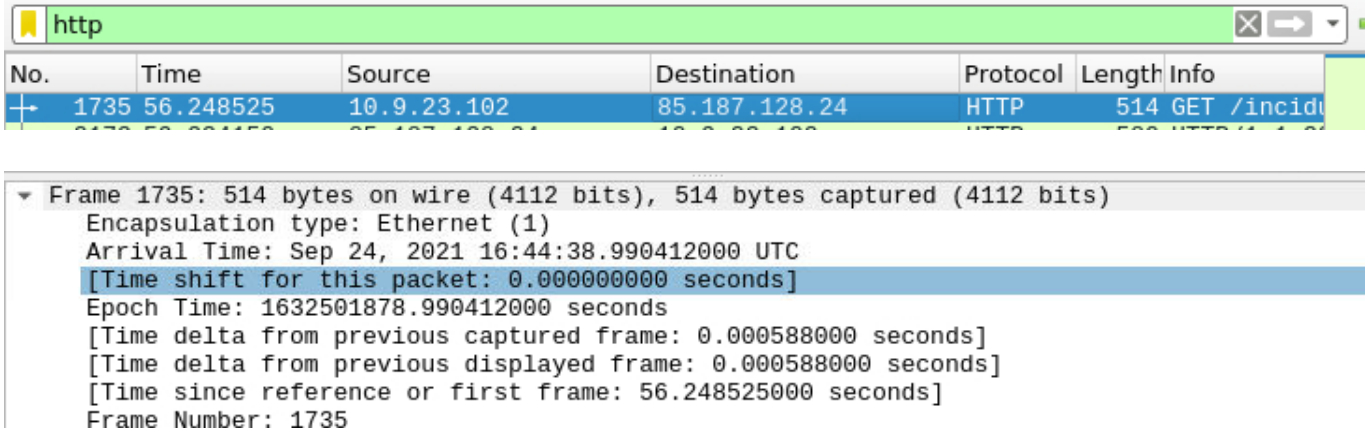
Overview

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.

Our first task is to establish when the first `HTTP` connection was seen, we use http in the filter bar to search for our first http connection then we can follow the frame drop down and we are able to see the arrival of the malicious IP made contact:

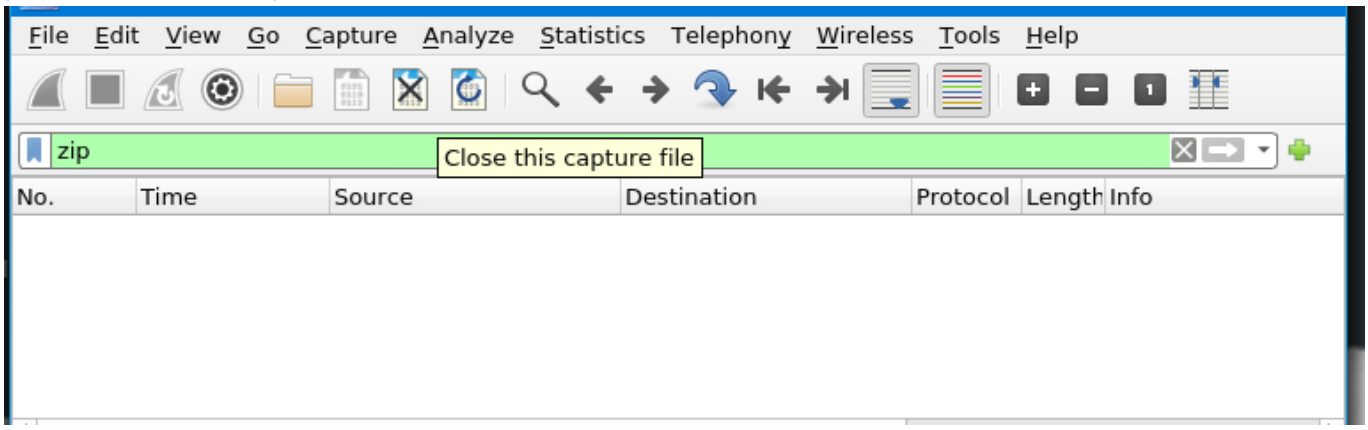


What was the date and time for the first HTTP connection to the malicious IP?

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

2021-09-24 16:44:38

Our next task is to identify a zip file that was downloaded, we need to find out what the name of this zip file is, trying to type `zip` in the filter bar shows up green but there is no signs of any packets with the zip file:

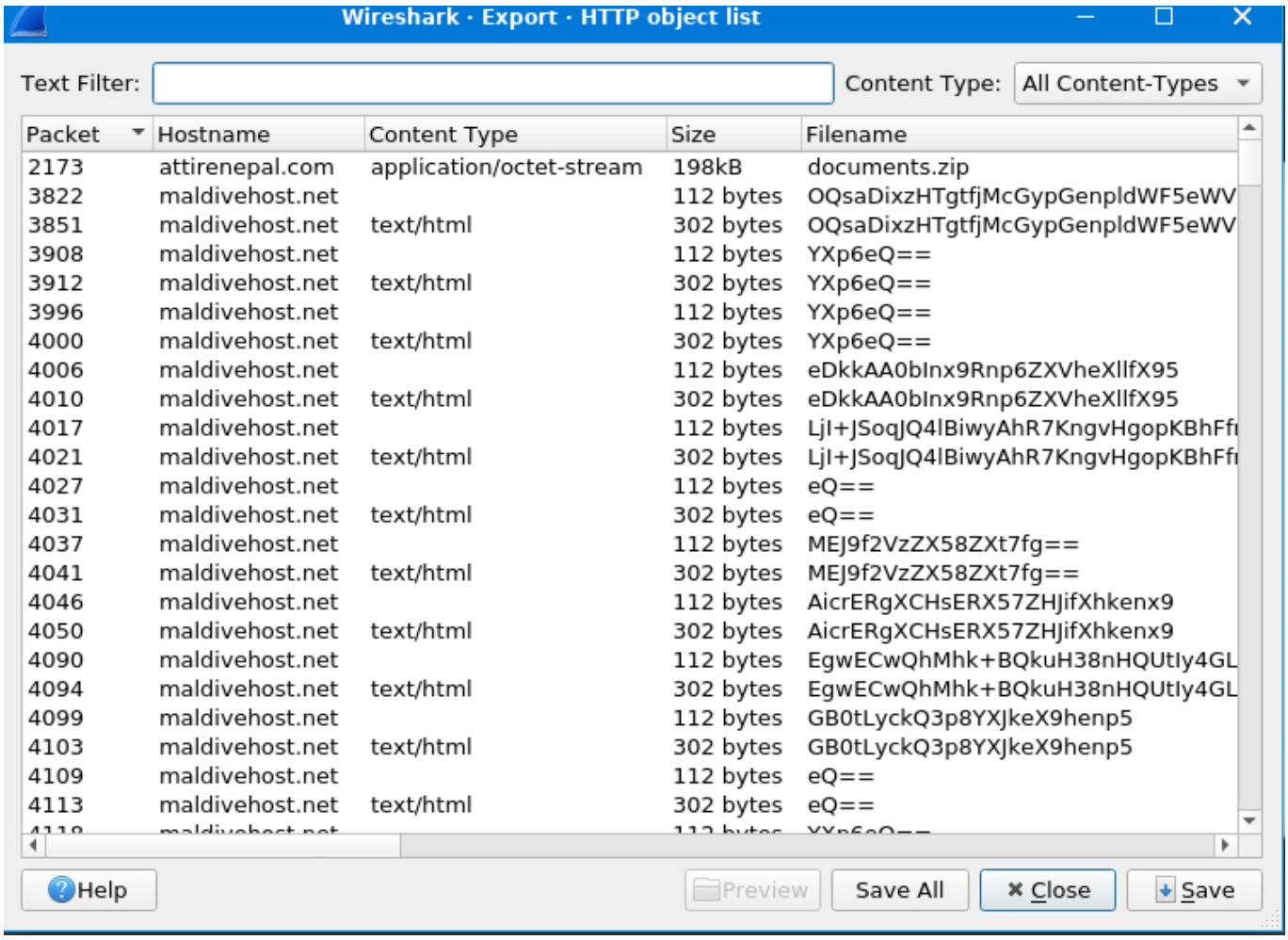


After searching through a few packets, I could not find any zip files in any of them, after googling `how to find a zip file in wireshark`, I found a link (https://www.rubyguides.com/2012/01/four-ways-to-extract-files-from-pcaps/#:~:text=1.,in%20all%20the%20http%20requests.) that showed me fouur ways to extract

files from Pcaps. I tried the first solution and managed to find the zip file by going into File > Export > Objects > Http:

1. Wireshark: http export

You can find this at **File > Export > Objects > Http**, you will be presented with a list of files found in all the http requests. The bad thing about this feature is that even with the latest version (1.6.5 at the time of this writing) you still can't sort by column or apply any filters which makes finding something specific hard.



