

Experiment 1:

Aim:

- 1 - Perform Email Header Analysis for extracting valuable information like sender IP address, email servers, and routing information.
- 2 - Conduct email address enumeration by attempting to verify the existence of email addresses within a target domain. Use tools like the Harvester or thehunter.io to search for email addresses associated with a specific domain. This can help identify valid email addresses within an organization.
- 3 - Analyze the metadata of an email, including date and time stamps, email clients used, or the originating IP address, email's origin, potential geographic location of the sender, or possible email routing

Theory:

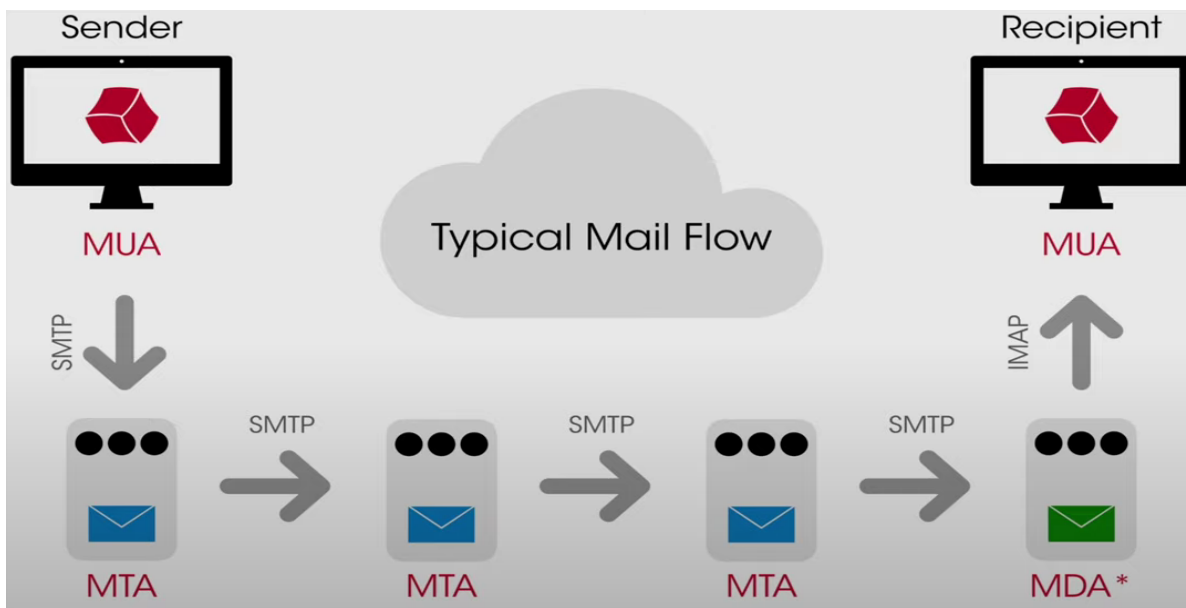
Email address analysis and enumeration are crucial for cybersecurity students as they enable threat investigation, incident response, social engineering awareness, attribution, forensics, and Open Source Intelligence (OSINT) activities. By analyzing email addresses, students can identify potential risks, trace the source of attacks, understand attacker tactics, contain incidents, detect social engineering attempts, establish evidence chains, and gather intelligence. These skills empower students to proactively defend against cyber threats and contribute to overall digital security. Before analyzing email header, let's understand the flow of mail and understand the important concepts of mail flow.

Mail flow:-

MUA (Mail User Agent): It is an application or software program that allows users to send, receive, and manage their email messages. Also known as an email client, the MUA provides an interface for users to compose, read, and organize emails. Examples of popular MUAs include Microsoft Outlook, Mozilla Thunderbird, Apple Mail, and Gmail. The MUA interacts with the mail server to send and receive emails, and it often includes additional features such as contact management, calendar integration, and spam filtering.

MTA (Mail Transfer Agent): It is a software or program responsible for the routing and delivery of email messages across different mail servers on the internet. The MTA acts as a communication bridge between the sender's mail server and the recipient's mail server. When an email is sent, the MTA receives the message from the Mail User Agent (MUA) and performs tasks such as address verification, routing, and relaying the email to the appropriate destination. Examples of popular

MTAs include Sendmail, Postfix, Microsoft Exchange Server, and Exim. The MTA plays a critical role in the reliable and efficient transmission of email across networks.



