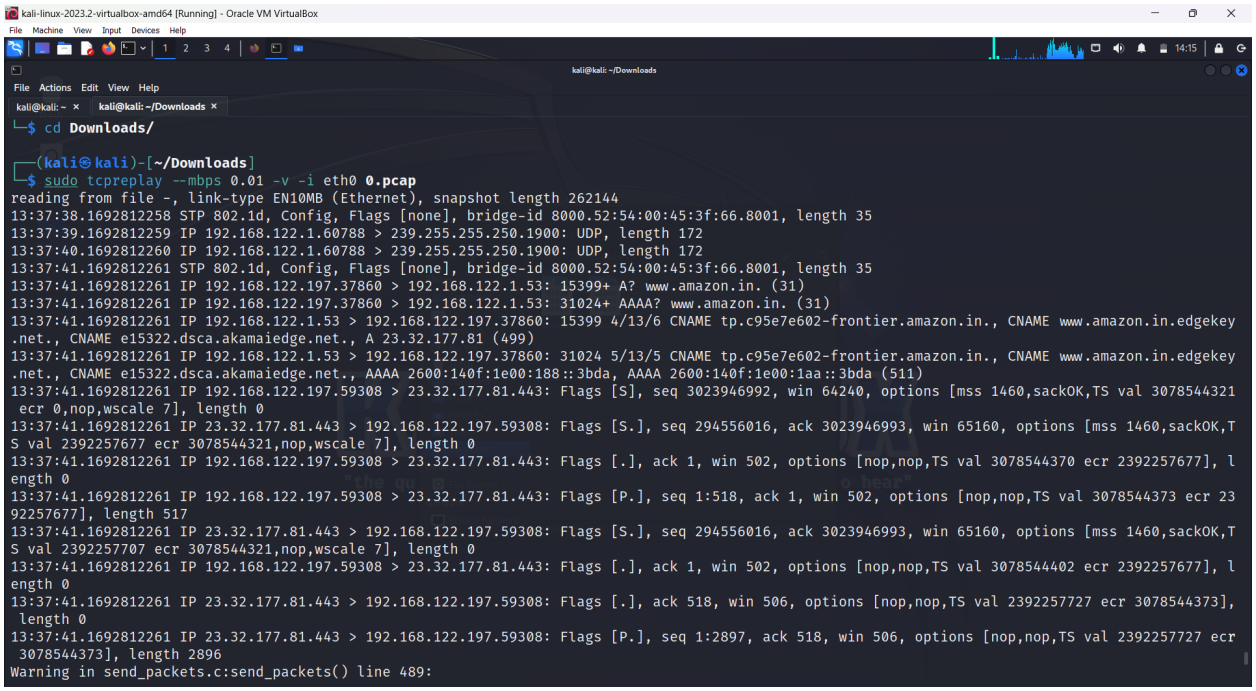
Shubh Singhal 21110206

Pratham Sagar 21110165

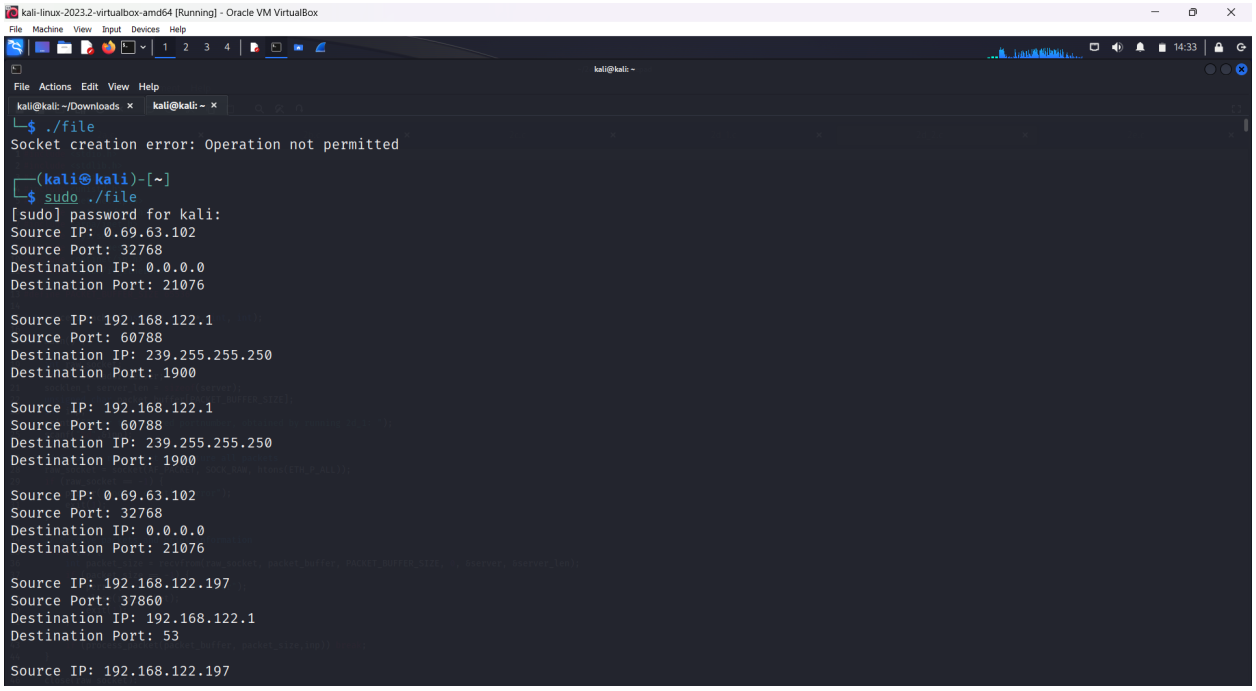
Part -1

a.total=15378

tcpreplay:



Captured packets:



b.

i. nslookup 52.16.32.113

113.32.16.52.in-addr.arpa name = ec2-52-16-32-113.eu-west-1.compute.amazonaws.com.

Authoritative answers can be found from:

. nameserver = d.root-servers.net.
. nameserver = h.root-servers.net.
. nameserver = f.root-servers.net.
. nameserver = c.root-servers.net.
. nameserver = e.root-servers.net.
. nameserver = b.root-servers.net.
. nameserver = m.root-servers.net.
. nameserver = a.root-servers.net.
. nameserver = k.root-servers.net.
. nameserver = l.root-servers.net.
. nameserver = g.root-servers.net.
. nameserver = i.root-servers.net.
. nameserver = j.root-servers.net.

h.root-servers.net internet address = 198.97.190.53
h.root-servers.net has AAAA address 2001:500:1::53
i.root-servers.net internet address = 192.36.148.17
i.root-servers.net has AAAA address 2001:7fe::53
j.root-servers.net internet address = 192.58.128.30
j.root-servers.net has AAAA address 2001:503:c27::2:30
k.root-servers.net internet address = 193.0.14.129

k.root-servers.net has AAAA address 2001:7fd::1
l.root-servers.net internet address = 199.7.83.42

