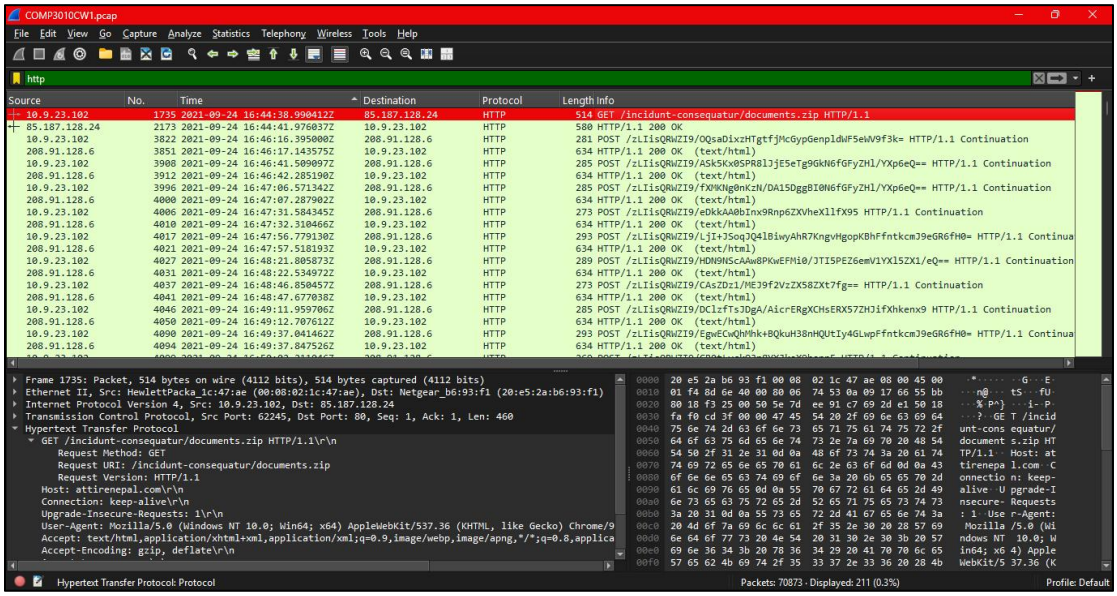
Question Set for Coursework 1:

Part 1: Initial Infection & File Transfer

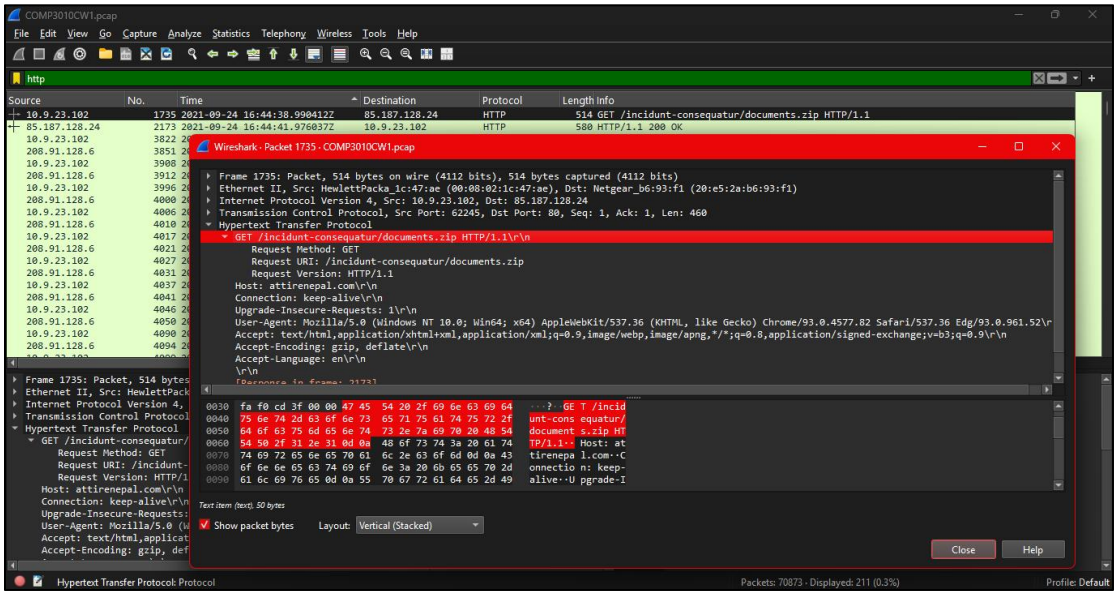
1. When did the initial malicious HTTP connection occur? (Provide the date and time in yyyy-mm-dd hh:mm:ss format).

2021-09-24 16:44:38 UTC



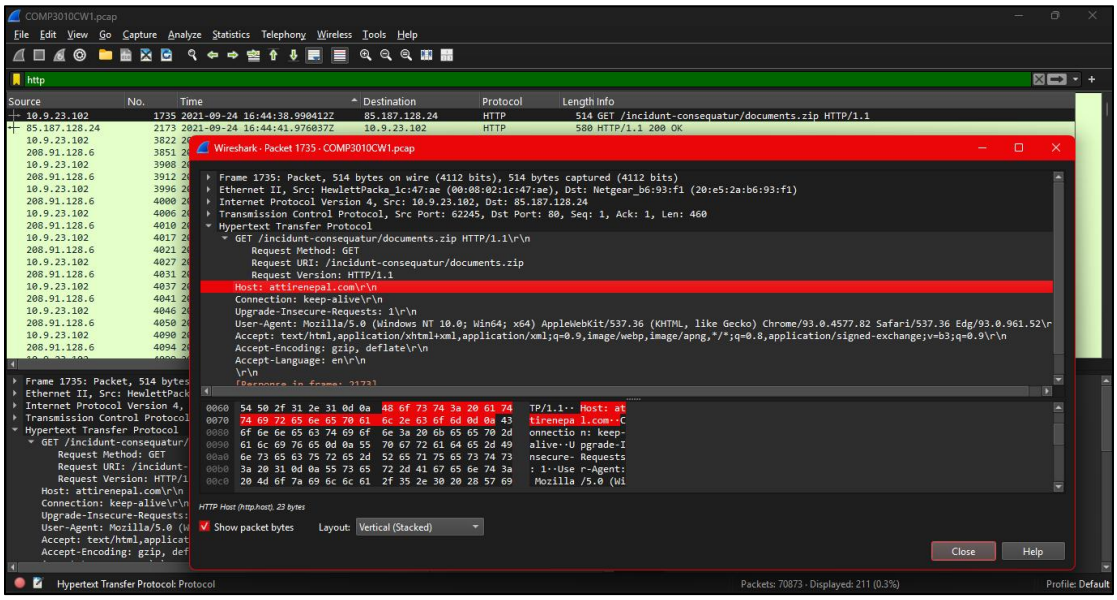
2. What is the name of the compressed file that the victim downloaded?

documents.zip.



