Task 1:

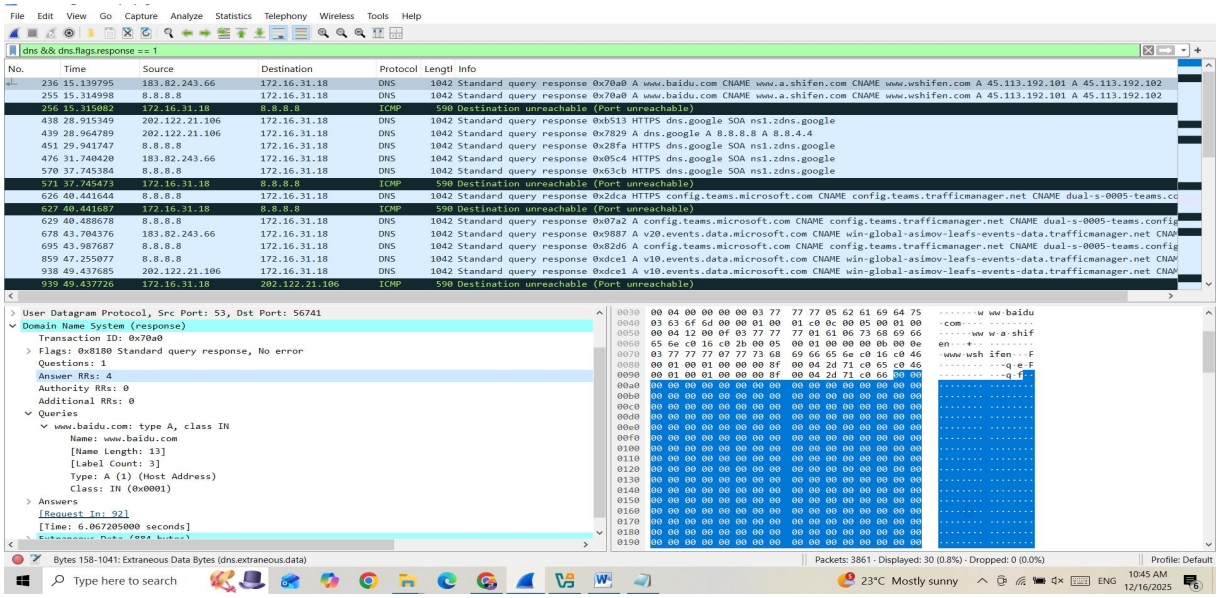
1.1 How many DNS queries are sent from your browser (host machine) to DNS Server(s) ? >DNS/Query-Response:

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Total	104		0.0005	0.0600	66.160	100%		

1.2.How many DNS servers are involved ?

Filter: dns && ip.src == 172.16.31.18 && dns.flags.response == 1

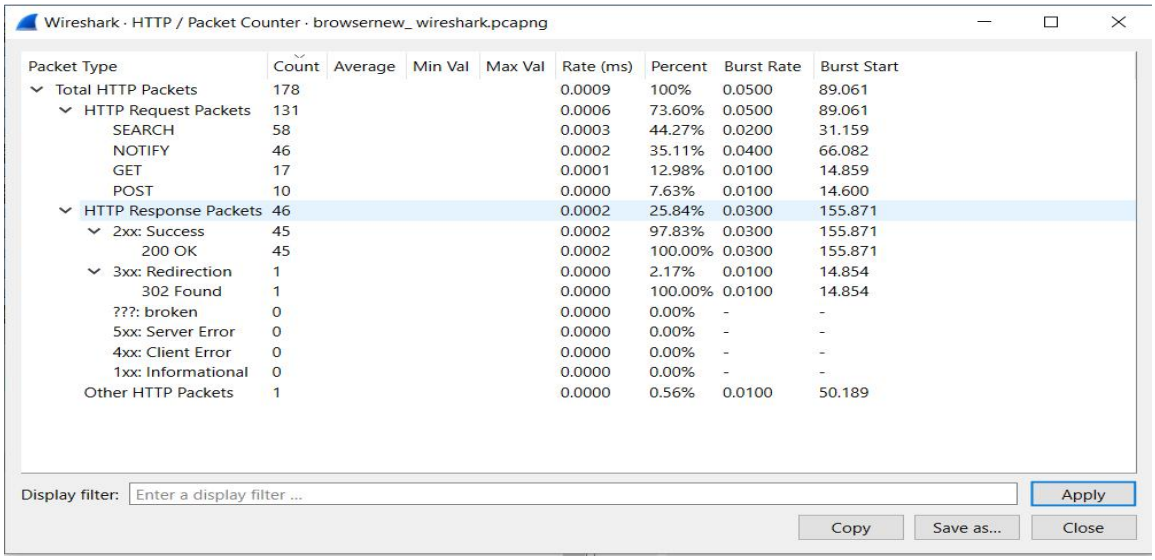
Ans=4



1.3.Which DNS Server replies with actual IP Address(es). Do all DNS servers respond ?

