

Submission by : Prerna Sidana
Training area: Cyber security
CS-June-2020

VERZEO

JUNE BATCH 2020

MENTOR: ANIMESH ROY

MINOR PROJECT ASSIGNMENT

Submission by : Prerna Sidana
Training area: Cyber security
CS-June-2020

Question 1)

Use Wireshark to see traffic, in terms of source/destination IP address/ports, is going through your computer. Mention and document the traffic using snapshots that you see when all applications are closed, except background applications, in tabular form.

Getting Started

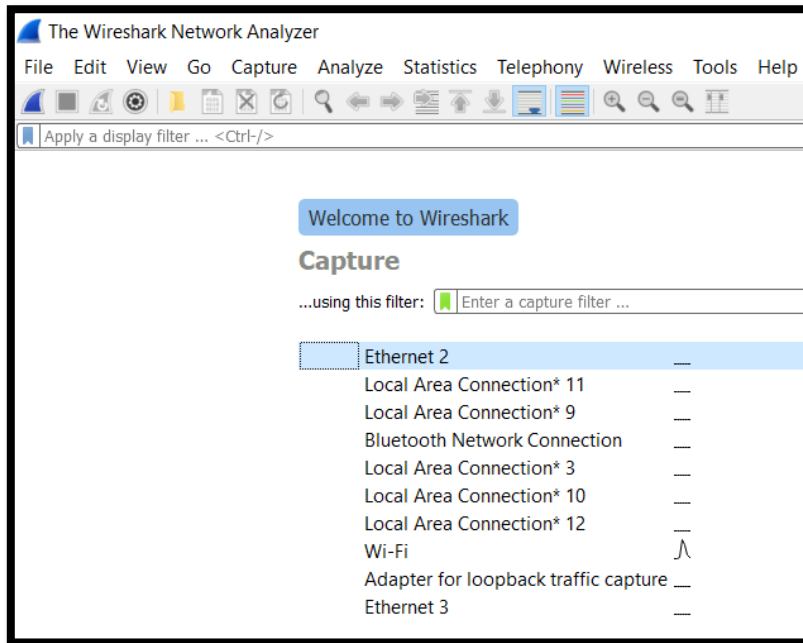
Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and displays them in human-readable format. Wireshark includes filters, colour coding, and other features that let you dig deep into network traffic and inspect individual packets. You can download Wireshark for Windows or macOS from its official website. If you're using Linux or another UNIX-like system, you'll probably find Wireshark in its package repositories. For example, if you're using Ubuntu, you'll find Wireshark in the Ubuntu Software Center.

PROCESS

1. Capturing Packets

After downloading and installing Wireshark, you can launch it and double-click the name of a network interface under Capture to start capturing packets on that interface.

Submission by : Prerna Sidana
Training area: Cyber security
CS-June-2020



2. As soon as you click the interface's name, you'll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system.

The screenshot shows the Wireshark Network Analyzer interface with a list of captured packets. The 'Stop capturing packets' button is visible in the top left corner. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	52.108.236.4	192.168.1.7	TLSv1.2	87	Application Data
2	0.040797	113.29.117.17	192.168.1.7	TCP	66	443 → 56039 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452 WS=64 SACK_PERM=1
3	0.040921	192.168.1.7	113.29.117.17	TCP	54	56039 → 443 [ACK] Seq=1 Ack=1 Win=516 Len=0
4	0.041058	192.168.1.7	113.29.117.17	TCP	54	56039 → 443 [FIN, ACK] Seq=1 Ack=1 Win=516 Len=0
5	0.048178	192.168.1.7	52.108.236.4	TCP	54	55963 → 443 [ACK] Seq=1 Ack=34 Win=515 Len=0
6	0.148114	113.29.117.17	192.168.1.7	TCP	54	443 → 56039 [ACK] Seq=1 Ack=2 Win=66752 Len=0
7	0.148114	113.29.117.17	192.168.1.7	TCP	54	443 → 56039 [FIN, ACK] Seq=1 Ack=2 Win=66752 Len=0
8	0.148240	192.168.1.7	113.29.117.17	TCP	54	56039 → 443 [ACK] Seq=2 Ack=2 Win=516 Len=0
9	0.465427	b8:c1:ac:a2:7f:b5	Broadcast	ARP	42	Who has 192.168.1.8? Tell 192.168.1.1
10	1.487898	b8:c1:ac:a2:7f:b5	Broadcast	ARP	42	Who has 192.168.1.8? Tell 192.168.1.1
11	3.128116	52.108.236.4	192.168.1.7	TLSv1.2	87	Application Data
12	3.182967	192.168.1.7	52.108.236.4	TCP	54	55963 → 443 [ACK] Seq=1 Ack=67 Win=515 Len=0
13	3.369118	192.168.1.7	66.110.49.30	SSL	352	Continuation Data
14	3.434960	b8:c1:ac:a2:7f:b5	Broadcast	ARP	42	Who has 192.168.1.3? Tell 192.168.1.1
15	3.747410	66.110.49.30	192.168.1.7	SSL	157	Continuation Data