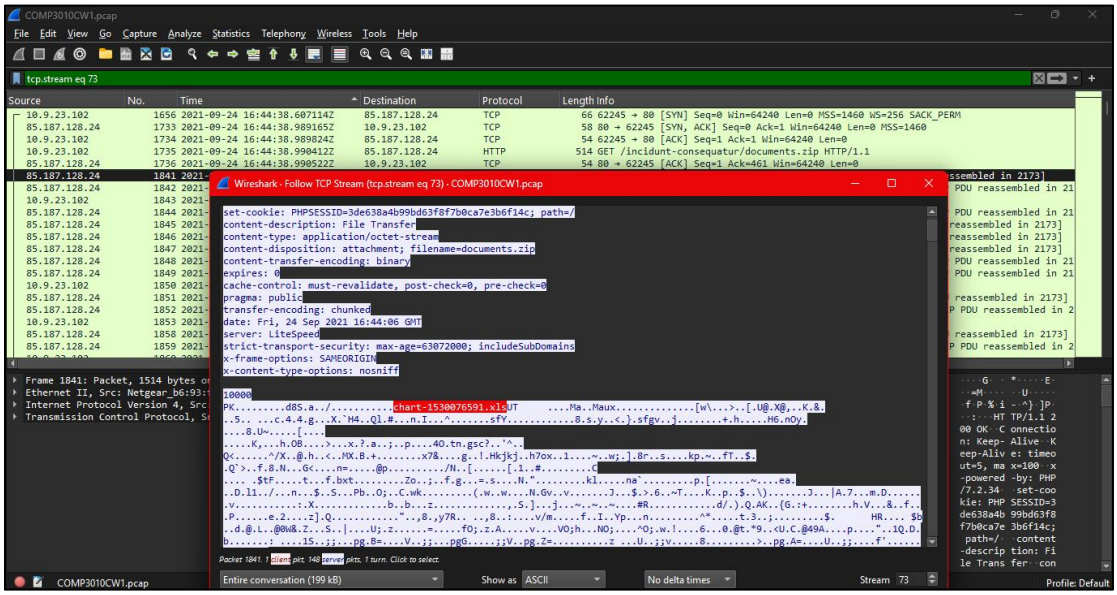
3. Which domain hosted the malicious compressed file?

attirenepal.com



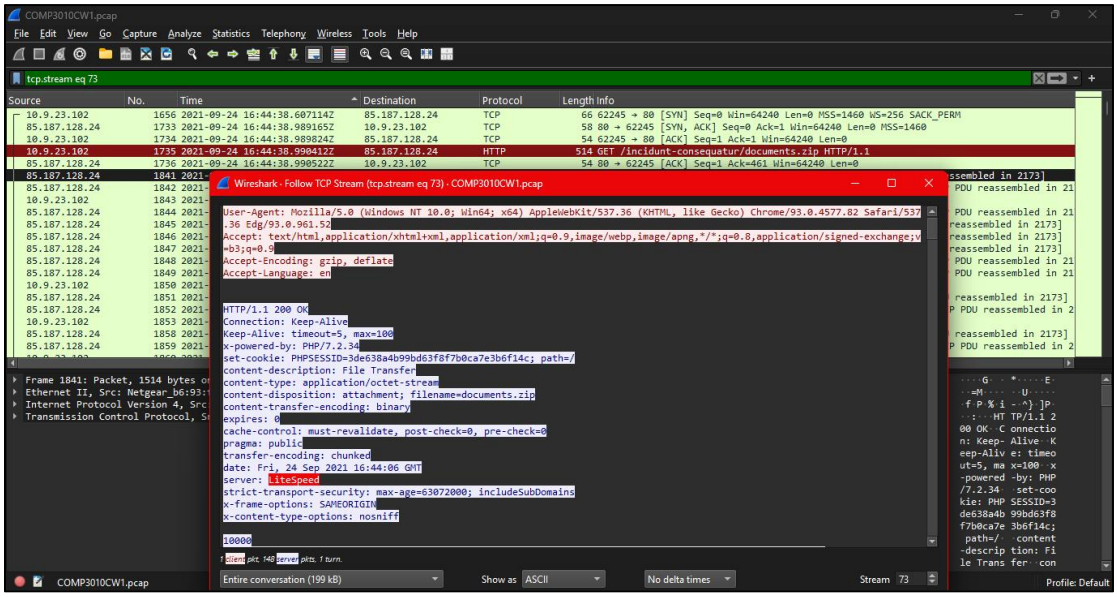
4. What is the name of the file located inside the compressed archive?

chart-1530076591.xls



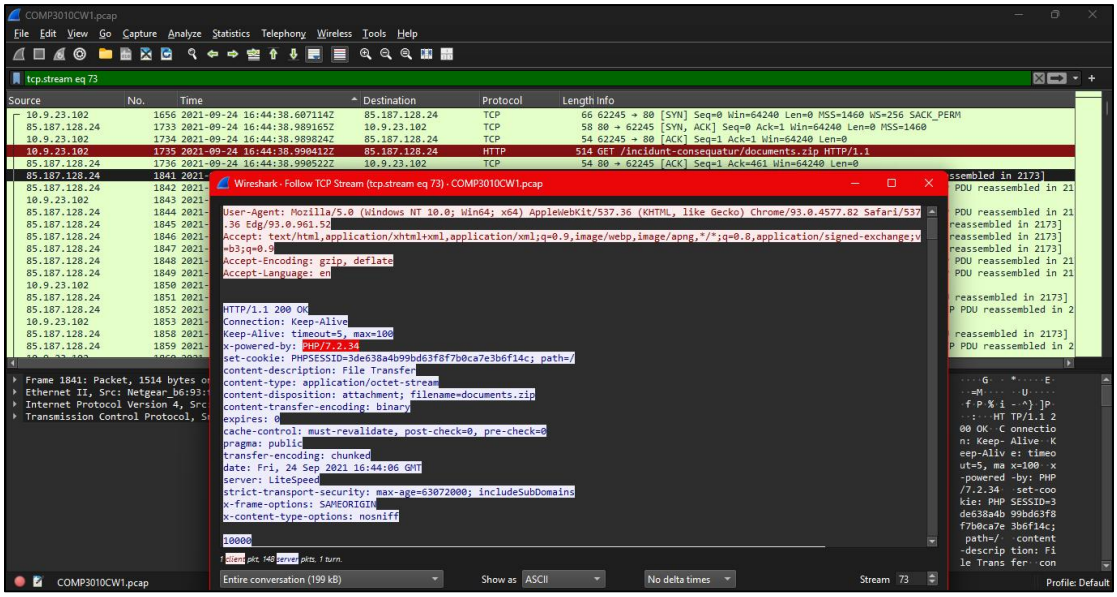
5. Identify the specific web server software (Server header) running on the malicious IP address that served the compressed file.

LiteSpeed



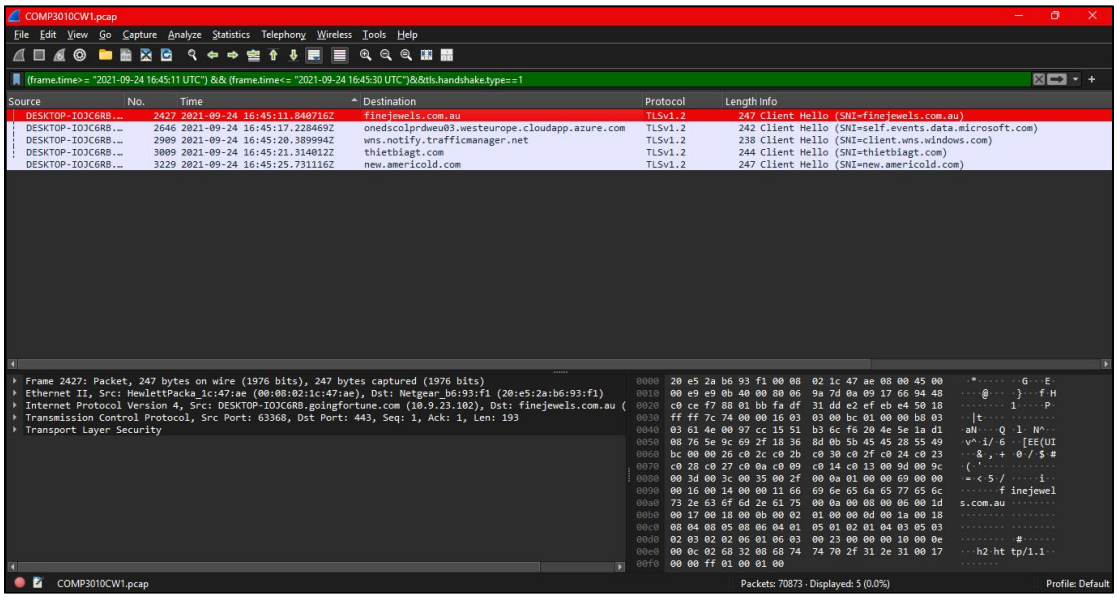
6. What is the version number of the web server identified in the previous question?

