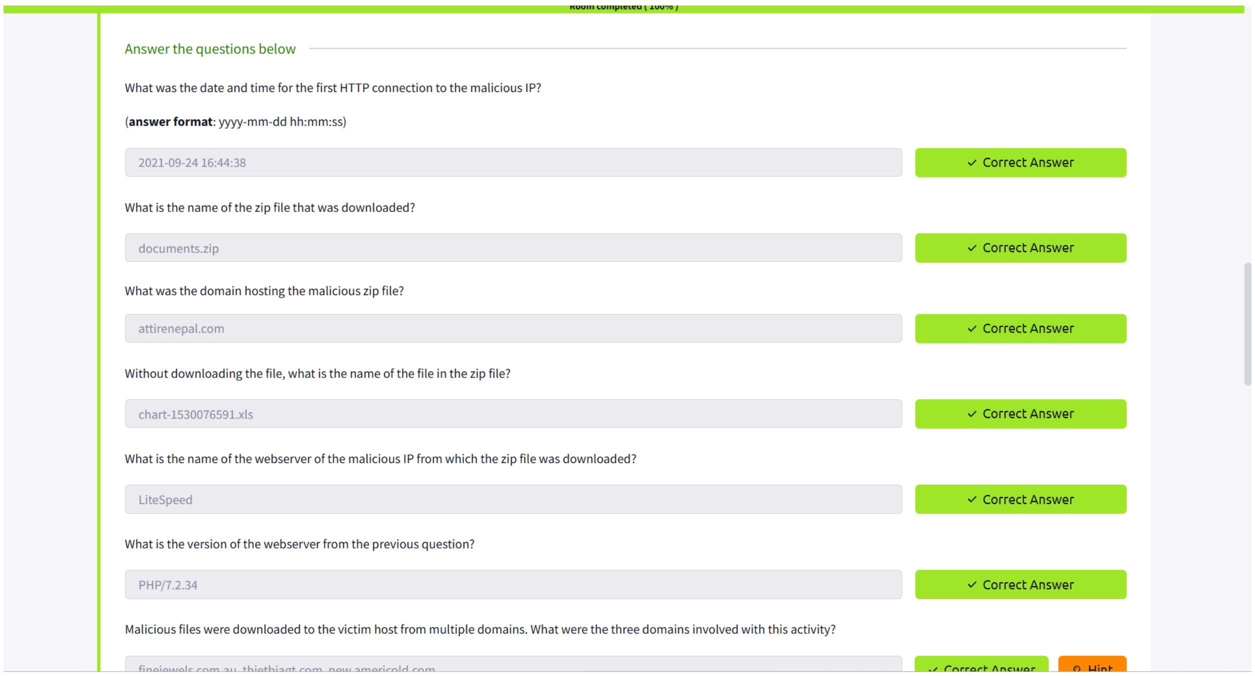
Name: Ram Haygrev.S Roll No: 231901039

EX 3: CARNAGE

Aim: Investigate the packet capture and uncover the malicious activities

ANSWERS TO QUESTIONS:



Answer the questions below

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

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

documents.zip

What was the domain hosting the malicious zip file?

attirenepal.com

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

chart-1530076591.xls

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

LiteSpeed

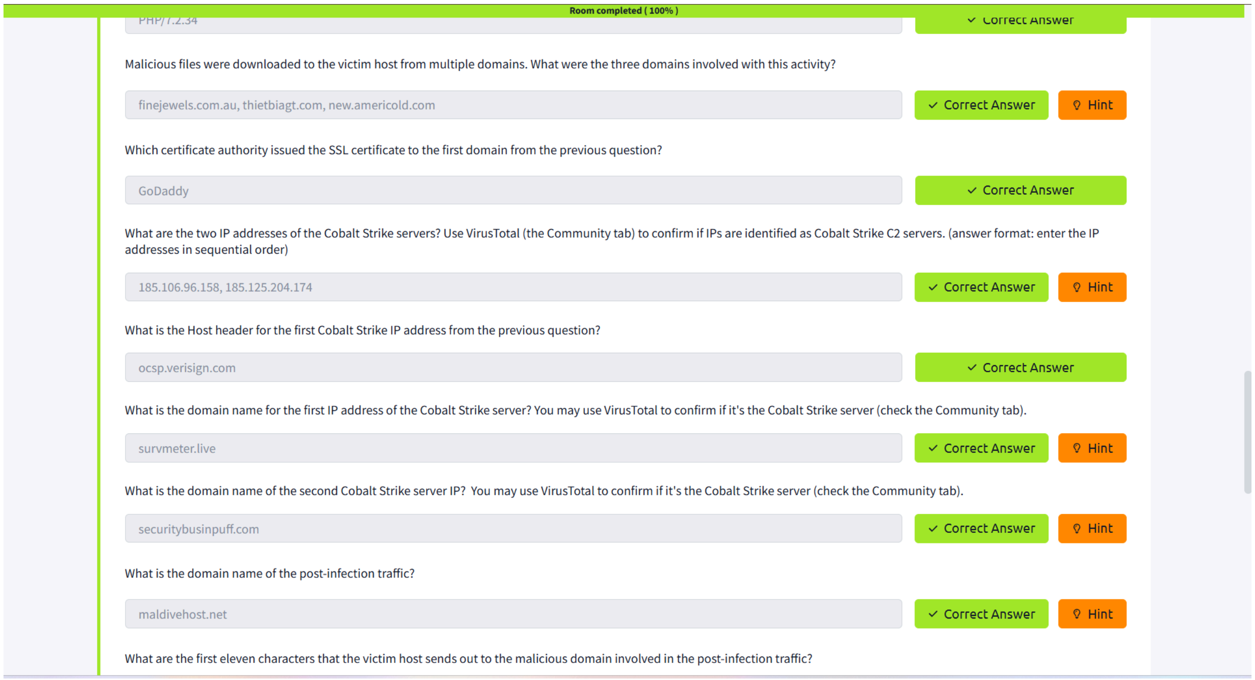
What is the version of the webserver from the previous question?

PHP/7.2.34

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

Name: Ram Haygrev.S Roll No: 231901039



PHP/7.2.34

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

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

GoDaddy

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

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

ocsp.verisign.com

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

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

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

maldivehost.net

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

Result: Thus the packets were captured and Analyzed successfully