Assignment 2

GOVIND MORE

August 2024

1 HTTP

Q1)Total number of packets-39
Total number of GET REQUEST - 30
Total number of GET REQUEST for the text - 1
Total number of GET REQUEST for embedded content - 29

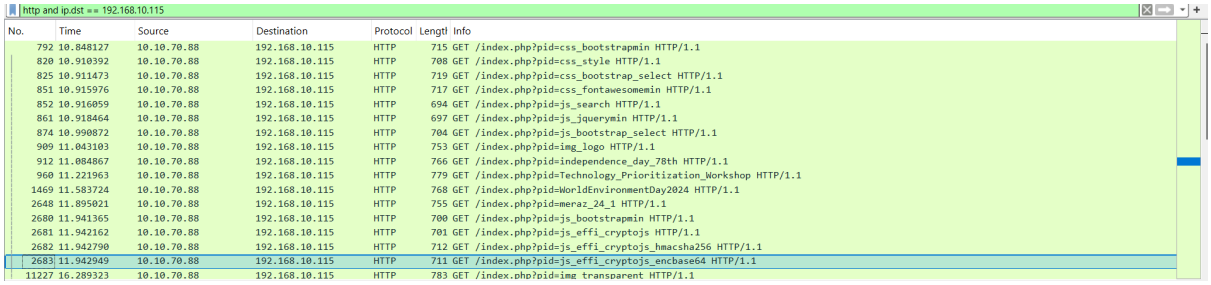


Figure 1: destination

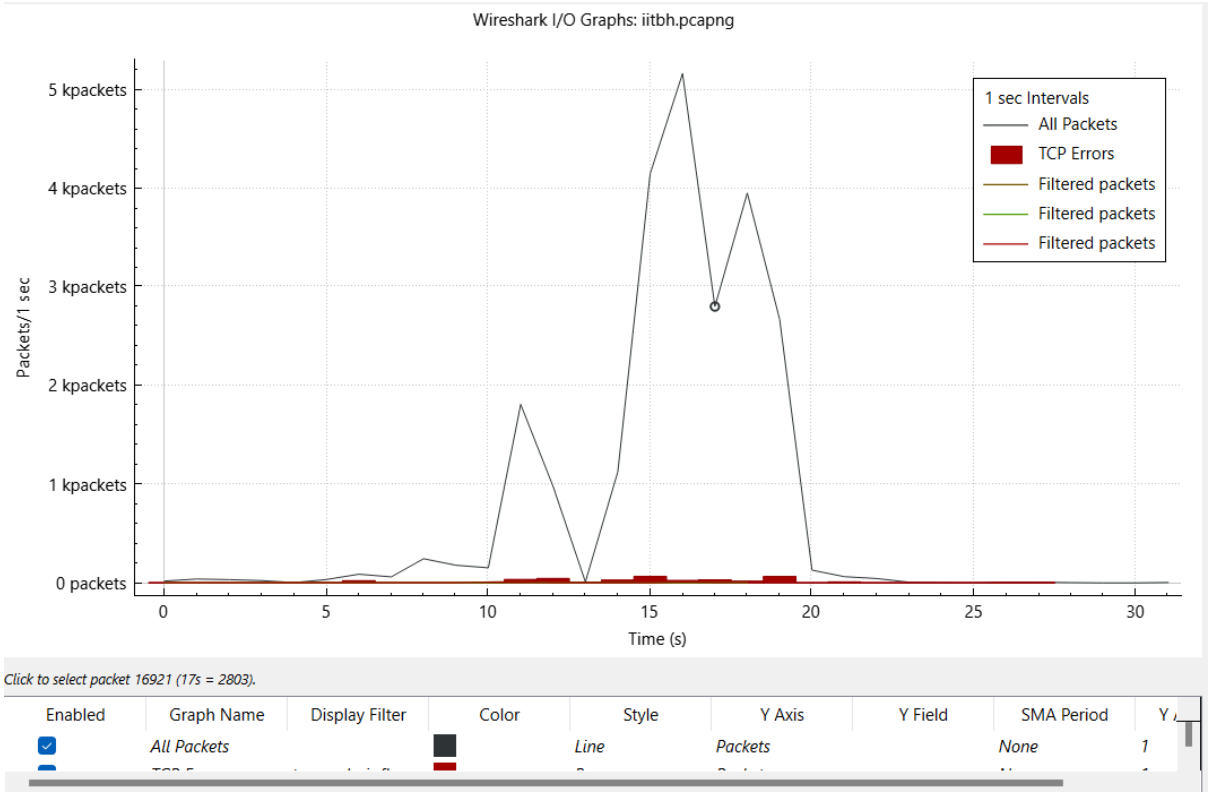


Figure 2: destination

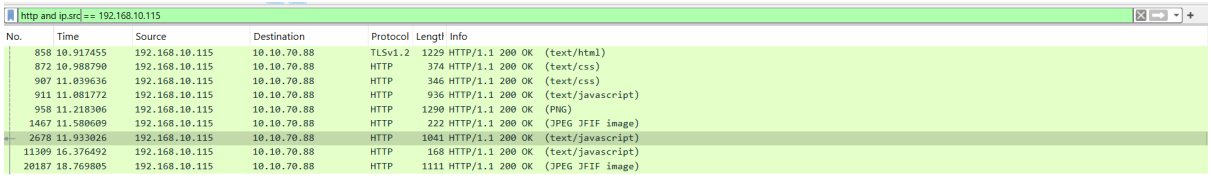


Figure 3: Source

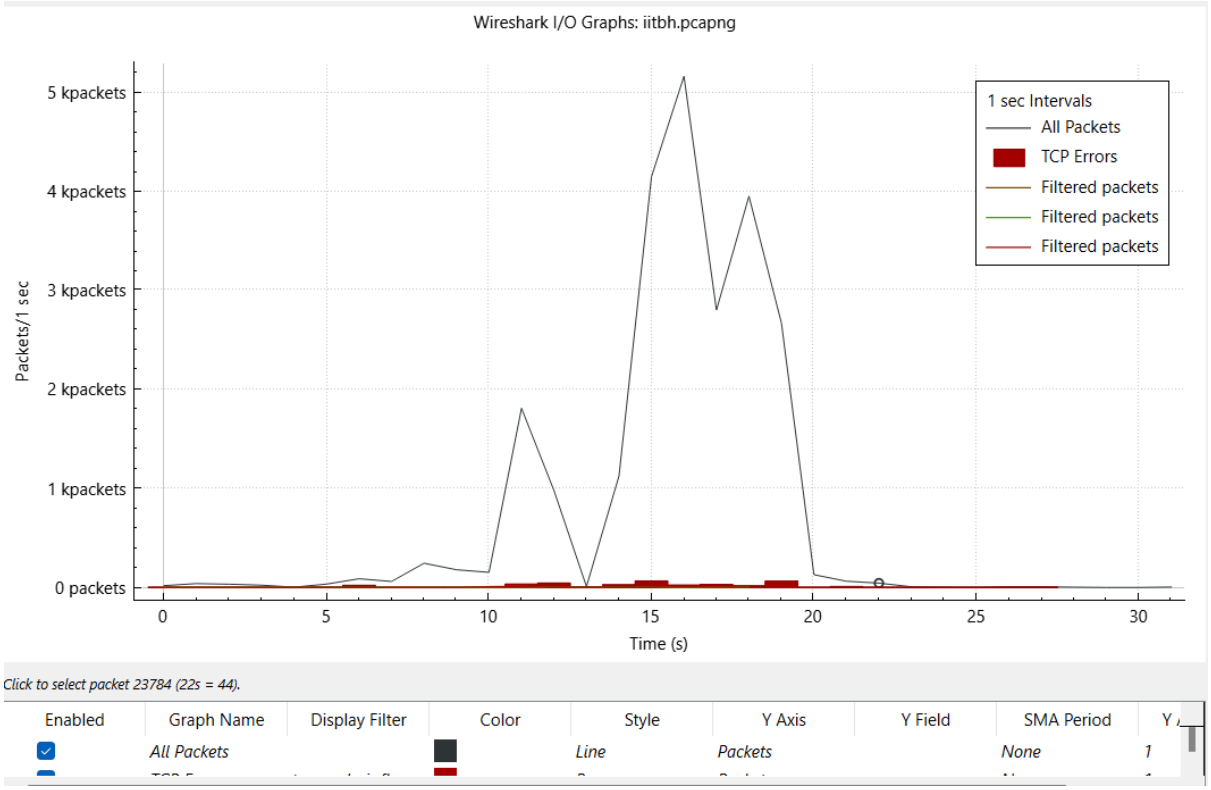


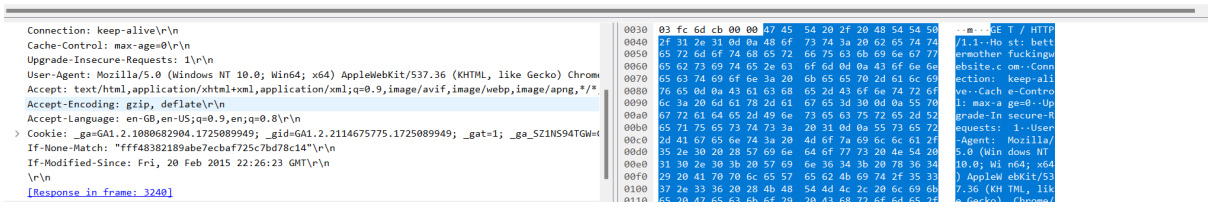
Figure 4: Source

Q2) HTTP GET /index.php?pid=css$_{b}ootstrapminHTTP/1.1 - 715
$HTTPGET/index.php?pid = css_{s}tyleHTTP/1.1 - 708$
$HTTPGET/index.php?pid = css_{b}ootstrap_{s}electHTTP/1.1 - 719$
$HTTPGET/index.php?pid = css_{f}ontawesomeminHTTP/1.1 - 717$
$HTTPGET/index.php?pid = js_{s}earchHTTP/1.1 - 694$
$HTTPGET/index.php?pid = js_{j}queryminHTTP/1.1 - 697$
$HTTPGET/index.php?pid = js_{b}ootstrap_{s}electHTTP/1.1 - 704$
$HTTPGET/index.php?pid = img_{l}ogoHTTP/1.1 - 753$
$HTTPGET/index.php?pid = independence_{d}ay_{7}8thHTTP/1.1 - 766$
$HTTPGET/index.php?pid = Technology_{P}rioritization_{W}orkshopHTTP/1.1 - 779$
$HTTPGET/index.php?pid = meraz_{2}4_{1}HTTP/1.1 - 755$
$HTTPGET/index.php?pid = WorldEnvironmentDay2024HTTP/1.1 - 768$
$HTTPGET/index.php?pid = js_{b}ootstrapminHTTP/1.1 - 700$
$Q3$)

Figure 6: hex to image

Q4.a)No,I didn't saw any "IF-MODIFIED-SINCE" in any HTTP GET.
Q4.b)Yes, the server giving the content explicitly as I can see "200 OK" in packets info.

o.	Time	Source	Destination	Protocol	Lengtl	Info
3214	5.463008	10.10.70.88	3.5.23.121	HTTP	607	GET /favicon.ico HTTP/1.1
3224	5.793699	3.5.23.121	10.10.70.88	HTTP	377	HTTP/1.1 403 Forbidden (text/html)
3239	7.733065	10.10.70.88	3.5.23.121	HTTP	775	GET / HTTP/1.1
3240	8.046296	3.5.23.121	10.10.70.88	HTTP	443	HTTP/1.1 304 Not Modified
3244	8.089307	10.10.70.88	3.5.23.121	HTTP	607	GET /favicon.ico HTTP/1.1
3256	8.353989	3.5.23.121	10.10.70.88	HTTP	377	HTTP/1.1 403 Forbidden (text/html)