iii. nslookup 142.250.183.195
195.183.250.142.in-addr.arpa name = bom07s33-in-f3.1e100.net.

Authoritative answers can be found from:
. nameserver = c.root-servers.net.
. nameserver = g.root-servers.net.
. nameserver = d.root-servers.net.
. nameserver = h.root-servers.net.
. nameserver = a.root-servers.net.
. nameserver = f.root-servers.net.
. nameserver = k.root-servers.net.
. nameserver = j.root-servers.net.
. nameserver = i.root-servers.net.
. nameserver = b.root-servers.net.
. nameserver = e.root-servers.net.
. nameserver = m.root-servers.net.
. nameserver = l.root-servers.net.
h.root-servers.net internet address = 198.97.190.53
h.root-servers.net has AAAA address 2001:500:1::53
i.root-servers.net internet address = 192.36.148.17
i.root-servers.net has AAAA address 2001:7fe::53
j.root-servers.net internet address = 192.58.128.30
j.root-servers.net has AAAA address 2001:503:c27::2:30
k.root-servers.net internet address = 193.0.14.129
k.root-servers.net has AAAA address 2001:7fd::1
l.root-servers.net internet address = 199.7.83.42
l.root-servers.net has AAAA address 2001:500:9f::42

Iii. nslookup 67.220.224.105
** server can't find 105.224.220.67.in-addr.arpa: NXDOMAIN
Iv. nslookup 192.58.128.30
30.128.58.192.in-addr.arpa name = j.root-servers.net.

