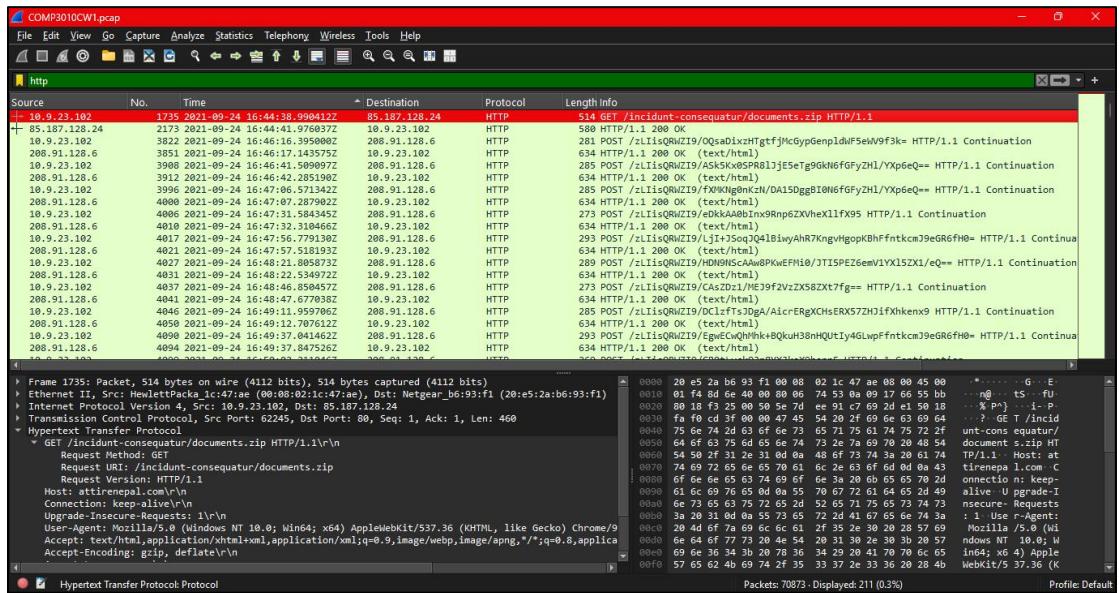


# Question Set for Coursework 1:

## Part 1: Initial Infection & File Transfer

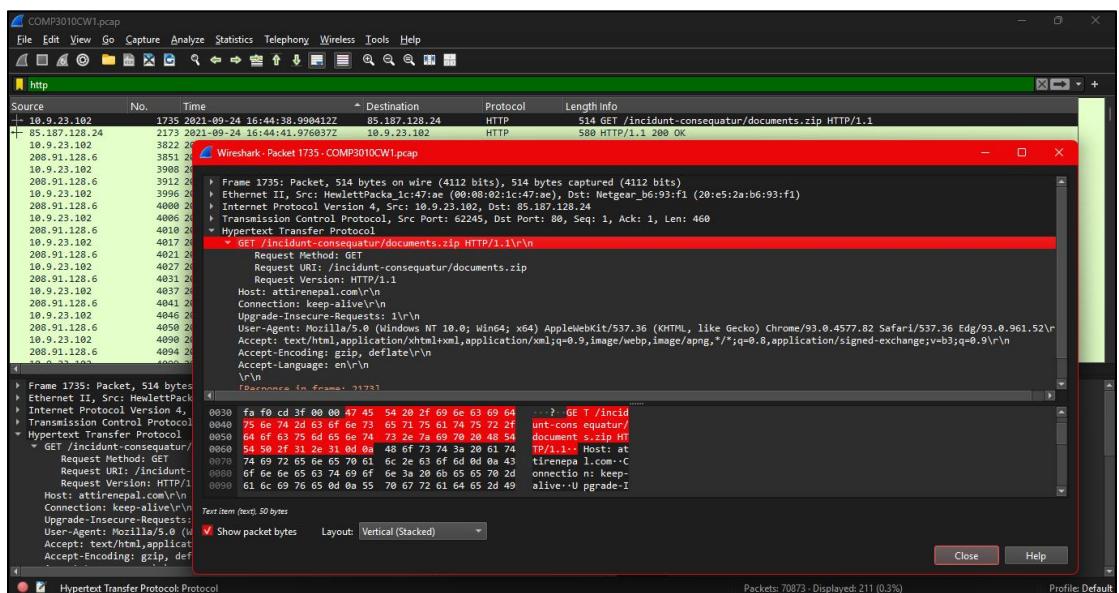
1. When did the initial malicious HTTP connection occur? (Provide the date and time in yyyy-mm-dd hh:mm:ss format).

2021-09-24 16:44:38 UTC



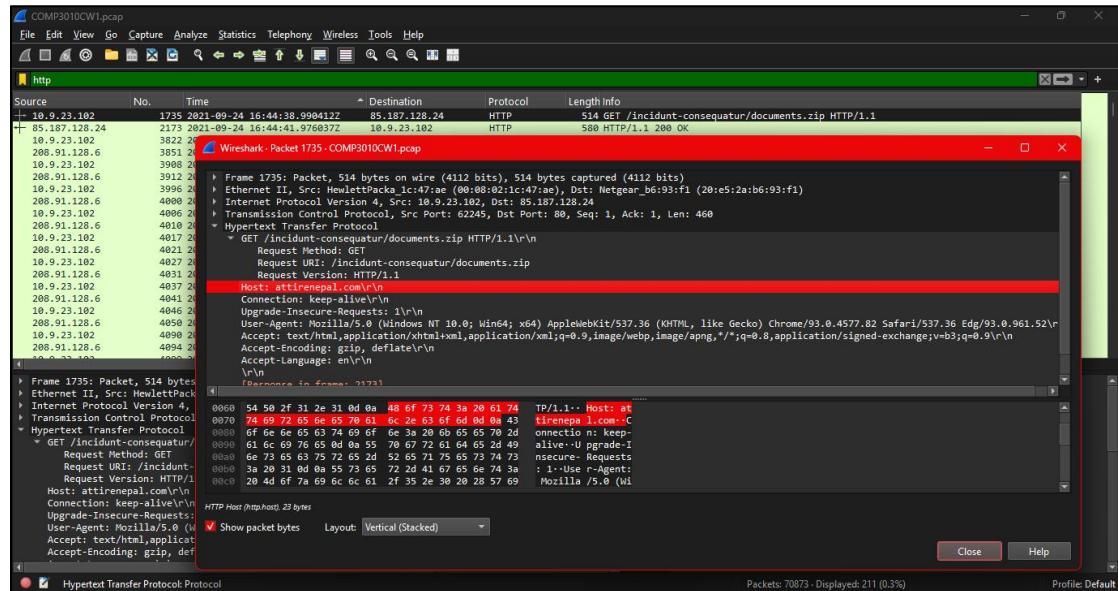
2. What is the name of the compressed file that the victim downloaded?

