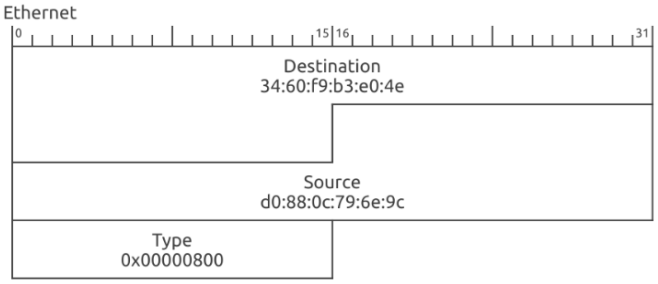
CS588 : Computer System Lab
(January - May 2023)
Assignment – 2 : Network Protocol Analysis Using Wireshark
Group 18 : MS Teams

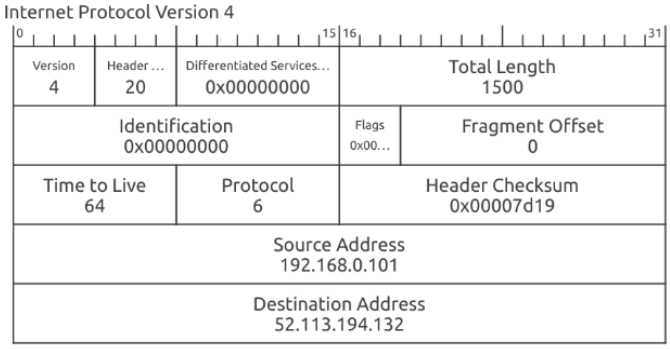
1. **List out all the protocols used by the application at different layers (only those which you can figure out from traces).Study and briefly describe their packet formats.**

   Protocols used by **MS Teams** at different layers are as follows :