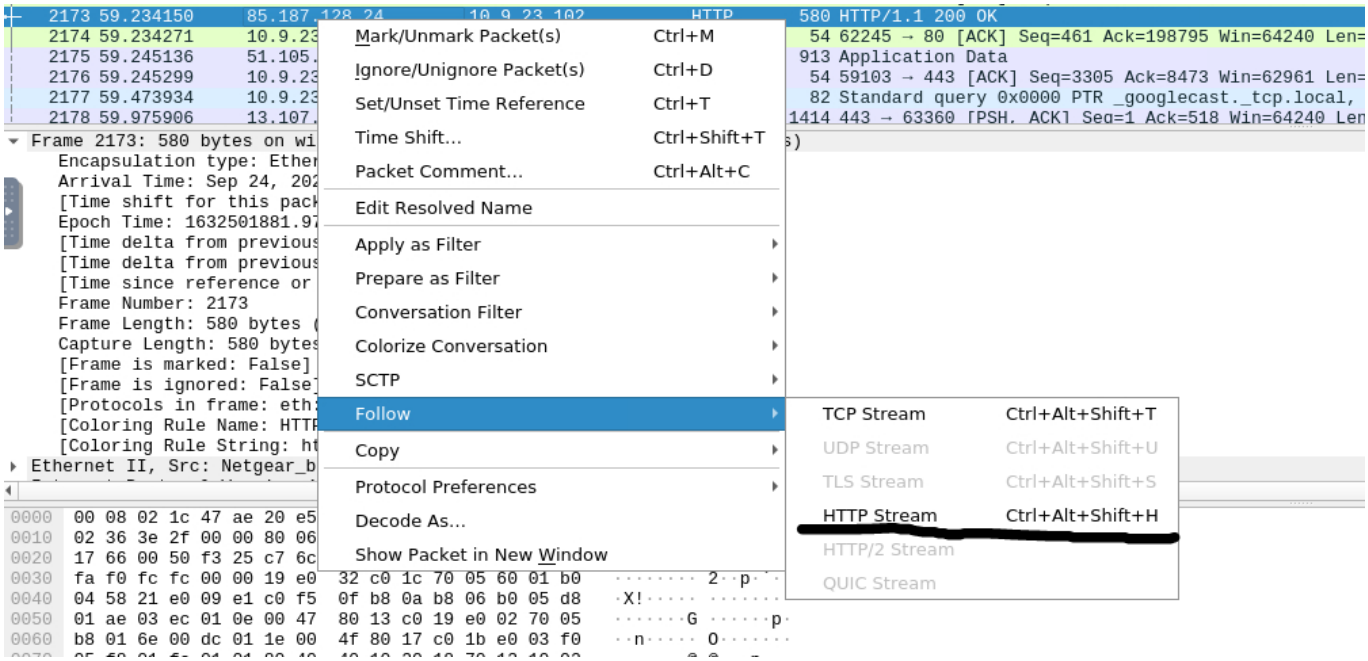
Packet	Hostname	Content Type	Size	Filename
2173	attirenepal.com	application/octet-stream	198kB	documents.zip
3822	maldivehost.net		112 bytes	OQsaDixzHTgtfjMcGypGenpldWF5eWV
3851	maldivehost.net	text/html	302 bytes	OQsaDixzHTgtfjMcGypGenpldWF5eWV
3908	maldivehost.net		112 bytes	YXp6eQ==
3912	maldivehost.net	text/html	302 bytes	YXp6eQ==
3996	maldivehost.net		112 bytes	YXp6eQ==
4000	maldivehost.net	text/html	302 bytes	YXp6eQ==
4006	maldivehost.net		112 bytes	eDkkAA0bInx9Rnp6ZXVheXllfX95
4010	maldivehost.net	text/html	302 bytes	eDkkAA0bInx9Rnp6ZXVheXllfX95
4017	maldivehost.net		112 bytes	LjI+JSoqJQ4lBiwyAhR7KngvHgopKBhFf
4021	maldivehost.net	text/html	302 bytes	LjI+JSoqJQ4lBiwyAhR7KngvHgopKBhFf
4027	maldivehost.net		112 bytes	eQ==
4031	maldivehost.net	text/html	302 bytes	eQ==
4037	maldivehost.net		112 bytes	MEJ9f2VzZX58ZXt7fg==
4041	maldivehost.net	text/html	302 bytes	MEJ9f2VzZX58ZXt7fg==
4046	maldivehost.net		112 bytes	AicrERgXCHsERX57ZHJifXhkenx9
4050	maldivehost.net	text/html	302 bytes	AicrERgXCHsERX57ZHJifXhkenx9
4090	maldivehost.net		112 bytes	EgwECwQhMhk+BQkuH38nHQUtIy4GL
4094	maldivehost.net	text/html	302 bytes	EgwECwQhMhk+BQkuH38nHQUtIy4GL
4099	maldivehost.net		112 bytes	GB0tLyckQ3p8YXJkeX9henp5
4103	maldivehost.net	text/html	302 bytes	GB0tLyckQ3p8YXJkeX9henp5
4109	maldivehost.net		112 bytes	eQ==
4113	maldivehost.net	text/html	302 bytes	eQ==

We have found the zip file that was downloaded, which is called `documents.zip`

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

Now our next step is to find the domain that was hosting this malicious zip file. We can see the packet is `2173`, so we find packet `2173` and we follow the HTTP Stream to find out the domain

that hosted this malicious zip file:



We then see a `GET` Request, which is used for retrieving and requesting data from a specified server, the `GET` request allows us to see the domain of where the malicious zip file was hosted:

```
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
```

What was the domain hosting the malicious zip file?
attirenepal.com

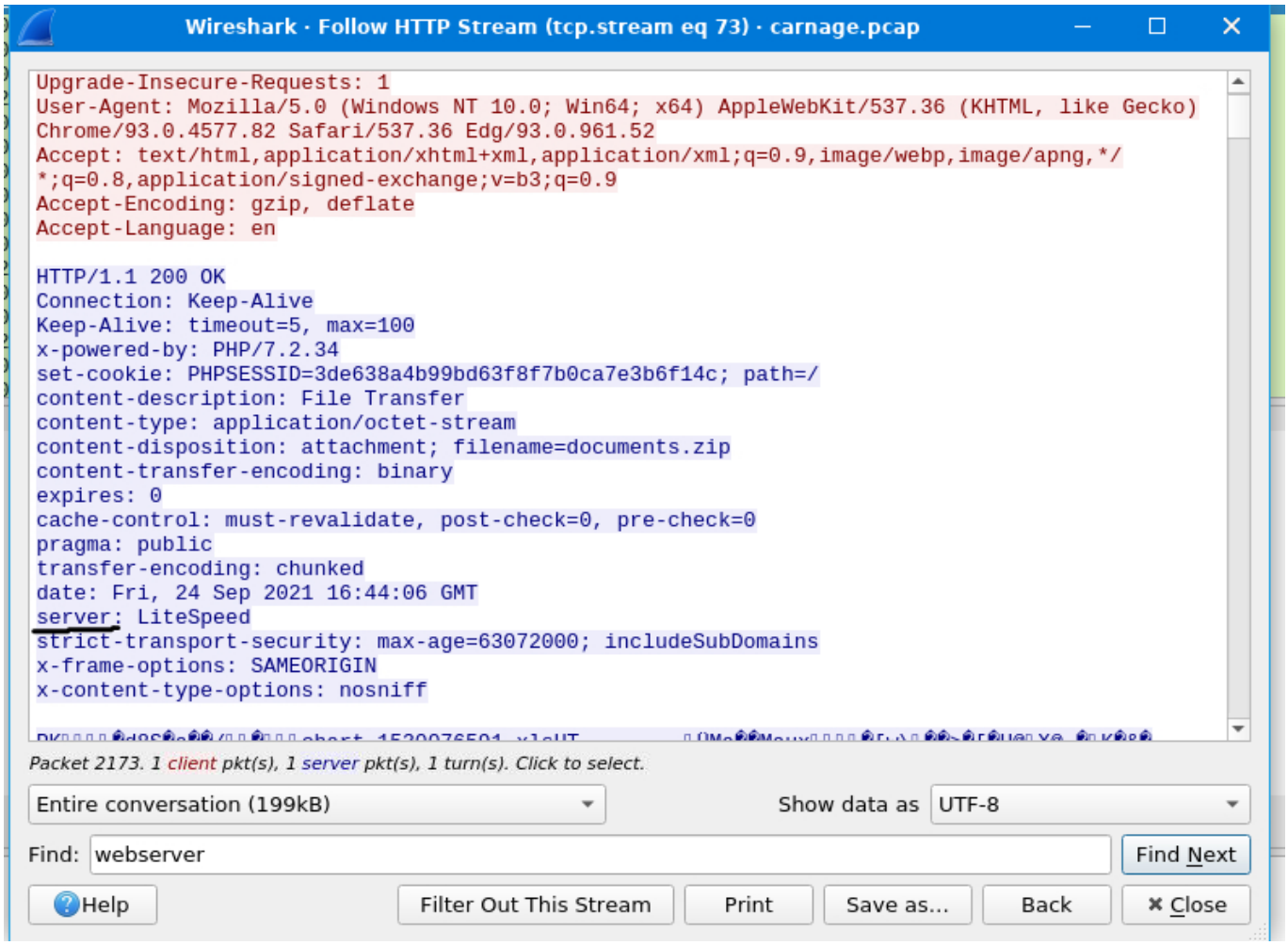
Now we have found the domain and the name of the zip file that was downlaoded, lets see what the file is called without trying to downlaod the file. By doing this we go back to packet `2173` and follow with another `HTTP Stream` and on the first line of encoding we are able to see a file called `chart-1530076591.xls`:

```
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.............
[w\...>..[.U@.X@,..K.&.
..5.. ...c.4.4.g...X.`H4..Ql.#...n.I...^.......sfY............8.s.y..<.}.sfgv..j........
```

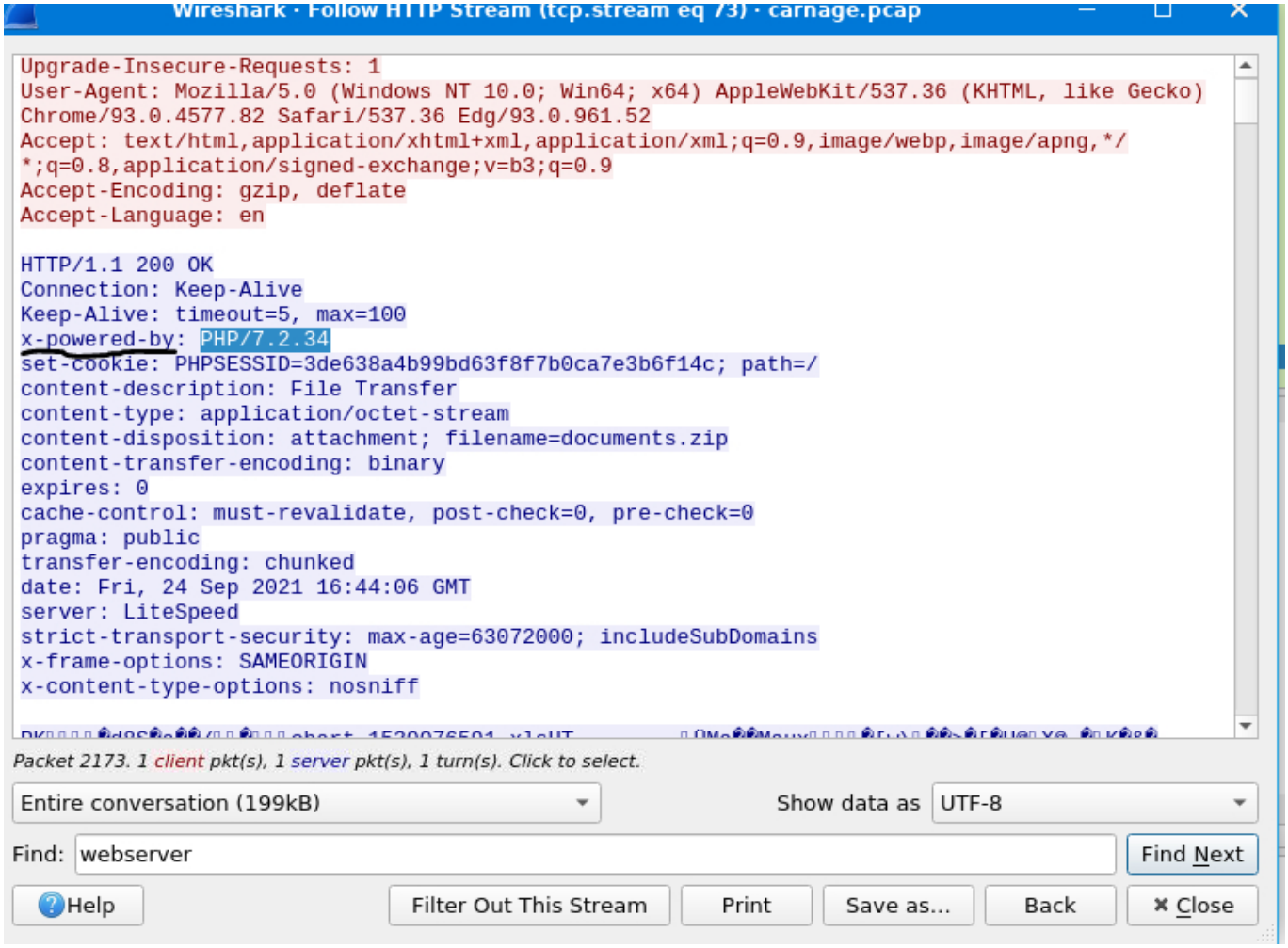
Without downloading the file, what is the name of the file in the zip file?
chart-1530076591.xls