3401	9.848383	10.10.70.88	3.5.23.121	HTTP	775	GET / HTTP/1.1
3421	10.108104	3.5.23.121	10.10.70.88	HTTP	443	HTTP/1.1 304 Not Modified
3430	10.158000	10.10.70.88	3.5.23.121	HTTP	607	GET /favicon.ico HTTP/1.1
3455	10.401377	3.5.23.121	10.10.70.88	HTTP	153	HTTP/1.1 403 Forbidden (text/html)
3919	11.510499	10.10.70.88	3.5.23.121	HTTP	775	GET / HTTP/1.1
4201	11.746547	3.5.23.121	10.10.70.88	HTTP	443	HTTP/1.1 304 Not Modified
4270	11.793104	10.10.70.88	3.5.23.121	HTTP	607	GET /favicon.ico HTTP/1.1
4656	12.035775	3.5.23.121	10.10.70.88	HTTP	377	HTTP/1.1 403 Forbidden (text/html)



```
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
Cookie: _ga=GA1.2.1080682904.1725089949; _gid=GA1.2.2114675775.1725089949; _gat=1; _ga_SZ1NS94TGW=
If-None-Match: "fff48382189abe7ecbaf725c7bd78c14"\r\n
If-Modified-Since: Fri, 20 Feb 2015 22:26:23 GMT\r\n
\r\n
[Response in frame: 3240]
```

```
0030  03 fc 6d cb 00 00 47 45  54 20 2f 20 48 54 54 50   ··m···GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 62 65 74 74   /1.1··Ho st: bett
0050  65 72 6d 6f 74 68 65 72  66 75 63 6b 69 6e 67 77   ermother fuckingw
0060  65 62 73 69 74 65 2e 63  6f 6d 0d 0a 43 6f 6e 6e   ebsite.c om··Conn
0070  65 63 74 69 6f 6e 3a 20  6b 65 65 70 2d 61 6c 69   ection:  keep-ali
0080  76 65 0d 0a 43 61 63 68  65 2d 43 6f 6e 74 72 6f   ve··Cach e-Contro
0090  6c 3a 20 6d 61 78 2d 61  67 65 3d 30 0d 0a 55 70   l: max-a ge=0··Up
00a0  67 72 61 64 65 2d 49 6e  73 65 63 75 72 65 2d 52   grade-In secure-R
00b0  65 71 75 65 73 74 73 3a  20 31 0d 0a 55 73 65 72   equests:  1··User
00c0  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
00d0  35 2e 30 20 28 57 69 6e  64 6f 77 73 20 4e 54 20   5.0 (Win dows NT
00e0  31 30 2e 30 3b 20 57 69  6e 36 34 3b 20 78 36 34   10.0; Wi n64; x64
00f0  29 20 41 70 70 6c 65 57  65 62 4b 69 74 2f 35 33   ) AppleW ebKit/53
0100  37 2e 33 36 20 28 4b 48  54 4d 4c 2c 20 6c 69 6b   7.36 (KH TML, lik
```