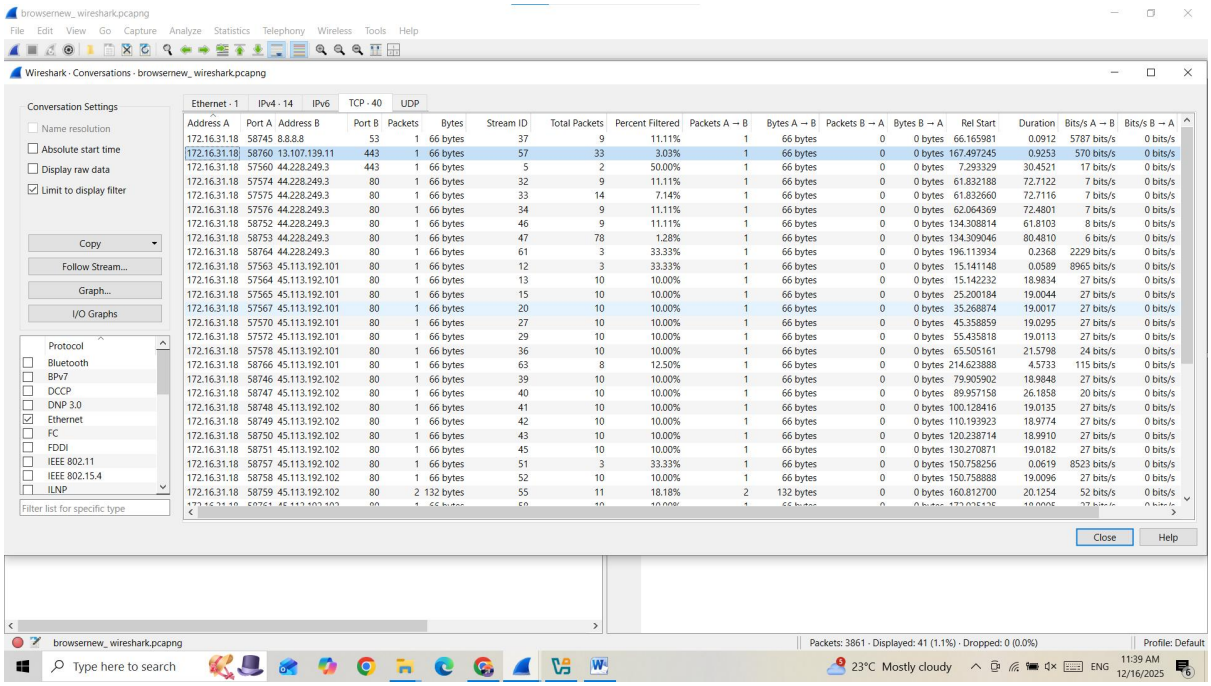
→ no

2. How many HTTP requests (Type and respective count of requests), responses (status code and phrase of each of the responses) did the browser send and receive ?

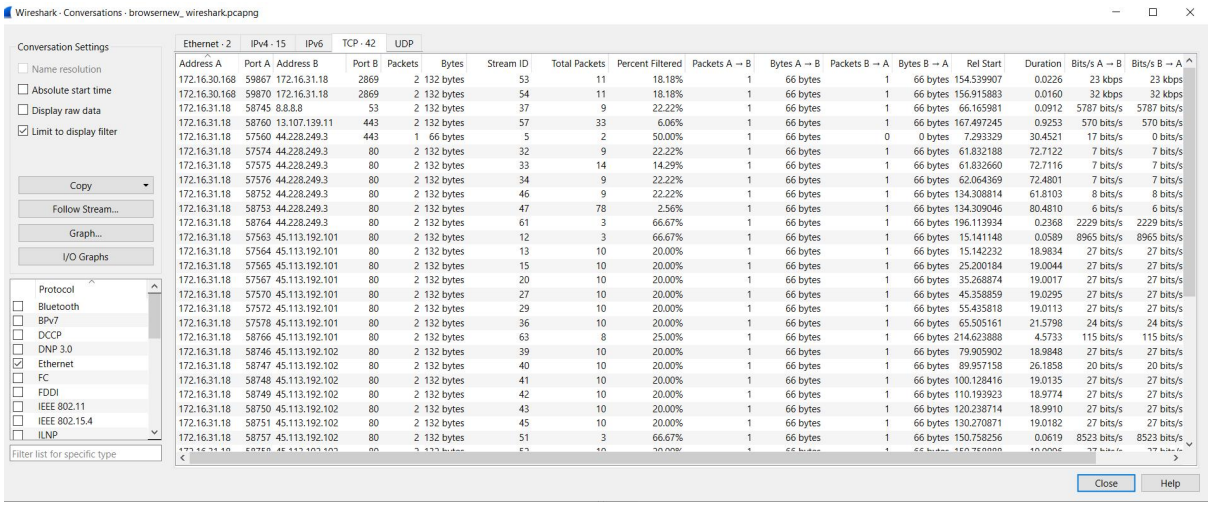


3. How many TCP Connections has the browser established overall ?

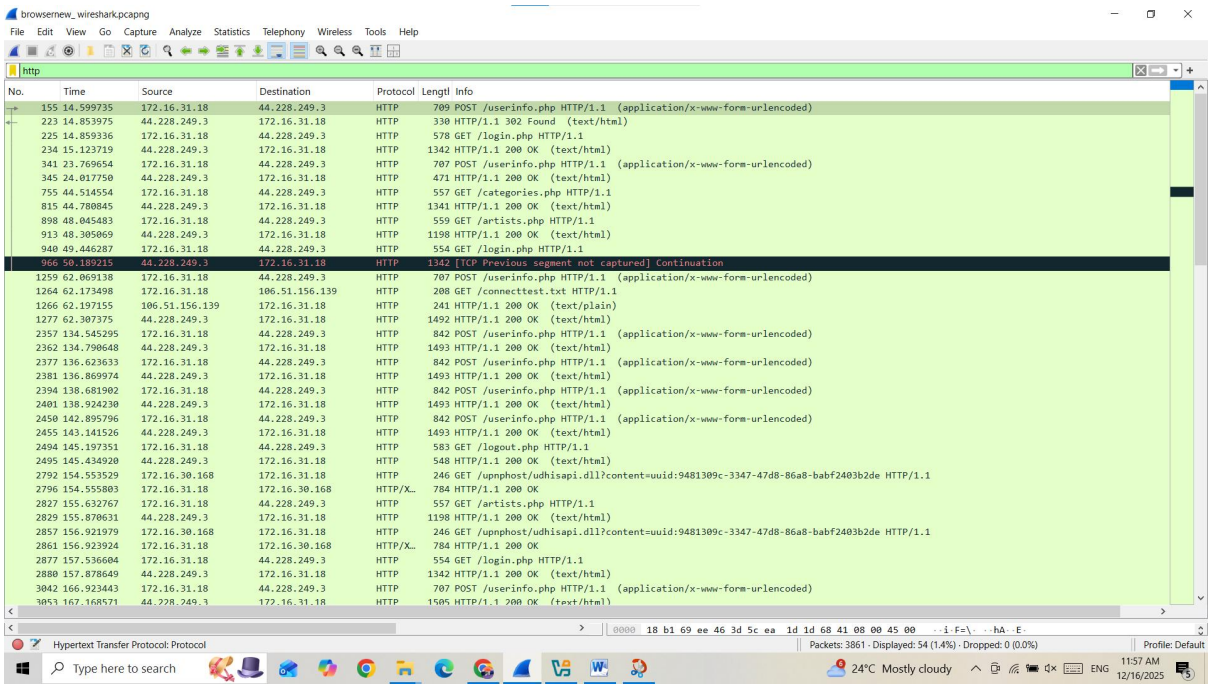
Filter: tcp.flags.syn == 1 && tcp.flags.ack == 0 && ip.src == 172.16.31.18