Authoritative answers can be found from:
. nameserver = c.root-servers.net.
. nameserver = b.root-servers.net.
. nameserver = i.root-servers.net.
. nameserver = l.root-servers.net.
. nameserver = d.root-servers.net.
. nameserver = k.root-servers.net.
. nameserver = f.root-servers.net.

.	nameserver = h.root-servers.net.
.	nameserver = m.root-servers.net.
.	nameserver = j.root-servers.net.
.	nameserver = a.root-servers.net.
.	nameserver = g.root-servers.net.
.	nameserver = e.root-servers.net.
h.root-servers.net	internet address = 198.97.190.53
h.root-servers.net	has AAAA address 2001:500:1::53
i.root-servers.net	internet address = 192.36.148.17
i.root-servers.net	has AAAA address 2001:7fe::53
j.root-servers.net	internet address = 192.58.128.30
j.root-servers.net	has AAAA address 2001:503:c27::2:30
k.root-servers.net	internet address = 193.0.14.129
k.root-servers.net	has AAAA address 2001:7fd::1
l.root-servers.net	internet address = 199.7.83.42
l.root-servers.net	has AAAA address 2001:500:9f::42
m.root-servers.net	internet address = 202.12.27.33

v.nslookup 202.12.27.33

33.27.12.202.in-addr.arpa	name = m.root-servers.net.

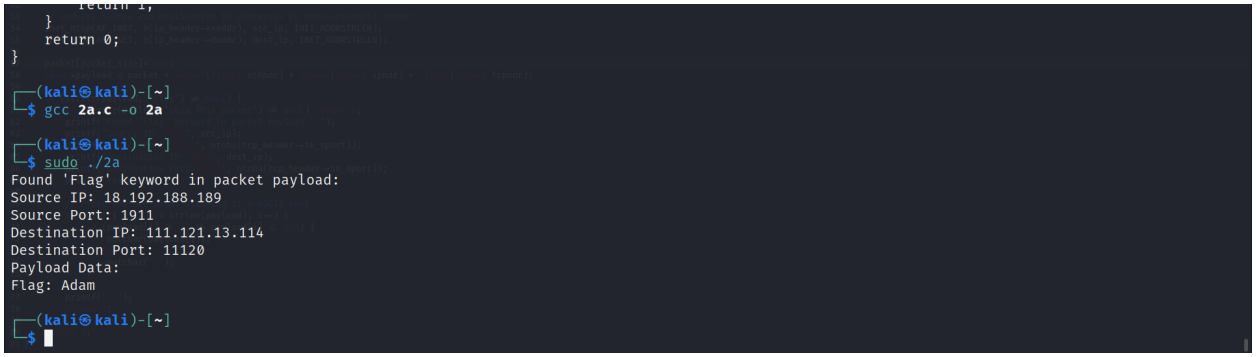
Authoritative answers can be found from:
.	nameserver = i.root-servers.net.
.	nameserver = h.root-servers.net.
.	nameserver = a.root-servers.net.
.	nameserver = d.root-servers.net.
.	nameserver = e.root-servers.net.
.	nameserver = m.root-servers.net.
.	nameserver = l.root-servers.net.
.	nameserver = f.root-servers.net.
.	nameserver = c.root-servers.net.
.	nameserver = k.root-servers.net.
.	nameserver = j.root-servers.net.
.	nameserver = b.root-servers.net.
.	nameserver = g.root-servers.net.
h.root-servers.net	internet address = 198.97.190.53
h.root-servers.net	has AAAA address 2001:500:1::53
i.root-servers.net	internet address = 192.36.148.17
i.root-servers.net	has AAAA address 2001:7fe::53
j.root-servers.net	internet address = 192.58.128.30
j.root-servers.net	has AAAA address 2001:503:c27::2:30
k.root-servers.net	internet address = 193.0.14.129
k.root-servers.net	has AAAA address 2001:7fd::1

l.root-servers.net internet address = 199.7.83.42
l.root-servers.net has AAAA address 2001:500:9f::42
m.root-servers.net internet address = 202.12.27.33