documents.zip



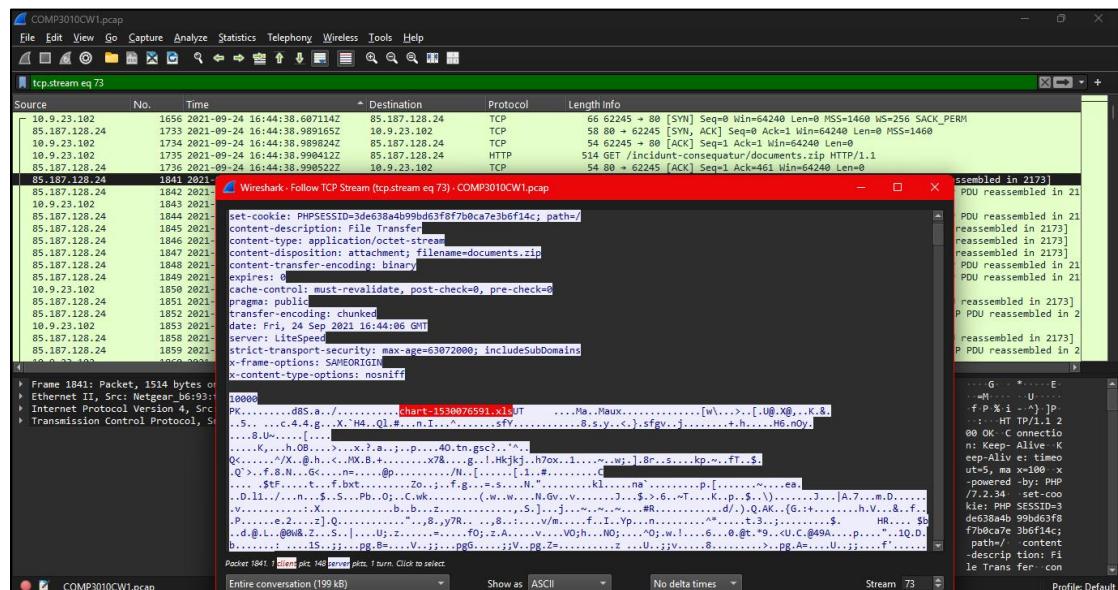
3. Which domain hosted the malicious compressed file?

[attirenepal.com](http://attirenepal.com)



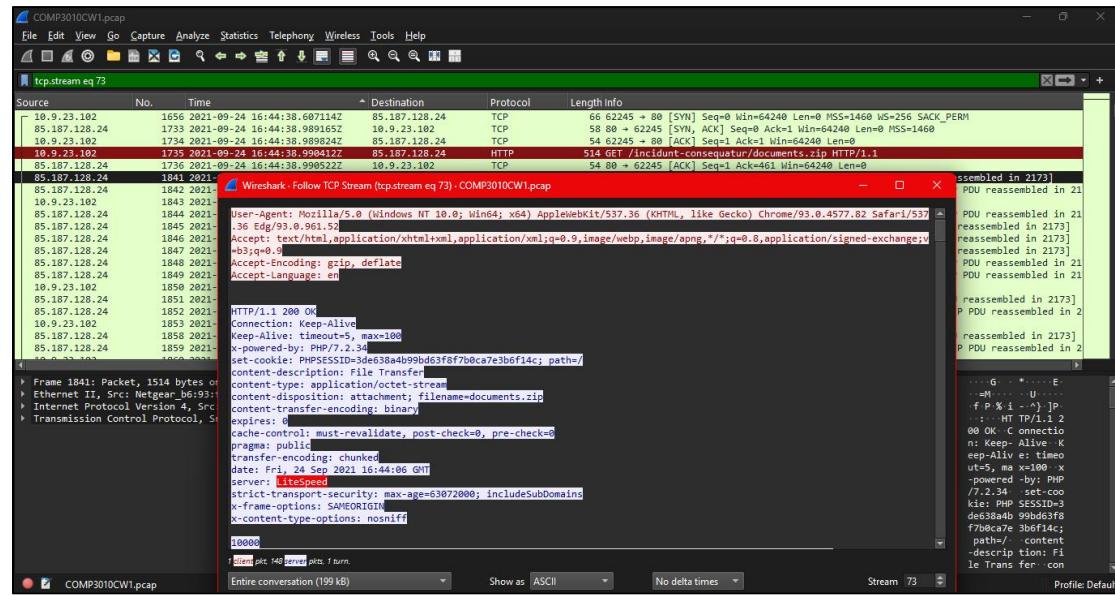
4. What is the name of the file located inside the compressed archive?

chart-1530076591.xls



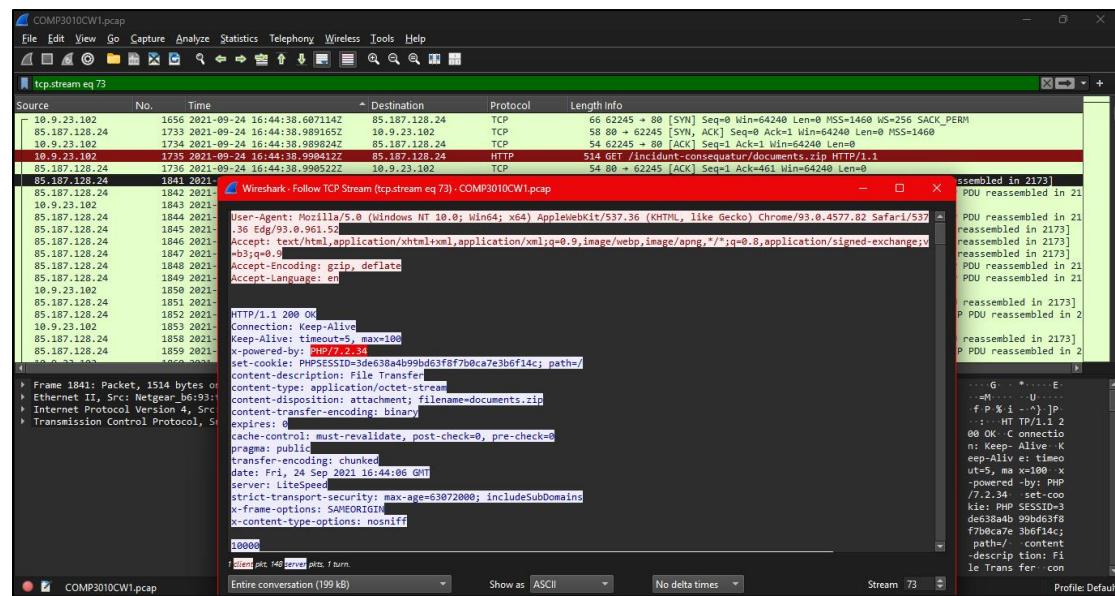
5. Identify the specific web server software (Server header) running on the malicious IP address that served the compressed file.