Figure 7: MODIFIED-SINCE

Q4.c)Yes, I saw this on wire shark during packet capture. "IF-MODIFIED-SINCE"- It defines the date and time.And the date represents the last time the resource was modified.And by this the server determines if the requested resource has changed since that time.
Q4.d)Here HTTP status code 304(Not modified) represents the requested resource has not been modified since the last time accessed.The server didn't returned the contents explicitly instead it informed the client that the cached version is still valid and can be used.
Q5)

5234	8.115343	10.10.70.88	192.168.10.115	TCP	66 60162 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
5235	8.119147	192.168.10.115	10.10.70.88	TCP	66 443 → 60162 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1250 SACK_PERM WS=128
5236	8.119219	10.10.70.88	192.168.10.115	TCP	54 60162 → 443 [ACK] Seq=1 Ack=1 Win=262400 Len=0
5237	8.119594	10.10.70.88	192.168.10.115	TLSv1.2	2055 Client Hello (SNI=www.iitbhilai.ac.in)
5238	8.121736	192.168.10.115	10.10.70.88	TCP	54 443 → 60162 [ACK] Seq=1 Ack=1251 Win=31744 Len=0
5239	8.121736	192.168.10.115	10.10.70.88	TCP	54 443 → 60162 [ACK] Seq=1 Ack=2002 Win=34304 Len=0
5240	8.124693	192.168.10.115	10.10.70.88	TLSv1.2	1304 Server Hello
5241	8.125371	192.168.10.115	10.10.70.88	TLSv1.2	900 Certificate, Server Key Exchange, Server Hello Done
5242	8.125406	10.10.70.88	192.168.10.115	TCP	54 60162 → 443 [ACK] Seq=2002 Ack=2097 Win=262400 Len=0
5243	8.126010	10.10.70.88	192.168.10.115	TLSv1.2	180 Client Key Exchange, Change Cipher Spec, Finished
5244	8.128260	192.168.10.115	10.10.70.88	TLSv1.2	328 New Session Ticket, Change Cipher Spec, Finished
5245	8.171127	10.10.70.88	192.168.10.115	TCP	54 60162 → 443 [ACK] Seq=2128 Ack=2371 Win=262144 Len=0
5268	8.363700	10.10.70.88	192.168.10.115	TCP	66 60165 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
5273	8.366387	192.168.10.115	10.10.70.88	TCP	66 443 → 60165 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1250 SACK_PERM WS=128
5274	8.366455	10.10.70.88	192.168.10.115	TCP	54 60165 → 443 [ACK] Seq=1 Ack=1 Win=262400 Len=0
5278	8.367519	10.10.70.88	192.168.10.115	TLSv1.2	1991 Client Hello (SNI=www.iitbhilai.ac.in)
5284	8.370664	192.168.10.115	10.10.70.88	TCP	54 443 → 60165 [ACK] Seq=1 Ack=1938 Win=33152 Len=0
5286	8.371303	192.168.10.115	10.10.70.88	TLSv1.2	191 Server Hello, Change Cipher Spec, Finished
5287	8.371727	10.10.70.88	192.168.10.115	TLSv1.2	105 Change Cipher Spec, Finished
5289	8.372634	10.10.70.88	192.168.10.115	HTTP	850 GET / HTTP/1.1
5298	8.413259	192.168.10.115	10.10.70.88	TCP	54 443 → 60165 [ACK] Seq=138 Ack=1989 Win=33152 Len=0
5299	8.414140	192.168.10.115	10.10.70.88	TCP	54 443 → 60162 [ACK] Seq=2371 Ack=2924 Win=36736 Len=0
5302	8.435645	192.168.10.115	10.10.70.88	TLSv1.2	1304 [TLS segment of a reassembled PDU]

The process begins at timestamp 8.115343 and concludes with the HTTP GET request at 8.372634. The time taken to establish the connection and send the GET request is approximately 0.257 seconds. The capture showing a singel TCP connection established between 10.10.70.88 and 192.168.10.115 on port 443 that indicates the use of HTTPS.

Ethernet · 1 | IPv4 · 1 | IPv6 | TCP · 1 | UDP

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A	Flows
10.10.70.88	57064	103.21.124.133	443	15	4 kB	12	15	100.00%	6	3 kB	9	1 kB	4.255759	0.3894	59 kbps	21 kbps	6

Figure 8: TCP

The connection is persistent as indicated by the use of TLS session tickets and the absence of connection terminators (FIN packets) before the HTTP GET request .The persistent connections allow multiple requests and responses over the same connection.
The capture isn't showing the number of objects transferred since it ends with GET request.
From the capture the first object took approximately 0.06445 seconds to download.
Q6)

Request

Pretty Raw Hex

```
GET /index.php?pid=js_bootstrap_select HTTP/1.1
Host: iitbhilai.ac.in
Cookie: PHPSESSID=7ou424281147plhnthtbebhf24
Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
Accept-Language: en-US
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://iitbhilai.ac.in/
Accept-Encoding: gzip, deflate, br
Priority: u=1
Connection: keep-alive
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Date: Sat, 31 Aug 2024 14:08:27 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16
X-Powered-By: PHP/5.4.16
Expires: 0
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check
Pragma: no-cache
Content-Disposition: inline; filename=61e7c83c5bc61.js
Content-Transfer-Encoding: binary
Content-Length: 31697
Keep-Alive: timeout=5, max=97
Connection: Keep-Alive
Content-Type: text/javascript

/*!
 * Bootstrap-select v1.10.0 (http://silviomoreto.github.io/bootstrap-select
 *
 * Copyright 2013-2016 bootstrap-select
 * Licensed under MIT (
https://github.com/silviomoreto/bootstrap-select/blob/master/LICENSE)
 */
!function(a,b){
  "function"==typeof define&&define.amd?define(["jquery"],function(a){
    return b(a)
```