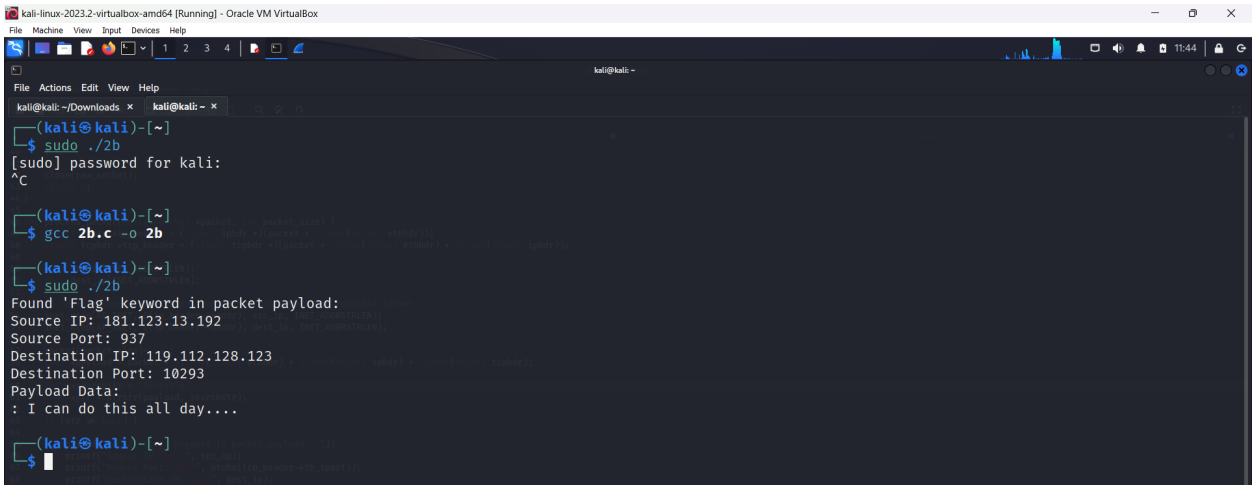
Part -2

ANS :-

1. Adam



2. I can do this all day



3. Your password is somewhere in this stream.

```
┌──(kali㉿kali)-[~]
└─$ gcc 2c.c -o 2c

┌──(kali㉿kali)-[~]
└─$ sudo ./2c
TCP Checksum: 0×46a4
Found 'Flag' keyword in packet
Source IP: 118.142.111.129
Source Port: 9291
Destination IP: 138.123.111.130
Destination Port: 1303
Payload Data:
GET /your-password-is-somewhere--in-this-stream HTTP/1.1....

┌──(kali㉿kali)-[~]
└─$
```

4. Sum of ports = 60237. It leads to John Keats

```
┌──(kali㉿kali)-[~]
└─$ sudo ./2d_1
Source IP: 131.144.126.118
Source Port: 121
Destination IP: 11.124.156.78
Destination Port: 60116
Payload Data:
Enter the number: 60237, as input for file 2d_2

┌──(kali㉿kali)-[~]
└─$ sudo ./2d_2
Enter the desired portnumber, obtained by running 2d_1: 60237
TCP Checksum: 0×fa89
Found 'Flag' keyword in packet
Source IP: 123.118.56.78
Source Port: 60237
Destination IP: 11.128.128.78
Destination Port: 443
Payload Data:
The person you are looking for is John Keats

┌──(kali㉿kali)-[~]
└─$
```