1. Click the red "Stop" button near the top left corner of the window when you want to stop capturing traffic.
2. Inspecting Packet: Click a packet to select it and you can dig down to view its details.

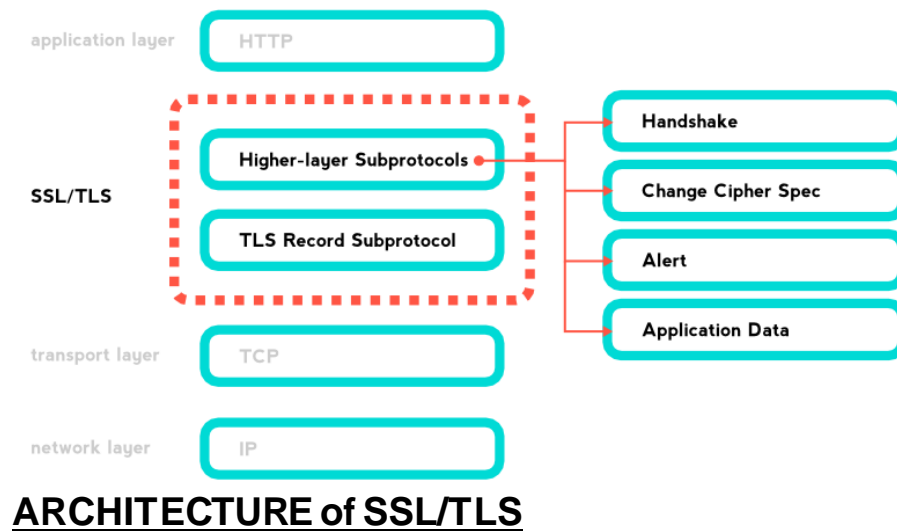
Submission by : Prerna Sidana
Training area: Cyber security
CS-June-2020

Examples of packets from above:

S.no.	Packet number	Source IP	Class of source IP	Destination IP	Class of dest. IP	Protocol
i)	1	52.108.236.4	A	192.168.1.7	C	TLSv1.2
ii)	8	192.168.1.7	C	113.29.117.17	A	TCP
iii)	15	66.110.49.30	A	192.168.1.7	C	SSL

SSL 2.0 and 3.0 are considered insecure, so they are being replaced by the newer TLS 1.0/1.1/1.2 versions.

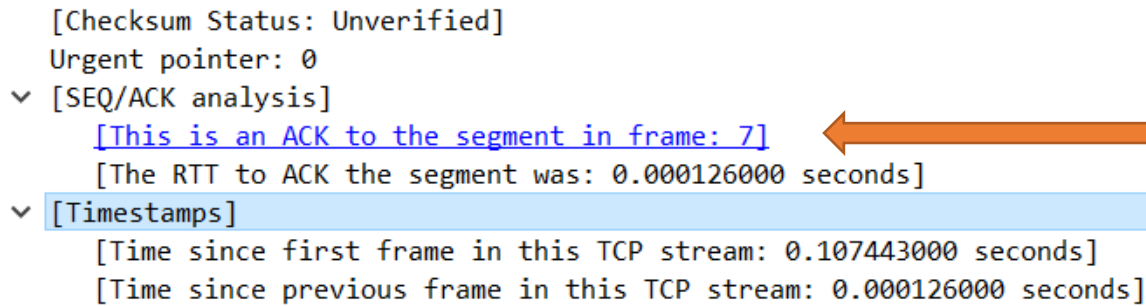
SSL and TLS between a high-level protocol (like HTTP) and a low-level protocol (like TCP) in the network stack and provide the necessary encryption and authentication functionality.