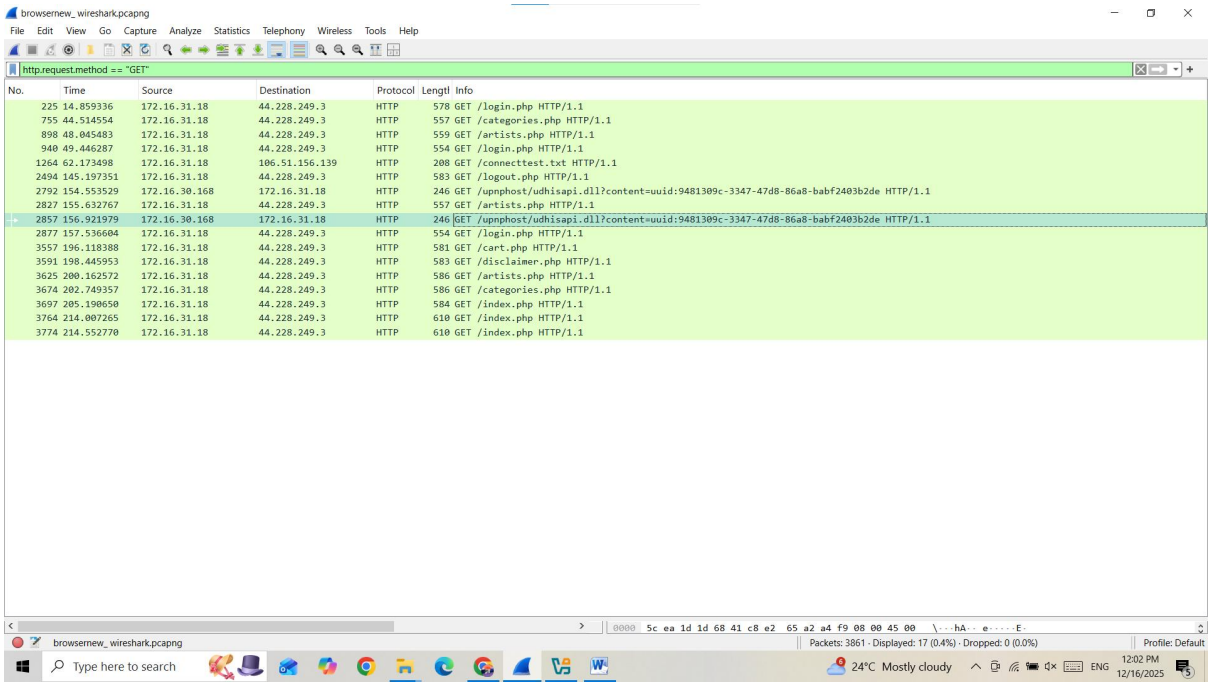
4. What is the time taken to establish TCP connection(s) ?. List this time taken value for each of the TCP connection(s).



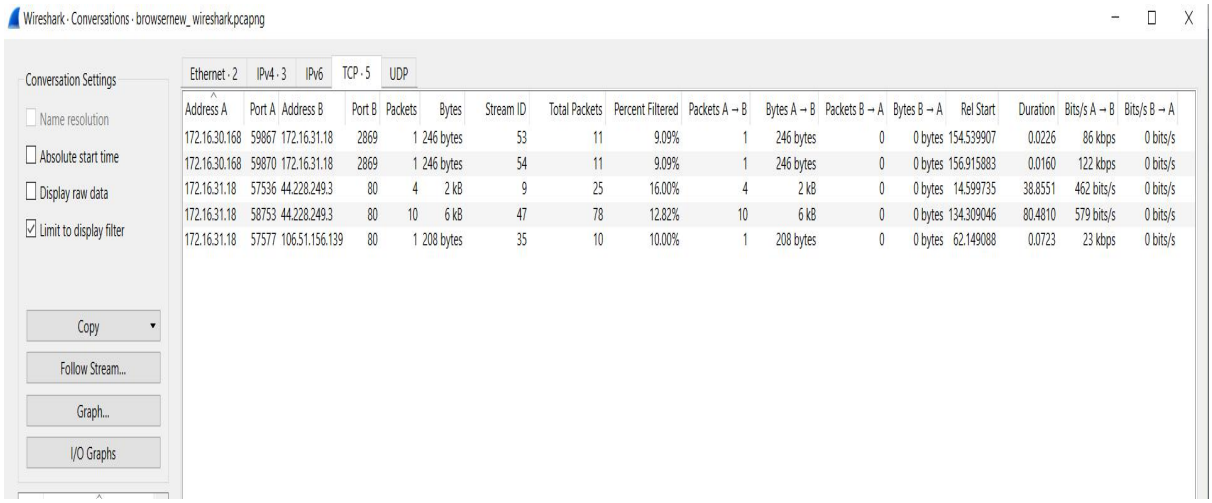
5.Browse the website by moving to various sub links, embedded objects listed in the site.



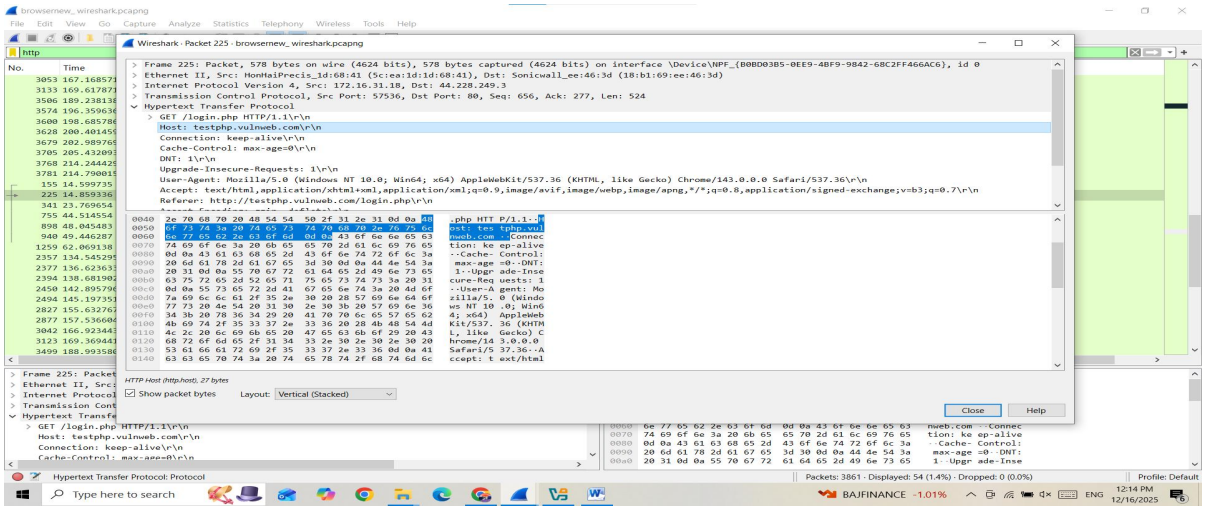
6. How many objects/files are downloaded?