## LiteSpeed



6. What is the version number of the web server identified in the previous question?

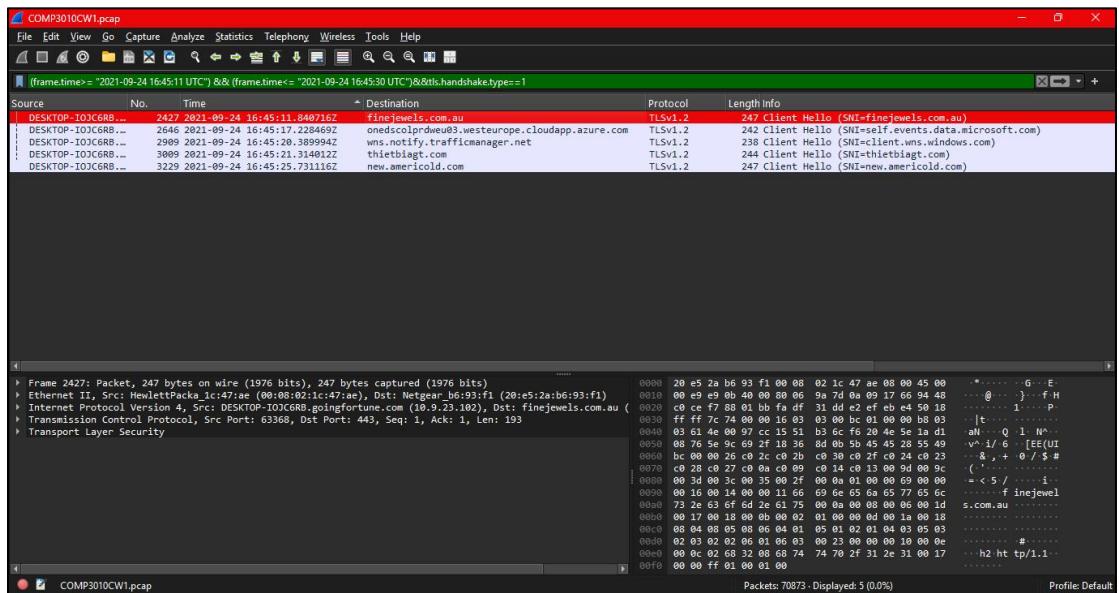
## PHP/7.2.34



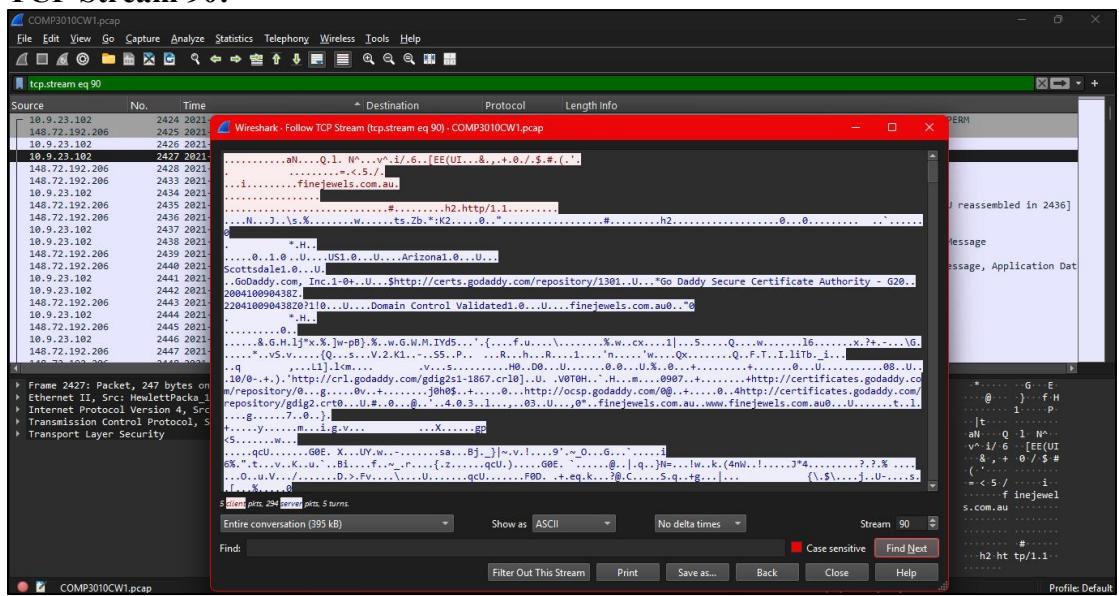
7. Identify the three additional domains that were involved in downloading malicious files to the victim host.

Hint: Inspect HTTPS traffic and focus on the time window between 16:45:11 and 16:45:30. Note this range is in UTC, not BST.

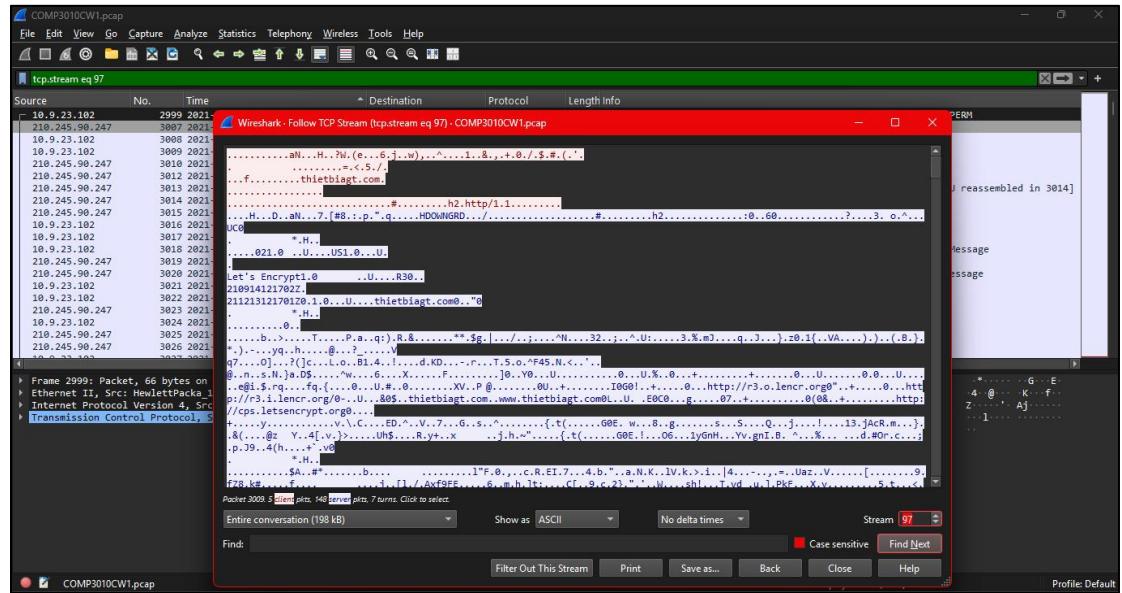
- [finejewels.com.au](http://finejewels.com.au)
- [thietbiagt.com](http://thietbiagt.com)
- [new.americold.com](http://new.americold.com)