TCP Analysis flags are added to the TCP protocol tree under “SEQ/ACK analysis”. Each flag is described below. Terms such as “next expected sequence number” and “next expected acknowledgement number” refer to the following”:

Submission by : Prerna Sidana
Training area: Cyber security
CS-June-2020

```
[Checksum Status: Unverified]
Urgent pointer: 0
v [SEQ/ACK analysis]
  [This is an ACK to the segment in frame: 7]
  [The RTT to ACK the segment was: 0.000126000 seconds]
v [Timestamps]
  [Time since first frame in this TCP stream: 0.107443000 seconds]
  [Time since previous frame in this TCP stream: 0.000126000 seconds]
```



Next expected sequence number

The last-seen sequence number plus segment length. Set when there are no analysis flags and for zero window probes. This is initially zero and calculated based on the previous packet in the same TCP flow. Note that this may not be the same as the tcp.nextseq protocol field.

Next expected acknowledgement number

The last-seen sequence number for segments. Set when there are no analysis flags and for zero window probe

Question 2)

Use google apps toolbox to review email headers

<https://toolbox.googleapps.com/apps/messageheader/>)

THEORY: An email header consists of 3 components:

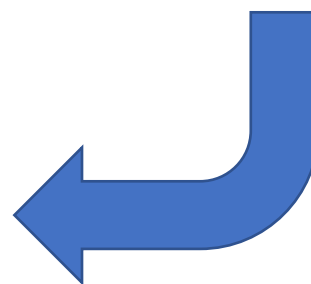
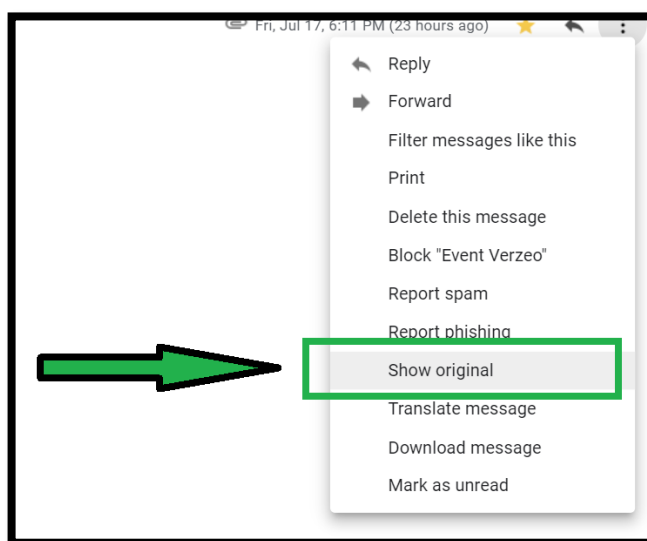
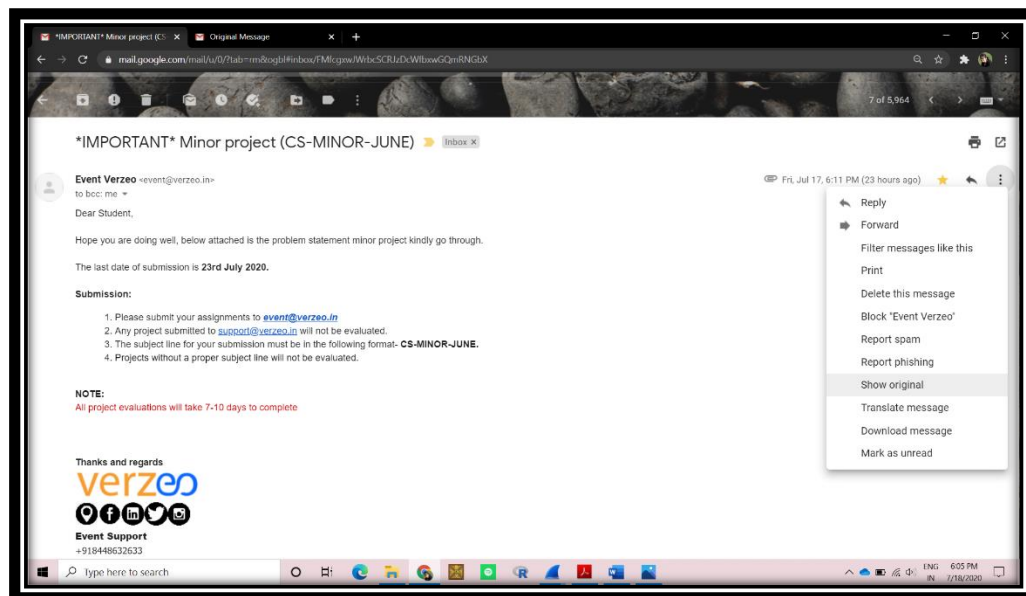
- 1. An envelope- It contains some server configuration settings files and data**
- 2. Body: Message transmitted by sender**
- 3. Header: Contains source IP, destination IP and other details like message ID, Date, to, from, User agent etc.**

We analyse email headers to detect whether the email received has come from a legitimate source or not.