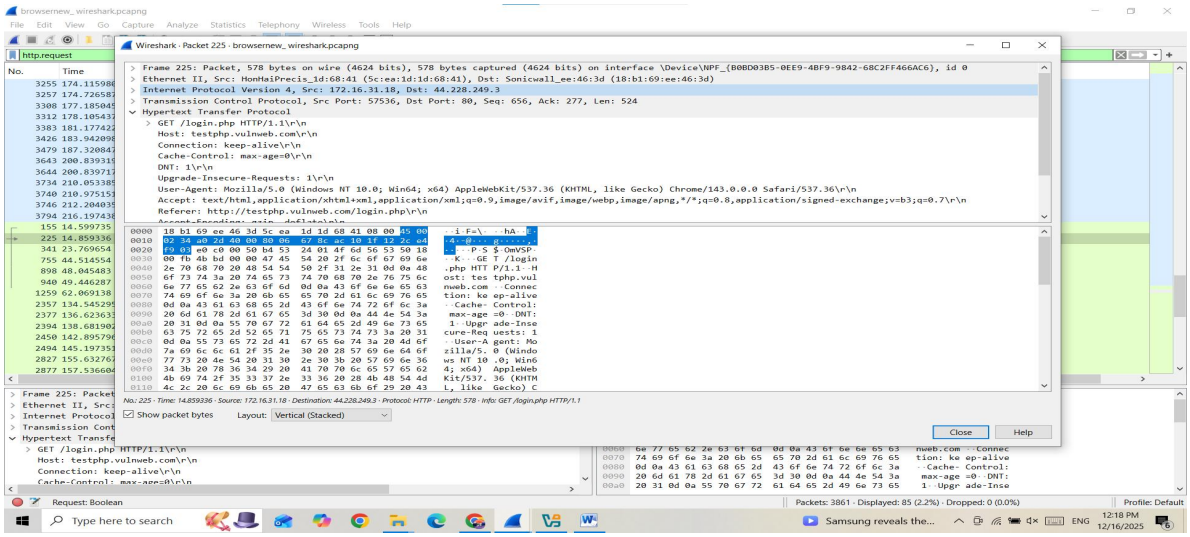


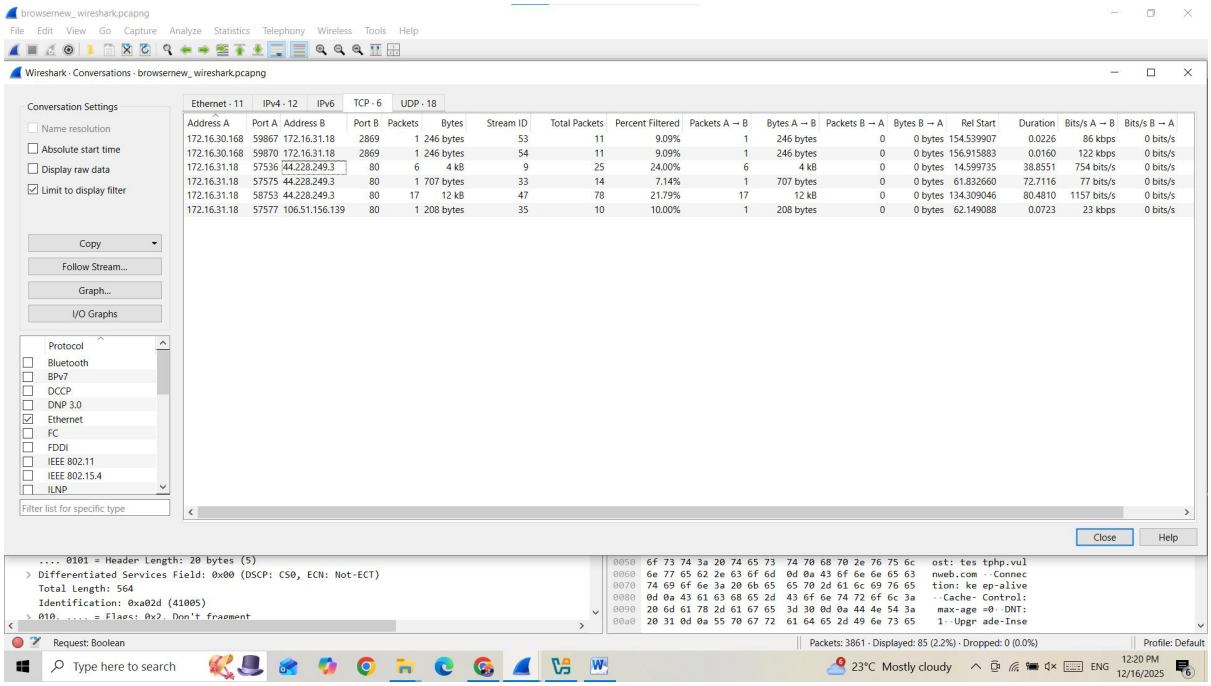
7. Make a detailed list including for each object/file downloaded what is the time taken for downloading the objects, the size of the object downloaded, object name, last modified time at the server