PHP/7.2.34

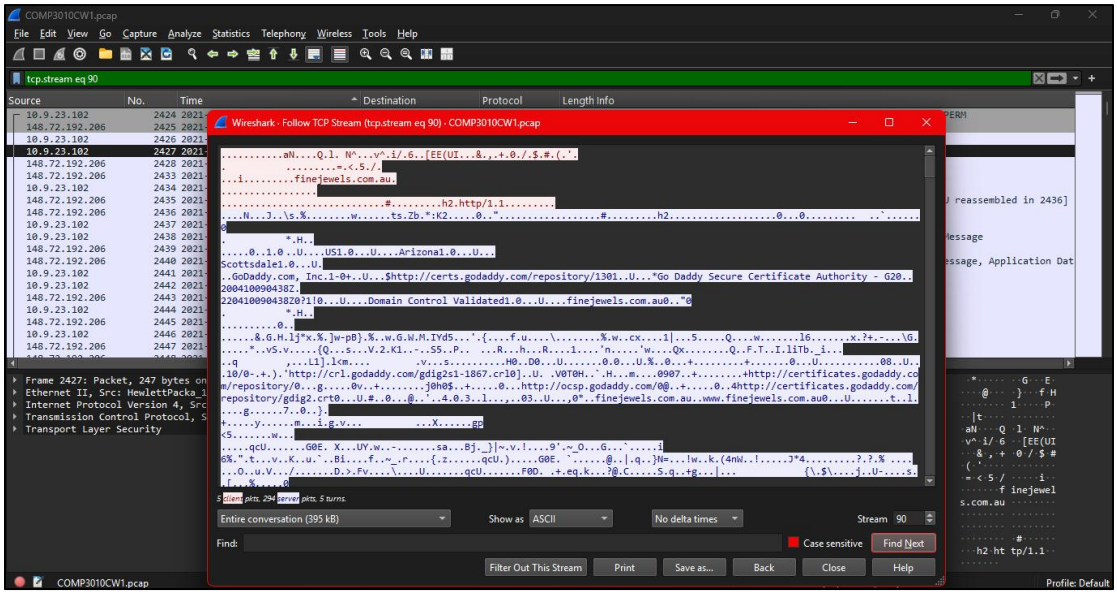


7. Identify the three additional domains that were involved in downloading malicious files to the victim host.
Hint: Inspect HTTPS traffic and focus on the time window between 16:45:11 and 16:45:30. Note this range is in UTC, not BST.

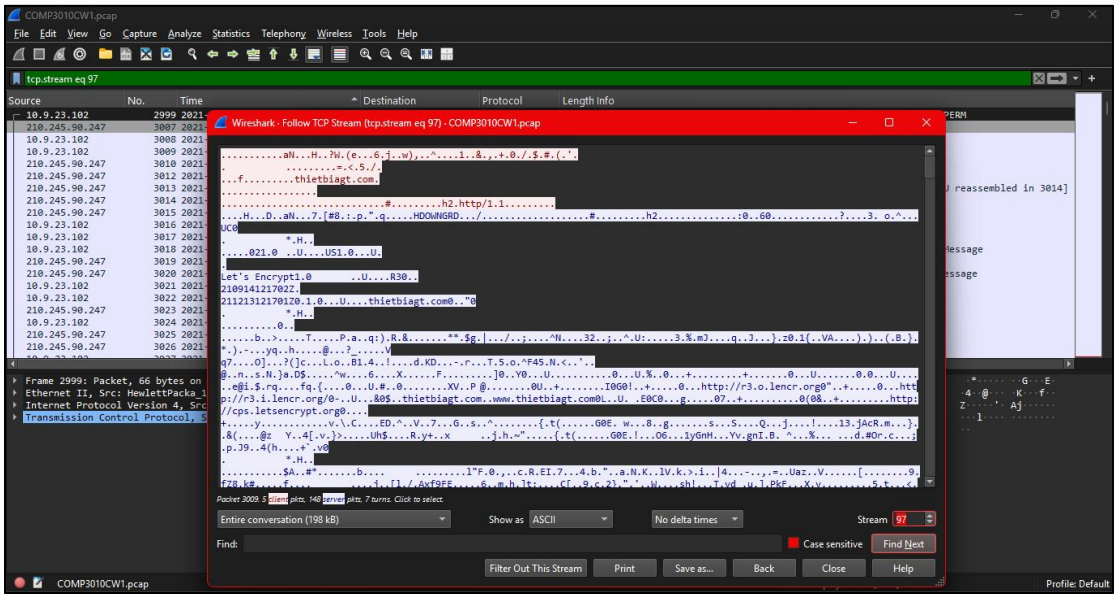
- **finejewels.com.au**
- **thietbiagt.com**
- **new.americold.com**



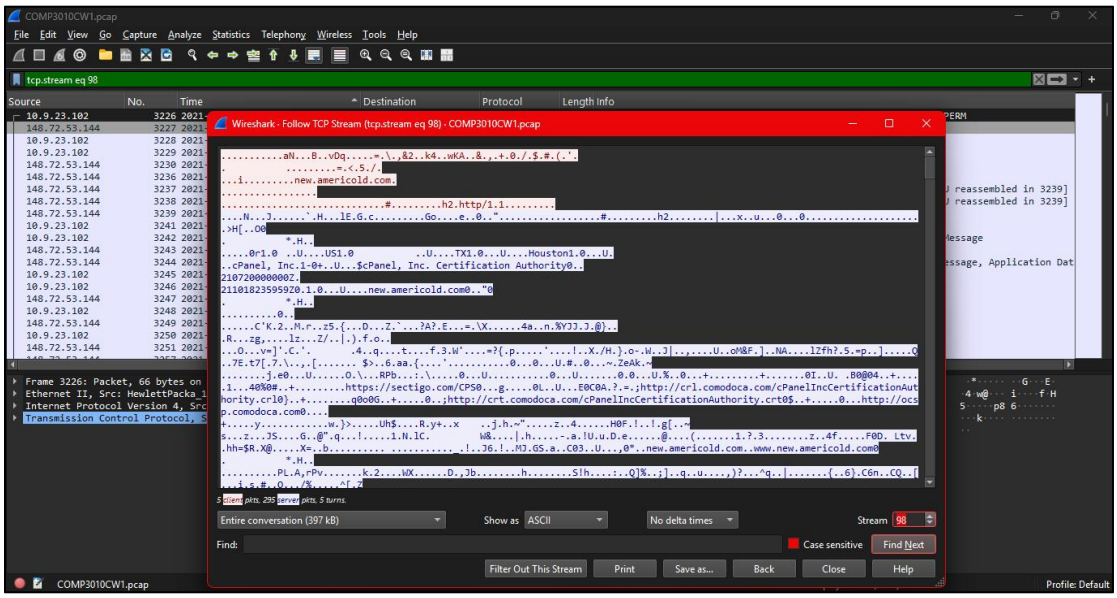
TCP Stream 90:



TCP Stream 97:



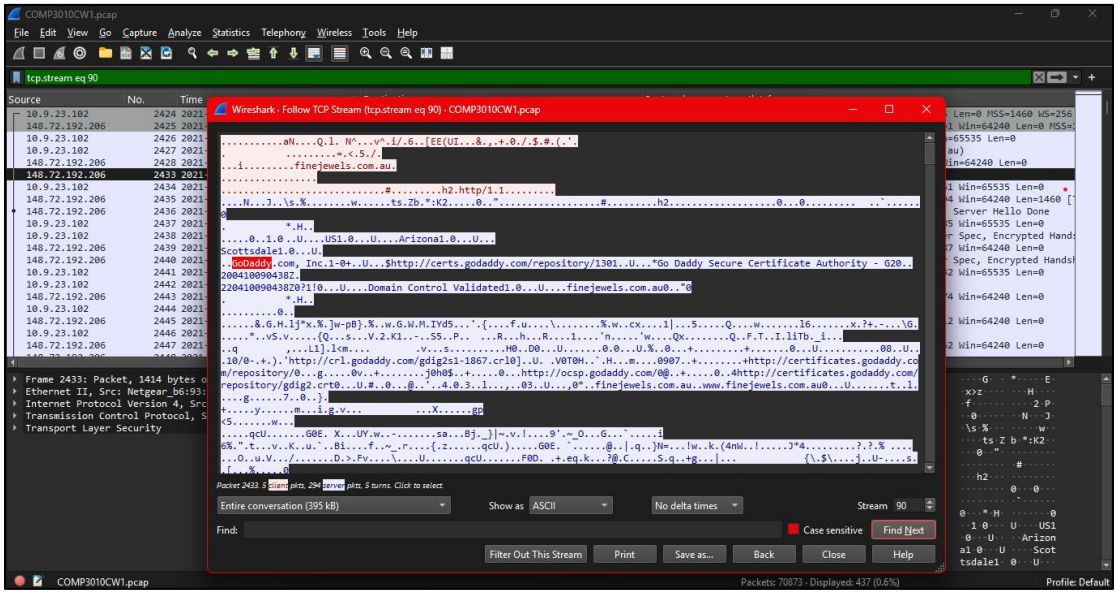
TCP Stream 98:



Part 2: Command and Control (C2) Activity

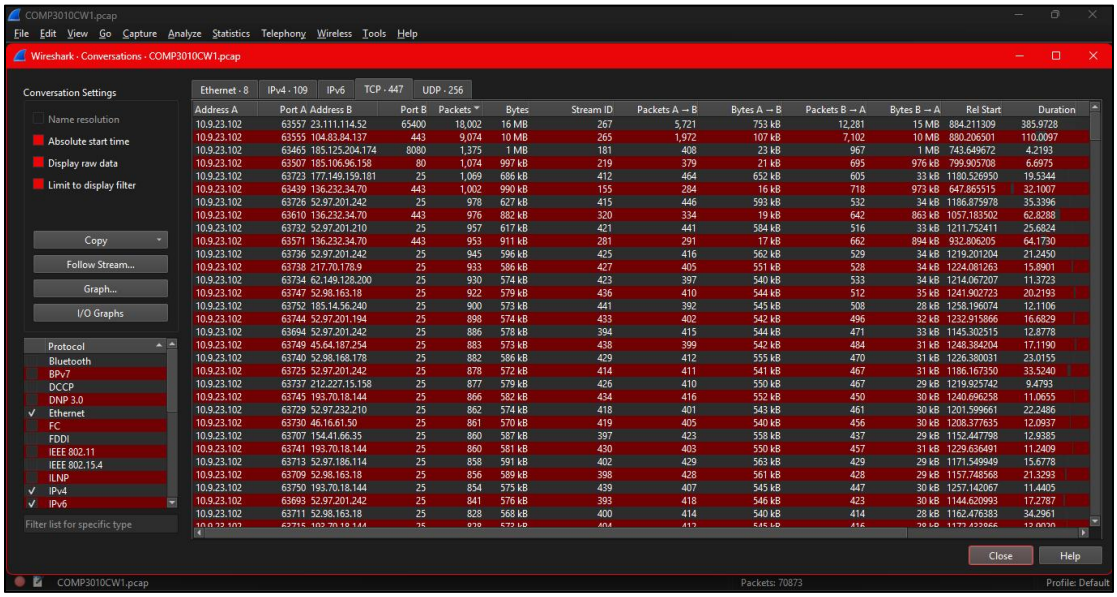
8. Which Certificate Authority (CA) issued the SSL certificate for the first domain identified in question 7?

GoDaddy

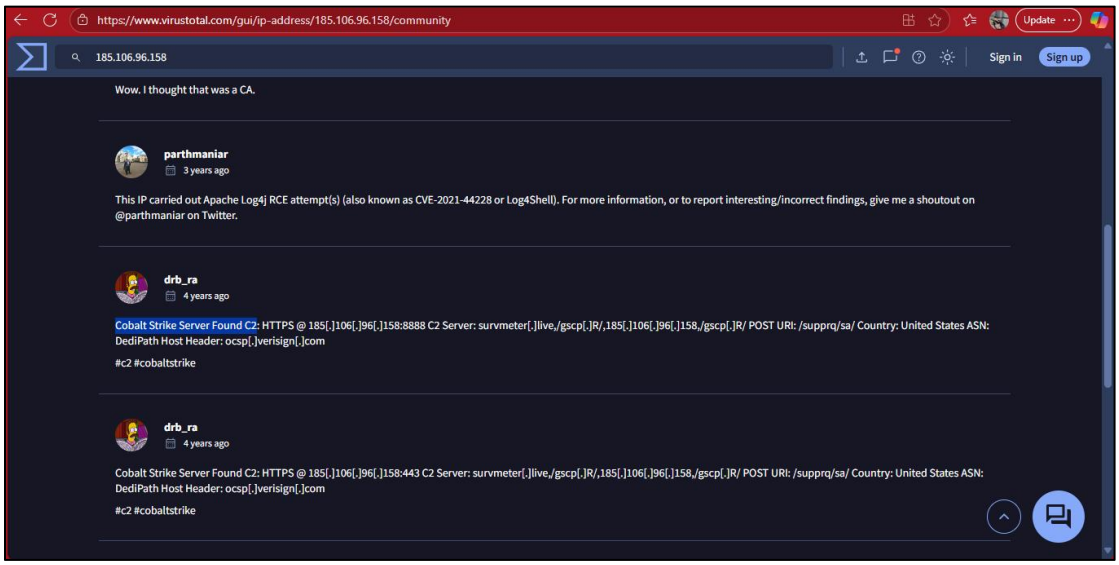


9. What are the two IP addresses of the Cobalt Strike servers? (Provide them in sequential order).
Hint: Inspect the Conversations menu option

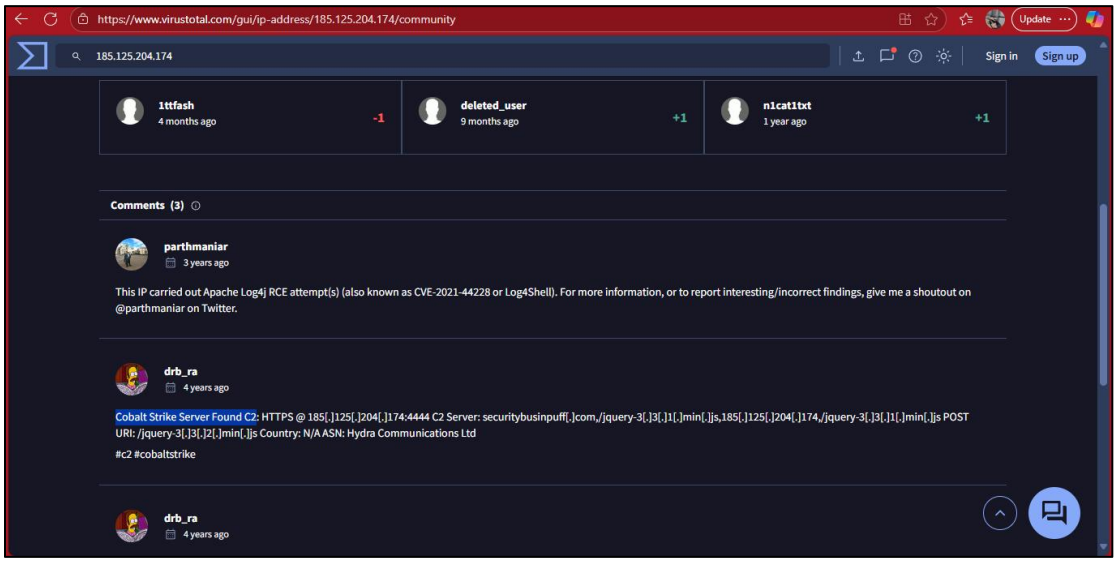
- **185.106.96.158**
- **185.125.204.174**