SMTP (Simple Message Transfer Protocol): It is a standard protocol used for sending and routing email messages between mail servers on the internet. It establishes a connection between the sender's and recipient's mail servers to transfer the email data. SMTP operates on TCP/IP and follows a set of rules and commands to ensure reliable email delivery.

SPF (Sender Policy Framework): It is an email authentication protocol that helps prevent email spoofing and unauthorized use of a domain's identity. SPF allows domain owners to specify which mail servers are authorized to send email on behalf of their domain. When an email is received, the recipient's mail server can check the SPF record to verify if the sending server is authorized to send emails for that domain. This helps to reduce spam, phishing, and other malicious activities by ensuring that only authorized servers can send emails on behalf of a domain.

Procedure:

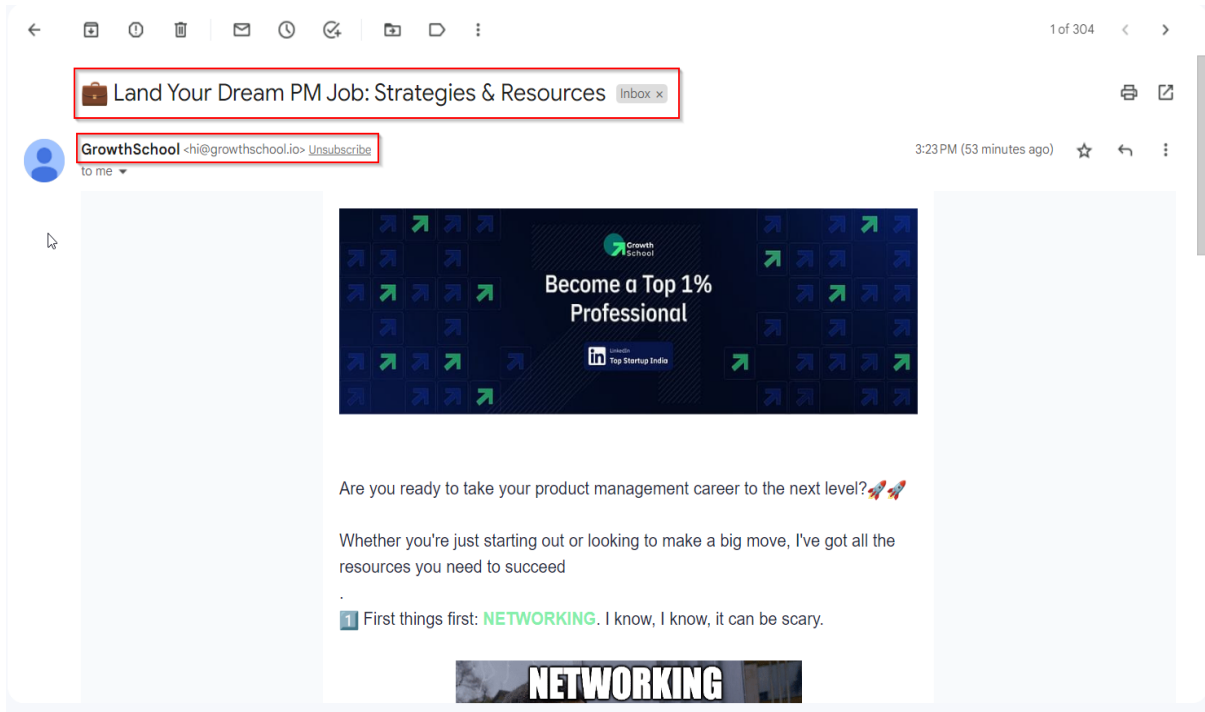
Task 1 -> Perform Email Header Analysis for extracting valuable information like sender IP address, email servers, and routing information.