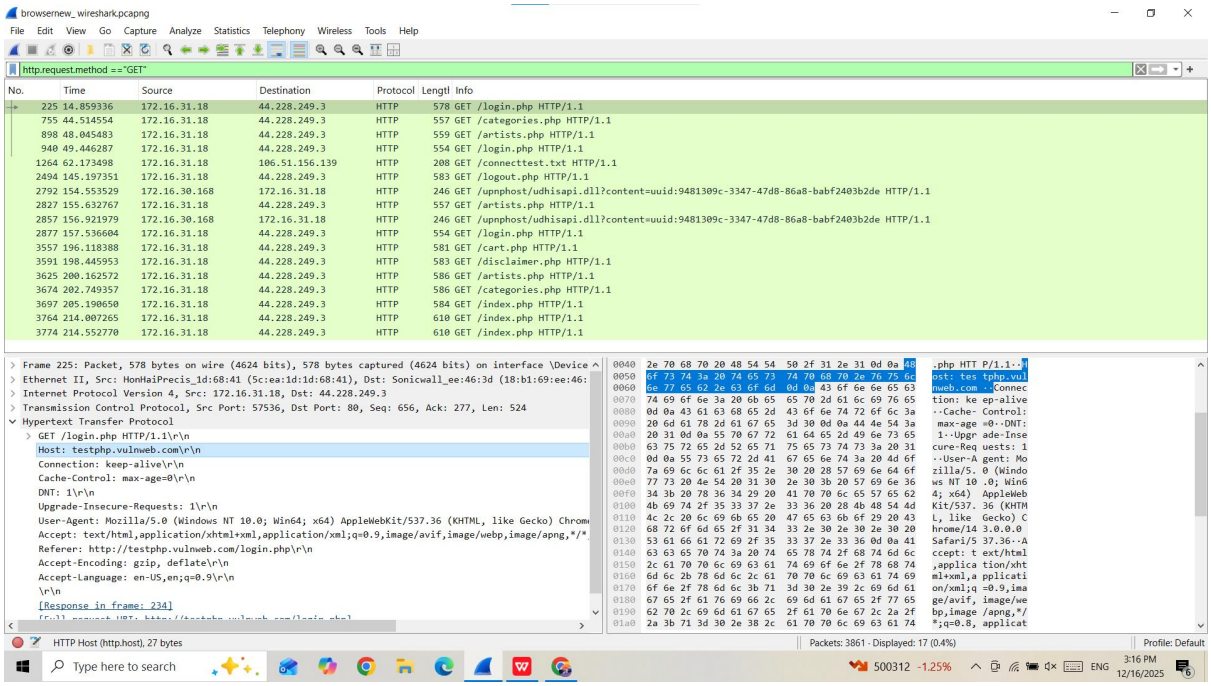
8. How many other websites are visited from this site, by clicking on to various possible links which take you to the other sites



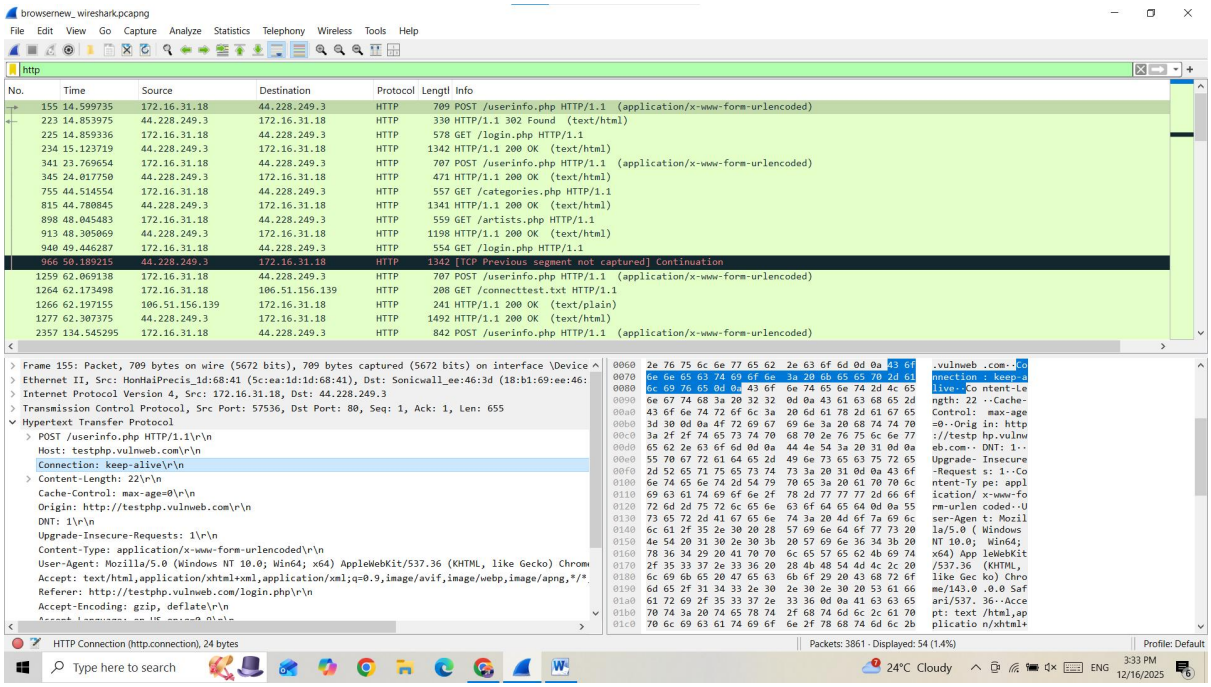




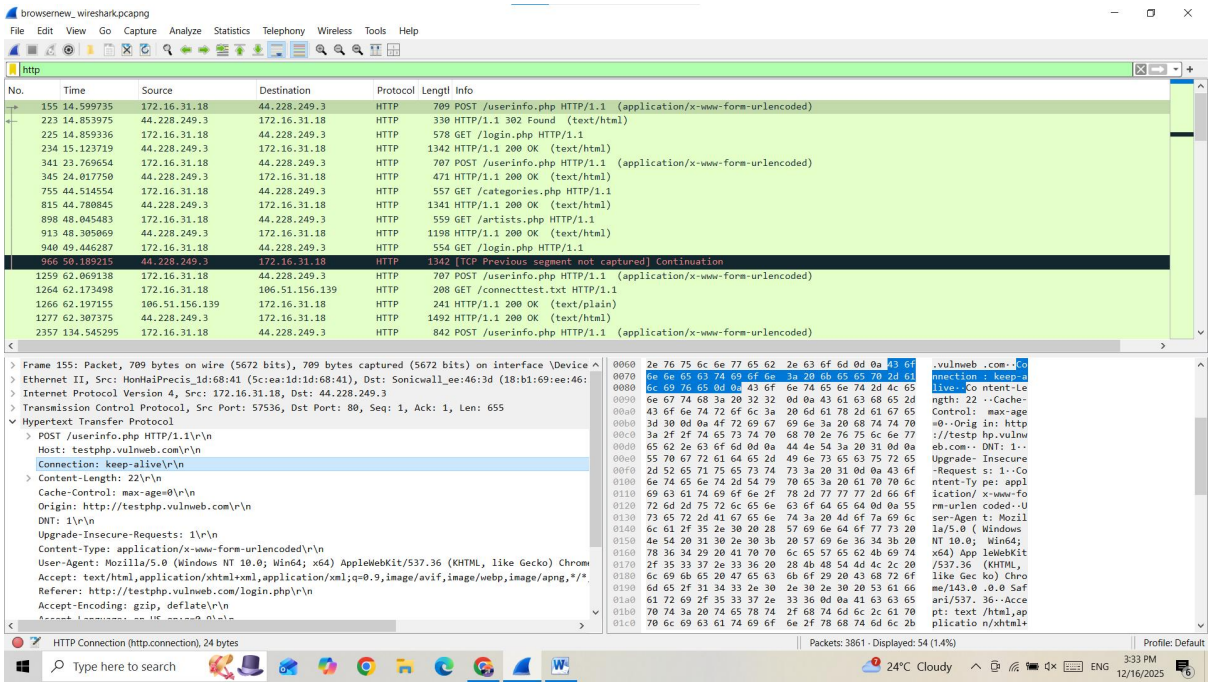
9. When http://testphp.vulnweb.com/login.php is entered, is there any embedded object shown/downloaded from different site(s) (other than http://testphp.vulnweb.com/login.php)?