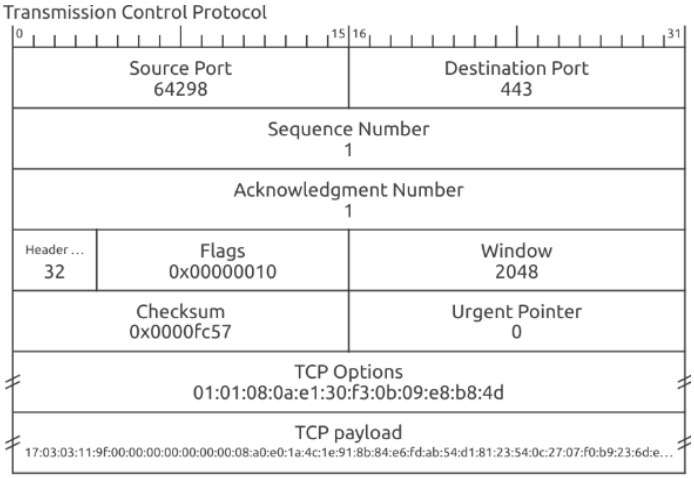
   - Data Link Layer - **Ethernet**



   - Network Layer - **IPv4**

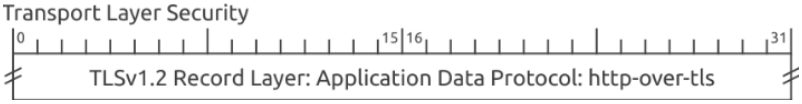


   - Transport Layer - **TCP**



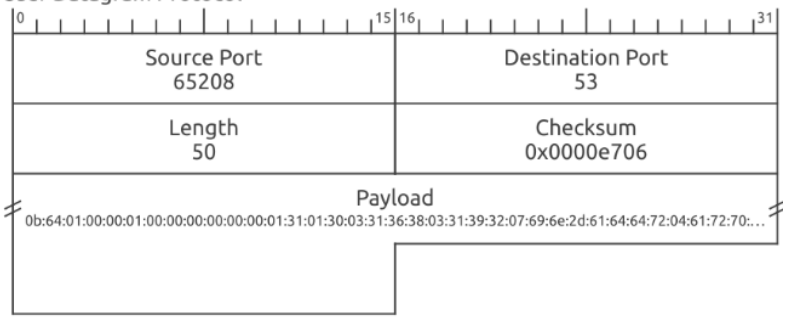
- Transport Layer - **TLS**

Transport Layer Security



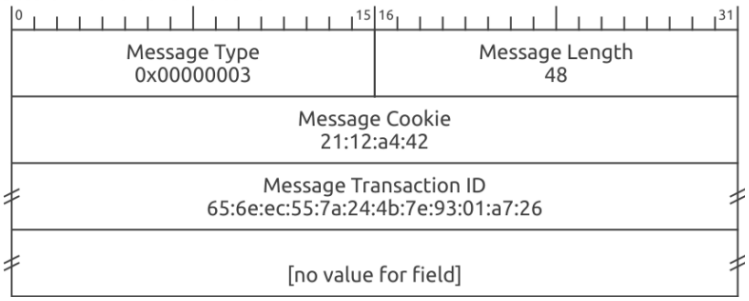
- Transport Layer - **UDP**

User Datagram Protocol



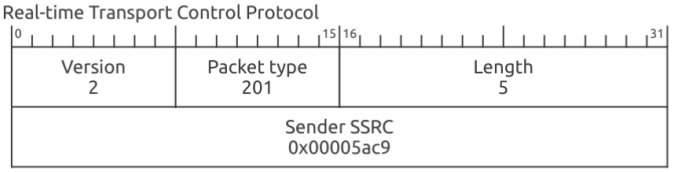
- Application Layer - **STUN**

Session Traversal Utilities for NAT



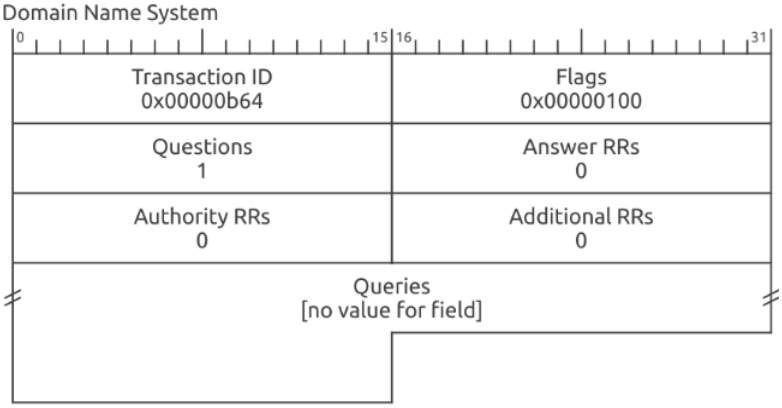
- Application Layer - **RTCP**

Real-time Transport Control Protocol



- Application Layer - **DNS**

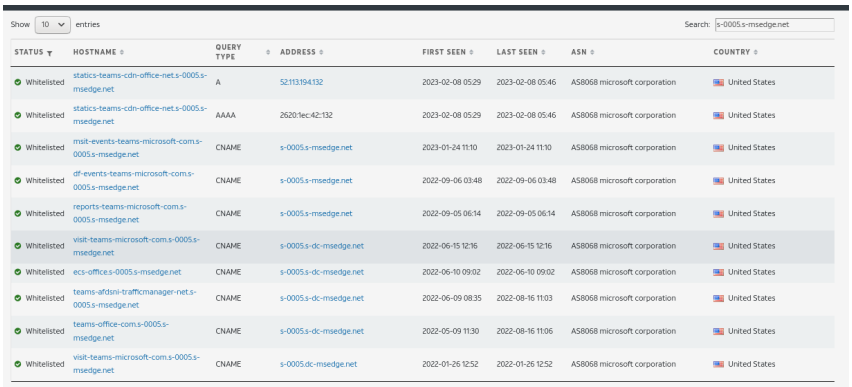
Domain Name System



2. **Highlight and explain the observed values for various fields of the protocols. Example : Source or destination IP address and port number, Ethernet address, protocol number, etc.**

Source IP Address :-
192.168.0.103 is a special IP reserved for accessing the admin panel of routers. This and other IPs like **192.168.0.1**, **192.168.0.254**, **192.168.0.20** etc are unanimously accepted worldwide standards for router IPs. It is also called "Default Gateway IP" in literature.

Destination IP adresses :-
The following screenshot shows a few of the different domains of Microsoft for various functions of MS Teams:
https://otx.alienvault.com/indicator/domain/s-0005.s-msedge.net