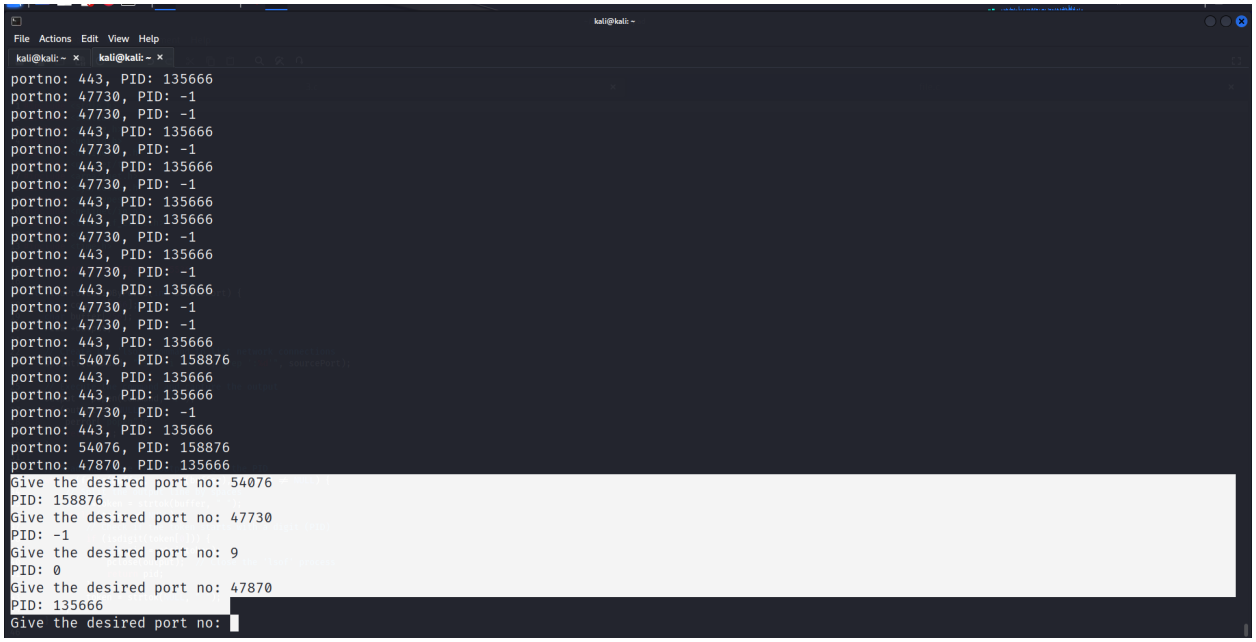
5. Pineapple

```
┌──(kali㉿kali)-[~]
└─$ gcc 2e.c -o 2e

┌──(kali㉿kali)-[~]
└─$ sudo ./2e
Found 'Flag' keyword in packet payload:
Source IP: 127.0.0.1
Source Port: 121
Destination IP: 198.33.76.78
Destination Port: 60116
Payload Data:
Pineapple
Cookie:

┌──(kali㉿kali)-[~]
└─$
```

Part -3



Part -4

1.

A.

I. SNMP: SNMP stands for Simple Network Management Protocol.

Application Layer (Layer 7) is the top operational layer.

SNMP is used to manage and keep an eye on network equipment like switches and routers. It enables retrieval and modification of device configuration and status data for network administrators. SNMPv2 and SNMPv3 are both described in RFC 1901 and RFC 3410, respectively.

B. BGP : BGP stands for Border Gateway protocol
Network Layer (Layer 3) is the top operational layer.

BGP is a routing protocol that allows autonomous systems (ASes) on the internet to communicate reachability and routing data. It is essential for the internet's primary routing architecture. Described in RFC 4271 is BGP-4.

C. ICMP : ICMP stands for Internet Control Message Protocol

Network layer protocol

Devices employ the network protocol ICMP to alert users of connection problems and faults. Devices may get a warning from ICMP that a forwarded message was too lengthy or arrived out of order and will be asked to resubmit the information.

RFC 792.