Figure 9: BURP

GET /index.php?pid=$js_{b}ootstrap_{s}electHTTP/1.1 : $ $itisanHTTPGETrequestforaresourcelocatedat/index.php.$
$Host : iitbhilai.ac.in : Itisthedomainoftheserverthathasbeenrequested.$
$Cookie : PHPSESSID = 7ou424281147plhnthtbebhf24 : Containsasessionidentifierformaintainingauser'ssession.$
$Sec-Ch-Ua : \text{"}Chromium\text{"};v = \text{"}127\text{"}, \text{"}NotA;Brand\text{"};v = \text{"}99\text{"} : Providinginformationaboutthebrowseroftheuser.$
$Accept - Language : en - US : Indicatingthelanguagethatpreferredfortheresponse.$
$Sec - Ch - Ua - Mobile : ?0 : Itisindicatingthatiftheuserisusingmobileornot.$
$User-Agent : Mozilla/5.0(WindowsNT10.0;Win64;x64)AppleWebKit/537.36(KHTML,likeGecko)Chrome/127.0.6$

$Itis Providing the details about the user's browser and operating system.$
$Sec-Ch-Ua-Platform : \backslash Windows" : Itspecifieswhichplatformtheuserisusing.$
$Accept : / : Itsaysthatanytypeofcontentisacceptable.$
$Sec-Fetch-Site : same-origin : Indicatesthattherequestisforaresourcefromthesameorigin.$
$Sec-Fetch-Mode : no-cors : Itidentifiesthemodeoftherequest.$
$Sec-Fetch-Dest : script : Itindicatesthedestinationofthefetchedresource.$
$Referer : https : //iitbhilai.ac.in/ : Itistheurlthatmadetherequest.$
$Accept-Encoding : gzip, deflate, br : Liststheencodingformatsthatareacceptablefortheresponse.$
(1)$https : //github.com/flutter/flutter/issues/23465.https : //github.com/flutter/flutter/issues/23465.$
(2)$https : //turreta.com/blog/2018/02/16/log-unencrypted-soapfault-messages-in-apache-cxf.$
$https : //turreta.com/blog/2018/02/16/log-unencrypted-soapfault-messages-in-apache-cxf/.$
(3)$https : //sourceforge.net/p/grampc/discussion/general/thread/607aa6fb2a.$
$https : //sourceforge.net/p/grampc/discussion/general/thread/607aa6fb2a/.$
(4)$https : //github.com/Microsoft/vscode-python/issues/5081.https : //github.com/Microsoft/vscode-python/issues/5081.$
(5)$https : //github.com/microsoft/vscode-python/issues/11465.https : //github.com/microsoft/vscode-python/issues/11465.$
(6)$CS39006 : NetworksLabAssignment1 - IITKgp.$
$https : //cse.iitkgp.ac.in/ sandipc/courses/cs39006/notes/CS39006_Assignment_{12}021.pdf.$
(7)$3.8.8Lab - ExploreDNSTraffic(Answers) - ITExamAnswers.https : //itexamanswers.net/3-8-8-lab-explore-dns-traffic-answers.html.$
(8)$HowDoesDNSResolveDomainNamestoIPAddresses?.https : //www.geeksforgeeks.org/how-does-dns-resolve-domain-names-to-ip-addresses/.$
(9)$undefined.https : //www.cornell.edu/.$
(10)$undefined.https : //www.cornell.edu.$
(11)$DNSAnalysisUsingWireshark.https : //www.networkcomputing.com/backbone-networking/dns-analysis-using-wireshark.$
(12)$HowtoUseWireshark : ComprehensiveTutorial+Tips-Varonis.https : //www.varonis.com/blog/how-to-use-wireshark.$
(13)$PacketCapture(PCAP)Analysis - DNSstuff.https : //www.dnsstuff.com/pcap-analysis.$
(14)$BasicPacketAnalysisUsingWireshark0xElshazly|MohamedAyman....$
$https : //0xelshazly.github.io/tools/wireshark/packet-analysis-using-wireshark/.$
(15)$undefined.https : //tryhackme.com/$

2 DNS

Q1.a)

```
DNS        90 Standard query 0xc802 A edge.microsoft.com
DNS        90 Standard query 0xccc0 HTTPS edge.microsoft.com
DNS       210 Standard query response 0xccc0 HTTPS edge.microsoft.com CNAME edge-microsoft-com.dual-a-0036.a-msedge.net CNAME dual-a-0036.a-m…
DNS       904 Standard query response 0xc802 A edge.microsoft.com CNAME edge-microsoft-com.dual-a-0036.a-msedge.net CNAME dual-a-0036.a-msedg…
DNS        88 Standard query 0x91c3 HTTPS web.whatsapp.com
DNS        88 Standard query 0x4cb8 A web.whatsapp.com
DNS       172 Standard query response 0x91c3 HTTPS web.whatsapp.com CNAME mmx-ds.cdn.whatsapp.net SOA a.ns.whatsapp.net
DNS       852 Standard query response 0x4cb8 A web.whatsapp.com CNAME mmx-ds.cdn.whatsapp.net A 163.70.144.60 NS h.gtld-servers.net NS b.gtld…
DNS        89 Standard query 0x387c A fonts.gstatic.com
DNS        87 Standard query 0x5e49 HTTPS www.gstatic.com
DNS        87 Standard query 0x6fed A www.gstatic.com
DNS        89 Standard query 0x5242 HTTPS fonts.gstatic.com
DNS       362 Standard query response 0x387c A fonts.gstatic.com A 142.250.183.195 NS ns2.google.com NS ns3.google.com NS ns1.google.com NS n…
DNS       146 Standard query response 0x5e49 HTTPS www.gstatic.com SOA ns1.google.com
DNS       148 Standard query response 0x5242 HTTPS fonts.gstatic.com SOA ns1.google.com
DNS       360 Standard query response 0x6fed A www.gstatic.com A 142.250.67.195 NS ns4.google.com NS ns1.google.com NS ns3.google.com NS ns2.…
DNS        86 Standard query 0x3fd6 HTTPS lh3.google.com
DNS        86 Standard query 0xff75 A lh3.google.com
DNS       372 Standard query response 0xff75 A lh3.google.com CNAME lh2.l.google.com A 142.250.71.110 NS ns4.google.com NS ns2.google.com NS …
DNS        96 Standard query 0x2127 A www.googleadservices.com
DNS        96 Standard query 0x6f24 HTTPS www.googleadservices.com
DNS       369 Standard query response 0x2127 A www.googleadservices.com A 142.250.76.194 NS ns2.google.com NS ns3.google.com NS ns1.google.co…
DNS       378 Standard query response 0x6f24 HTTPS www.googleadservices.com HTTPS NS ns4.google.com NS ns2.google.com NS ns3.google.com NS ns…
DNS       158 Standard query response 0x3fd6 HTTPS lh3.google.com CNAME lh2.l.google.com SOA ns1.google.com
```