+

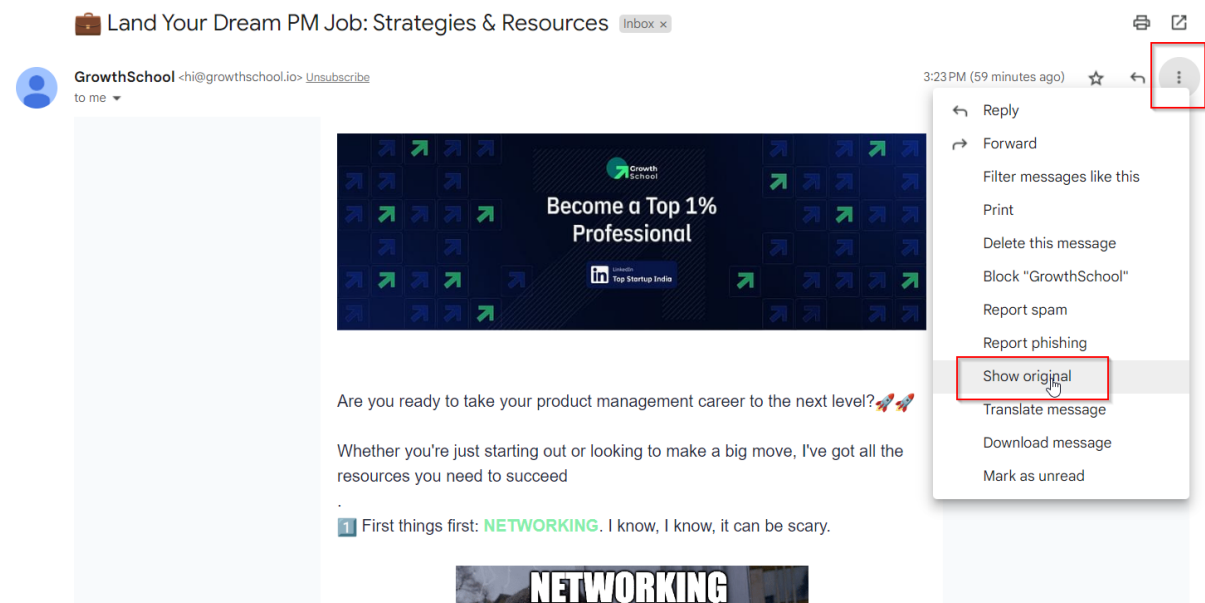
Task 2 -> Conduct email address enumeration by attempting to verify the existence of email addresses within a target domain. Use tools like the Harvester or thehunter.io to search for email addresses associated with a specific domain. This can help identify valid email addresses within an organization.

Step 1: To perform this task I am going to analyse any one email of my inbox.

I have highlighted the header and sender info as it shows. I am not sure if it is correct.



Step 2: Go to the top right corner -> click on 3 dots -> click on show original to see headers of email.



Step 3: New page will open with all header information. At top you can see overview of header in human readable format and then you'll see a block of text containing various lines.

To Analyze in detail, download original

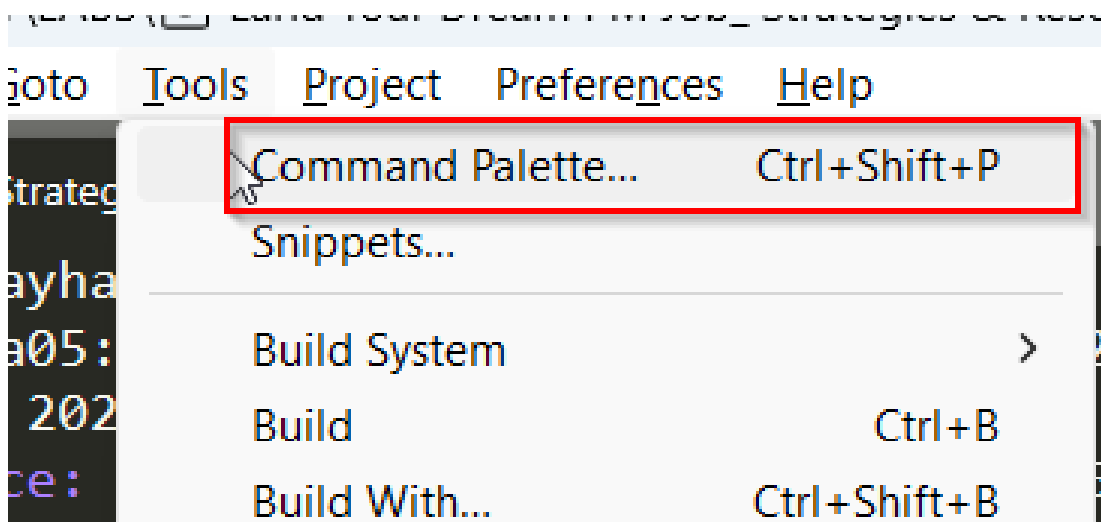
Original Message

Message ID	<9D.0D.25130.3BD35A46@in.mta1vrest.cc.pr.d.sparkpost>
Created at:	Wed, Jul 5, 2023 at 3:23 PM (Delivered after 1 second)
From:	GrowthSchool <hi@growthschool.io>
To:	thejayhack@gmail.com
Subject:	📁 Land Your Dream PM Job: Strategies & Resources
SPF:	PASS with IP 156.70.151.37 Learn more
DKIM:	'PASS' with domain growthschool.io Learn more
DMARC:	'PASS' Learn more