Analyze **185.106.96.158 using VirusTotal.**

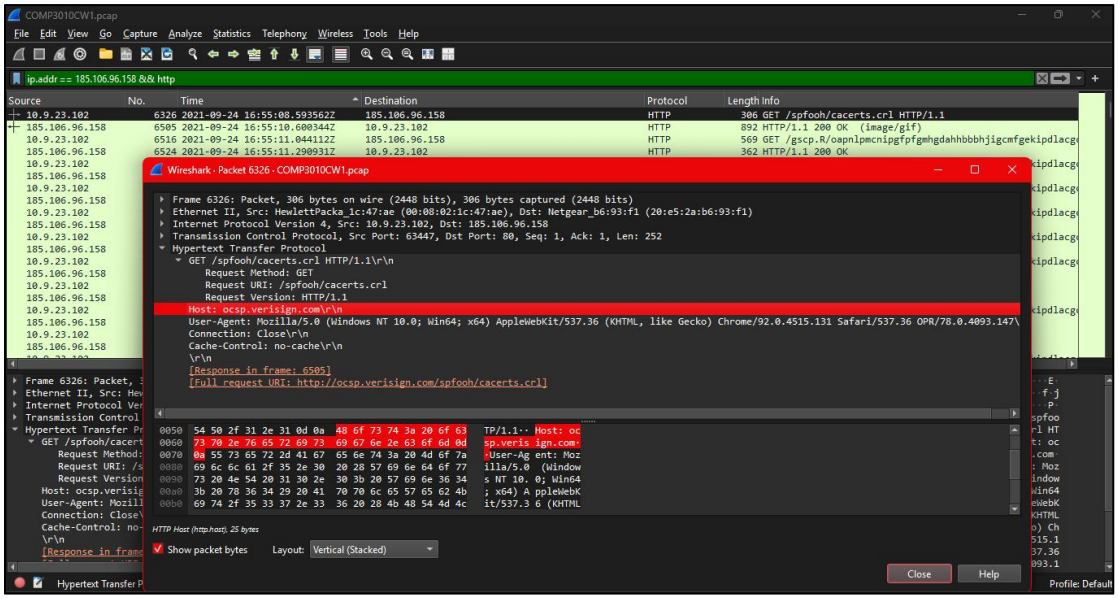


Analyze **185.125.204.174 using VirusTotal.**

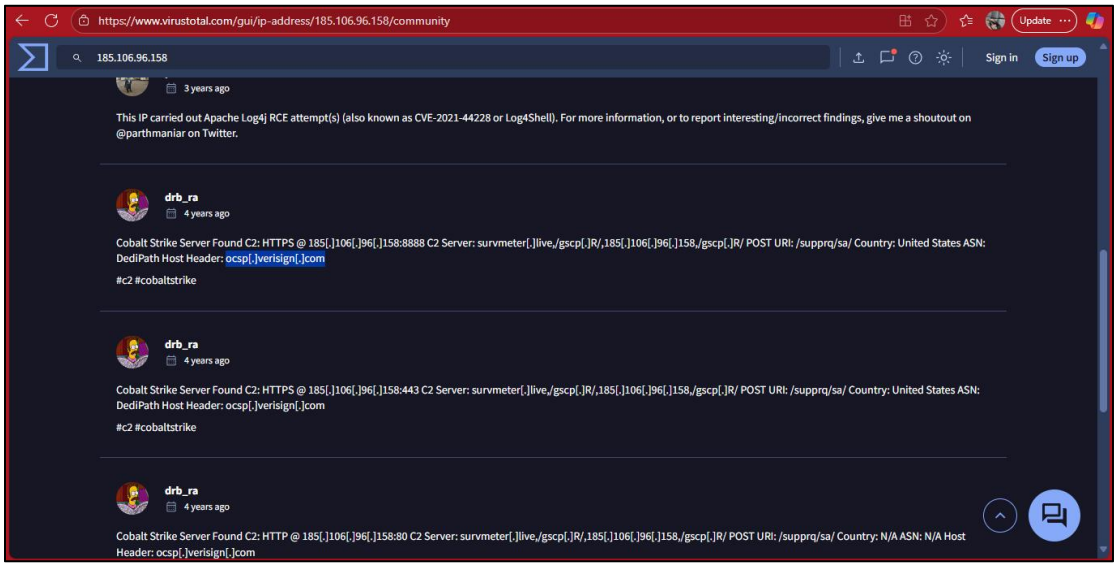


10. What is the value of the Host header for the first Cobalt Strike IP address?
Hint: Apply a filter to isolate DNS queries.

ocsp.verisign.com

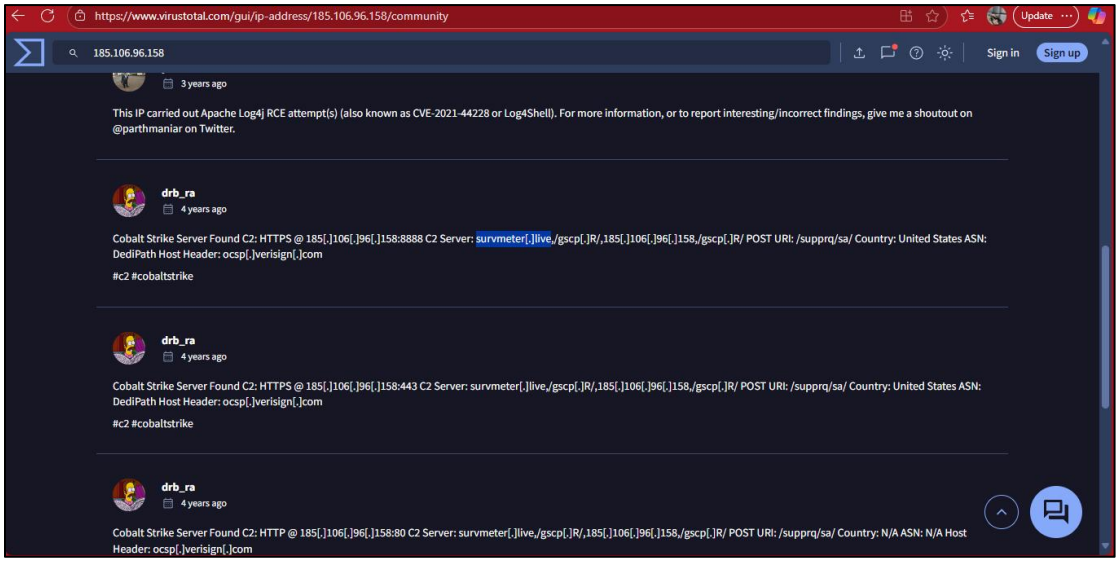


Verify in VirusTotal:



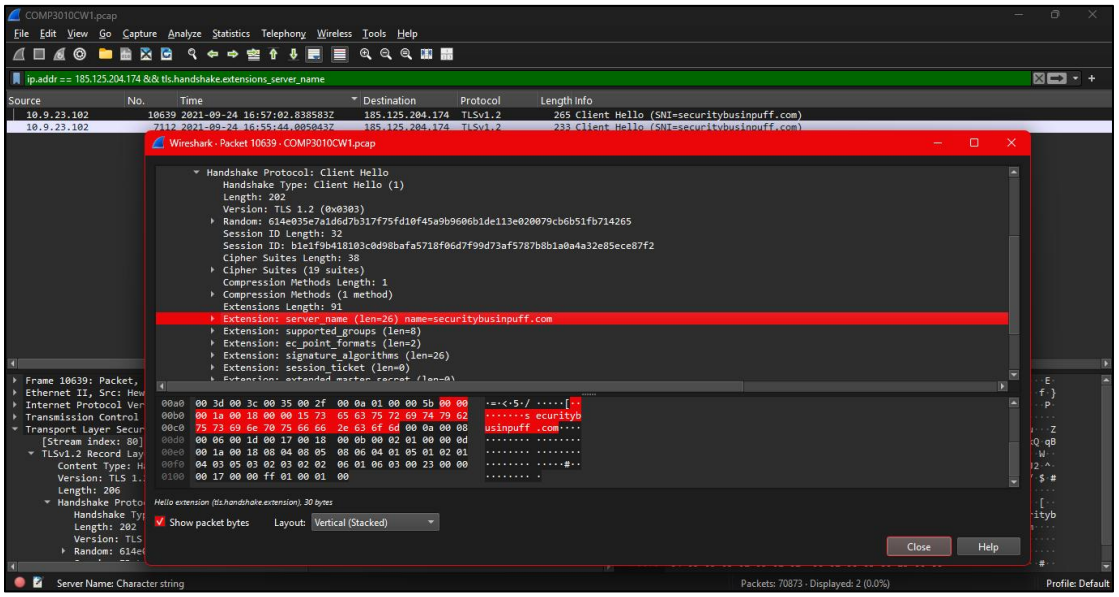
11. What is the domain name associated with the first Cobalt Strike IP address?
Hint: Take a closer look at HTTPS (443)