Figure 10: DNS

Domain Name	IP Address
edge.microsoft.com	13.107.42.16
web.whatsapp.com	163.70.144.60
fonts.gstatic.com	142.250.183.195
www.gstatic.com	142.250.67.195
1h3.google.com	142.250.71.110
www.googleadservices.com	142.250.76.194

Table 1: Domain Name and IP Address Table

Q1.b)

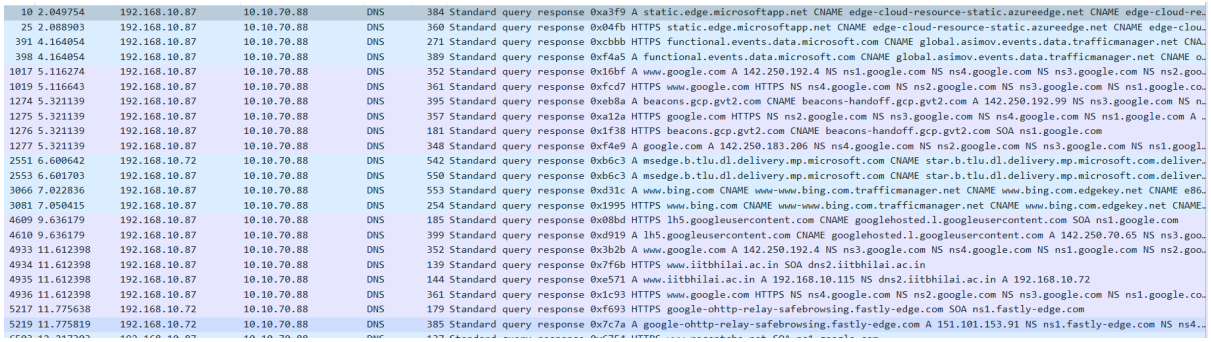


Figure 11: Source and destination

192.168.10.87 and 192.168.10.72 are the ip addresses of the sources and 10.10.70.88 is the ip address of the Destination.