[Download Original](#)[Copy to clipboard](#)

```
Delivered-To: thejayhack@gmail.com
Received: by 2002:a05:651c:235:0:0:0 with SMTP id z21csp4646112ljn;
    Wed, 5 Jul 2023 02:53:56 -0700 (PDT)
X-Goog-Smtp-Source: APBjJlHw/Ym4bzEJA0nqpI2CN8EuKGG6SIDYj8n5MGwRds1SbEIMTd0Esgg8G8nsthKL/lpxaNM
X-Received: by 2002:a17:90a:f00c:b0:262:c9f4:141 with SMTP id bt12-20020a17090af00c00b00262c9f40141mr14160942pjb.42.1688550836273;
    Wed, 05 Jul 2023 02:53:56 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1688550836; cv=none;
    d=google.com; s=arc-20160816;
```

Open file in sublime text editor -> Go to Tools -> Click on Command Palette -> install “Package control install” -> now again open Command Palette -> open installed package “Package Control” -> Install “email header”



Step 4: Open header originals in Sublime text editor

You can see the colour scheme which really help to understand long header text.

```
1 Delivered-To: thejayhack@gmail.com
2 Received: by 2002:a05:651c:235:0:0:0 with SMTP id z21csp46461121jn;
3   Wed, 5 Jul 2023 02:53:56 -0700 (PDT)
4 X-Google-Smtp-Source: APBJ1lHw/Ym4bzEJA0nqpI2CN8EuUkG63SIDYj8n5MGwRdS1SbEIMTdOEsgg8GBnsthKL/lpxaNM
5 X-Received: by 2002:a17:90a:f00c:b0:262:c9f4:141 with SMTP id bt12-20020a17090af00c00b00262c9f40141mr14160942pjb.42.1688550836273;
6   Wed, 05 Jul 2023 02:53:56 -0700 (PDT)
7 ARC-Seal: i=1; a=rsa-sha256; t=1688550836; cv=none;
8   d=google.com; s=arc-20160816;
9   b=y8KIthzaI+xiOjVDN0r1fBT/pVGWhY1ZE2IPuqIAhZtetnGF1a+wwK5VGepZwDeqYLj
10   09B1KKZcue00he6PL1L5j3rxLMq2R1YuUPZreaaYu7oFF2KV7qYP04F9YQcTqL6Phhd+
11   b2ZpPcSb1Ny+LGtk6pDc9jcs06I/5oy3h9z9iNbGEdQR/mJTOV/xKY/Y6W8tmF4Eo6t
12   xrbtZfFkKCyP1eoMxtvZzapK4RaNXAGjDdgHLo72/3oEC4JYk16a7rCyEz904sQpEezP
13   tTdVb56BknAJwdIqeOhrANyCAibQxcB+gpgTWjj53kF65NmFLJaZ/TCnQGeYenq6udsK
14   YV8w==
15 ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
16   h=list-id:list-unsubscribe:feedback-id:reply-to:campaignid:from
17   :subject:emailidentifier:isdebug:userId:mime-version:date:message-id
18   :to:dkim-signature;
19   bh=Zwwcdl0ioshBUeNI2mIKBE1b90apEZfbK+URMMBREFY=;
20   fh=66EGIAowGzfbqyP2TXdeLE0prkCjs6xoRKm+6jMj+3w=;
21   b=uyui1x1cm8AAQXh/HA0jdpN19G/mkrD8Q3CKQURrFnMTSGsx0Fk40oqTNp3su1q4hy
22   jWitCaMD5E4AP2akeBtKRW57H1wnARg5XkgBTW06K+/rcfUzthZ0/9orhNPIdONobPfg
23   aPdcC1wamSpCOWdZ3Kv+mKoqy9TDSyiH5P5id1dp5must54xKz9IQnk94d82IuHkg4
24   p20PC8vv1xwBn/LujusEdHfLJvNSxvFH3P7t54G708WZTW/ejGkT6EZRPma1JcsKLzYY
25   m/CqFTFhVU0PvXwZVYw66bWP6294Kw06TdjIMEaCPn9DI5I+HbnhxCrczkeGSVvxtjc2
26   dbTw==
27 ARC-Authentication-Results: i=1; mx.google.com;
28   dkim=pass header.i=@growthschool.io header.s=mailmodo header.b=Dk9eZ2TB;
29   spf=pass (google.com: domain of msprvs1=19550wb5z5iko=bounces-303287-3967@bounce.mailmodo.email designates 156.70.151.37 as permitted sender)
30   smtp.mailfrom="msprvs1=19550wb5z5iko=bounces-303287-3967@bounce.mailmodo.email";
31   dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=growthschool.io
32 Return-Path: <msprvs1=19550wb5z5iko=bounces-303287-3967@bounce.mailmodo.email>
33 Received: from mta-70-151-37.sparkpostmail.com (mta-70-151-37.sparkpostmail.com. [156.70.151.37])
34   by mx.google.com with ESMTPS id p4-20020a63c14400000b00530b6228f91si23684904pgi.895.2023.07.05.02.53.56
35   for <thejayhack@gmail.com>
36   (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
37   Wed, 05 Jul 2023 02:53:56 -0700 (PDT)
38 Received-SPF: pass (google.com: domain of msprvs1=19550wb5z5iko=bounces-303287-3967@bounce.mailmodo.email designates 156.70.151.37 as permitted sender)
39 client-ip=156.70.151.37;
40 Authentication-Results: mx.google.com;
```