Now we need to identify the webserver, which is pretty easy to spot as it is under the server section when follwing the `HTTP Stream`:



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

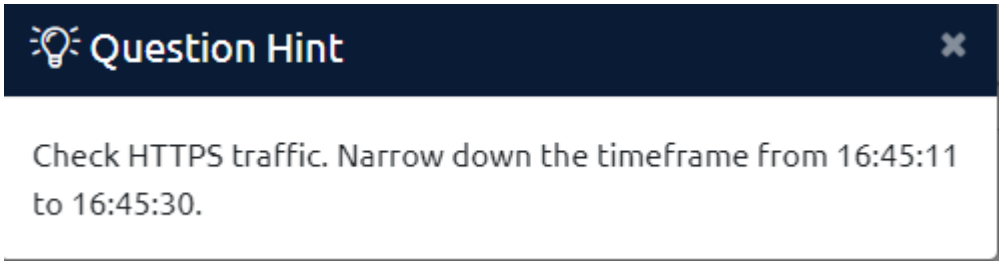
We have also been asked to identify the version of the server, which is also very easy to spot, it is under the `x-powered-by`:



What is the version of the webserver from the previous question?
PHP/7.2.34

We have now found out that the malicious files were downloaded from multiple domains, so let's track them down

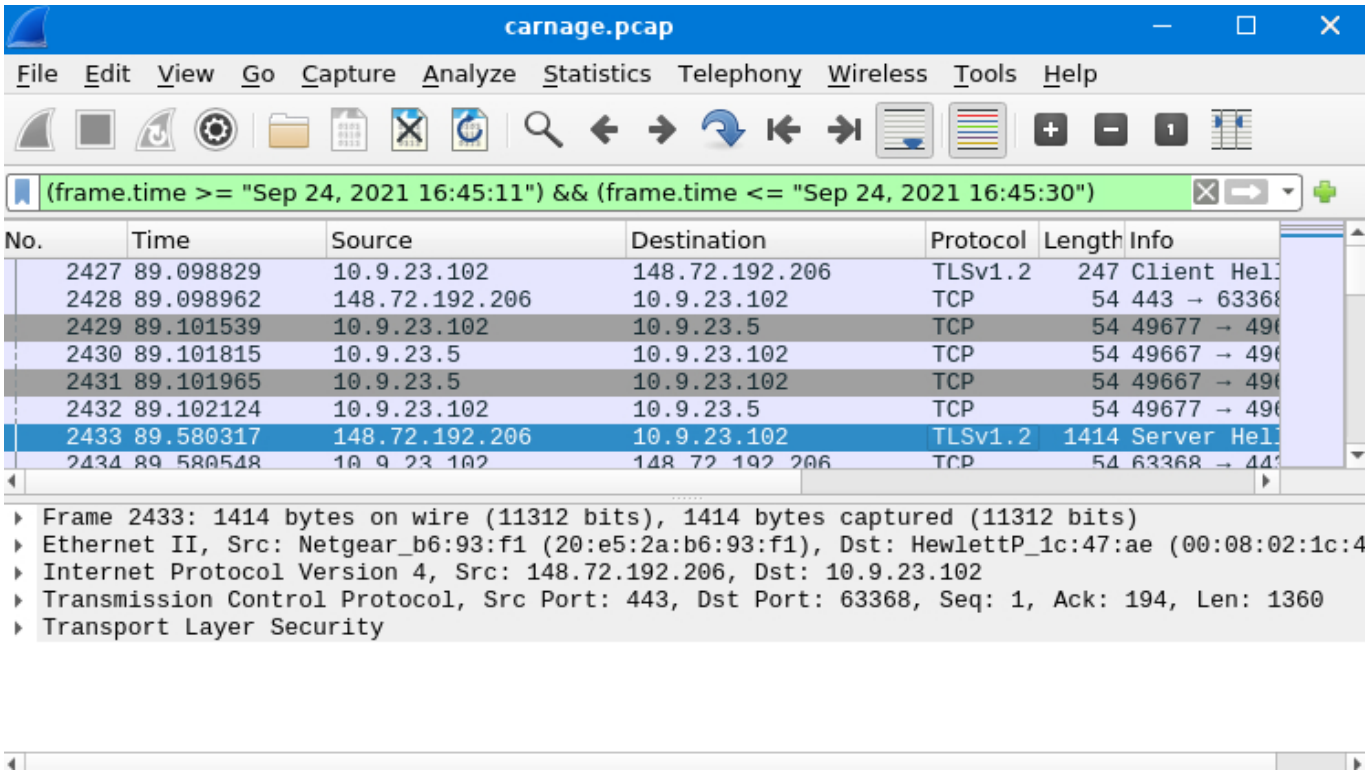
After looking through so many packets, I was unable to find any of the other domains, luckily the room gives us a hint to find these:



As I was unaware on how to do this, I searched up `how to search through time frames in wireshark` - I found this link (https://securitronlinux.com/bejiitaswrath/filter-for-a-specific-time-frame-in-wireshark/) that showed how to apply th filter in wireshark

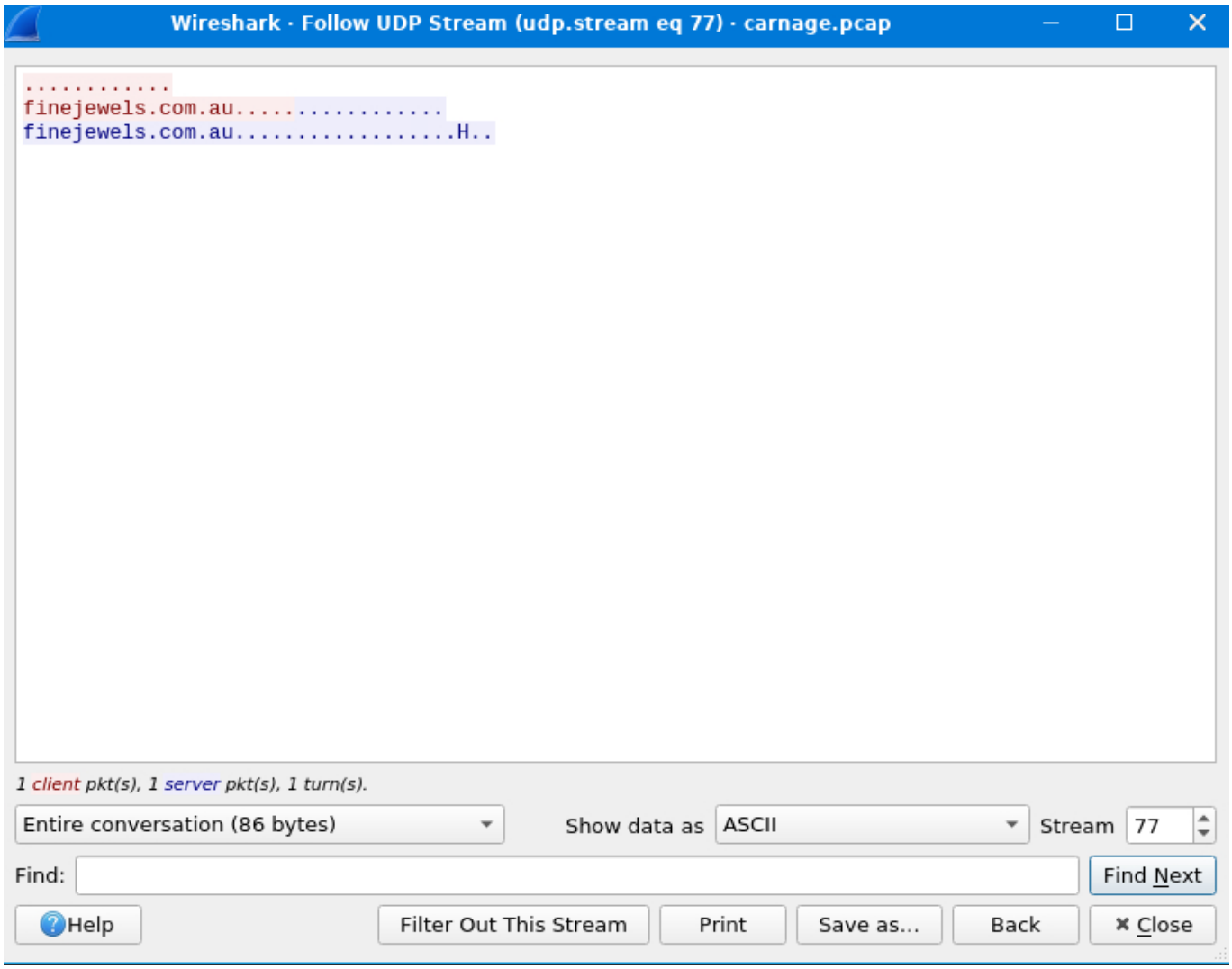
Going back to Wireshark we apply the filter `(frame.time >= "Sep 24, 2021 16:45:11") && (frame.time <= "Sep 24, 2021 16:45:30")` - This looks for packets between September 24 2021