Submission by : Prerna Sidana
Training area: Cyber security
CS-June-2020

Procedure:

1. Open the email message in Gmail application.
2. Click on the drop down arrow, which is located next to **Reply** button.
3. Choose **Show Original** option to read Gmail header.

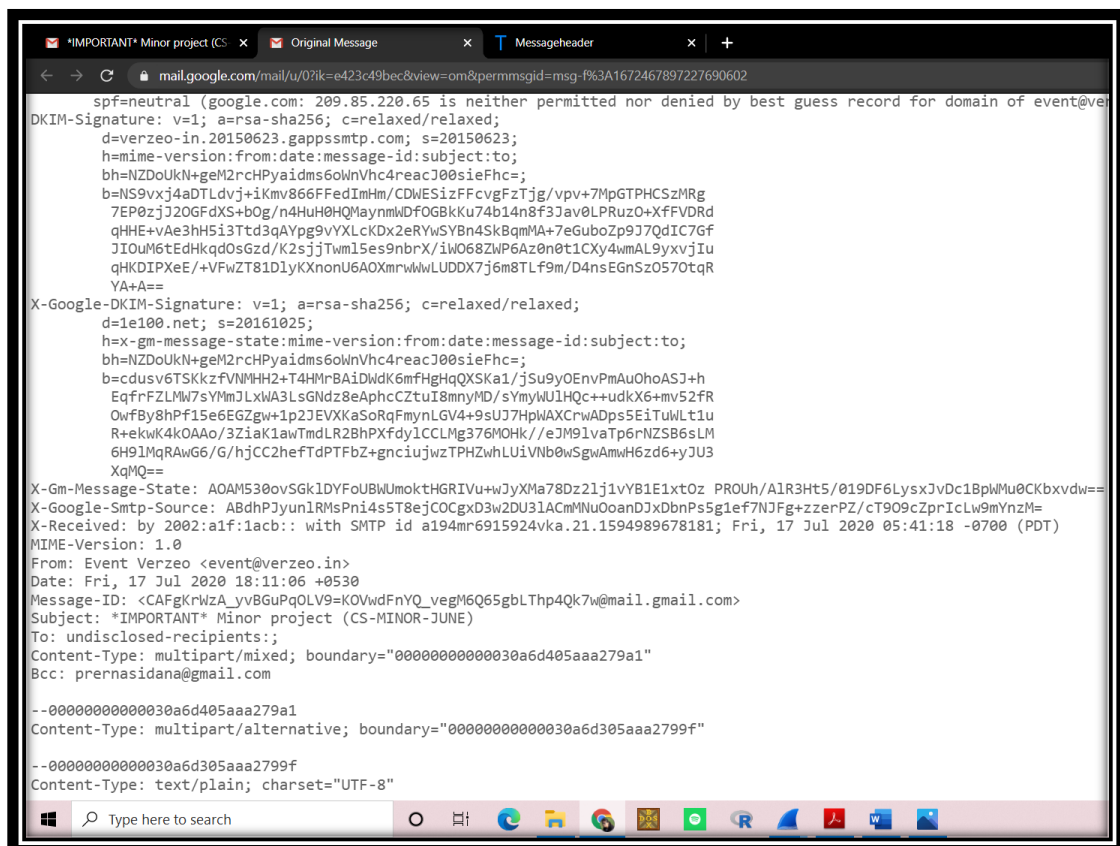
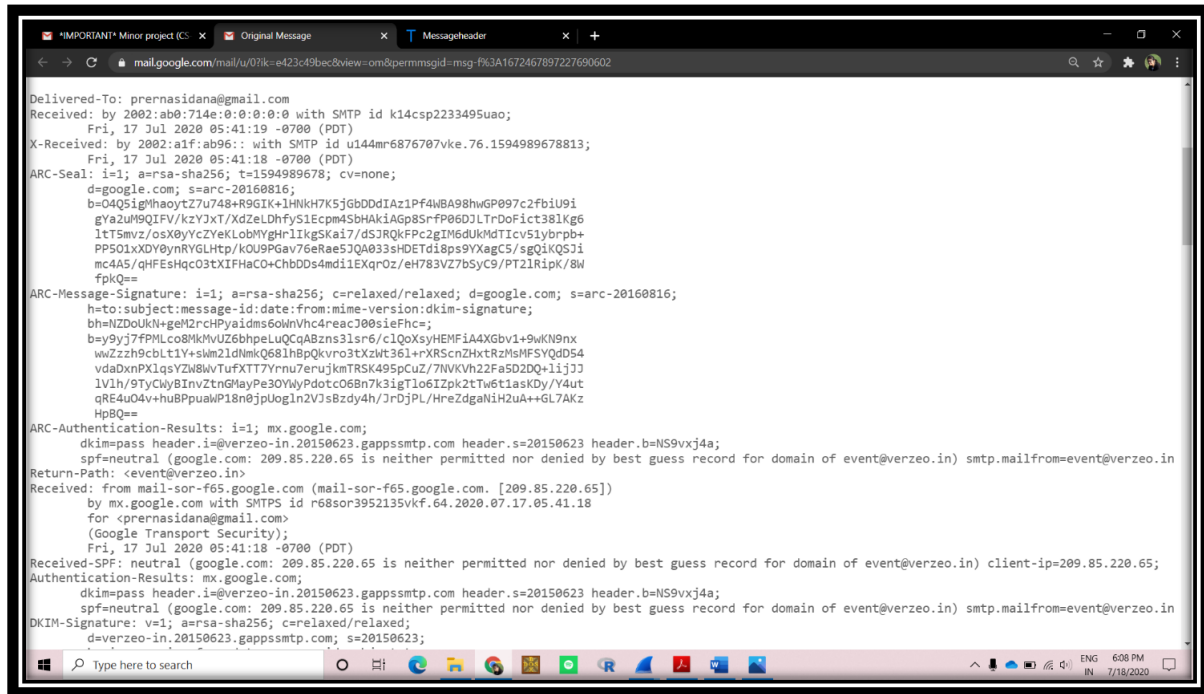