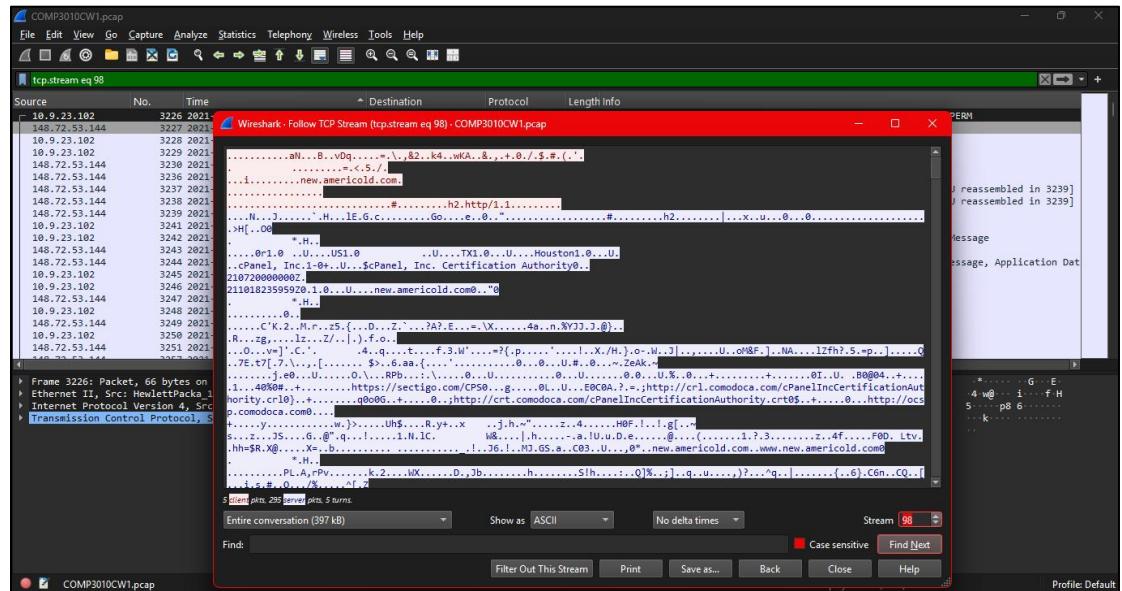
## TCP Stream 90:



## **TCP Stream 97:**



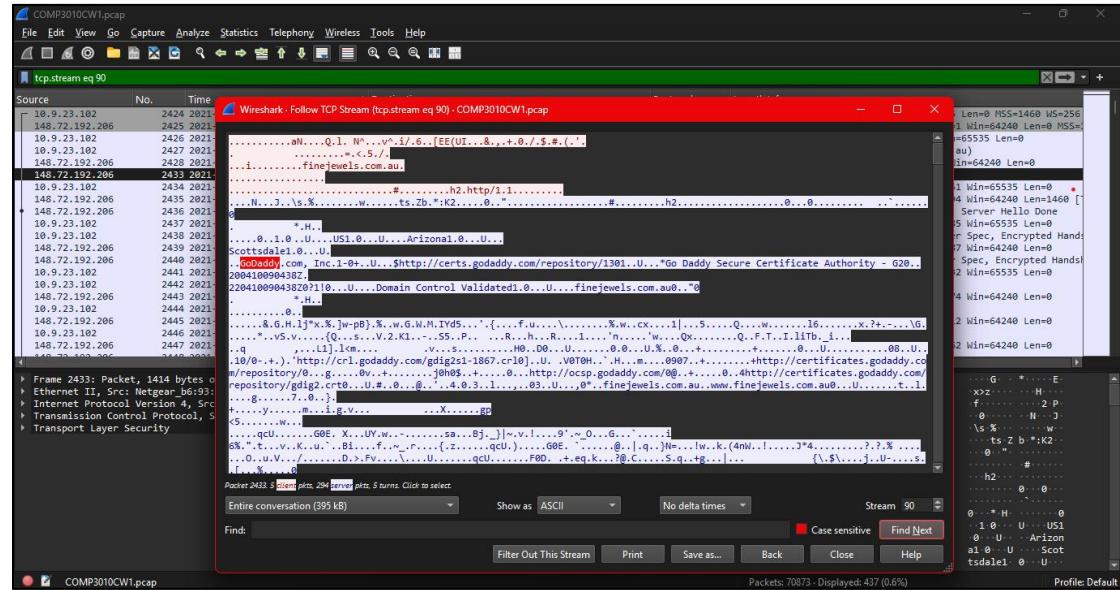
## TCP Stream 98:



## Part 2: Command and Control (C2) Activity

8. Which Certificate Authority (CA) issued the SSL certificate for the first domain identified in question 7?

### GoDaddy



9. What are the two IP addresses of the Cobalt Strike servers? (Provide them in sequential order).

Hint: Inspect the Conversations menu option

- 185.106.96.158
- 185.125.204.174

Wireshark - Conversations - COMP3010CWI1.pcap													
Conversation Settings		Conversation List											
		Ethernet - 8	Port A Address A	Port B	Packets ▾	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
<input type="checkbox"/> Name resolution		10.9.23.102	63557.23.111.114.52	65400	18,002	16 MB	267	5,721	753 kB	12,281	15 MB	884.211309	385.9728
<input checked="" type="checkbox"/> Absolute start time		10.9.23.102	63555.104.483.84.137	443	9,074	10 MB	265	1,972	107 kB	7,102	10 MB	880.206501	110.0097
<input checked="" type="checkbox"/> Display raw data		10.9.23.102	63465.185.25.204.174	8090	1,375	1 MB	181	408	23 kB	967	1 MB	743.649672	4.2193
<input checked="" type="checkbox"/> Limit to display filter		10.9.23.102	63507.185.106.96.158	80	1,074	997 kB	219	379	21 kB	695	976 kB	799.905708	6.6975
		10.9.23.102	63723.177.49.159.181	25	1,069	686 kB	412	464	652 kB	605	33 kB	1180.526950	19.5344
		10.9.23.102	63439.136.232.34.70	443	1,002	990 kB	155	284	16 kB	718	973 kB	647.865515	32.1007
		10.9.23.102	63726.52.97.201.210	25	978	627 kB	415	446	593 kB	532	34 kB	1106.875978	35.3396
		10.9.23.102	63610.136.232.34.70	443	976	882 kB	320	334	19 kB	642	863 kB	1057.163902	62.8288
		10.9.23.102	63571.136.232.34.70	443	953	911 kB	281	291	17 kB	662	894 kB	932.806205	64.1730
		10.9.23.102	63578.20.178.178.9	25	945	596 kB	425	416	562 kB	529	24 kB	122.920763	21.5930
		10.9.23.102	63740.52.98.168.178	25	933	591 kB	437	405	551 kB	505	34 kB	122.920763	15.8901
		10.9.23.102	63734.62.149.128.200	25	930	574 kB	423	397	540 kB	533	34 kB	121.067207	11.3723
		10.9.23.102	63747.52.98.161.19	25	922	579 kB	436	410	544 kB	512	35 kB	124.902723	20.2193
		10.9.23.102	63752.185.14.56.240	25	900	573 kB	441	382	545 kB	508	28 kB	125.919670	12.1106
		10.9.23.102	63744.52.97.201.194	25	898	574 kB	433	402	542 kB	496	32 kB	123.915986	16.6829
		10.9.23.102	63694.52.97.201.242	25	886	578 kB	394	415	544 kB	471	33 kB	1145.302515	12.8778
		10.9.23.102	63749.45.64.187.254	25	883	573 kB	438	399	542 kB	484	31 kB	126.384204	17.1190
		10.9.23.102	63740.52.98.168.178	25	882	586 kB	429	412	555 kB	470	31 kB	126.380031	23.0155
		10.9.23.102	63725.52.97.201.242	25	878	572 kB	414	411	541 kB	467	31 kB	1186.167390	33.5240
		10.9.23.102	63737.21.22.27.15.158	25	877	579 kB	426	410	550 kB	467	29 kB	1219.925742	9.4793
		10.9.23.102	63745.198.70.18.144	25	866	582 kB	434	416	552 kB	450	30 kB	1240.6962638	11.0655
		10.9.23.102	63729.52.97.232.210	25	862	574 kB	418	401	543 kB	461	30 kB	1201.559961	22.2486
		10.9.23.102	63741.52.97.201.194	25	861	591 kB	419	404	560 kB	456	30 kB	1211.559961	13.9393
		10.9.23.102	63707.154.41.66.35	25	860	587 kB	397	422	558 kB	457	29 kB	1122.447798	12.9385
		10.9.23.102	63741.198.70.18.144	25	860	581 kB	430	403	559 kB	457	31 kB	1239.636491	11.2409
		10.9.23.102	63713.52.97.198.114	25	858	591 kB	402	429	563 kB	439	29 kB	1171.549949	15.6778
		10.9.23.102	63709.52.98.163.18	25	856	589 kB	398	428	561 kB	428	29 kB	1157.748568	21.3293
		10.9.23.102	63750.198.70.18.144	25	854	575 kB	439	407	545 kB	447	30 kB	1257.142067	11.4405
		10.9.23.102	63693.52.97.201.242	25	841	576 kB	393	418	546 kB	423	30 kB	1144.620993	17.2787
		10.9.23.102	63711.52.98.163.18	25	828	568 kB	400	414	540 kB	414	28 kB	1162.476383	34.2961
		10.9.23.102	63715.107.70.18.144	25	830	573 kB	404	419	545 kB	416	29 kB	1177.422066	12.0000

## Analyze 185.106.96.158 using VirusTotal.

Wow. I thought that was a CA.

parthmaniar 3 years ago

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 4 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/ POST URI: /supprq/sa/ Country: United States ASN: DediPath Host Header: ocsp[.]verisign[.]com #c2 #cobaltstrike

drb.ra 4 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 URI: /supprq/sa/ Country: United States ASN: DediPath Host Header: ocsp[.]verisign[.]com #c2 #cobaltstrike

## Analyze 185.125.204.174 using VirusTotal.

1tfash 4 months ago -1

deleted\_user 9 months ago +1

n1catitxt 1 year ago +1

Comments (3)

parthmaniar 3 years ago

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 4 years ago

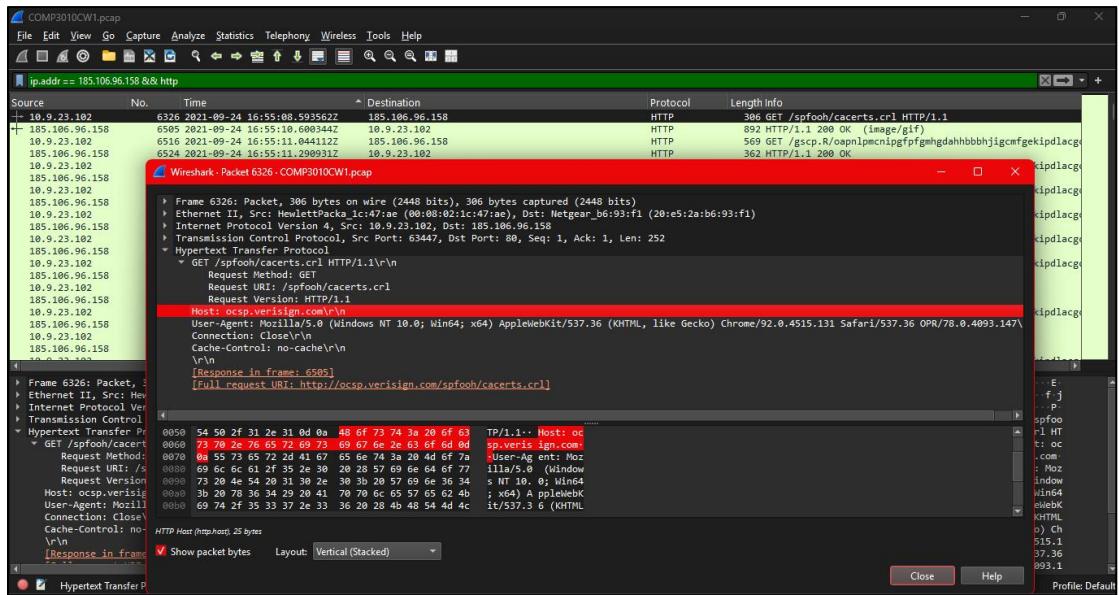
Cobalt Strike Server Found C2: HTTPS @ 185[.]125[.]204[.]174:4444 C2 Server: securitybusinpuff[.]com./jquery-3[.]3[.]1[.]min[.]js,185[.]125[.]204[.]174./jquery-3[.]3[.]1[.]min[.]js POST URI: /jquery-3[.]3[.]2[.]min[.]js Country: N/A ASN: Hydra Communications Ltd #c2 #cobaltstrike

drb.ra 4 years ago

## 10. What is the value of the Host header for the first Cobalt Strike IP address?

Hint: Apply a filter to isolate DNS queries.