Show 10 entries Search: s-0005.s-msedge.net

STATUS	HOSTNAME	QUERY TYPE	ADDRESS	FIRST SEEN	LAST SEEN	ASN	COUNTRY
Whitelisted	statics-teams-cdn-office-net.s-0005.s-msedge.net	A	52.113.194.132	2023-02-08 05:29	2023-02-08 05:46	AS8068 microsoft corporation	United States
Whitelisted	statics-teams-cdn-office-net.s-0005.s-msedge.net	AAAA	2620:1ec:42::132	2023-02-08 05:29	2023-02-08 05:46	AS8068 microsoft corporation	United States
Whitelisted	msit-events-teams-microsoft-com.s-0005.s-msedge.net	CNAME	s-0005.s-msedge.net	2023-01-24 11:10	2023-01-24 11:10	AS8068 microsoft corporation	United States
Whitelisted	df-events-teams-microsoft-com.s-0005.s-msedge.net	CNAME	s-0005.s-msedge.net	2022-09-06 03:48	2022-09-06 03:48	AS8068 microsoft corporation	United States
Whitelisted	reports-teams-microsoft-com.s-0005.s-msedge.net	CNAME	s-0005.s-msedge.net	2022-09-05 06:14	2022-09-05 06:14	AS8068 microsoft corporation	United States
Whitelisted	visit-teams-microsoft-com.s-0005.s-msedge.net	CNAME	s-0005.s-dc-msedge.net	2022-06-15 12:16	2022-06-15 12:16	AS8068 microsoft corporation	United States
Whitelisted	ecs-office.s-0005.s-msedge.net	CNAME	s-0005.s-dc-msedge.net	2022-06-10 09:02	2022-06-10 09:02	AS8068 microsoft corporation	United States
Whitelisted	teams-afdsni-trafficmanager-net.s-0005.s-msedge.net	CNAME	s-0005.s-dc-msedge.net	2022-06-09 08:35	2022-08-16 11:03	AS8068 microsoft corporation	United States
Whitelisted	teams-office-com.s-0005.s-msedge.net	CNAME	s-0005.s-dc-msedge.net	2022-05-09 11:30	2022-08-16 11:06	AS8068 microsoft corporation	United States
Whitelisted	visit-teams-microsoft-com.s-0005.s-msedge.net	CNAME	s-0005.dc-msedge.net	2022-01-26 12:52	2022-01-26 12:52	AS8068 microsoft corporation	United States

Protocol numbers:
TCP - 6
UDP - 17

Ethernet address:-

34:60:f9:b3:e0:4e - is the mac address for the gateway(WiFi).
33:00:00:00:00:01 - is the mac for the system used for analysis.
Port numbers:

443 in case of HTTPS connection
Rest of the port numbers are numerous as they are listed for each video/audio or chat connection after each API call etc.

Address A	Port A	Address B	Port B
192.168.0.101	64313	dual-spo-0003.spo-msedge.net	https
192.168.0.101	64305	13.89.178.26	https
192.168.0.101	64316	e40491.dscd.akamaiedge.net	https
192.168.0.101	64298	s-0005.s-msedge.net	https
192.168.0.101	64309	sa-azsc-urlp.cloudapp.net	https
192.168.0.101	64311	s-0005.s-msedge.net	https
192.168.0.101	64310	s-0005.s-msedge.net	https
192.168.0.101	64312	msgapi-prod-sin.cloudapp.net	https
192.168.0.101	64318	asia2.ocws1.live.com.akadns.net	https
192.168.0.101	59348	www.tm.ak.prd.aadg.akadns.net	https
192.168.0.101	64315	e40491.dscd.akamaiedge.net	https
192.168.0.101	64314	southindia1-0-pushnp.southindia.cloudapp.azure.com	https
192.168.0.101	64307	20.42.73.27	https
192.168.0.101	64317	southindia1-0-pushnp.southindia.cloudapp.azure.com	https
192.168.0.101	64271	52.114.15.102	https
192.168.0.101	64295	52.114.15.111	https
192.168.0.101	64274	52.114.15.102	https
192.168.0.101	64288	20.198.118.190	https
192.168.0.101	64291	52.114.15.140	https
192.168.0.101	64297	52.114.36.191	https
192.168.0.101	64293	40.99.33.242	https
192.168.0.101	64294	52.114.36.191	https
192.168.0.101	64304	52.111.252.0	https

3. **Explain the sequence of messages exchanged by the application for using the available functionalities in the application. For example : upload, download, play, pause ,etc. Check whether there are any handshaking sequences in the application. Briefly explain the handshaking message sequence,if any.**