D.NTP: Network Time Protocol
Application Layer Protocol.
NTP offers the protocol mechanisms necessary to synchronise time in theory with precisions on the order of nanoseconds while maintaining a clear date, at least for the twenty-first century. The protocol has clauses that indicate the local clock's accuracy, estimated error, and the parameters of the reference clock to which it may be synchronised.
RFC 958

E. PPP: Point-to-Point Protocol
Data Link Layer Protocol
A common mechanism for moving multi-protocol datagrams across point-to-point lines is the Point-to-Point Protocol (PPP). PPP is made up of three primary parts:

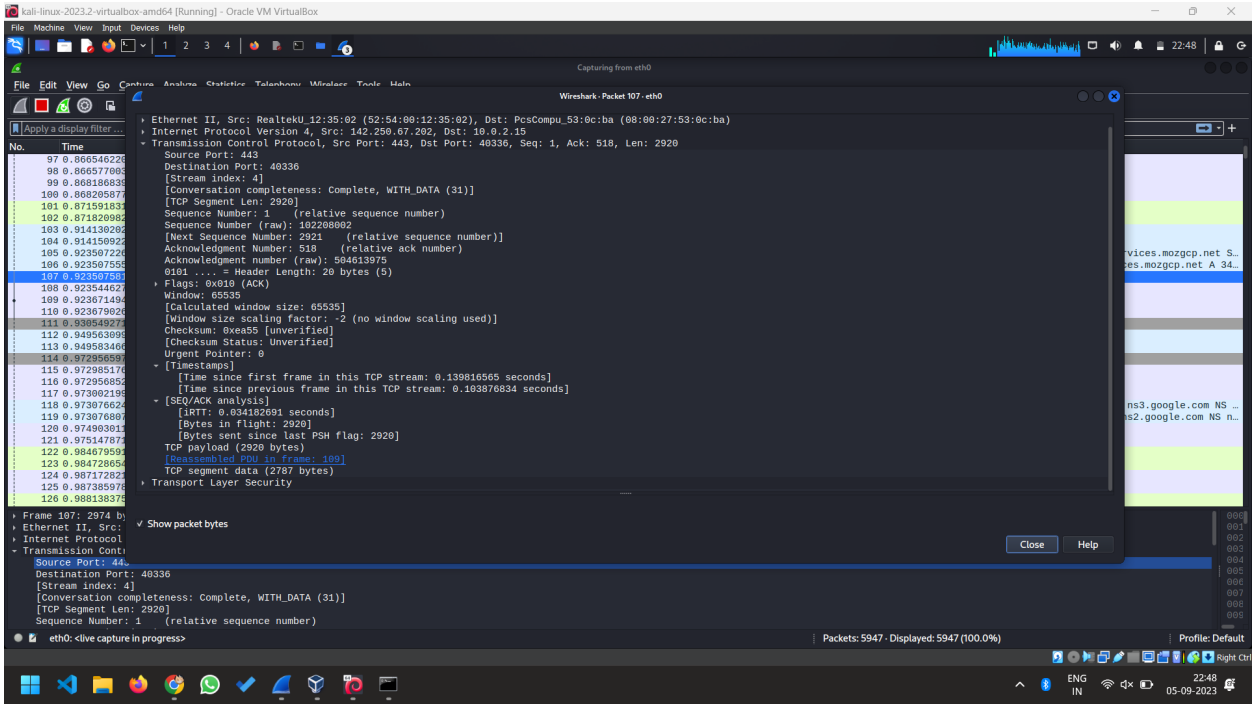
1. A technique for encapsulating datagrams with many protocols.
2. The Link Control Protocol (LCP), which is used to set up, configure, and test the data-link connection.
3. A group of Network Control Protocols (NCPs) used to set up and customise various network-layer protocols.

RFC 1661

REFERENCES:
[A, B, C]: Keary, T. (2023) *9 types of network protocols & when to use them*, *Forbes*. Available at: https://www.forbes.com/advisor/business/types-network-protocols/ (Accessed: 06 September 2023).