[ocsp.verisign.com](http://ocsp.verisign.com)



Verify in VirusTotal:

https://www.virustotal.com/gui/ip-address/185.106.96.158/community

drb\_ra 3 years ago

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 4 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/ POST URI: /supprq/sa/ Country: United States ASN: DediPath Host Header: ocsp[.]verisign[.]com

#c2 #cobaltstrike

drb\_ra 4 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 URI: /supprq/sa/ Country: United States ASN: DediPath Host Header: ocsp[.]verisign[.]com

#c2 #cobaltstrike

drb\_ra 4 years ago

Cobalt Strike Server Found C2: HTTP @ 185[.]106[.]96[.]158:80 C2 Server: survmeter[.]live/gscp[.]R/185[.]106[.]96[.]158/gscp[.]R/ POST URI: /supprq/sa/ Country: N/A ASN: N/A Host Header: ocsp[.]verisign[.]com

11. What is the domain name associated with the first Cobalt Strike IP address?  
 Hint: Take a closer look at HTTPS (443)

**survmeter.live**

The screenshot shows the VirusTotal interface for the IP address 185.106.96.158. It displays three comments from a user named drb.ra:

- Comment 1 (3 years ago): "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."
- Comment 2 (4 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/ POST URL: /supprq/sa/ Country: United States ASN: DediPath Host Header: ocsp[.]verisign[.]com #c2 #cobaltstrike"
- Comment 3 (4 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"

12. What is the domain name associated with the second Cobalt Strike IP address?

Hint: Apply a filter to capture HTTP POST requests.

**securitybusinpuff.com**

The screenshot shows a Wireshark capture of a TLS handshake. A red box highlights the Client Hello extension in the details pane, which lists the server name as "securitybusinpuff.com".

Wireshark details pane (highlighted area):
 

- Handshake Protocol: Client Hello (1)
- Length: 202
- Version: TLS 1.2 (0x0003)
- Random Value: 7e33037c773d76317f75fd10f45a9b9608b1de113e020079cb6b51fb714265
- Session ID Length: 32
- Session ID: b6fffb18103c0d9baf5718f0ed7f99d73af5787b0b1a0a4a32e85ece87f2
- Cipher Suites Length: 38
- Cipher Suites (19 suites)
- Compression Methods Length: 1
- Compression Methods (1 method)
- Extensions Length: 91
- Extension: server\_name (len=26) name=securitybusinpuff.com
- Extension: supported\_groups (len=8)
- Extension: ec\_point\_formats (len=2)
- Extension: signature\_algorithms (len=26)
- Extension: session\_ticket (len=0)
- Extension: extended\_master\_secret (len=0)

<https://www.virustotal.com/gui/ip-address/185.125.204.174/community>

 185.125.204.174

[Comments \(3\)](#) 

---

 **parthmaniar**  
3 years ago

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**  
4 years ago

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

---

 **drb\_ra**  
4 years ago

Cobalt Strike Server Found C2: HTTPS @ 185[.]125[.]204[.]174:8080 C2 Server: securitybusinpu[.]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  
#c2 #cobaltstrike

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

maldivehost.net

The screenshot shows a Wireshark interface with several captured network frames. Frame 3822 is selected, showing a POST request to `/LiiisQRWzI9/QOsadIx:HTgtfjMcGypGenpldWfSeW9f3k=`. The packet details pane shows the raw HTTP request:

```

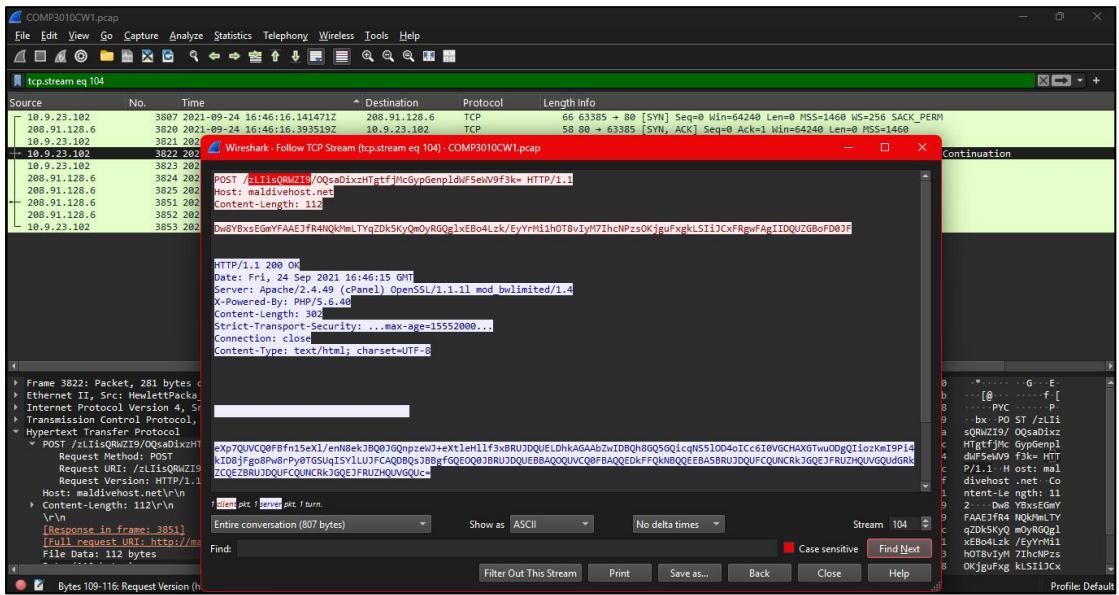
POST /LiiisQRWzI9/QOsadIx:HTgtfjMcGypGenpldWfSeW9f3k= HTTP/1.1
Host: maldivewebsit.net
Content-Length: 112
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.113 Safari/537.36
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: keep-alive
Referer: http://maldivewebsit.net/LiiisQRWzI9/QOsadIx:HTgtfjMcGypGenpldWfSeW9f3k=

```

The packet bytes pane shows the raw hex and ASCII data of the request.