16:45:11 between a 19 second gap as the filter ends at September 24 2021 16:45:30:

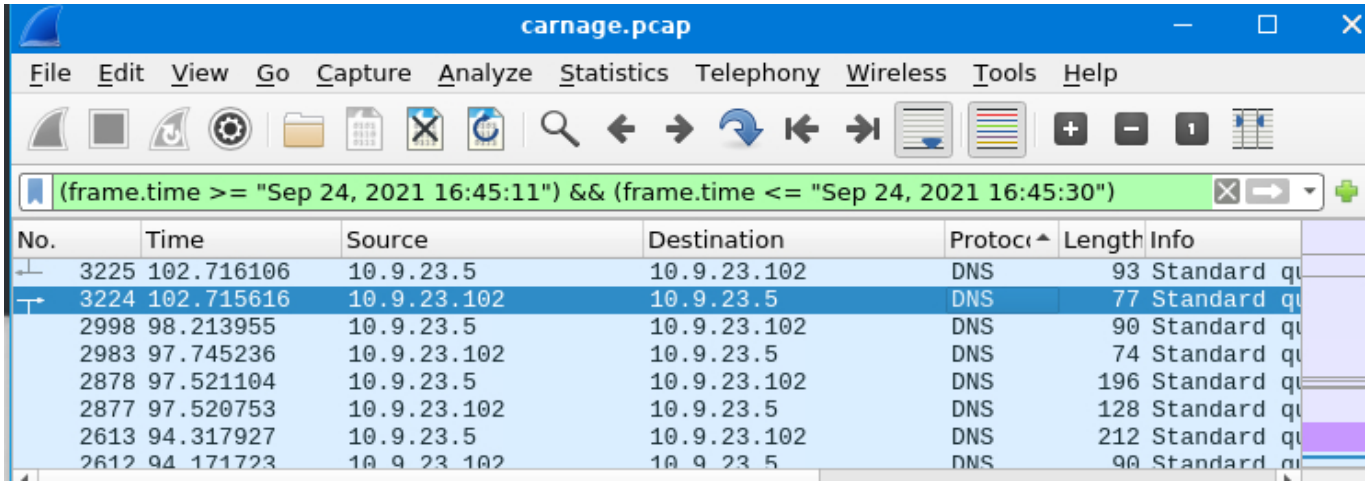


And by follwing the UDP stream we successfully find out the first domain out of the three that was involved with the malicious activity:

finejewels.com.au



As we are looking for domains I filtered the packets by protcol to find DNS and this tidied up all the packets to keep all the DNS packets in one place:



Here I was able to find the other two domains:
new.americold.com:

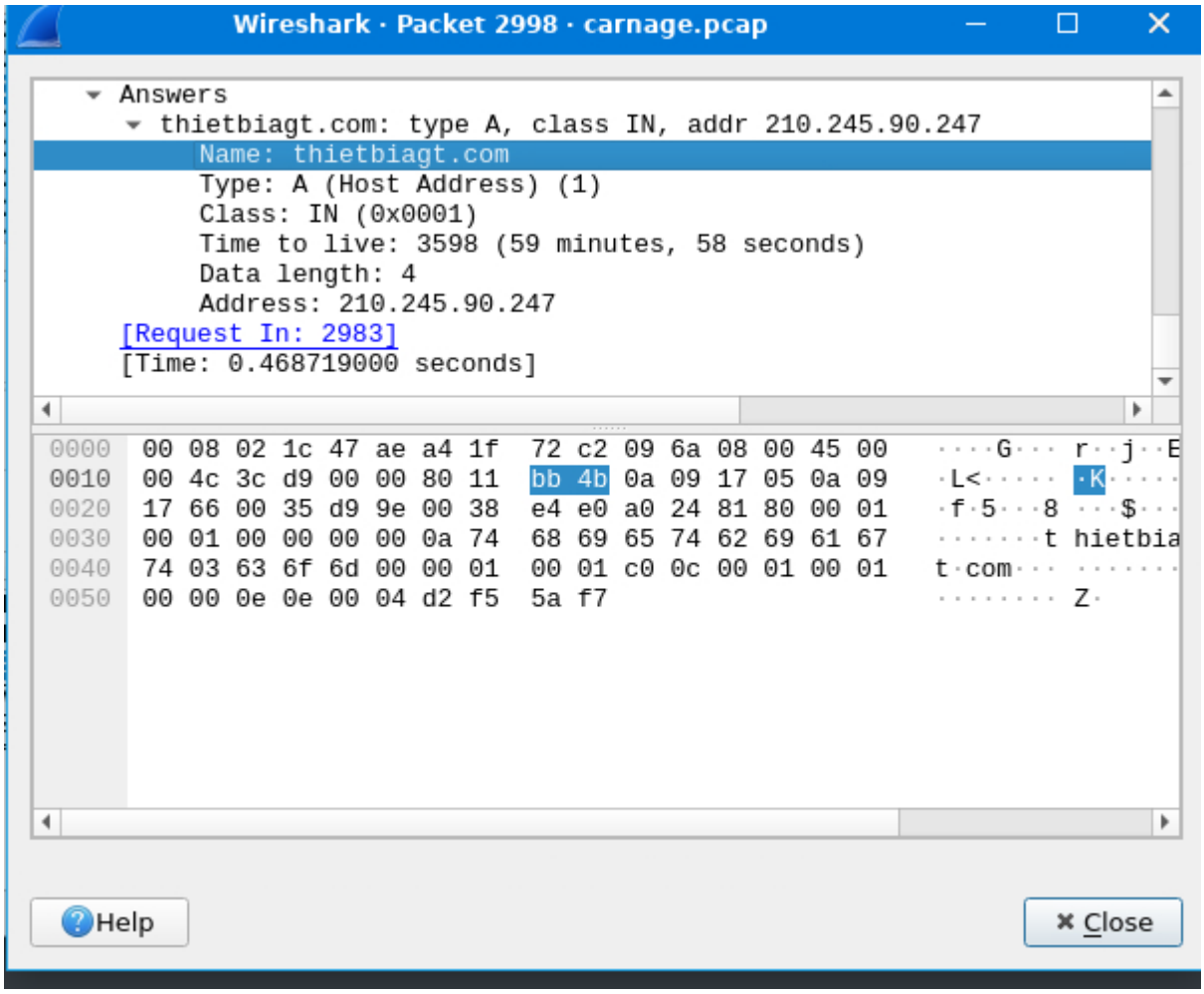
Wireshark · Packet 3224 · carnage.pcap

```
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ new.americold.com: type A, class IN
        Name: new.americold.com
        [Name Length: 17]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 3225]
```

```
0000  a4 1f 72 c2 09 6a 00 08  02 1c 47 ae 08 00 45 00   ··r··j·· ··G···E
0010  00 3f bf 3d 00 00 80 11  38 f4 0a 09 17 66 0a 09   ·?·=···· 8····f·
0020  17 05 e6 d6 00 35 00 2b  d8 a0 65 b4 01 00 00 01   ·····5·+ ··e····
0030  00 00 00 00 00 00 03 6e  65 77 09 61 6d 65 72 69   ·····n ew·amer
0040  63 6f 6c 64 03 63 6f 6d  00 00 01 00 01             cold·com ·····
```

Help Close

thietbiagt.com:



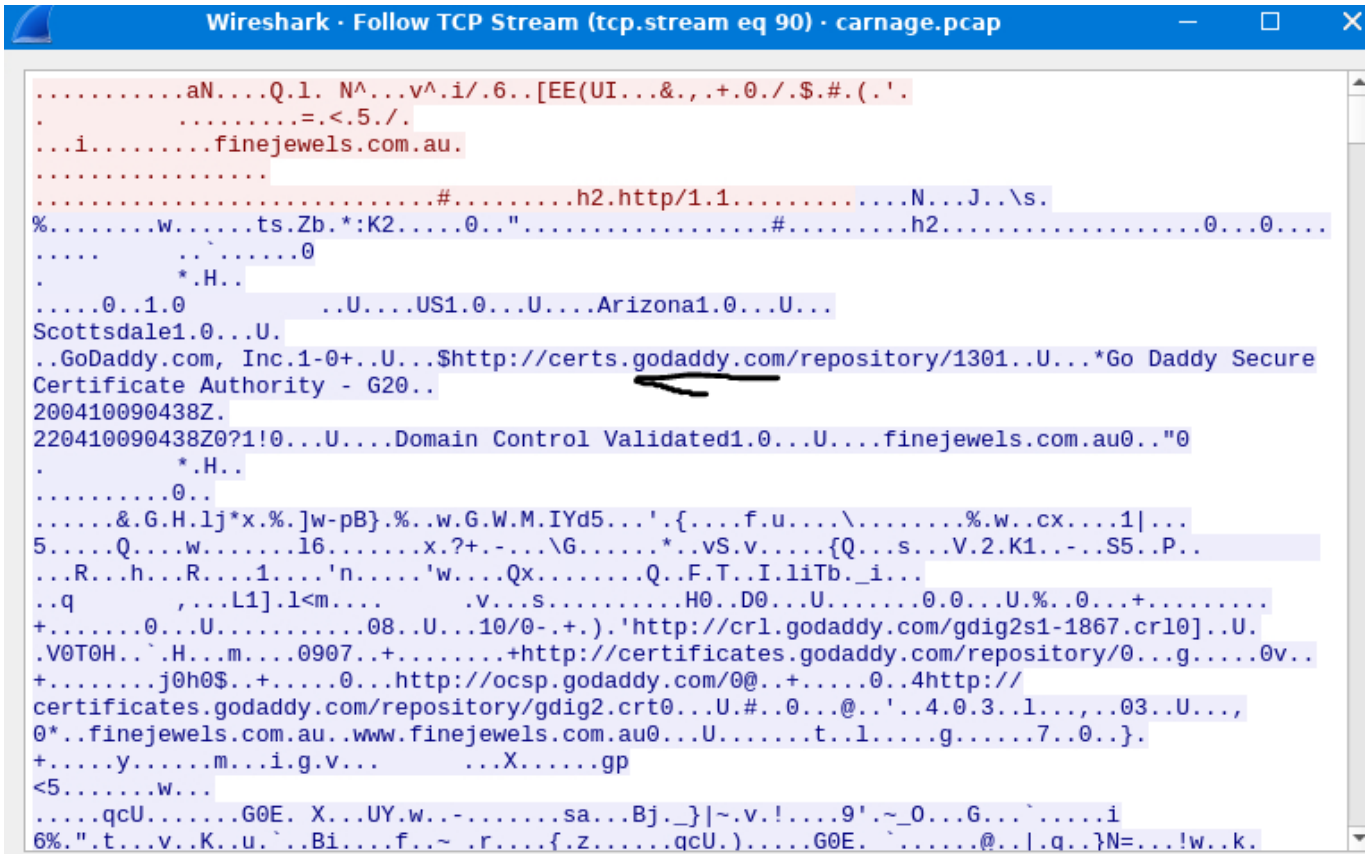
W have successfully captured all 3 domains that was a part of this malicious activity