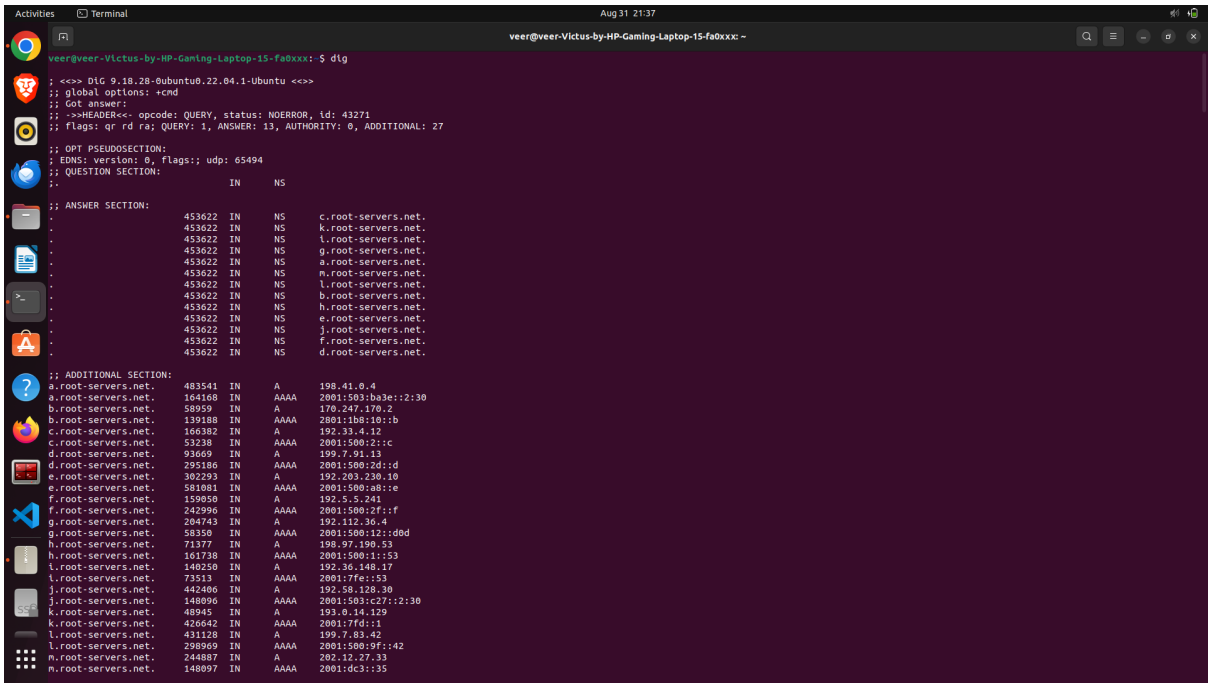


Figure 12: Enter Caption

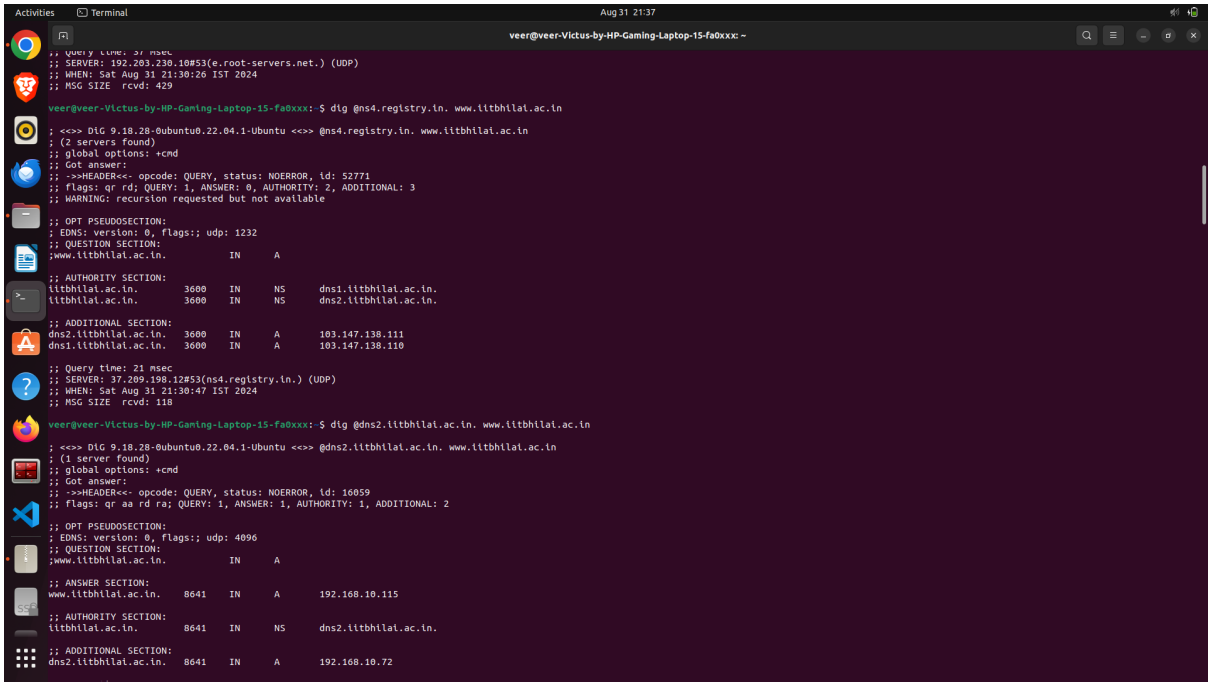


Figure 13: Enter Caption

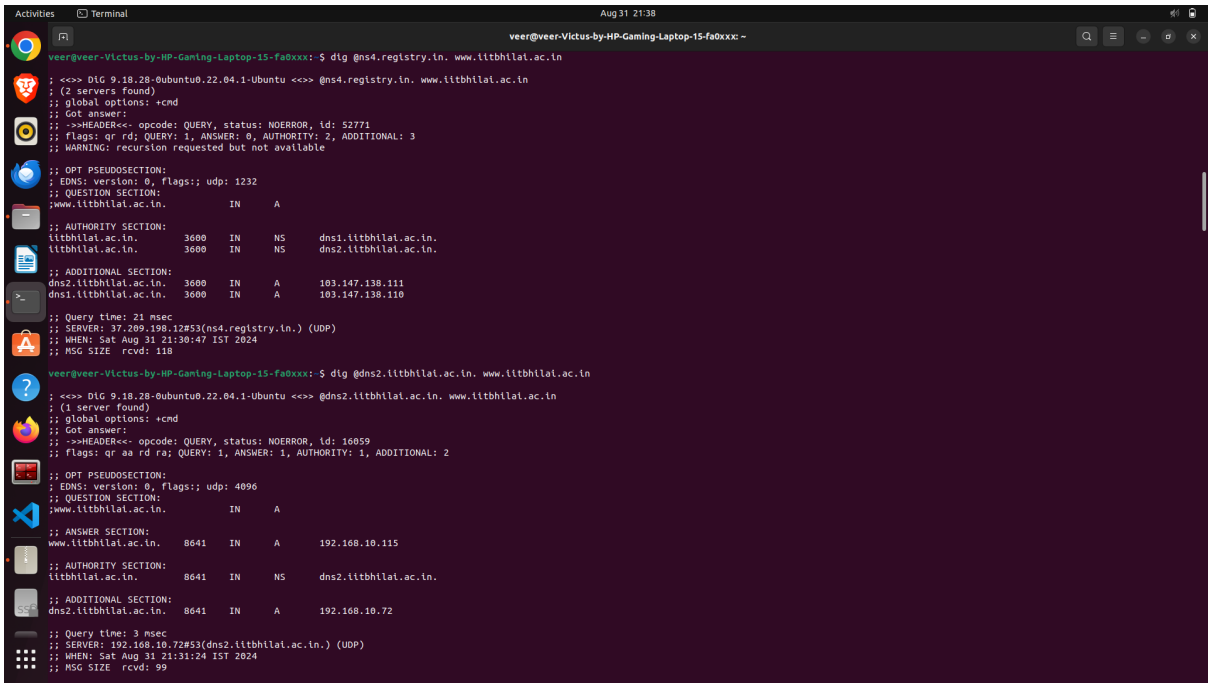


Figure 14: Enter Caption