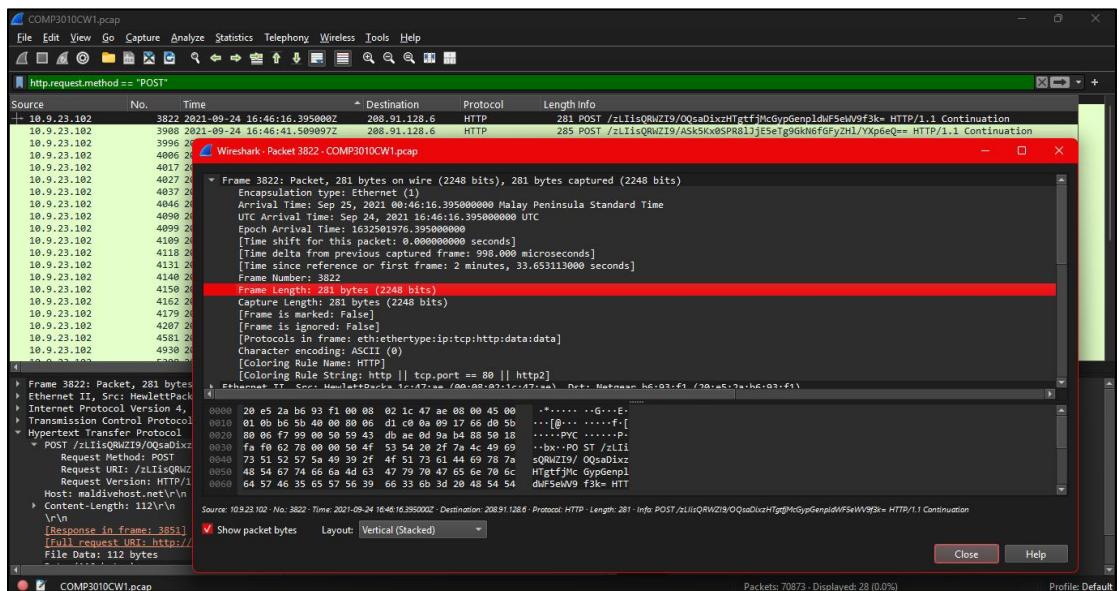
14. What are the first eleven characters of the data the victim host sends to the malicious domain identified in the previous question?

**zLiiQRWZI9**



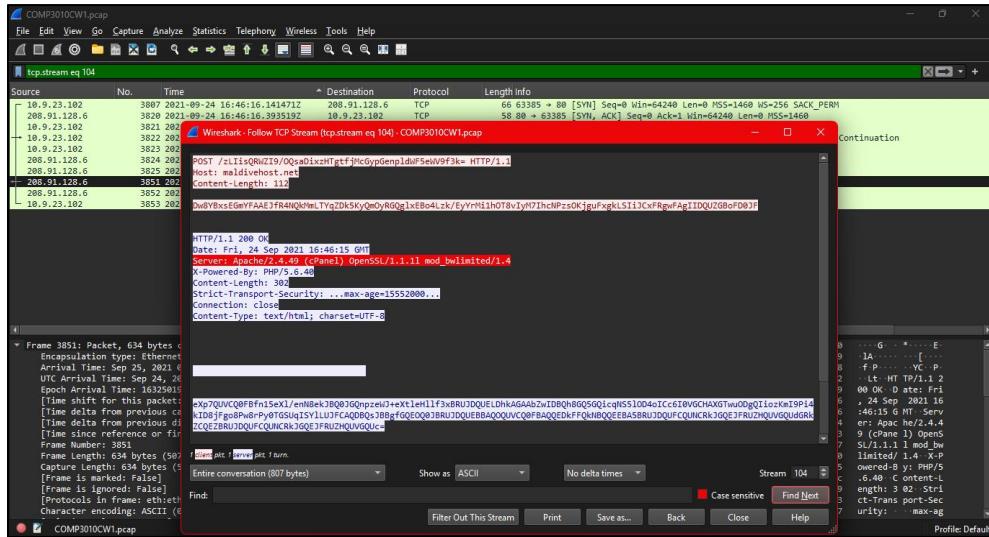
15. What was the length of the first packet the victim sent to the C2 server?

**281 bytes (2248 bits)**



16. What was the Server header value for the malicious domain from question 13?

### Server: Apache/2.4.49 (cPanel) OpenSSL/1.1.1l mod\_bwlimited/1.4



## Part 3: Final Exfiltration/Check-in

17. What was the date and time (in yyyy-mm-dd hh:mm:ss UTC format) when the DNS query occurred for the domain used by the malware to check the victim's external IP address?

**2021-09-24 17:00:04 UTC**

The screenshot shows a Wireshark capture of network traffic from a host with IP 10.9.23.102. The traffic includes several DNS queries. A red box highlights the DNS query at index 24147, which is a standard query to the domain `api.ipify.org`. The details pane shows the DNS request and its response.

Frame 24147: Packet, 73 bytes on wire (584 bits), 73 bytes captured (584 bits)  
Arrival Time: Sep 25, 2021 01:00:04.093354000 Malay Peninsula Standard Time  
UTC Arrival Time: Sep 24, 2021 17:00:04.093354000 UTC  
Epoch Arrival Time: Sep 25, 2021 01:00:04.093354000  
[Time shift for this frame: 0 seconds]  
[Time delta from previous frame: 15 minutes, 41.818659000 seconds]  
[Time since reference or first frame: 16 minutes, 21.351467000 seconds]  
Frame Number: 24147  
Frame Length: 73 bytes (584 bits)  
Capture Length: 73 bytes (584 bits)  
Frame is marked: False  
Frame is ignored: False  
Protocols in frame: et  
Character encoding: ASCII (8)  
[Coloring Rule Name: UDP]  
[Coloring Rule String: udp]  
Frame is ignored: False  
Frame is marked: False  
Protocols in frame: ip:udp:dns  
Character encoding: ASCII (8)  
[Coloring Rule Name: UDP]  
[Coloring Rule String: udp]  
Absolute time when this frame was captured in Coordinated Universal Time (UTC) (frame.time\_uts)  
Show packet bytes Layout: Vertical (Stacked)

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

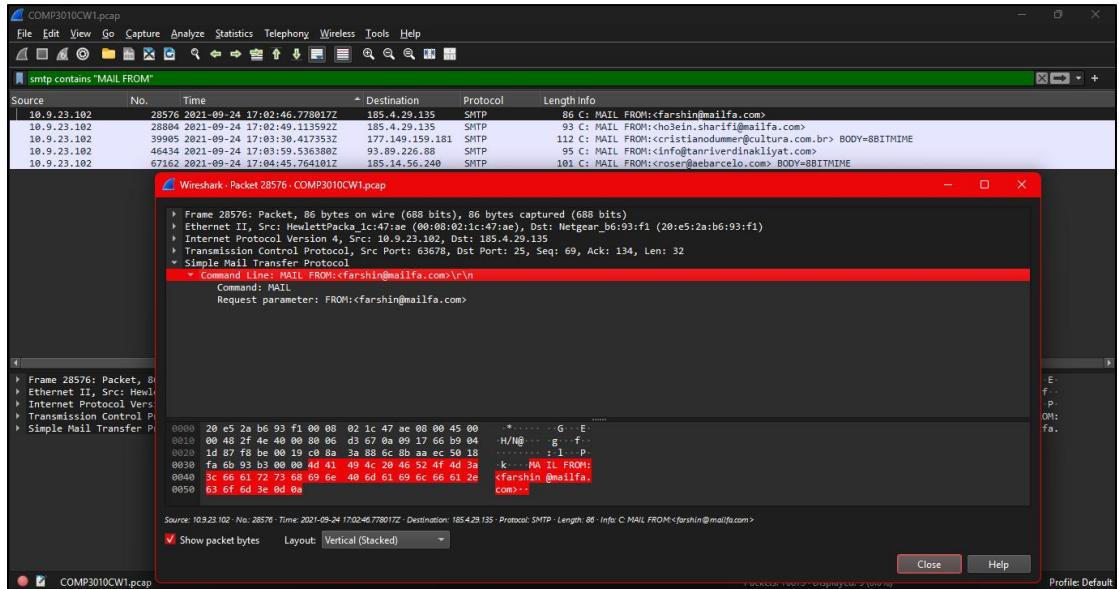
**api.ipify.org**

The screenshot shows the detailed view of the DNS query highlighted in the previous Wireshark capture. The 'Name' field in the DNS query message is highlighted with a red box. The message is a standard query to the domain `api.ipify.org`.