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

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

Now we have been asked to identify what CA (Certificate Authority) was issued by the SSL certificate in the first domain - I followd the TCP stream of the first TCP packet within the time

frame filter we used and found out the CA:

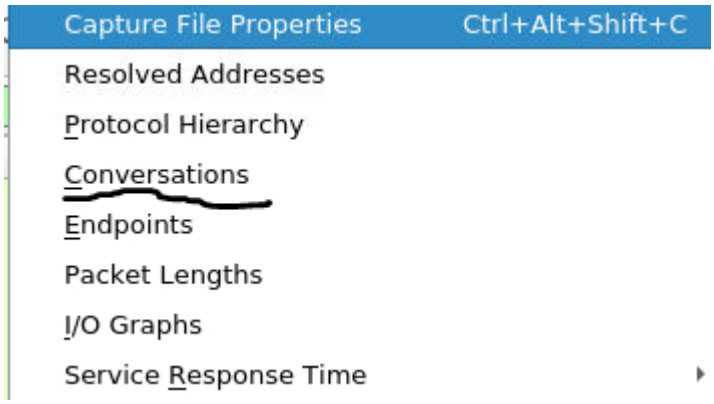


Which certificate authority issued the SSL certificate to the first domain from the previous question?

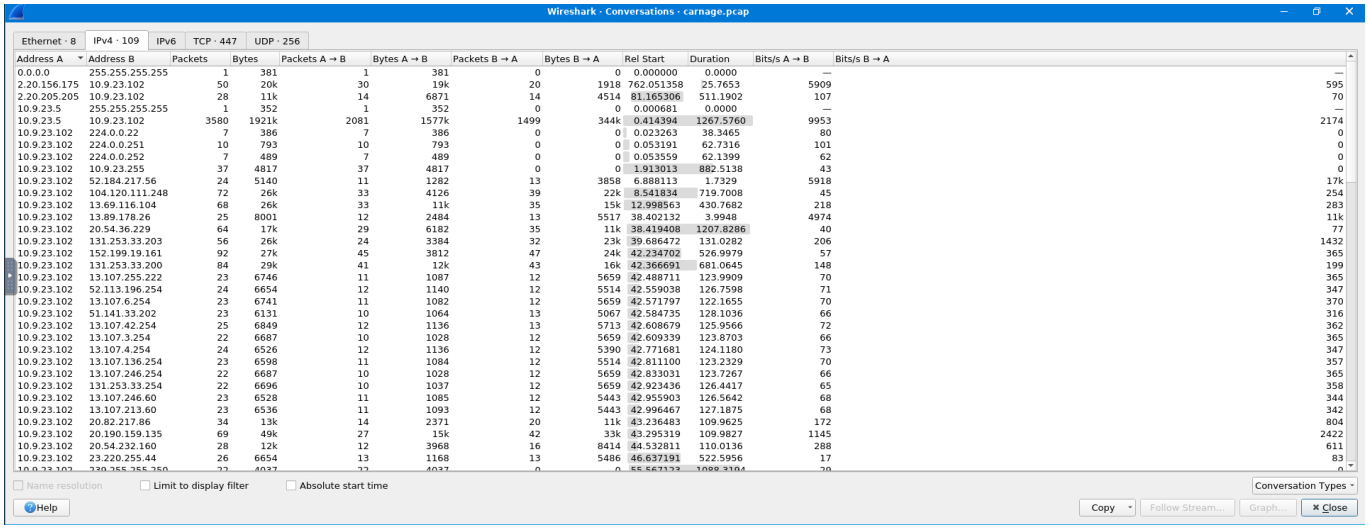
Godaddy

Our next task is to find two IP addresses of the cobalt strike servers - We filter all packets to HTTP as we are trying to find the Cobalt Strike C2 servers, however I did not find anything by doing this

Then I learned that we can see multiple IPs due to different conversations being made from different servers by going to `statistics > conversations`:

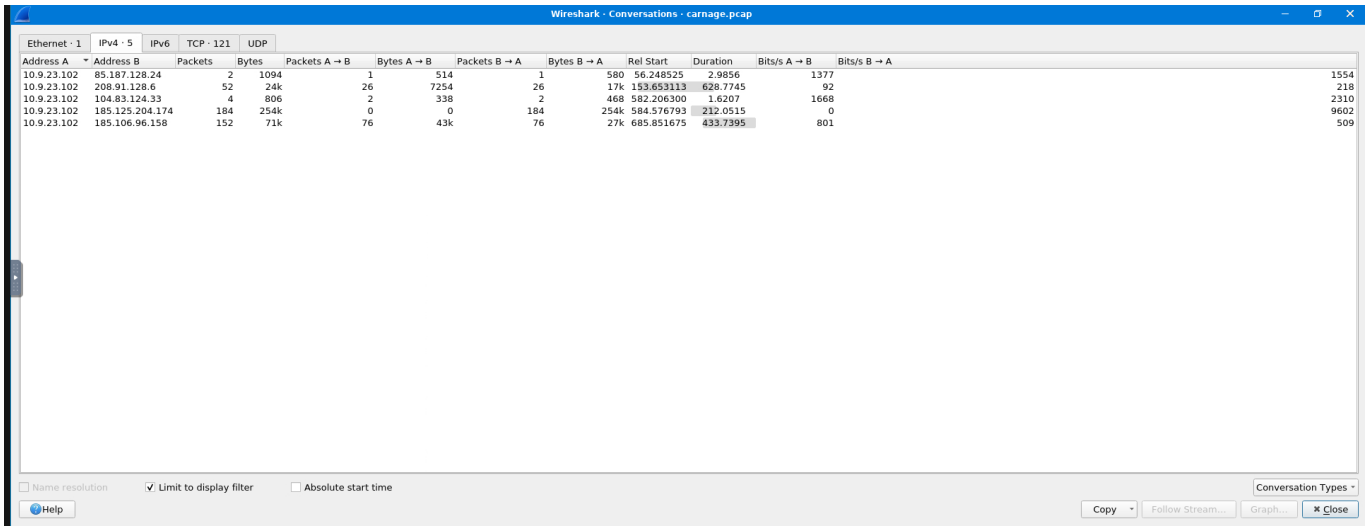


Opening this up shows us mutiple conversations that have been made and we also want to view IPv4 to find the ip addresses:



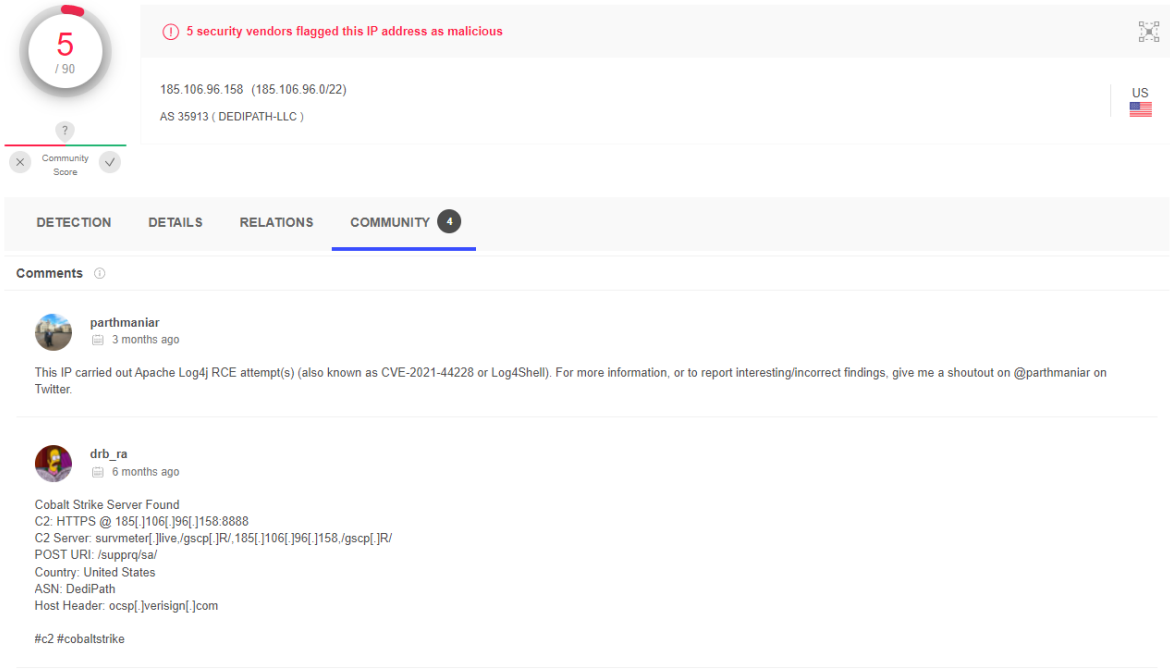
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
0.0.0.0	255.255.255.255	1	381	1	381	0	0	0.000000	0.0000	—	—
2.20.156.175	10.9.23.102	50	20k	30	19k	20	1918	762.051358	25.7653	5909	595
2.20.205.205	10.9.23.102	28	11k	14	6871	14	4514	81.165306	511.1902	107	70
10.9.23.5	255.255.255.255	1	352	1	352	0	0	0.000681	0.0000	—	—
10.9.23.5	10.9.23.102	3580	1921k	2081	1577k	1499	344k	0.414394	1267.5760	9953	2174
10.9.23.102	224.0.0.22	7	386	7	386	0	0	0.023263	38.3465	80	0
10.9.23.102	224.0.0.251	10	793	10	793	0	0	0.053191	62.7316	101	0
10.9.23.102	224.0.0.252	7	489	7	489	0	0	0.053559	62.1399	62	0
10.9.23.102	10.9.23.255	37	4817	37	4817	0	0	1.913013	882.5138	43	0
10.9.23.102	52.184.217.56	24	5140	11	1282	13	3858	6.888113	1.7329	5918	17k
10.9.23.102	104.120.111.248	72	26k	33	4126	39	22k	8.541834	719.7008	45	254
10.9.23.102	13.69.116.104	68	26k	33	11k	35	15k	12.998563	430.7682	218	283
10.9.23.102	13.89.178.26	25	8001	12	2484	13	5517	38.402132	3.9948	4974	11k
10.9.23.102	20.54.36.229	64	17k	29	6182	35	11k	38.419408	1207.8286	40	77
10.9.23.102	131.253.33.203	56	26k	24	3384	32	23k	39.686472	131.0282	206	1432
10.9.23.102	152.199.19.161	92	27k	45	3812	47	24k	42.234702	526.9979	57	365
10.9.23.102	131.253.33.200	84	29k	41	12k	43	16k	42.366691	681.0645	148	199
10.9.23.102	13.107.255.222	23	6746	11	1087	12	5659	42.488711	123.9909	70	365
10.9.23.102	52.113.196.254	24	6654	12	1140	12	5514	42.559038	126.7598	71	347
10.9.23.102	13.107.6.254	23	6741	11	1082	12	5659	42.571797	122.1655	70	370
10.9.23.102	51.141.33.202	23	6131	10	1064	13	5067	42.584735	128.1036	66	316
10.9.23.102	13.107.42.254	25	6849	12	1136	13	5713	42.608679	125.9566	72	362
10.9.23.102	13.107.3.254	22	6687	10	1028	12	5659	42.609339	123.8703	66	365
10.9.23.102	13.107.4.254	24	6526	12	1136	12	5390	42.771681	124.1180	73	347
10.9.23.102	13.107.136.254	23	6598	11	1084	12	5514	42.811100	123.2329	70	357
10.9.23.102	13.107.246.254	22	6687	10	1028	12	5659	42.833031	123.7267	66	365
10.9.23.102	131.253.33.254	22	6696	10	1037	12	5659	42.923436	126.4417	65	358
10.9.23.102	13.107.246.60	23	6528	11	1085	12	5443	42.955903	126.5642	68	344
10.9.23.102	13.107.213.60	23	6536	11	1093	12	5443	42.996467	127.1875	68	342
10.9.23.102	20.82.217.86	34	13k	14	2371	20	11k	43.236483	109.9625	172	804
10.9.23.102	20.190.159.135	69	49k	27	15k	42	33k	43.295319	109.9827	1145	2422
10.9.23.102	20.54.232.160	28	12k	12	3968	16	8414	44.532811	110.0136	288	611
10.9.23.102	23.220.255.44	26	6654	13	1168	13	5486	46.637191	522.5956	17	83