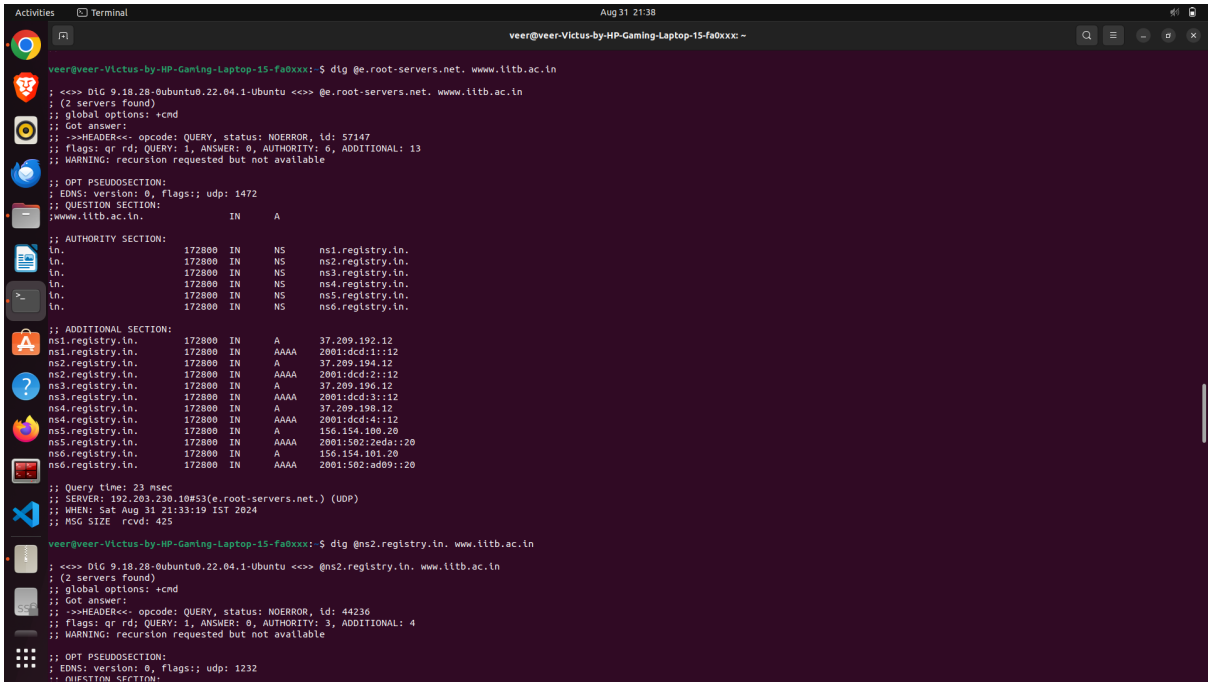


Figure 15: Enter Caption

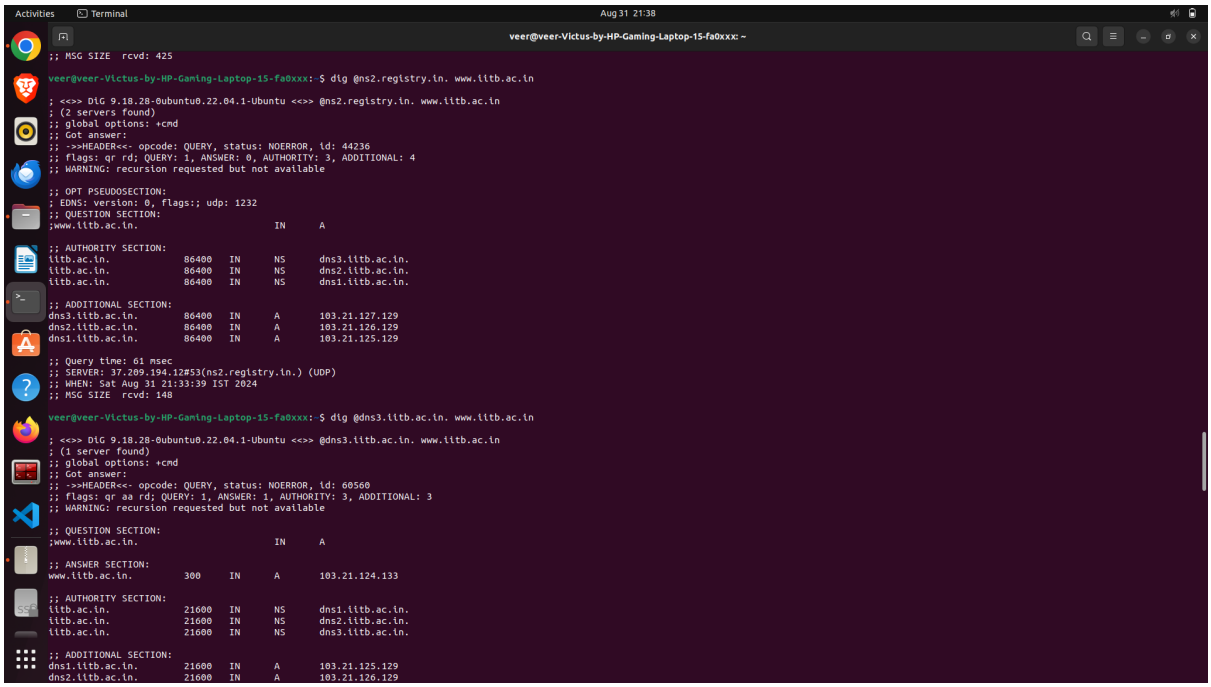


Figure 16: Enter Caption

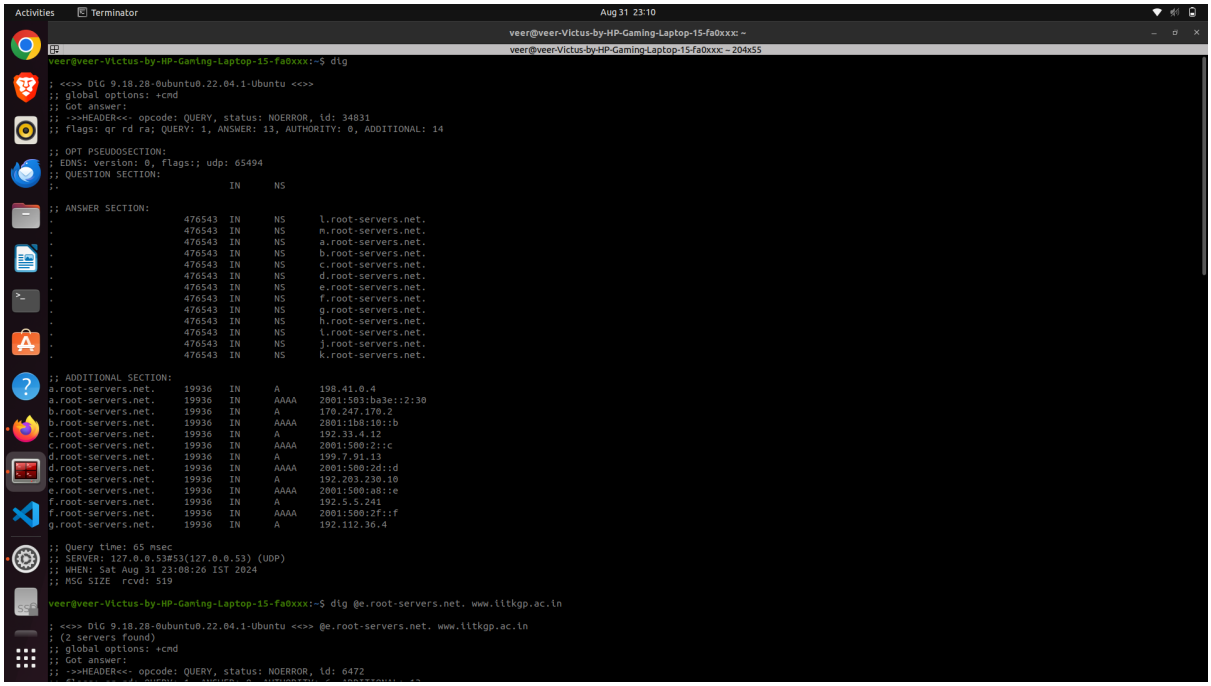


Figure 17: Enter Caption