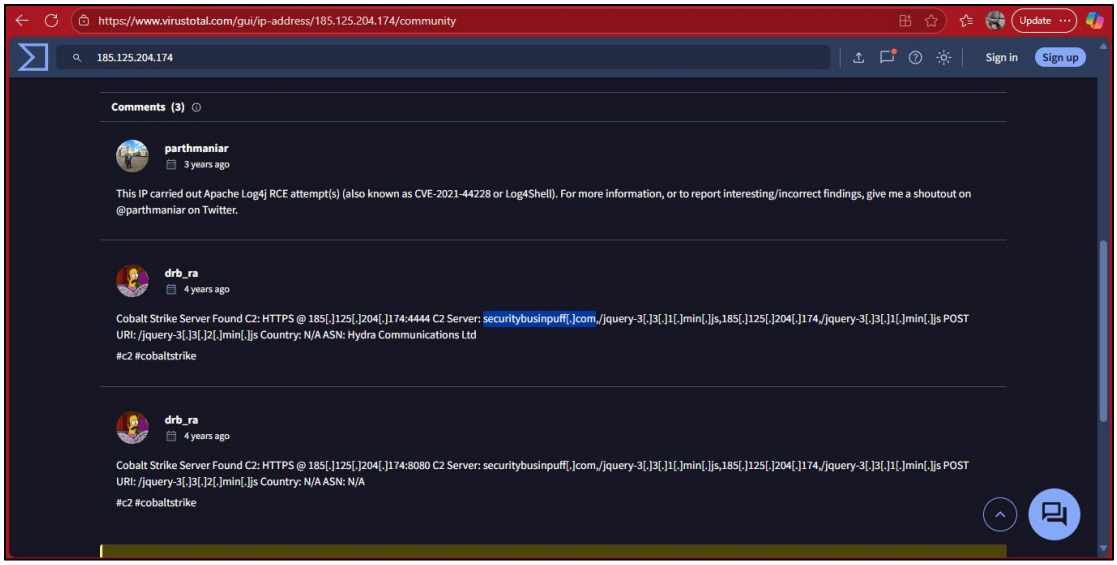
survmeter.live



12. What is the domain name associated with the second Cobalt Strike IP address?
Hint: Apply a filter to capture HTTP POST requests.

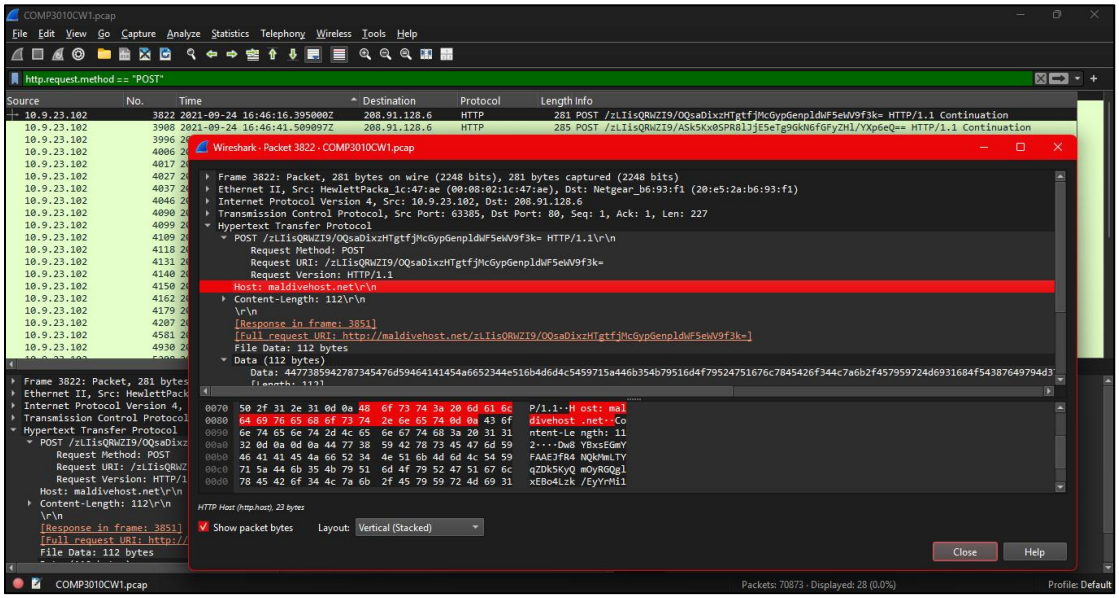
securitybusinpuff.com





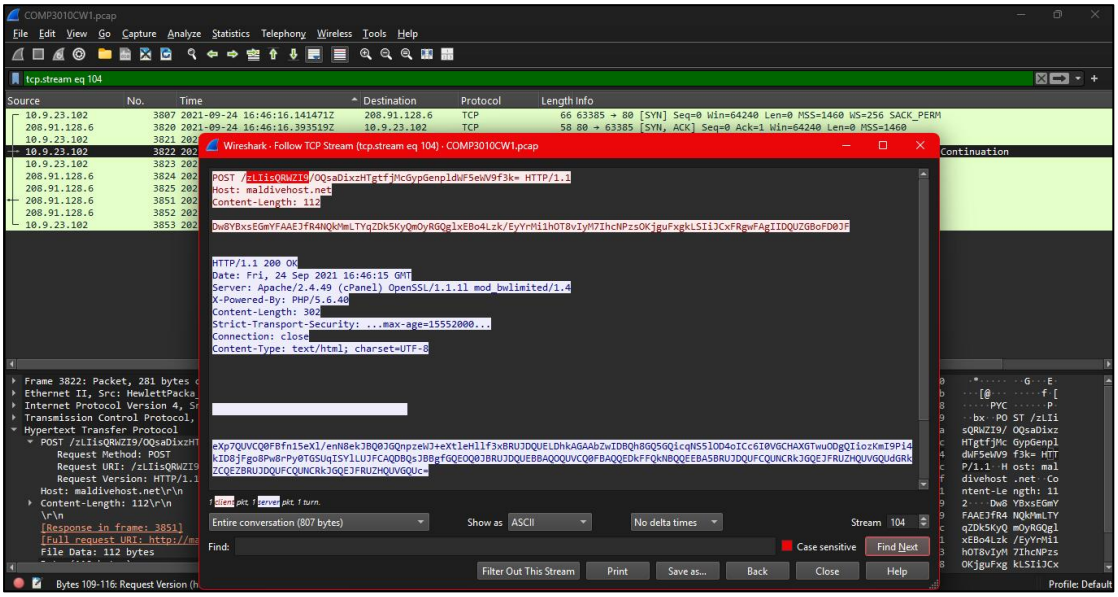
13. What is the domain name used for the post-infection traffic?