As there is 109 differnt IPs, i decide to check the box at the bottom to limit to display filter, whihc this narrows it down to 5 IP addresses, after checking the top three IPs in virustotal they were not a part of the Cobalt Strike srver:

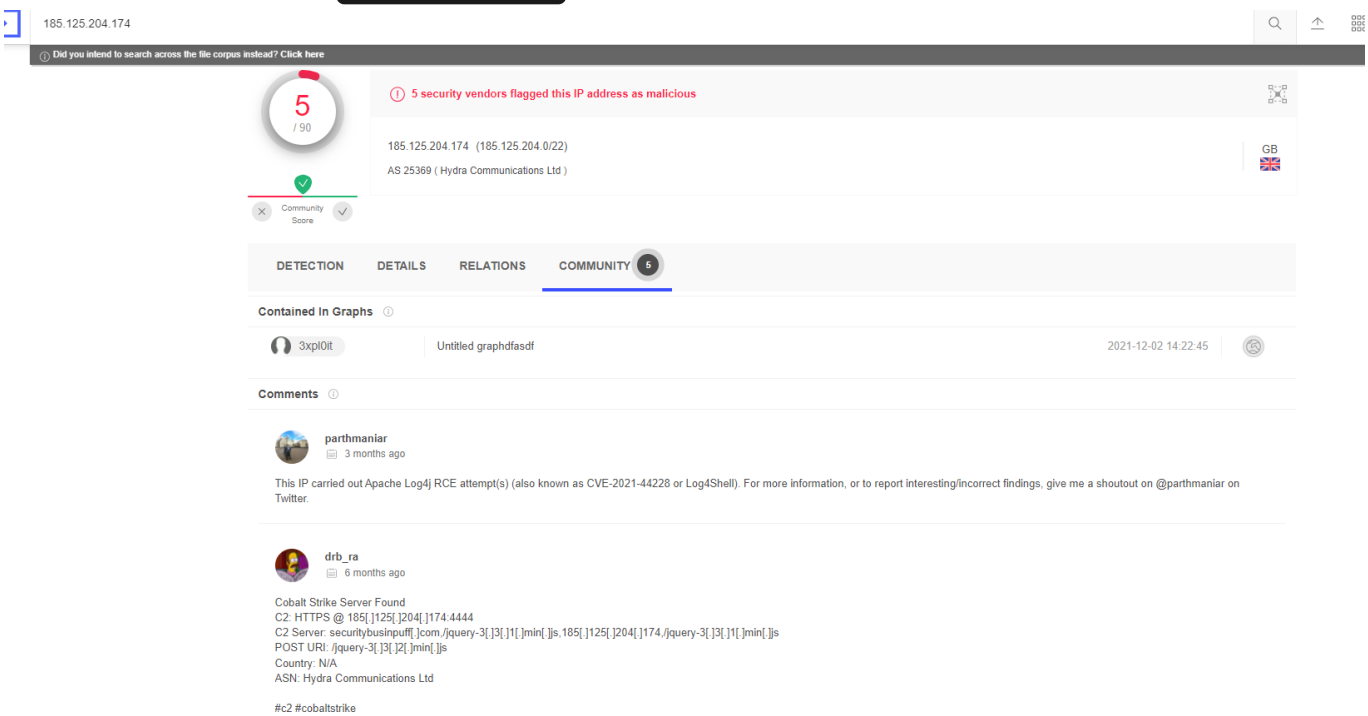


Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
10.9.23.102	85.187.128.24	2	1094	1	514	1	580	56.248525	2.9856	1377	1554
10.9.23.102	208.91.128.6	52	24k	26	7254	26	17k	153.653113	628.7745	92	218
10.9.23.102	104.83.124.33	4	806	2	338	2	468	582.206300	1.6207	1668	2310
10.9.23.102	185.125.204.174	184	254k	0	0	184	254k	584.576793	212.0515	0	9602
10.9.23.102	185.106.96.158	152	71k	76	43k	76	27k	685.851675	433.7395	801	509

With the ip address `185.106.96.158` being put into VirusTotal and heading over to th community tab we can see it is a part of the C2 server:



The second IP address `185.125.204.174`:



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

We are then asked to identify the `Host-Header` of the first IP address which can also be seen in the community tab of VirusTotal:

drb_ra
6 months 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 URI: /supprq/sa/
Country: United States
ASN: DediPath
Host Header: ocsp[.]verisign[.]com

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

ocsp.verisign.com

After we need to identify the domain of the first IP address which we can see under `C2 Server`:

drb_ra
6 months 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 URI: /supprq/sa/
Country: United States
ASN: DediPath
Host Header: ocsp[.]verisign[.]com

#c2 #cobaltstrike

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

After checking a few of the First IP address details we thn check the second IP address domain name:

drb_ra
6 months ago

Cobalt Strike Server Found
C2: HTTPS @ 185[.]125[.]204[.]174:4444
C2 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: Hydra Communications Ltd

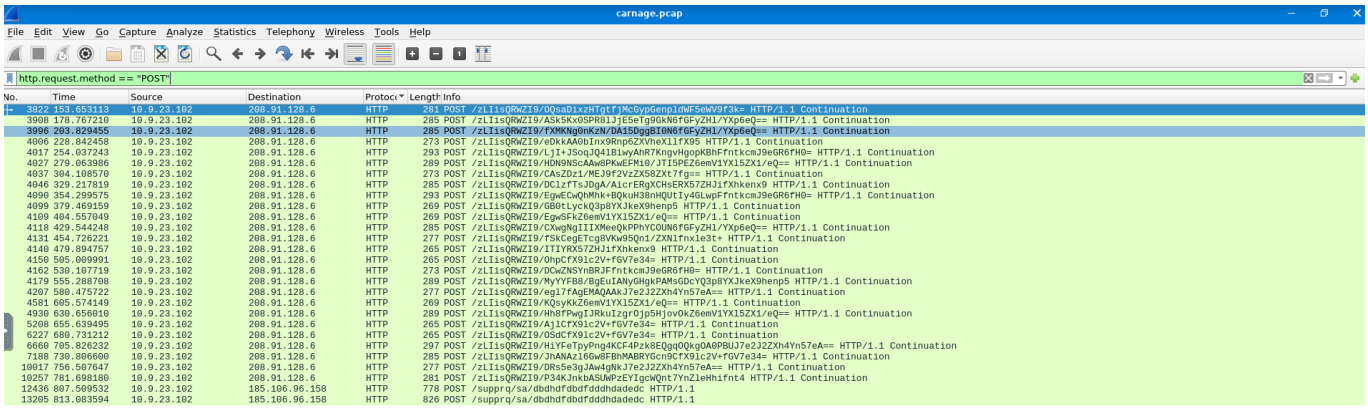
#c2 #cobaltstrike

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).