[D]: MILLS, D.L. (1985) *RFC 958: Network Time Protocol (NTP)*, *IETF Datatracker*. Available at: https://datatracker.ietf.org/doc/html/rfc958 (Accessed: 06 September 2023).

[E]: Simpson, W.A. (1994) *RFC 1661: The point-to-point protocol (PPP)*, *IETF Datatracker*. Available at: https://datatracker.ietf.org/doc/html/rfc1661 (Accessed: 06 September 2023).



RTT = 0.034182691 seconds

2. Identify the application layer protocols and their versions used when visiting the following websites:

Github.com HTTP/2

Netflix.com HTTP/2

Google.com HTTP/3

Explain in a few lines the differences and similarities between the protocols. (2 points)

(HTTP2) HTTP/2:

Multiple requests and answers may now be sent and received concurrently over a single connection thanks to HTTP/2's introduction of multiplexing. Performance is enhanced and latency is decreased.

It employs binary framing, which makes parsing easier and increases the protocol's effectiveness for machines.

Header compression is a feature of HTTP/2 that reduces costs by compressing headers prior to delivery.

HTTP/3:

Transport Protocol: The QUIC transport protocol, which aims to decrease latency and increase security, is built on top of HTTP/3. Instead than using TCP, it uses UDP.

Parallel data transfers can be made possible through multiplexing, which is a feature of HTTP/3

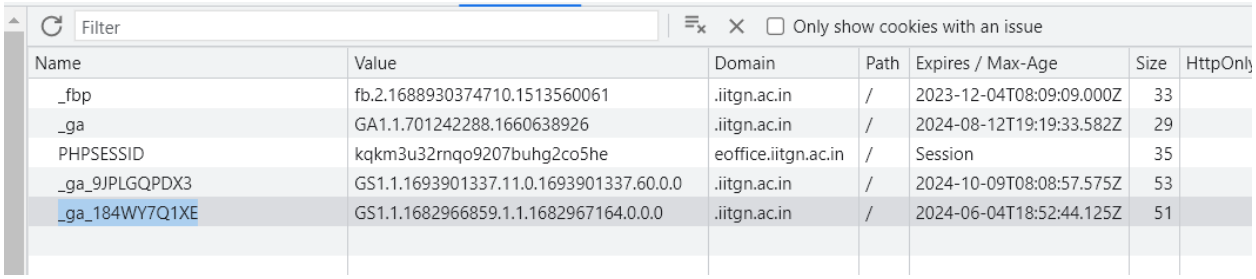
that is similar to HTTP/2's support for it.

HTTP/3's mandatory encryption requirement improves security. TLS 1.3 is used for encryption.

Header Compression: Compared to HTTP/2, HTTP/3 uses a new header compression method called QPACK that is more effective.

Reduced Head-of-Line Blocking: HTTP/3 is made to make head-of-line blocking problems less of a problem, thus enhancing speed.

3. The cookies found on the page *eoffice.iitgn.ac.in* are:



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly
_fbp	fb.2.1688930374710.1513560061	.iitgn.ac.in	/	2023-12-04T08:09:09.000Z	33	
_ga	GA1.1.701242288.1660638926	.iitgn.ac.in	/	2024-08-12T19:19:33.582Z	29	
PHPSESSID	kqkm3u32rnqo9207buhg2co5he	eoffice.iitgn.ac.in	/	Session	35	
_ga_9JPLGQPDX3	GS1.1.1693901337.11.0.1693901337.60.0.0	.iitgn.ac.in	/	2024-10-09T08:08:57.575Z	53	
_ga_184WY7Q1XE	GS1.1.1682966859.1.1.1682967164.0.0.0	.iitgn.ac.in	/	2024-06-04T18:52:44.125Z	51	

a) _fbp cookie is a cookie associated with facebook pixel and used to track and optimize various advertising campaigns
b) _ga is associated with google analytics. These usually last 2 years and used to distinguish users on a website, store clientIDs and timestamps.
c) PHPSESSID used in PHP-based web applications to maintain user's session information and essential for maintaining stateful interactions.
d) and e) both are some more specific cookies for google analytics.