Download file

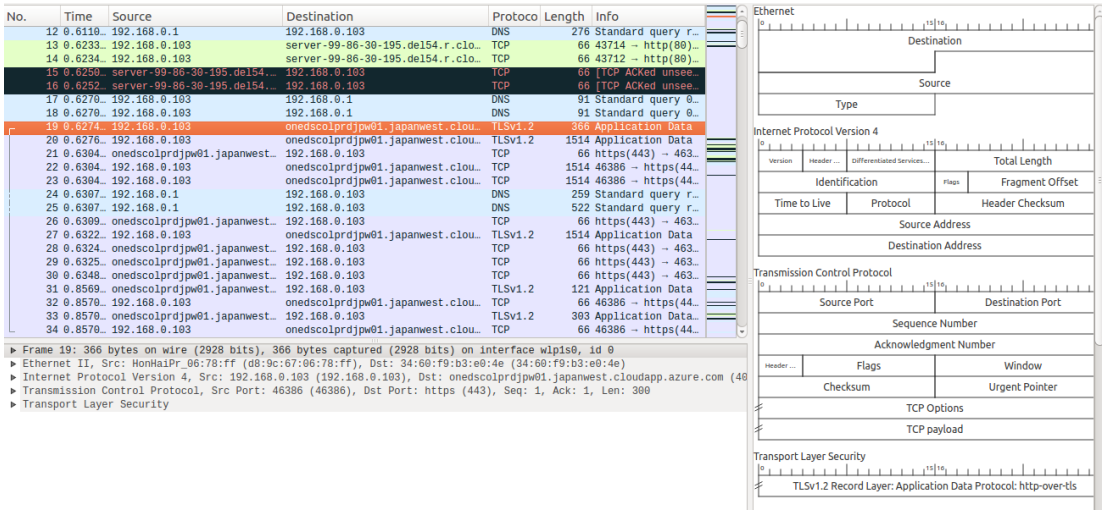
No	Time	Source	Destination	Protocol	Len	Info
2310	21.1821682 33	TPLink Wifi	onedscolprdfrc04.**francecentral**.cloudapp.azure.com	TCP	74	2310 49384 → https(443) **[SYN]** Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1618778809 TSecr=0 WS=128
2314	21.1880024 88	onedscolprdfrc04.**francecentral**.cloudapp.azure.com	TPLink Wifi	TCP	74	https(443) → 49384 **[SYN, ACK]** Seq=0 Ack=1 Win=18328 Len=0 MSS=1460 SACK_PERM=1 TSval=155526948 TSecr=1618778809 WS=128
Handshake Completed						
2316	21.1921997 68	TPLink Wifi	onedscolprdfrc04.**francecentral**.cloudapp.azure.com	TLSv1.2	583	Client Hello
Downloads Requested File						
3396	56.6567663 11	onedscolprdfrc04.**francecentral**.cloudapp.azure.com	TPLink Wifi	TCP	66	**[TCP Keep-Alive ACK]** https(443) → 49384 **[ACK]** Seq=8700 Ack=61152 Win=147968 Len=0 TSval=155530495

						TSecr=1618793918

Video/Audio Call

No	Time	Source	Destination	Protocol	Len	Info
82	18.559140	192.168.0.101	223.238.105.28	STUN	154	Binding Request user: ZIKa:4Rlk
140	19.277345	223.238.105.28	192.168.0.101	STUN	154	Binding Request user: 4Rlk:ZIKa
153	19.318319	192.168.0.101	223.238.105.28	STUN	130	Binding Success Response XOR-MAPPED-ADDRESS: **223.238.105.28**:50022
1622	25.790130	192.168.0.101	223.238.105.28	UDP	98	50026 → 50022 Len=56
Call established… **Call is in progress…** Call ended…						

Chat



Here also TLS handshake can be observed in No. 19 and 20.
Alse, we can observe TCP communication from 21.
Note : There are other functions which exhibit a similar sequence of protocols.We can get a detailed view from the **FLOW GRAPH** feature in wire shark.

4. **Explain how the particular protocol(s) used by the application is relevant for functioning of the application.**

The following protocols are being used in the application: -

- **Ethernet** (IEEE 803.2)
    a) It provides high speed video data transfer and reliability.
- **IPv4** (Internet Protocol version 4)
    a) Provides Server Network Address.

- **TCP** (Transmission Control Protocol)
    a) It contains a destination port. (Provides end-to-end connection).To begin with, pre-fetching and buffering are used while using MS teams to ensure seamless application usage, for which TCP provides the buffer.
    b) While downloading files from MS teams we can observe it uses TCP unlike video or audio calling where UDP is preferred. TCP provides dependable transmission assurance with no frame loss.Error control of TCP allows for error detection. TCP provides a reliable and quick transfer of packets.
- **UDP** (User Datagram Protocol)
    a) For DNS query, Video and Audio calling in MS teams where unreliability is tolerated we have observed UDP being used. Since UDP is unreliable and has no error checking mechanism. It is simple and faster than TCP which makes it the logical option.
    b) **STUN** (Session Traversal Utilities for NAT) is a standardized set of methods, including a network protocol, for traversal of network address translator (**NAT**) gateways in applications of real-time voice, video, messaging, and other interactive communications which are functions of MS Teams.
- **RTCP**
    a) The primary function of RTCP is to provide feedback on the quality of service (QoS) in media distribution by periodically sending statistics information such as packet counts, packet loss, packet delay variation, and round-trip delay time to participants in a streaming multimedia session.