Frame 24147: Packet, 73 bytes on wire (584 bits), 73 bytes captured (584 bits)  
Arrival Time: Sep 25, 2021 01:00:04.093354000 Malay Peninsula Standard Time  
UTC Arrival Time: Sep 24, 2021 17:00:04.093354000 UTC  
Epoch Arrival Time: Sep 25, 2021 01:00:04.093354000  
[Time shift for this frame: 0 seconds]  
[Time delta from previous frame: 15 minutes, 41.818659000 seconds]  
[Time since reference or first frame: 16 minutes, 21.351467000 seconds]  
Frame Number: 24147  
Frame Length: 73 bytes (584 bits)  
Capture Length: 73 bytes (584 bits)  
Frame is marked: False  
Frame is ignored: False  
Protocols in frame: et  
Character encoding: ASCII (8)  
[Coloring Rule Name: UDP]  
[Coloring Rule String: udp]  
Frame is ignored: False  
Frame is marked: False  
Protocols in frame: ip:udp:dns  
Character encoding: ASCII (8)  
[Coloring Rule Name: UDP]  
[Coloring Rule String: udp]  
Absolute time when this frame was captured in Coordinated Universal Time (UTC) (frame.time\_uts)  
Show packet bytes Layout: Vertical (Stacked)

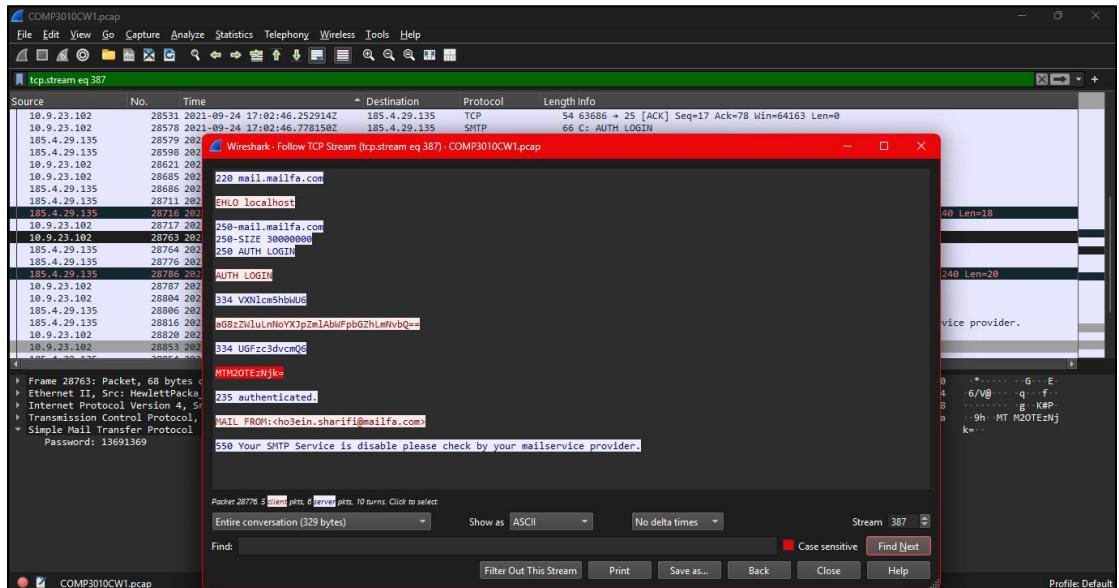
19. What was the first email address observed in the SMTP traffic in the pcap file (the MAIL FROM address)?

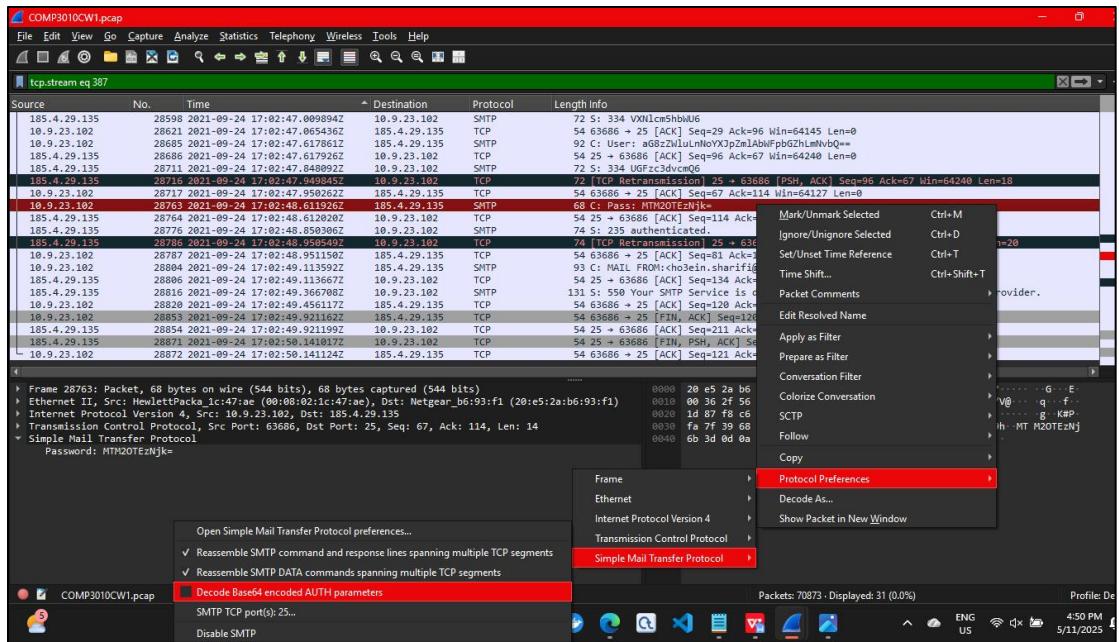
**farshin@mailfa.com**



20. Follow the stream from Q19. What is ho3ein.sharifi's password?

The Password is Encoded: **MTM2OTEzNjk=**





The Password is Decoded: **13691369**