4. A new window named '**Original Message**' opens.

Submission by : Prerna Sidana

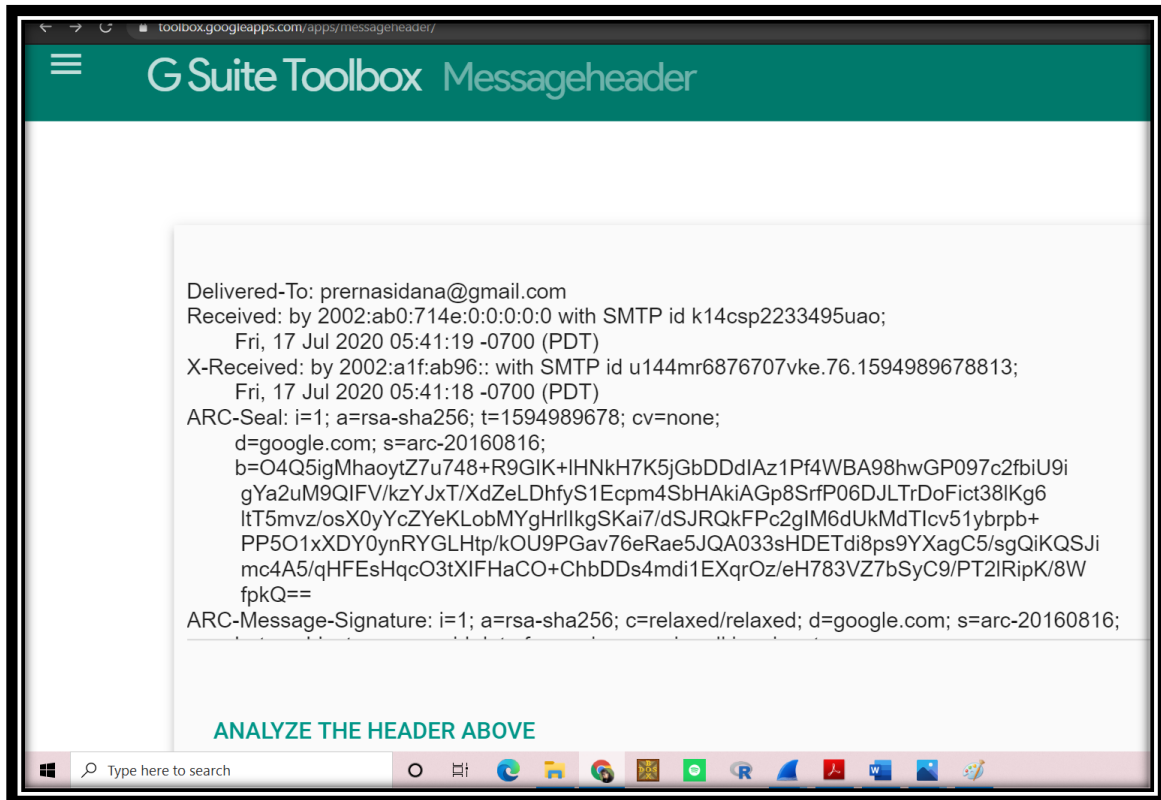
Training area: Cyber security

CS-June-2020



Submission by : Prerna Sidana
Training area: Cyber security
CS-June-2020

5. Copy the text in the previous two screenshots i.e, excluding the body of the actual content which you see normally on the gmail account.
6. Open <https://toolbox.googleapps.com/apps/messageheader/> in a new tab. Paste the copied content in the Paste email headers here window.



7. Click on ***ANALYZE THE HEADER ABOVE*** button to review email headers.

Submission by : Prerna Sidana
Training area: Cyber security
CS-June-2020

MessageId	CAFgKrWzA_yvBGUPqOLV9=KOVwdFnYQ_vegM6Q65gbLThp4Qk7w@mail.gmail.com				
Created at:	7/17/2020, 6:11:06 PM GMT+5:30 (Delivered after 13 sec)				
From:	Event Verzeo <event@verzeo.in>				
To:	undisclosed-recipients;;				
Subject:	*IMPORTANT* Minor project (CS-MINOR-JUNE)				
SPF:	neutral				
DKIM:	pass				

#	Delay	From *	To *	Protocol	Time received
0	12 sec		→ [Google] 2002:a1f:1acb::	SMTP	7/17/2020, 6:11:18 PM GMT+5:30
1		mail-sor-f65.google.com.	→ [Google] mx.google.com		7/17/2020, 6:11:18 PM GMT+5:30 <i>Originated at Gmail</i>
2			→ [Google] 2002:a1f:ab96::	SMTP	7/17/2020, 6:11:18 PM GMT+5:30
3	1 sec		→ [Google] 2002:ab0:714e:0:0:0:0	SMTP	7/17/2020, 6:11:19 PM GMT+5:30

REVIEW:

Delivered To: The delivered-to email field indicates the email address of the intended recipient. Thus, it generally contains the same email id for which Gmail header is being analyzed.

Received By: The received email header denotes the information related to the last SMTP server visited by message:

- The IP address of the server
- The SMTP id for the visited server
- The date and time at which message was received by SMTP server

Received From: It portrays the server related IP address, email address of the receiver, encryption related information, date and time for the received message thread.

Received-SPF: SPF(Sender Policy Framework) check is applied to check whether the email is from the valid sender or not. It verifies the identity with the domain address

