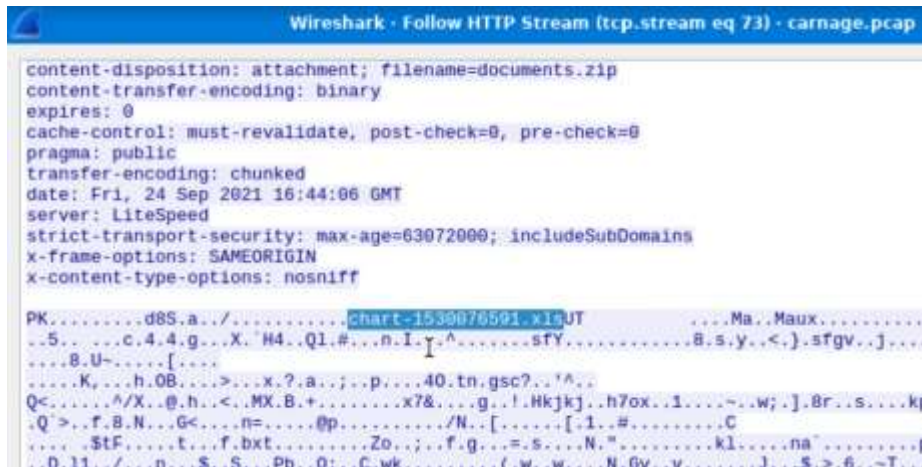


4. Without downloading the file, what is the name of the file in the zip file?

To get more information on the packet we have to follow the TCP Stream and that is accomplished by first right-clicking on the packet and selecting the “Follow” option then “TCP Stream”. A new window will be displayed showing the full stream conversation where we can also get the GET request of the file downloaded and the domain where the file is being hosted.

The name of the malicious file is displayed in the same stream as an .xls file (Microsoft Excel).

Ans: **chart-1530076591.xls**



```
Wireshark - Follow HTTP Stream (tcp.stream eq 73) - carnage.pcap

content-disposition: attachment; filename=documents.zip
content-transfer-encoding: binary
expires: 0
cache-control: must-revalidate, post-check=0, pre-check=0
pragma: public
transfer-encoding: chunked
date: Fri, 24 Sep 2021 16:44:06 GMT
server: LiteSpeed
strict-transport-security: max-age=63072000; includeSubDomains
x-frame-options: SAMEORIGIN
x-content-type-options: nosniff

PK.....d8S.a../.....chart-1530076591.xlsUT.....Ma..Maux.....
..5...c.4.4.g...X..H4..Q1.#...n.I.Y..^.....sfY.....B.s.y.<.)..sfgv..j...
...B.U~.....[.....
...K...h.OB....>...x.?..a...;...p...40.tn.gsc?..'A..
Q<...^/X..@.h.<..MX.B.+.....x7&...g...!..Hkjkj...h7ox..1...~..w;..].8r..s...kp
.Q'>..f.B.N...G<...n=...@p...../N..[.....[.1.#.....C
..StF...t...f.bxt.....Zo...;..f.g...=.S...N..^.....kl.....na'.....p
..D.11../...n...S..S...Pb..O:..C.wk.....f.w.w...N.Gv..v.....J...S.>.6..~T..
```

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

The webserver and version as also displayed on the same stream window. Ans: **LiteSpeed**

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

Ans: **PHP/7.2.34**



```
Wireshark - Follow TCP Stream (tcp.stream eq 73) - carnage.pcap

GET /incident-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/93.0.961.52 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
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=/
content-description: File Transfer
content-type: application/octet-stream
content-disposition: attachment; filename=documents.zip
content-transfer-encoding: binary
expires: 0
cache-control: must-revalidate, post-check=0, pre-check=0
pragma: public
transfer-encoding: chunked
date: Fri, 24 Sep 2021 16:44:06 GMT
server: LiteSpeed
strict-transport-security: max-age=63072000; includeSubDomains
x-frame-options: SAMEORIGIN
x-content-type-options: nosniff
```

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

The hint specifies that we check HTTPS traffic and narrow down the timeframe from 16:45:11 to 16:45:30. To make the search easier for us we can use the following filter:

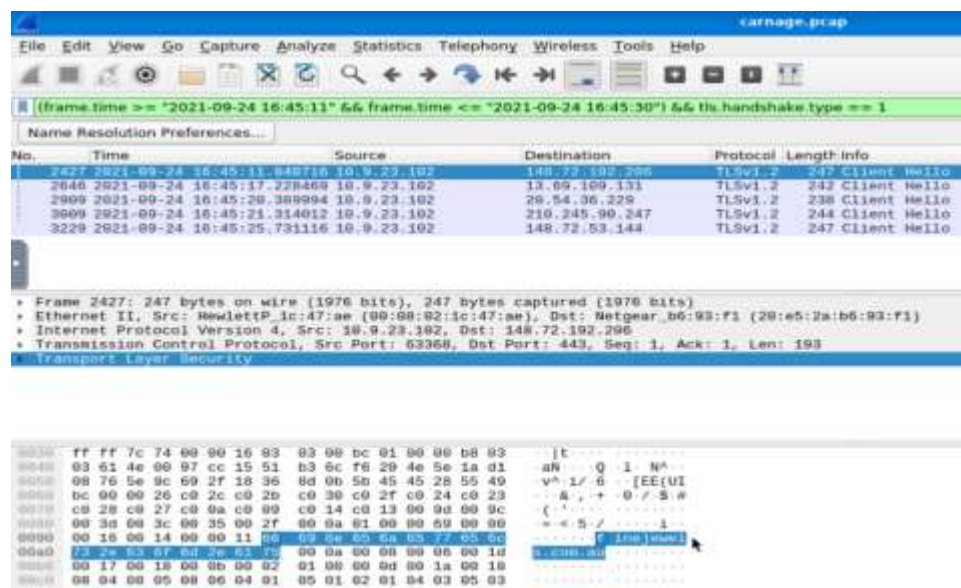
`(frame.time >= "2021-09-24 16:45:11" && frame.time <= "2021-09-24 16:45:30") && tls.handshake.type == 1`

The filter is broken down as follows:

- First we use **`frame.time`** to specify a specific time in the pcap as specified by THM. The operators `>=` and `<=` specify that we are interested in the time in between.
- **`tls.handshake.type == 1`** is used to specify the beginning of a TLS handshake where the client sends a “hello” to the server. Note that HTTPS uses TLS/SSL encryption.

Applying the filter will bring up 5 packets displayed and by examining each you will be able to come up with 3 domain names from the. A search through Virus Total will help you pick out the malicious ones.

Ans: **`finejewels.com.au`**, **`thietbiagt.com`**, **`new.americold.com`**



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

We have already identified the first domain to be “**`finejewels.com.au`**” which we got from the first packet of our previous filter. To view the certificate, we will follow the TCP stream conversation. From the resulting window we will find the Certificate Authority as it has been highlighted in several instances.

Ans: **`GoDaddy`**



drb_ra

2 years ago

Cobalt Strike Server Found
C2: HTTPS @ 185[.]106[.]96[.]158:8888
C2 Server: [survmeter\[.\]live\[.\]gscp\[.\]R/185\[.\]106\[.\]96\[.\]158\[.\]gscp\[.\]R/](https://survmeter[.]live[.]gscp[.]R/185[.]106[.]96[.]158[.]gscp[.]R/)
POST URI: /supprq/sa/
Country: United States
ASN: DediPath
Host Header: [ocsp\[.\]verisign\[.\]com](https://ocsp[.]verisign[.]com)

#c2 #cobaltstrike

Note: The domain name and Host Header are defanged and can be resolved into to their original state using CyberChef.

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).

As was with the first IP address, information on the second can be obtained from Virus Total and the domain name resolved with CyberChef. Ans: **securitybusinpuff.com**



drb_ra

2 years ago

Cobalt Strike Server Found
C2: HTTPS @ 185[.]125[.]204[.]174:4444
C2 Server: [securitybusinpuff\[.\]com\[.\]jquery-3\[.\]](https://securitybusinpuff[.]com[.]jquery-3[.])
POST URI: /jquery-3[.]3[.]2[.]min[.]js
Country: N/A
ASN: Hydra Communications Ltd

#c2 #cobaltstrike

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

The hint specifies that we look into the POST traffic so we shall use the following filter to achieve that: **http.request.method == POST** then we will follow the TCP stream conversation and that will reveal the host/domain name. Ans: **maldivehost.net**



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

The same stream conversation will also reveal the first eleven characters of the POST request. Ans: **zLlisQRWZI9**



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

From the earlier POST filter, the packet length is shown in the Length column. Ans: **281**