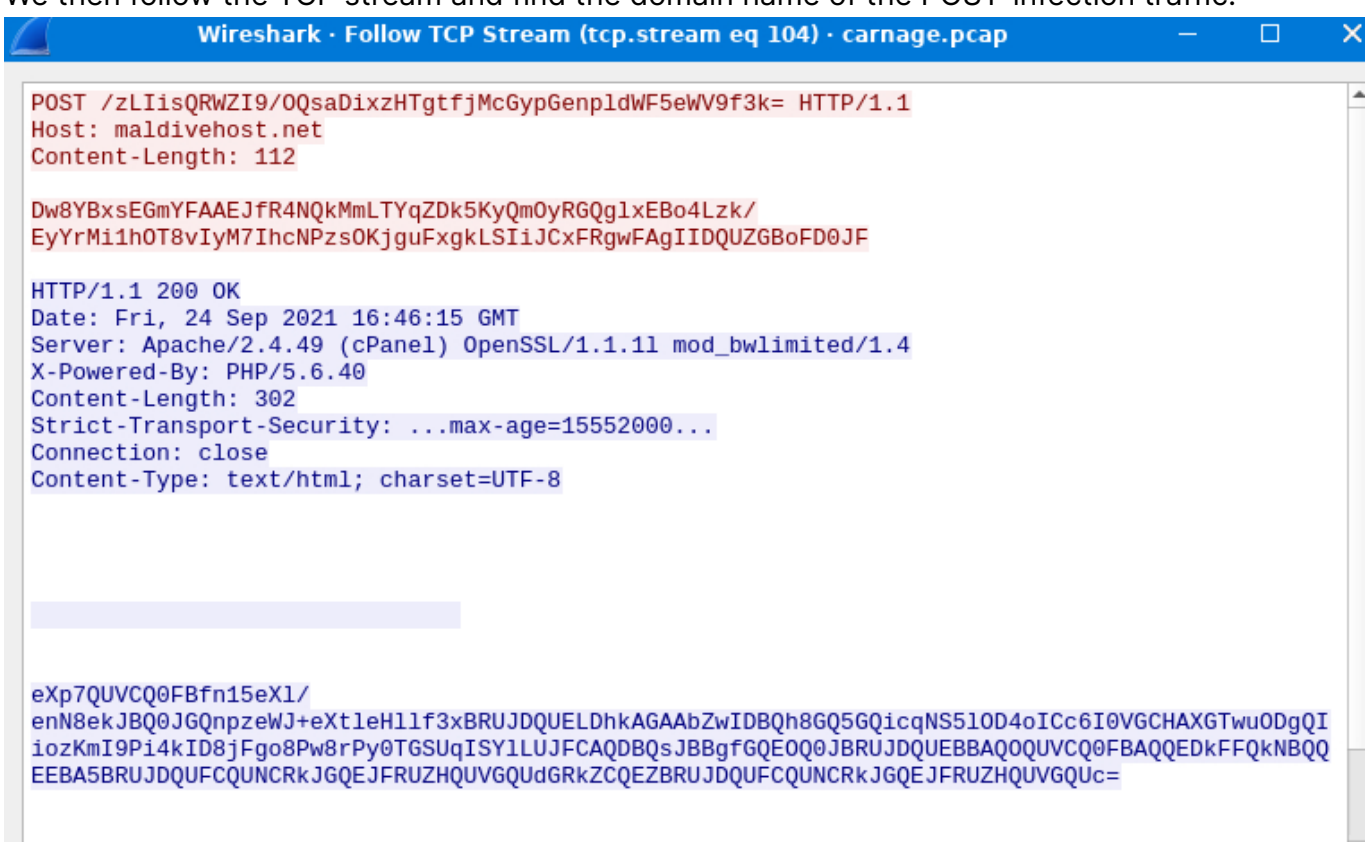
securitybusinpuff.com

As we have got all the details from VirusTotal, it is now time to go back to Wireshark, as we now ned to find the domain name of the post infection traffic

On stackoverflow I managed to find how to filter `POST` traffic and to filter post traffic we use the follwing filter `http.rquest.method == "POST"`:



We then follow the TCP stream and find the domain name of the POST-infection traffic:



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

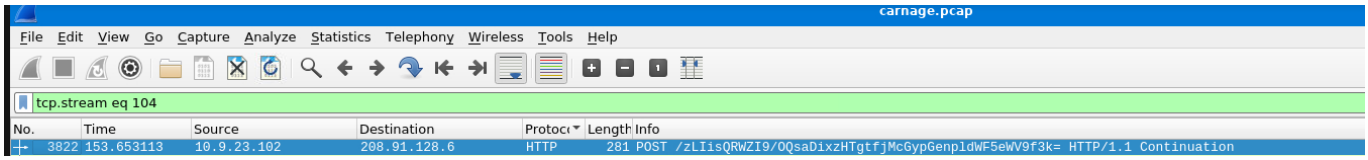
maldivehost.net

At the `POST` we can see the encoded base64 payload and see the first 11 characters that the victim sends out to th malicious domain

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

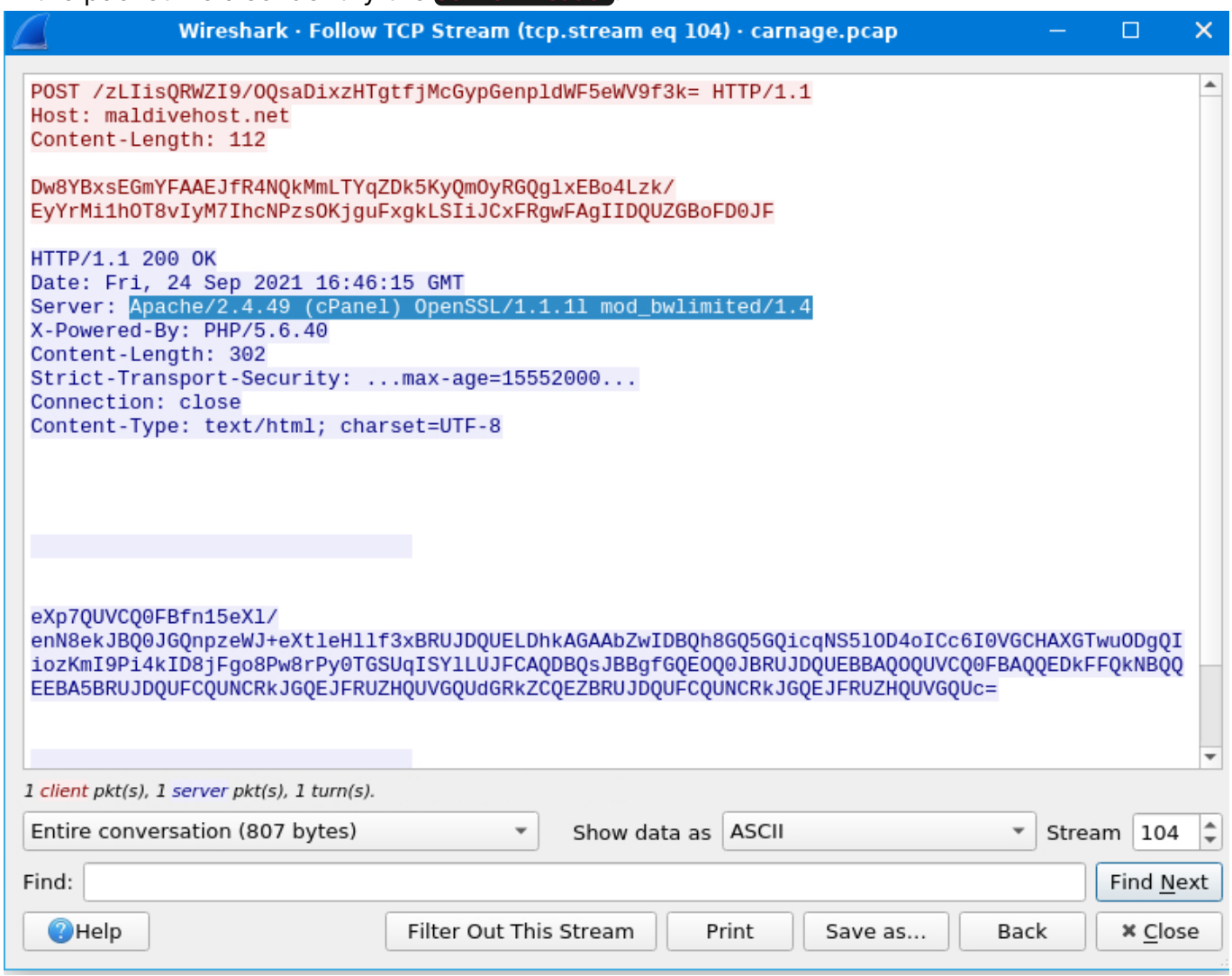
zLIisQRWZI9

Wirshark allows us to see the length of packets, which is where we are able to identify the lenght of the packet sent from the C2 server:



What was the length for the first packet sent out to the C2 server?
281

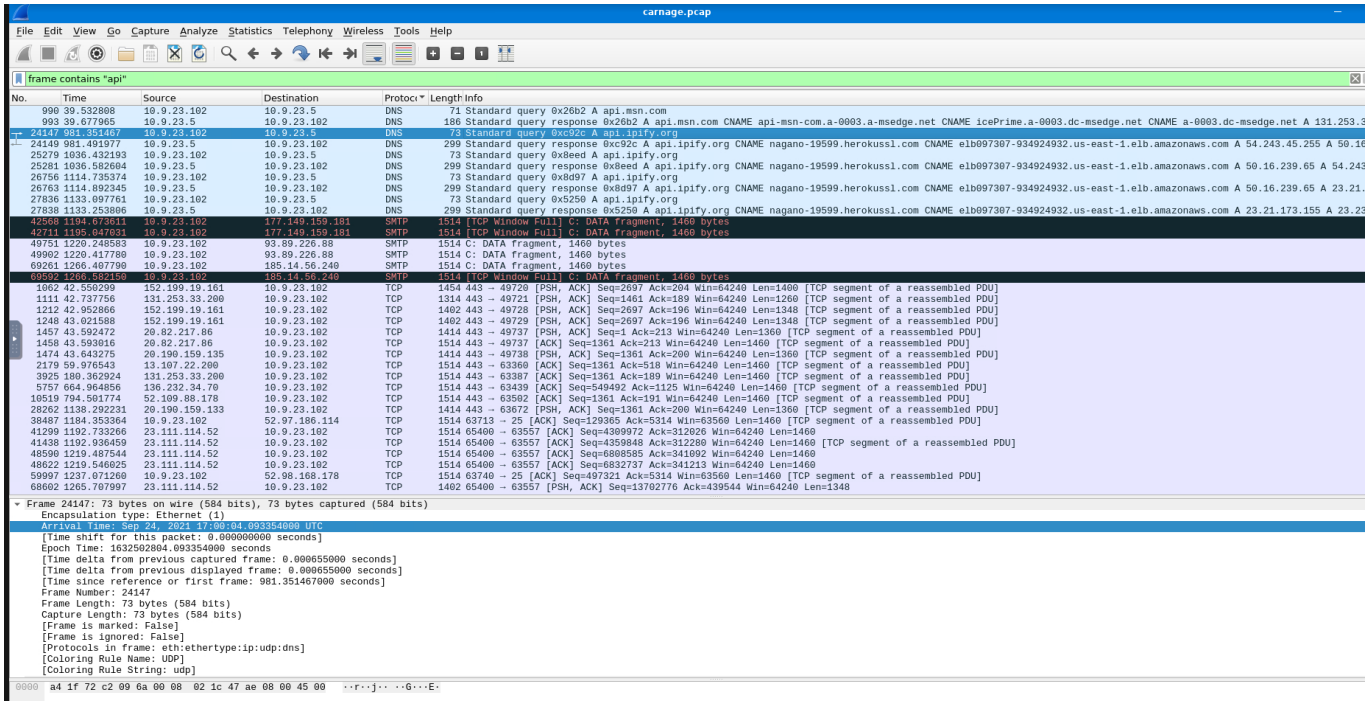
In the packet we also identify the `Server-Header`:



What was the Server header for the malicious domain from the previous question?
Apache/2.4.49 (cPanel) OpenSSL/1.1.1l mod_bwlimited/1.4

We find out that the malware used an API to check for the IP addresses and we need to track down the timne this occured

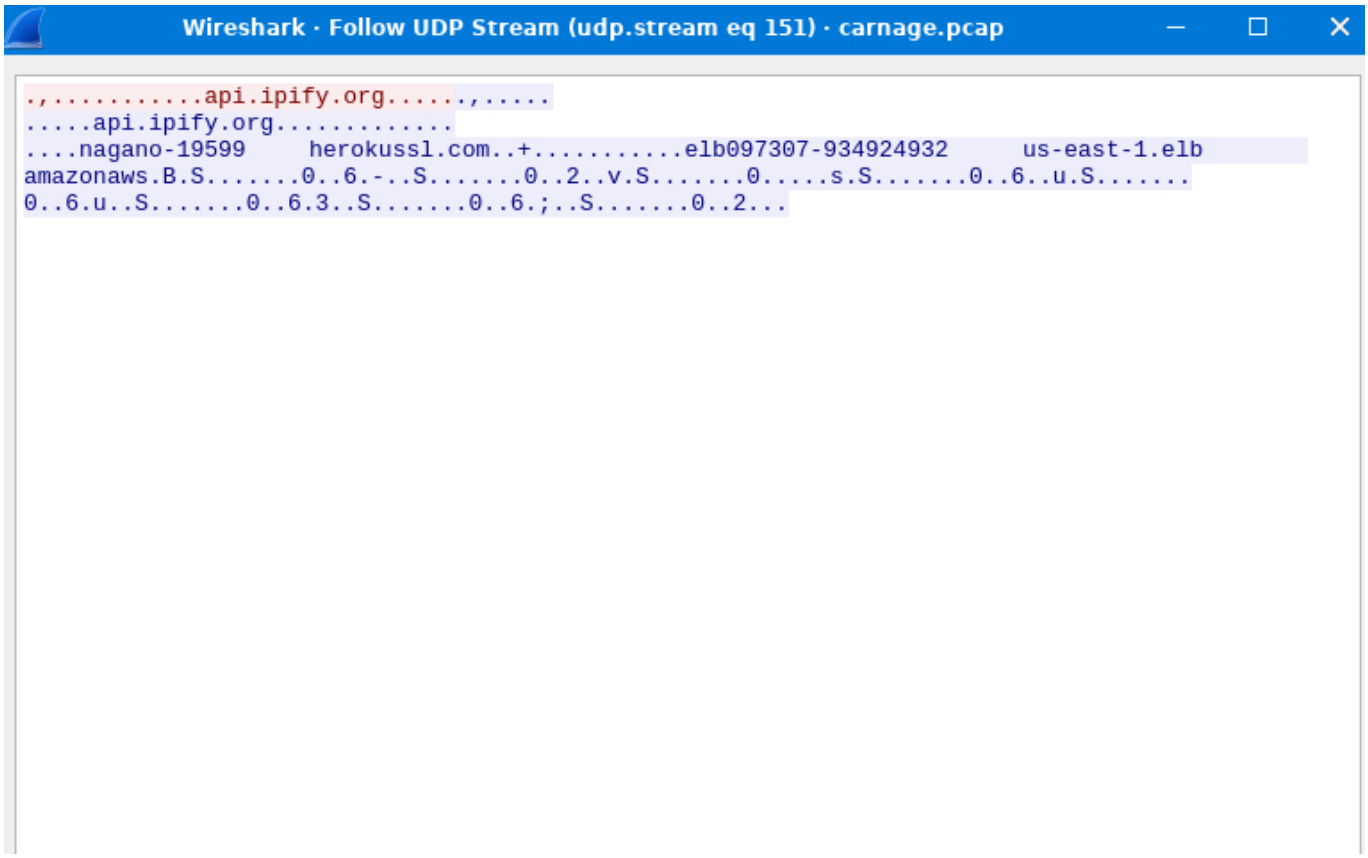
Using filter `frame contains "api"` this helps track down the frame time and helps us find any packets that contain the word api - The third packet is where we find our answer of when the malware used the API:



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

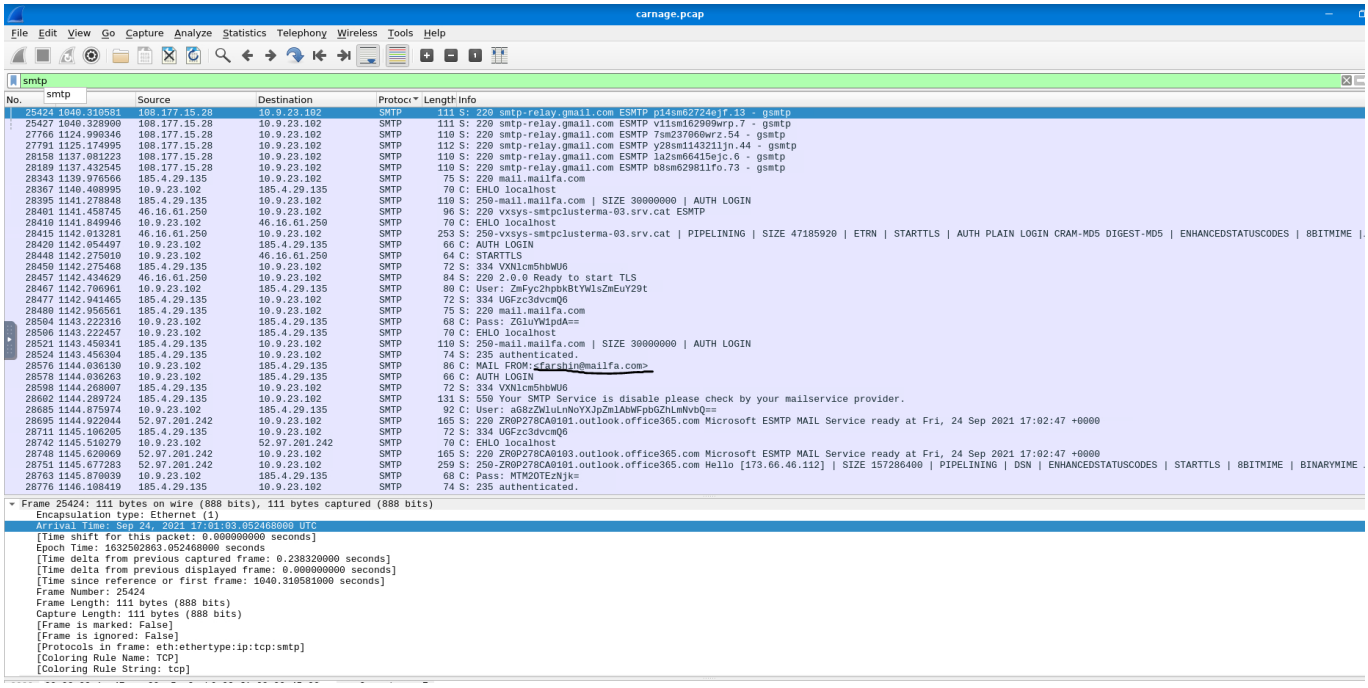
W also mange to find th domain name of the api:



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

api.ipify.org

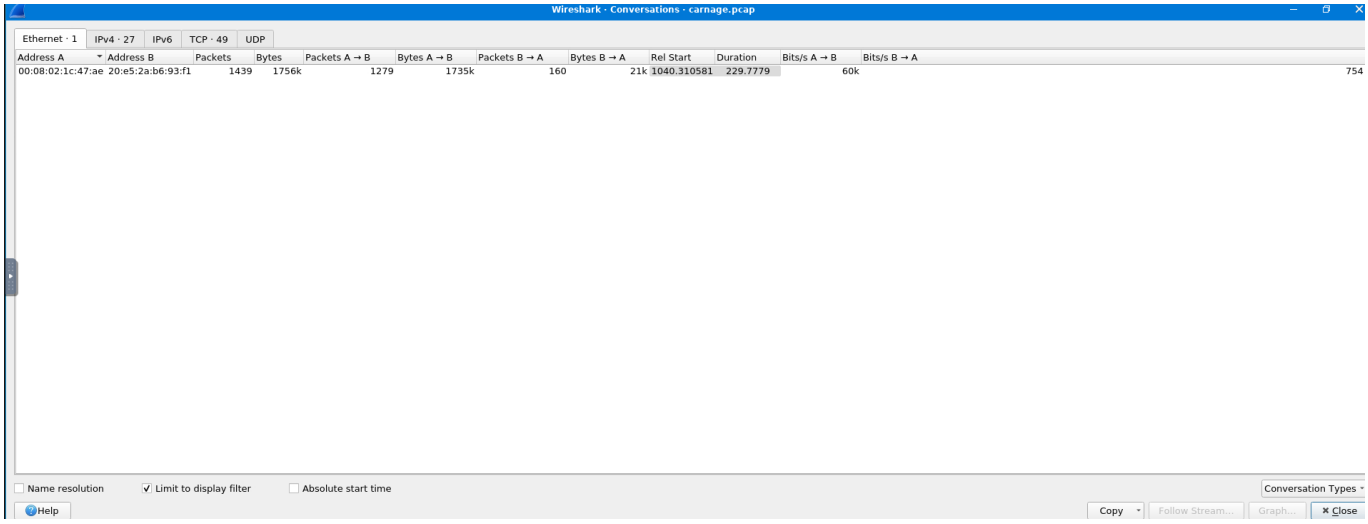
We hav almost finished locating everything from the pcap files, the last two things we are asked to identify is a malcious email that was sent - We know that mail servers run from a port called SMTP so we filter this in wireshark and we find out who sent the email:



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

For our last task we need to identify how many packts wre observed for the SMTP traffic - We idntiyf this by going to `statistics > conversations` after we select `ethernet` as it is on the network and we click `limit to display filter` and we have completed our final task and have successfully identified every malicious domain/IP:



How many packets were observed for the SMTP traffic?

1439