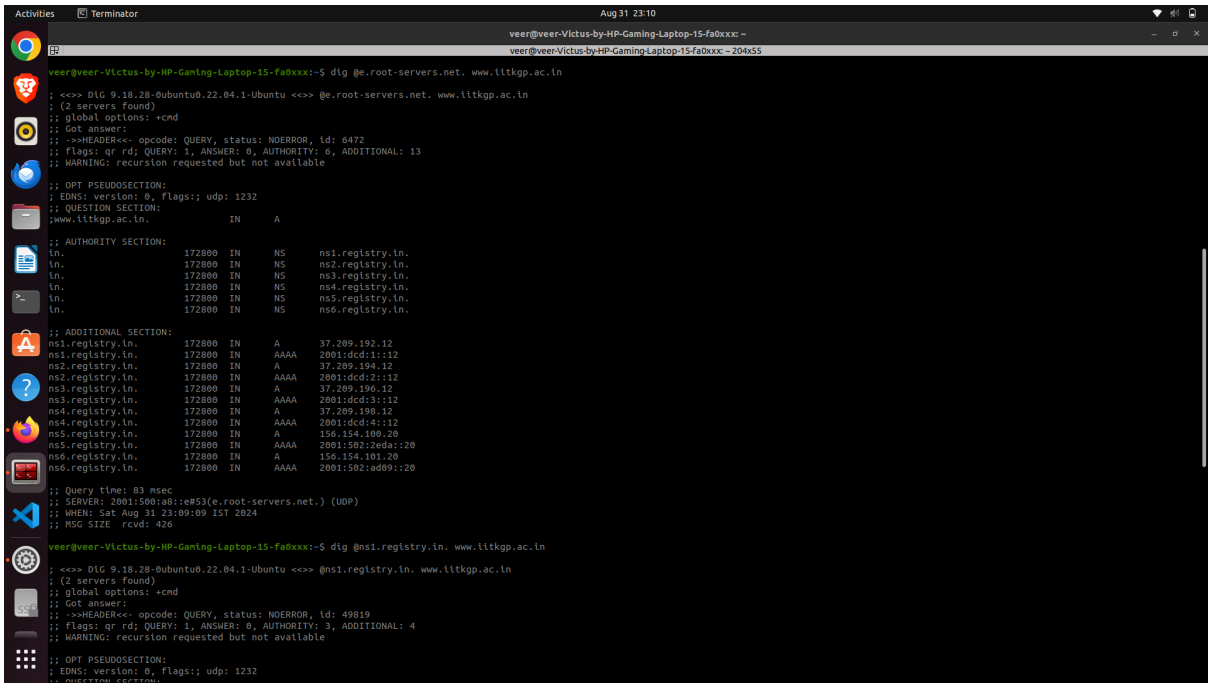


Figure 18: Enter Caption

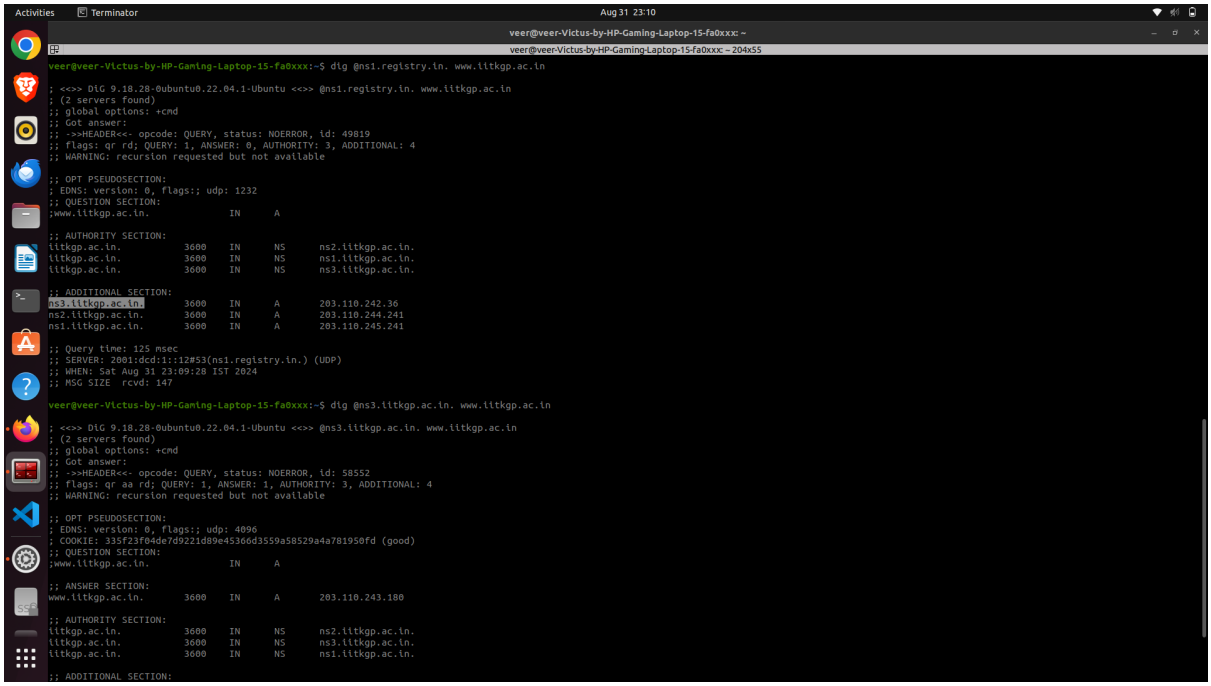


Figure 19: Enter Caption

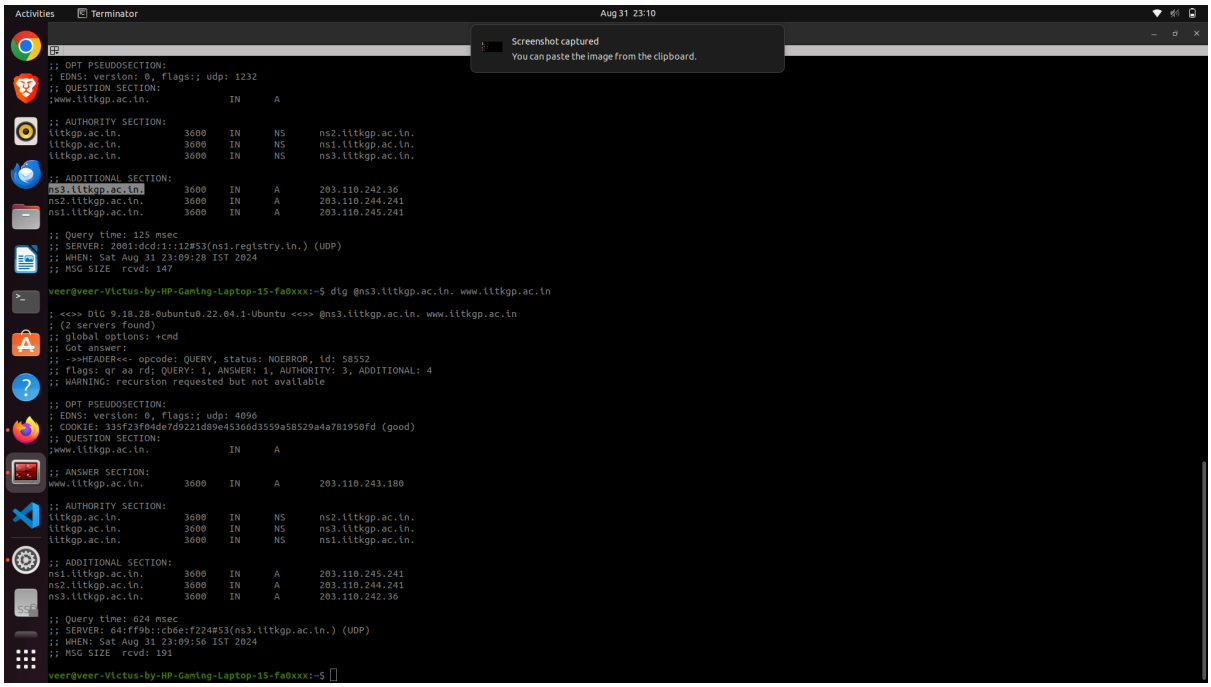


Figure 20: Enter Caption