maldivehost.net



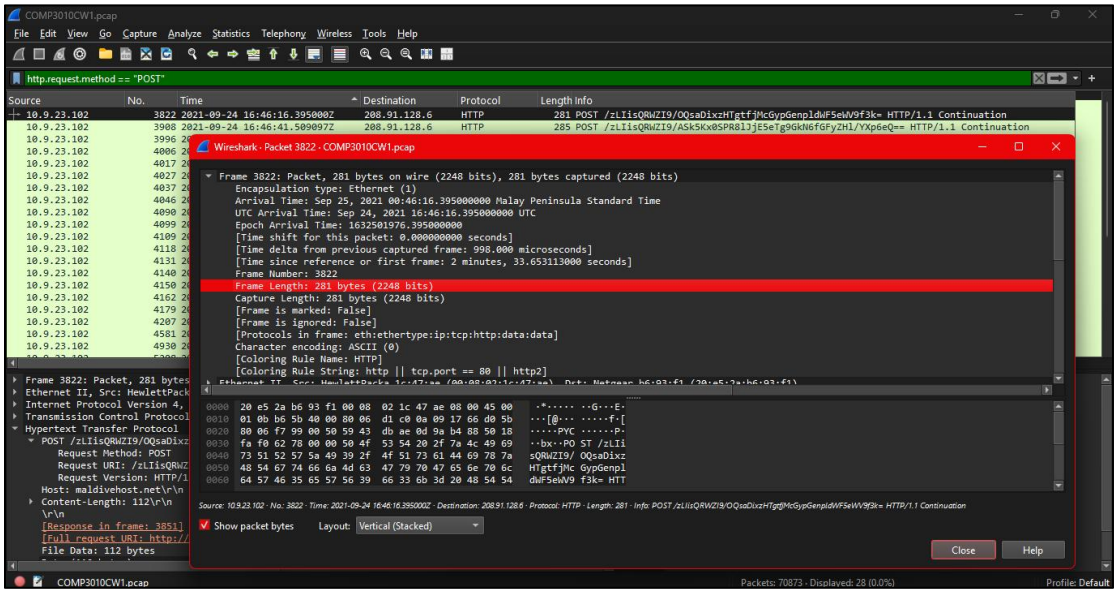
14. What are the first eleven characters of the data the victim host sends to the malicious domain identified in the previous question?

zLIisQRWZI9



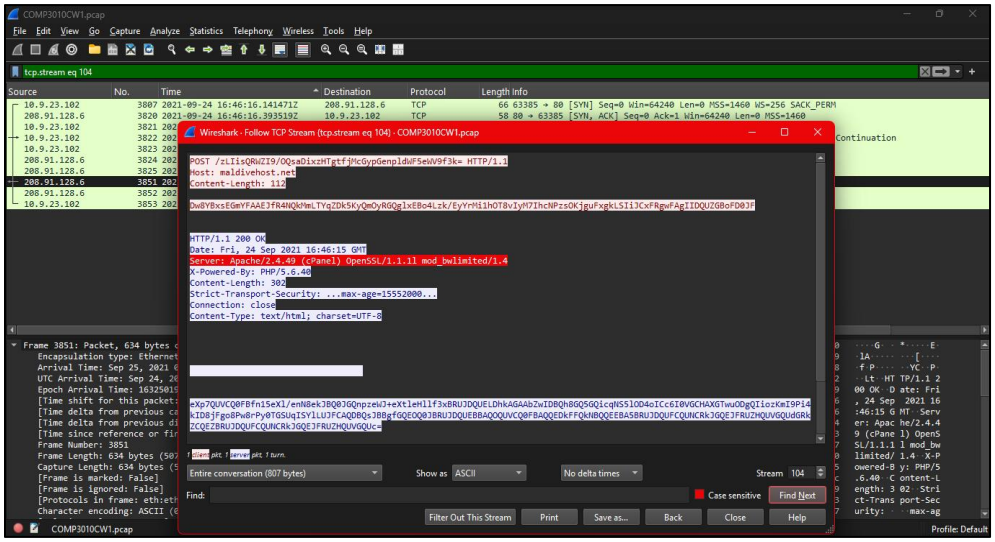
15. What was the length of the first packet the victim sent to the C2 server?

281 bytes (2248 bits)



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

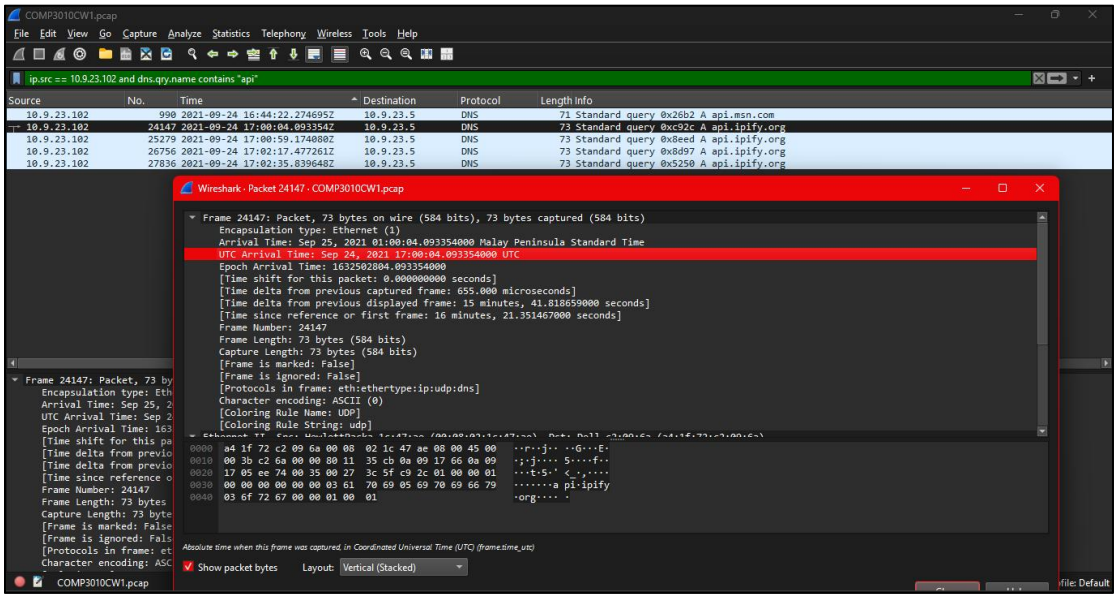
Server: Apache/2.4.49 (cPanel) OpenSSL/1.1.1l mod_bwlimited/1.4



Part 3: Final Exfiltration/Check-in

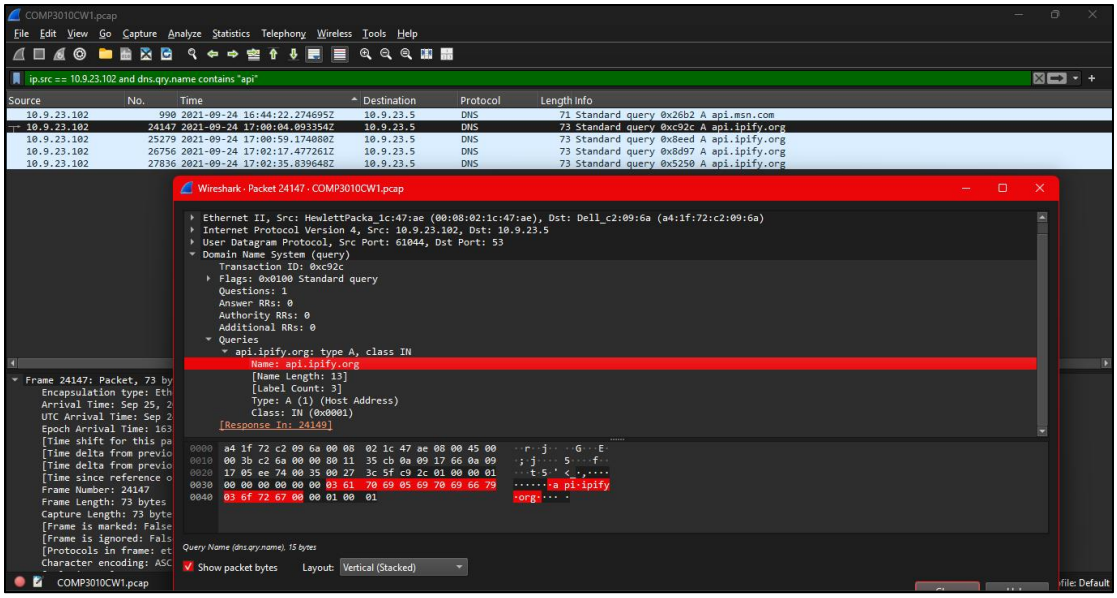
17. What was the date and time (in yyyy-mm-dd hh:mm:ss UTC format) when the DNS query occurred for the domain used by the malware to check the victim's external IP address?