Step 5: Now we will see routing of mail. To understand routing we have to start from bottom. You have to see last “received:” parameter in the header. You can use ctrl+f to find this parameter.

```
1 Delivered-To: thejayhack@gmail.com
2 Received: by 2002:a05:651c:235:0:0:0 with SMTP id z21csp46461121jn;
3   Wed, 5 Jul 2023 02:53:56 -0700 (PDT)
4 X-Google-Smtp-Source: APBJ1lHw/Ym4bzEJA0nqpI2CN8EuUkG63SIDYj8n5MGwRdS1SbEIMTdOEsgg8GBnsthKL/lpxaNM
5 X-Received: by 2002:a17:90a:f00c:b0:262:c9f4:141 with SMTP id bt12-20020a17090af00c00b00262c9f40141mr14160942pjb.42.1688550836273;
6   Wed, 05 Jul 2023 02:53:56 -0700 (PDT)
7 ARC-Seal: i=1; a=rsa-sha256; t=1688550836; cv=none;
8   d=google.com; s=arc-20160816;
9   b=y8KIthzaI+xiOjVDN0r1fBT/pVGWhY1ZE2IPuqIAhZtetnGF1a+wwK5VGepZwDeqYLj
10   09B1KKZcue00he6PL1L5j3rxLMq2R1YuUPZreaaYu7oFF2KV7qYP04F9YQcTqL6Phhd+
11   b2ZpPcSb1Ny+LGtk6pDc9jcs06I/5oy3h9z9iNbGEdQR/mJTOV/xKY/Y6W8tmF4Eo6t
12   xrbtZfFkKCyP1eoMxtvZzapK4RaNXAGjDdgHLo72/3oEC4JYk16a7rCyEz904sQpEezP
13   tTdVb56BknAJwdIqeOhrANyCAibQxcB+gpgTWjj53kF65NmFLJaZ/TCnQGeYenq6udsK
14   YV8w==
15 ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
16   h=list-id:list-unsubscribe:feedback-id:reply-to:campaignid:from
17   :subject:emailidentifier:isdebug:userId:mime-version:date:message-id
18   :to:dkim-signature;
19   bh=Zwwcdl0ioshBUeNI2mIKBE1b90apEZfbK+URMMBREFY=;
20   fh=66EGIAowGzfbqyP2TXdeLE0prkCjs6xoRKm+6jMj+3w=;
21   b=uyui1x1cm8AAQXh/HA0jdpN19G/mkrD8Q3CKQURrFnMTSGsx0Fk40oqTNp3su1q4hy
22   jWitCaMD5E4AP2akeBtKRW57H1wnARg5XkgBTW06K+/rcfUzthZ0/9orhNPIdONobPfg
23   aPdcC1wamSpCOWdZ3Kv+mKoqy9TDSyiH5P5id1dp5must54xKz9IQnk94d82IuHkg4
24   p20PC8vv1xwBn/LujusEdHfLJvNSxvFH3P7t54G708WZTW/ejGkT6EZRPma1JcsKLzYY
25   m/CqFTFhVU0PvXwZVYw66bWP6294Kw06TdjIMEaCPn9DI5I+HbnhxCrczkeGSVvxtjc2
26   dbTw==
27 ARC-Authentication-Results: i=1; mx.google.com;
28   dkim=pass header.i=@growthschool.io header.s=mailmodo header.b=Dk9eZ2TB;
29   spf=pass (google.com: domain of msprvs1=19550wb5z5iko=bounces-303287-3967@bounce.mailmodo.email designates 156.70.151.37 as permitted sender)
30   smtp.mailfrom="msprvs1=19550wb5z5iko=bounces-303287-3967@bounce.mailmodo.email";
31   dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=growthschool.io
32 Return-Path: <msprvs1=19550wb5z5iko=bounces-303287-3967@bounce.mailmodo.email>
33 Received: from mta-70-151-37.sparkpostmail.com (mta-70-151-37.sparkpostmail.com. [156.70.151.37])
34   by mx.google.com with ESMTPS id p4-20020a63c14400000b00530b6228f91si23684904pgi.895.2023.07.05.02.53.56
35   for <thejayhack@gmail.com>
36   (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
37   Wed, 05 Jul 2023 02:53:56 -0700 (PDT)
```