10. How many times does the browser ask the site to keep the connection alive ?

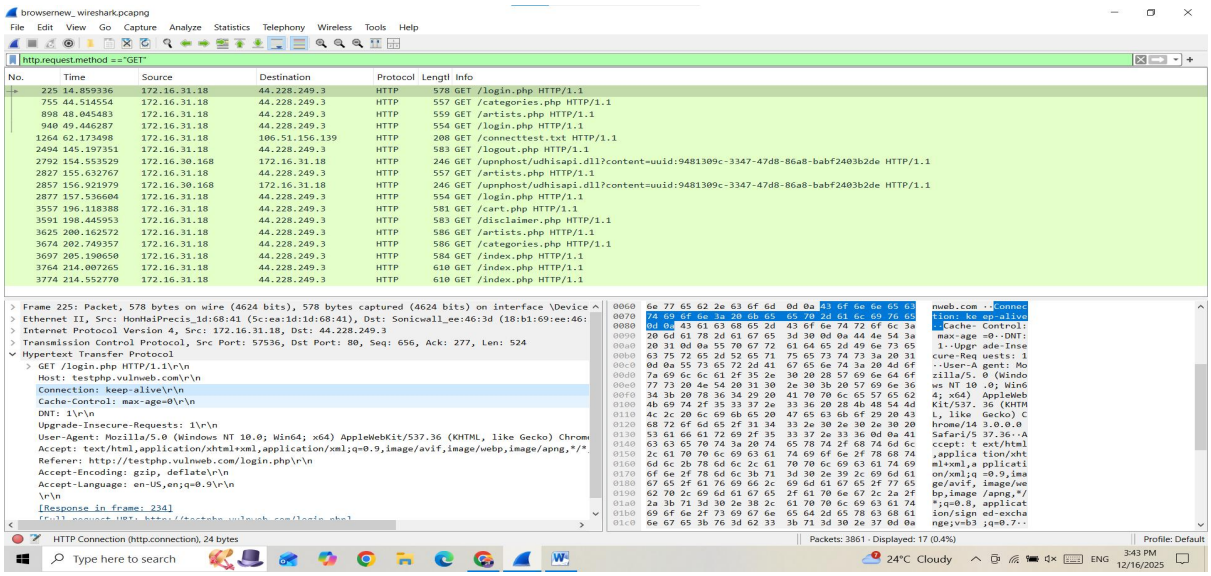


11. Which version of the HTTP is your browser running ?

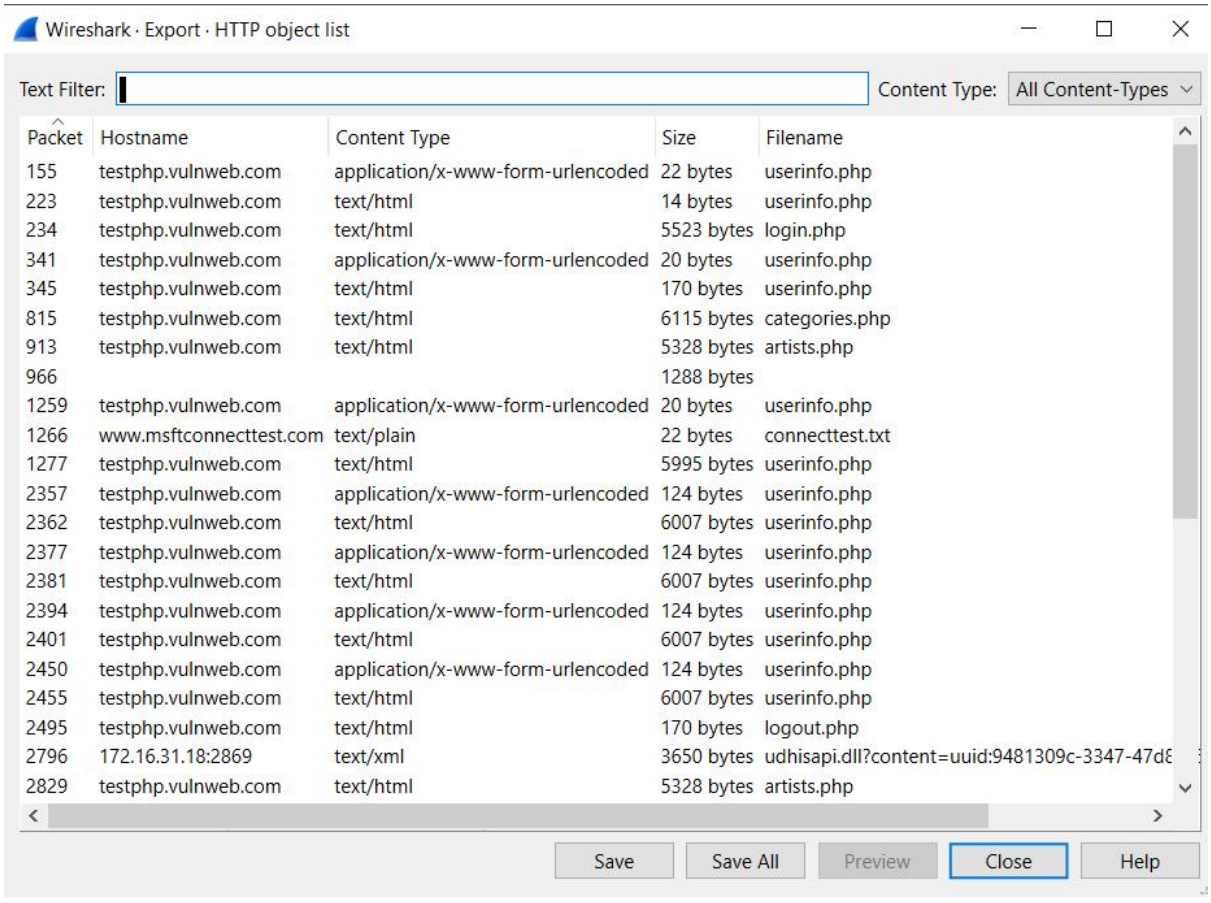


Task 2:

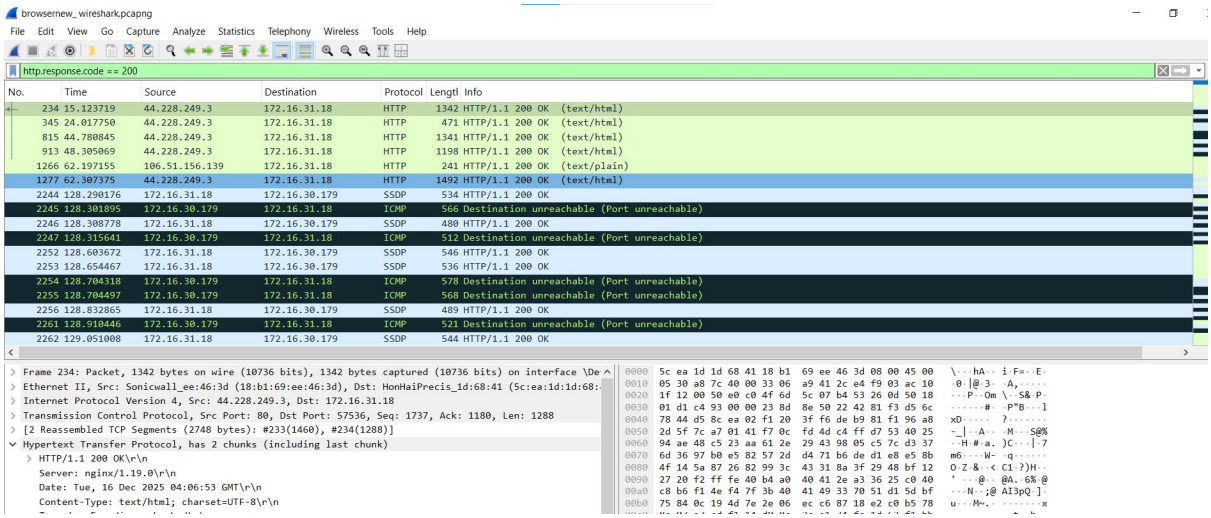
1. How many conditional GETs are sent by browser to the server ?



2. Make a list for each of the file/object downloaded, how many times the server sends the full contents of the respective file/object ?



Packet	Hostname	Content Type	Size	Filename
155	testphp.vulnweb.com	application/x-www-form-urlencoded	22 bytes	userinfo.php
223	testphp.vulnweb.com	text/html	14 bytes	userinfo.php
234	testphp.vulnweb.com	text/html	5523 bytes	login.php
341	testphp.vulnweb.com	application/x-www-form-urlencoded	20 bytes	userinfo.php
345	testphp.vulnweb.com	text/html	170 bytes	userinfo.php
815	testphp.vulnweb.com	text/html	6115 bytes	categories.php
913	testphp.vulnweb.com	text/html	5328 bytes	artists.php
966			1288 bytes	
1259	testphp.vulnweb.com	application/x-www-form-urlencoded	20 bytes	userinfo.php
1266	www.msftconnecttest.com	text/plain	22 bytes	connecttest.txt
1277	testphp.vulnweb.com	text/html	5995 bytes	userinfo.php
2357	testphp.vulnweb.com	application/x-www-form-urlencoded	124 bytes	userinfo.php
2362	testphp.vulnweb.com	text/html	6007 bytes	userinfo.php
2377	testphp.vulnweb.com	application/x-www-form-urlencoded	124 bytes	userinfo.php