2021-09-24 17:00:04 UTC



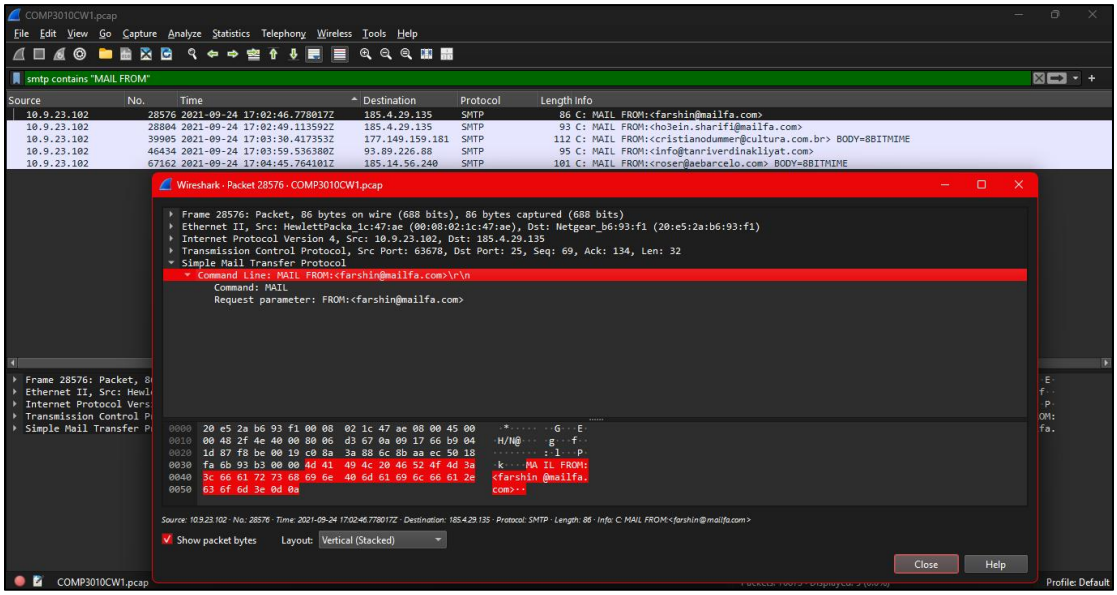
18. What was the domain name in the DNS query from the previous question?

api.ipify.org



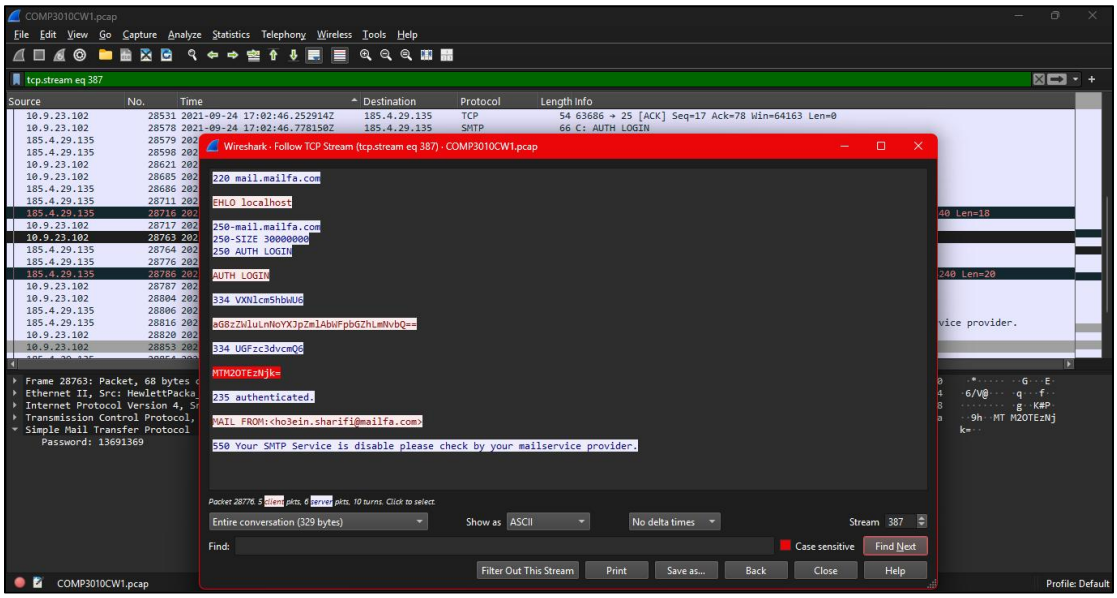
19. What was the first email address observed in the SMTP traffic in the pcap file (the MAIL FROM address)?

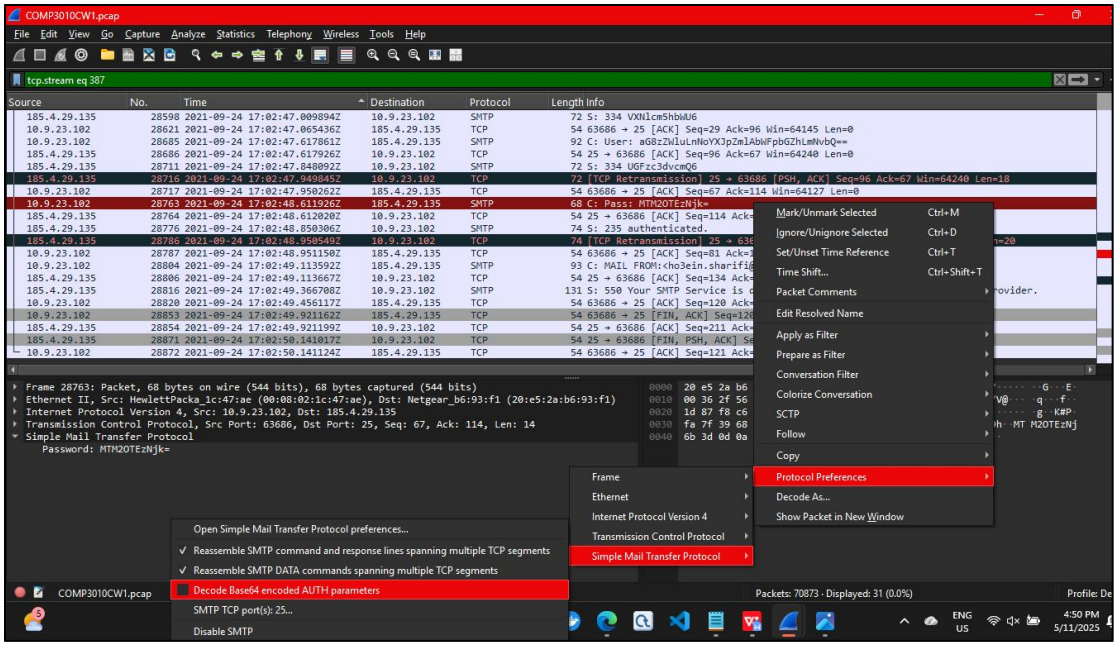
farshin@mailfa.com



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

The Password is Encoded: **MTM2OTEzNjk=**





The Password is Decoded: **13691369**