  MS teams use this information to control quality of service parameters, perhaps by limiting flow, or using a different codec.

5. Calculate the following statistics from your traces while performing experiments at different times of the day: Throughput, RTT, Packet size, Number of packets lost, Number of UDP & TCP packets, Number of responses received with respect to one request sent. Report the observed values in your answer,preferably using tables.

Trace	Throughput (bits/sec)	RTT(ms)	Packet size(B)	Number of Packets lost	Number of UDP & TCP packets	Number of responses received	Time and Location
Download	Max = $2*10^7$ Min ~ 100	Max = 16.5 Min ~ 0.1	Min = 40 Max = 2559	0	TCP : 3973 UDP : 48	94	Lab 1 : 00 pm
Video Call	Max = $3*10^6$ Min ~ 100	Max = 4.2 Min ~ 0,2	Min = 42 Min = 1514	0	TCP : 458 UDP : 6189	116	Hostel 8 : 00 pm
Audio	Max = $5*10^4$	Max = 15	Min = 42	0	TCP ; 81	57	Hostel

Call	Min ~ 100	Min ~ 2.5	Max = 1514		UDP :		10 : 25 pm
Chat	Max = 6*10^ Min ~ 100	Max = 44 Min ~ 2	Max = 14546 Min = 42	0	TCP : 4127 UDP : 621	278	Lab 11 :13 am

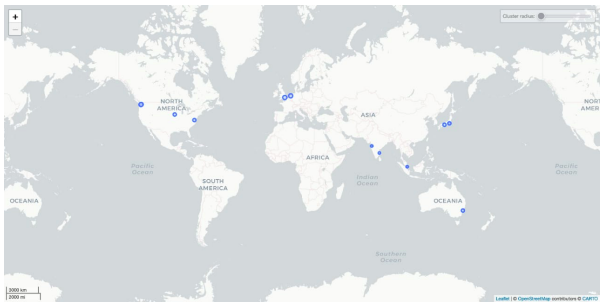
6. **Check whether the whole content is being sent from the same location/source. List out the IP addresses of content providers if multiple sources exist,and explain the reason behind this.**

No, each time we use MS teams,for every function we use one of the different domains of Microsoft. They are predefined for various functions of MS Teams:
The following website contains the documentation for the same :
https://otx.alienvault.com/indicator/domain/s-0005.s-msedge.net

onedscolprdcus00.centralus.cloudapp.azure.com
part-0009.t-0009.fb-t-msedge.net
part-0009.t-0009.fb-t-msedge.net
onedscolprdeus12.eastus.cloudapp.azure.com
20.189.173.15
20.198.118.190
40.99.33.242
fast-prod-cluster-loki.centralindia.cloudapp.azure.com
52.113.194.132
52.114.15.102
52.114.15.111
52.114.32.14
52.114.36.191
flightproxy-ince-02-teams.cloudapp.net

The Azure instance keeps changing every session like France, Central US, Japan etc.

The following map obtained from wireshark shows the regions to which the client is communicating



13.78.209.250
server-18-66-63-16.del51.r.cloudfront.net
server-18-164-212-222.del54.r.cloudfront.net
ec2-18-205-249-252.compute-1.amazonaws.com
onedscolprdeus02.eastus.cloudapp.azure.com
20.190.146.32
prod.detectportal.prod.cloudops.mozgcp.net
prod.ingestion-edge.prod.dataops.mozgcp.net
76.237.120.34.bc.googleusercontent.com
191.144.160.34.bc.googleusercontent.com
15.42.188.35.bc.googleusercontent.com
150.9.241.35.bc.googleusercontent.com
onedscolprdjpw01.japanwest.cloudapp.azure.com
ec2-52-35-30-160.us-west-2.compute.amazonaws.com
52.111.252.0
52.114.15.121
52.114.15.123
52.114.15.134

Reasons for using multiple content providers :-

- It provides a high level of reliability and availability.
- It implements load balancing very efficiently.
- Receives the data in chunks so prefetching and buffering is quick.

Trace Files :-
https://iitgoffice-my.sharepoint.com/:f:/g/personal/r_sri_iitg_ac_in/EuYFHRUpa5ZKnHrT7_1ruJIBB_ghxRisiZtoSdraxFxzcg?e=MA0s4l