No.	Time	Source	Destination	Protocol	Length	Info
3822	153.653113	10.9.23.102	208.91.128.6	HTTP	281	POST
3908	178.767210	10.9.23.102	208.91.128.6	HTTP	285	POST
3996	203.829455	10.9.23.102	208.91.128.6	HTTP	285	POST
4006	228.842458	10.9.23.102	208.91.128.6	HTTP	273	POST
4017	254.837243	10.9.23.102	208.91.128.6	HTTP	293	POST
4027	279.063986	10.9.23.102	208.91.128.6	HTTP	289	POST
4037	304.108570	10.9.23.102	208.91.128.6	HTTP	273	POST
4046	329.217819	10.9.23.102	208.91.128.6	HTTP	285	POST
4090	354.299575	10.9.23.102	208.91.128.6	HTTP	293	POST

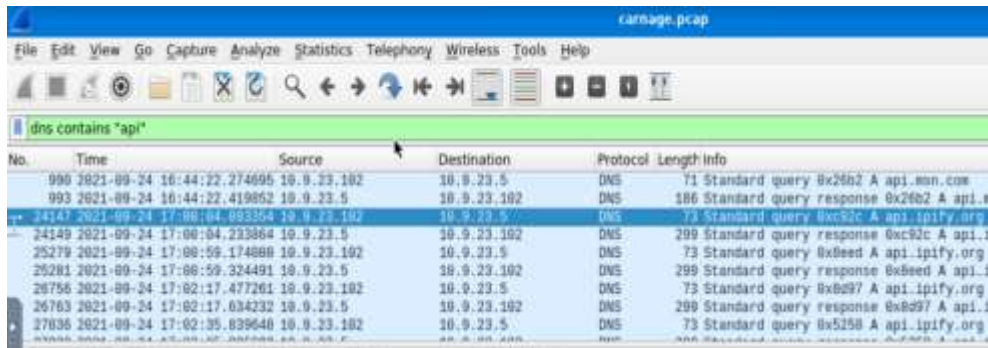
16. What was the Server header for the malicious domain from the previous question?

We can get this from the earlier TCP stream conversation window. Ans: **Apache/2.4.49 (cPanel) OpenSSL/1.1.1l mod_bwlimited/1.4**



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)

We are requested to look for at DNS queries that use “api” to check for IP addresses, we can tailor our filter our packets to display DNS and anything containing “api”. Our filter will be as follows: **dns contains “api”**. Applying that filter will display DNS packets with the word “api”. Ans: **2021-09-24 17:00:04**



The screenshot shows a Wireshark packet capture of a network traffic. The filter bar at the top is set to 'dns contains api'. The packet list shows several DNS packets. The selected packet is a standard query response from 10.9.23.5 to 10.9.23.102, containing a query for 'api.ipify.org'.