2381	testphp.vulnweb.com	text/html	6007 bytes	userinfo.php
2394	testphp.vulnweb.com	application/x-www-form-urlencoded	124 bytes	userinfo.php
2401	testphp.vulnweb.com	text/html	6007 bytes	userinfo.php
2450	testphp.vulnweb.com	application/x-www-form-urlencoded	124 bytes	userinfo.php
2455	testphp.vulnweb.com	text/html	6007 bytes	userinfo.php
2495	testphp.vulnweb.com	text/html	170 bytes	logout.php
2796	172.16.31.18:2869	text/xml	3650 bytes	udhisapi.dll?content=uuid:9481309c-3347-47d8
2829	testphp.vulnweb.com	text/html	5328 bytes	artists.php



3. Explain in detail what is the difference in server's behaviour between first and second request/browsing ?

->First Request

During the first request, the browser cache is empty. The browser sends normal HTTP GET requests for the main HTML page and all embedded objects. Since the server has no information about any cached copies at the client side, it unconditionally sends the full content of every requested resource.

http method – 200 Ok – full content will be delivered

Second Request

During the second request, the browser already has cached copies of the previously downloaded resources. Instead of requesting the full content again, the browser sends conditional GET requests that include cache validation headers.

http method – 304 not modified – where it will not send any content if it was same.