Submission by : Prerna Sidana
Training area: Cyber security
CS-June-2020

and adds the status of check in the header field. The most commonly used result codes include:

CODE	INTERPRETATION
Pass	The email source is valid
Softfail	There might be possibility of fake source
Fail	The email source is absolutely invalid
Neutral	Difficult to distinguish between valid & invalid source
None	The SPF record is not found for domain
Unknown	The SPF check cannot be performed
Error	An error has occurred while performing SPF check

DKIM Signature: The DKIM signature header is basically a field to represent the digital signature embedded in the email. It is basically another authentication key maintained by the mail server to share data in secure form.

X-Google-DKIM-Signature: In addition to various authentications, Google itself adds an X-Google-DKIM Signature field in email header to improve authentication of signatures. The subsequent fields located within the field signifies the information related to digital signatures encoding.

- **MIME-Version:** The Gmail message can support multiple data including plain text files, audio, video, applications etc.
- **Reply-To:** The reply-to email header field simply lists the email address at which the reply to the message is received. Generally, it corresponds to the sender's address.
- **X-Originating IP:** It contains the IP address of the sender.
- **Message Id:** Each email message is assigned a unique message ID, which distinguishes it from other emails. No two emails can have the same message id as it acts as a primary unique value for each message.

Submission by : Prerna Sidana
Training area: Cyber security
CS-June-2020

- **Date:** The Date field in header indicates the date and time at which message was received at the destination.
- **Subject:** The subject field in email message tends to display the major subject or purpose of communication.
- **From:** It indicates the email address of the sender.
- **To:** This field represents the receiver's email address.
- **CC:** It contains the list of all receiver, who are intended to receive the message as a carbon copy.