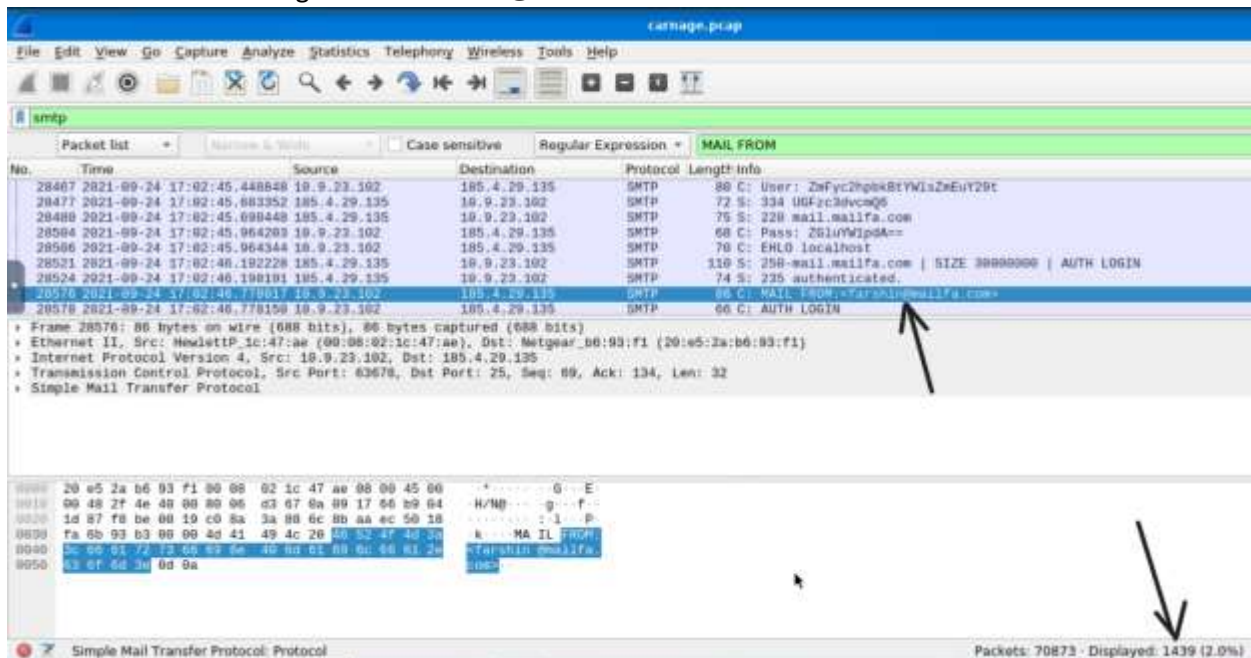
No.	Time	Source	Destination	Protocol	Length	Info
990	2021-09-24 16:44:22.274695	10.9.23.102	10.9.23.5	DNS	71	Standard query 0x26b2 A api.msn.com
993	2021-09-24 16:44:22.419852	10.9.23.5	10.9.23.102	DNS	186	Standard query response 0x26b2 A api.msn.com
24142	2021-09-24 17:00:04.893354	10.9.23.102	10.9.23.5	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
25279	2021-09-24 17:00:09.174889	10.9.23.102	10.9.23.5	DNS	73	Standard query 0x8edc A api.ipify.org
25281	2021-09-24 17:00:09.324491	10.9.23.5	10.9.23.102	DNS	299	Standard query response 0x8edc A api.ipify.org
26756	2021-09-24 17:02:17.477261	10.9.23.102	10.9.23.5	DNS	73	Standard query 0xb097 A api.ipify.org
26763	2021-09-24 17:02:17.034232	10.9.23.5	10.9.23.102	DNS	299	Standard query response 0xb097 A api.ipify.org
27036	2021-09-24 17:02:35.839640	10.9.23.102	10.9.23.5	DNS	73	Standard query 0xb258 A api.ipify.org

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

Looking at the packet, the domain is displayed. Ans: **api.ipify.org**

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

SMTP (Simple Mail Transfer Protocol) is used when sending/receiving mail so a global SMTP search will reveal all packets related to SMTP. A further “find” search (Ctrl + F) for “MAIL FROM” will reveal the exact mail we are looking for. Ans: **farshin@mailfa.com**



The screenshot shows a Wireshark packet capture of a network traffic. The filter bar at the top is set to 'smtp'. The packet list shows several SMTP packets. The selected packet is an SMTP AUTH LOGIN packet from 10.9.23.102 to 105.4.29.135, containing the MAIL FROM address 'farshin@mailfa.com'.

No.	Time	Source	Destination	Protocol	Length	Info
28467	2021-09-24 17:02:45.448848	10.9.23.102	105.4.29.135	SMTP	88	C: User: Zmfyc2pex8TYW1sZuEuY29t
28477	2021-09-24 17:02:45.683352	105.4.29.135	10.9.23.102	SMTP	72	S: 334 UGFic3dvcmQ6
28489	2021-09-24 17:02:45.698448	105.4.29.135	10.9.23.102	SMTP	75	S: 220 mail.mailfa.com
28504	2021-09-24 17:02:45.964203	10.9.23.102	105.4.29.135	SMTP	68	C: Pass: Z51uWlpsA==
28506	2021-09-24 17:02:45.964344	10.9.23.102	105.4.29.135	SMTP	70	C: EHLO localhost
28521	2021-09-24 17:02:48.192228	105.4.29.135	10.9.23.102	SMTP	119	S: 250-mail.mailfa.com SIZE 38888888 AUTH LOGIN
28524	2021-09-24 17:02:48.198191	105.4.29.135	10.9.23.102	SMTP	74	S: 235 authenticated.
28576	2021-09-24 17:02:48.778017	10.9.23.102	105.4.29.135	SMTP	88	C: MAIL FROM:farshin@mailfa.com
28578	2021-09-24 17:02:48.778159	10.9.23.102	105.4.29.135	SMTP	66	C: AUTH LOGIN

The packet details pane shows the selected packet (28576) and its structure. The 'MAIL FROM' field is highlighted, showing the address 'farshin@mailfa.com'.

Simple Mail Transfer Protocol: Protocol

Packets: 70873 · Displayed: 1439 (2.0%)

20. How many packets were observed for the SMTP traffic?

Ans: **1439**