4. List the headers of HTTP which influence this functionality.

->List of HTTP method Headers

For 200

If modified since

If none match

Cache control

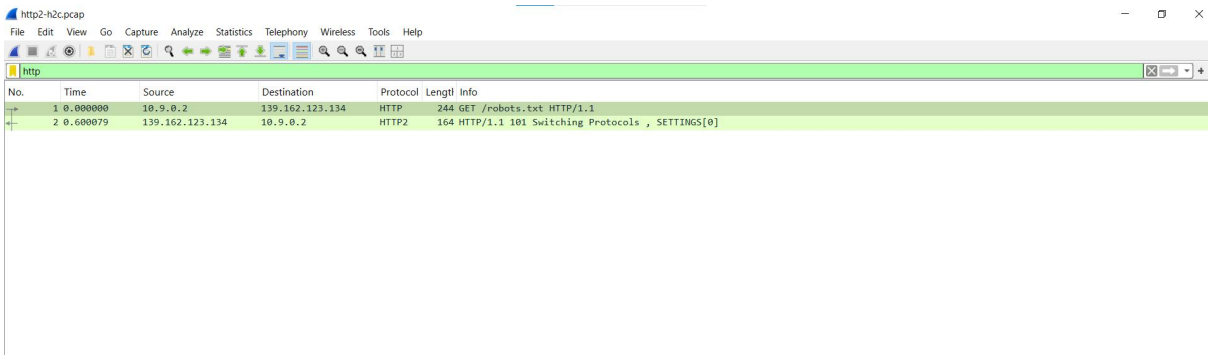
For 304

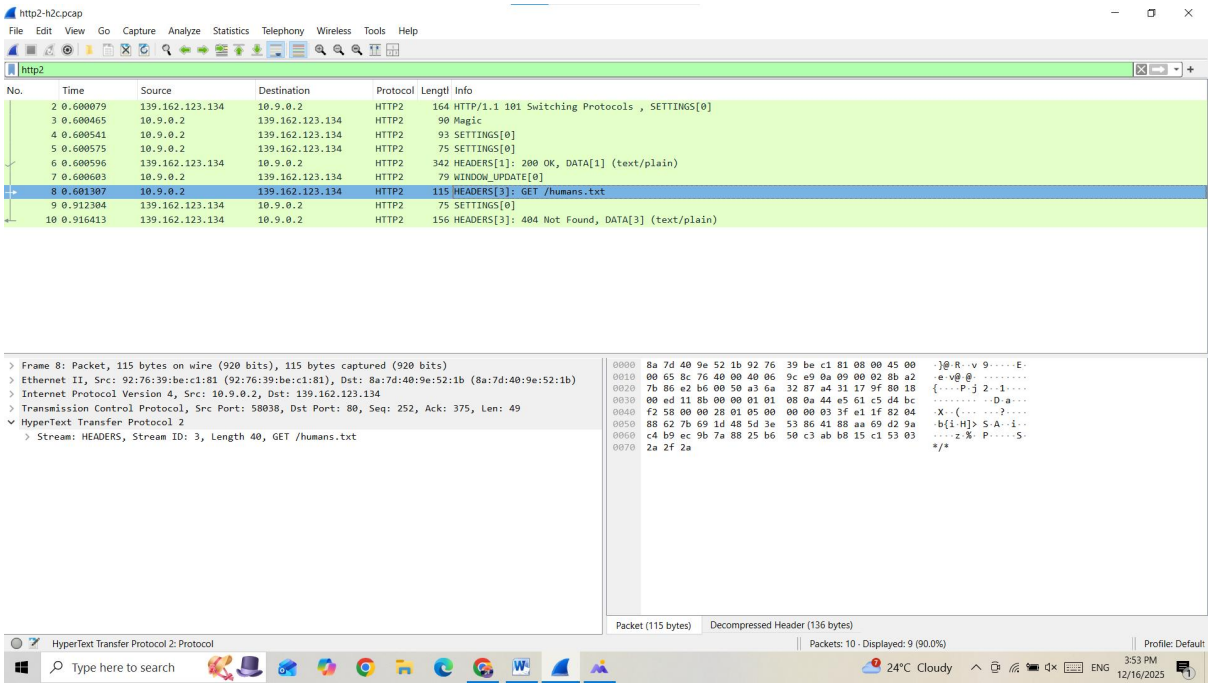
Last modified

Etag

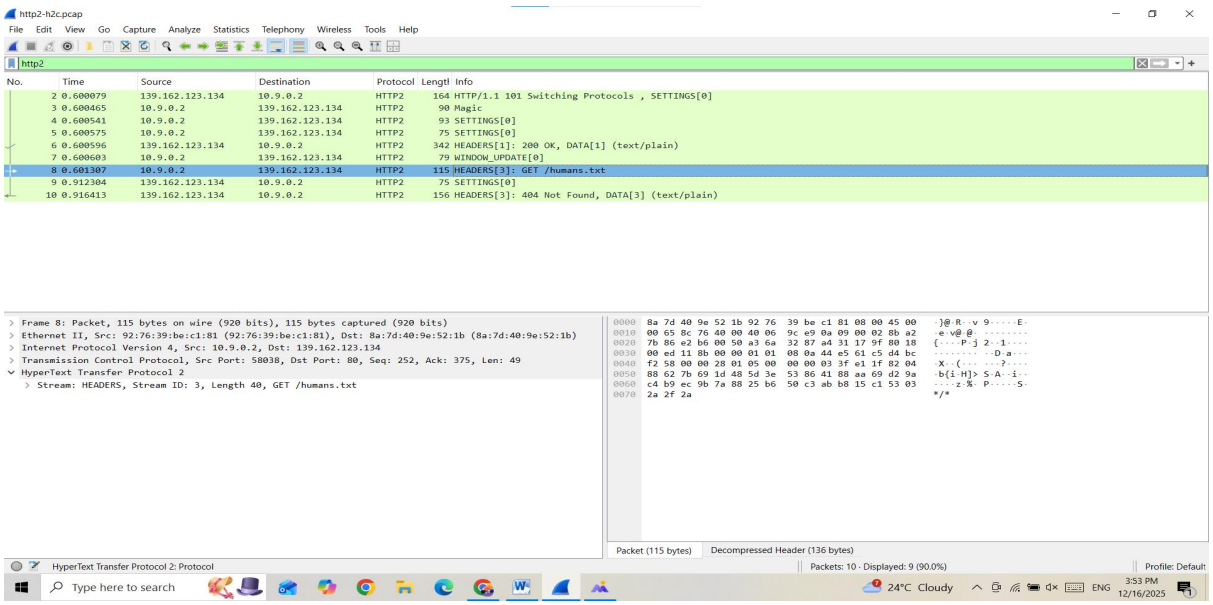
Task-3:

1. How many HTTP/2 and HTTP/1.1 packets are present?





2. How many HTTP/2 packets are exchanged between client and server here before the first object is fetched ?



3. What main difference do you observe in headers of HTTP/2 packets displayed here, compared to the headers of HTTP/1.1 packets ?