Here we can see we have two "received:" parameters in some cases it can be more than this. The last one will show the closest server from source side (sender) and the recent one (top most) will show the closest server from the receiver side.

```
Return-Path: <msprvs1=19550wb5Z5IK0=bounces-303287-3967@bounce.mailmodo.email>
Received: from mta-70-151-37.sparkpostmail.com (mta-70-151-37.sparkpostmail.com. [156.70.151.37])
        by mx.google.com with ESMTPS id p4-20020a63c144000000b00530b6228f91si23684904pgi.895.2023.07.05.02.53.56
        for <thejayhack@gmail.com>
        (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
        Wed, 05 Jul 2023 02:53:56 -0700 (PDT)
```

In the last "received:" parameter, you can see the sender server detail. The IPv4 address of the sender's server is 156.70.151.37 and they are using spark post mail as their mail server.

Now let's check the genuineness of this server. I will run whois on this server IPv4.

```
NetRange:      156.70.150.0 - 156.70.151.255
CIDR:          156.70.150.0/23
NetName:       MS-820
NetHandle:     NET-156-70-150-0-1
Parent:        NET156 (NET-156-0-0-0-0)
NetType:       Direct Allocation
OriginAS:      AS23528
Organization:  Sparkpost (MS-820)
RegDate:       2020-01-17
Updated:       2021-12-14
Ref:           https://rdap.arin.net/registry/ip/156.70.150.0

OrgName:       Sparkpost
OrgId:         MS-820
Address:       9160 Guilford Rd
City:          Columbia
StateProv:     MD
PostalCode:    21046
Country:       US
RegDate:       2015-12-09
Updated:       2023-01-24
Ref:           https://rdap.arin.net/registry/entity/MS-820
```

You can see the range of IPv4 networks they are using, you can see the Organisation name and it seems genuine and it is. If in the header it is named differently and whois shows a different name then you have to research more on the genuineness of the sender's server.

```
Delivered-To: thejayhack@gmail.com
Received: by 2002:a05:651c:235:0:0:0:0 with SMTP id z21csp46461121jn;
        Wed, 5 Jul 2023 02:53:56 -0700 (PDT)
```

You can see receiver end details on top. You can understand routing by investigating all request parameters from bottom to top.

Task 3 -> Analyze the metadata of an email, including date and time stamps, email clients used, or the originating IP address, email's origin, potential geographic location of the sender, or possible email routing

Step 1:

```
Wed, 05 Jul 2023 02:53:56 -0700 (PDT)
Received-SPF: pass (google.com: domain of msprvs1=19550wb5z5iko=bounces-303287-3967@bounce.mailmodo.email designates 156.70.151.37 as permitted sender) client-ip=156.70.151.37;
Authentication-Results: mx.google.com;
```

First thing to check the genuineness of the sender we have to check SPF (Sender Policy Framework). If the domain is not listed in this policy framework then the receiver side will be marked as spam mail.

Step 2:

```
Wed, 05 Jul 2023 02:53:56 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1688550836; cv=none;
d=google.com; s=arc-20160816;
b=y8K1hza1xIOjVDN0r1fBT/pVGwhY1ZE2IPuqIAhZtetnGF1a+wwK5VGepZwDeqylj
09B1KKzcue00he6PL1L5j3rxLMq2R1YUUPZreaaYu7oFF2KV7qYPO4F9YQcTqL6Phhd+
b2ZpPcSbNtYg+LGtk6pDc9jcs06T/5oy3h9z9iNbGedQR/mJT0V/xKY/Y6W8tmF4Eo6t
xrbtzzfKCyPleOmxvZzapK4RANxAGjDdgHLo72/3oEC4JYk36a7rCyEz904sQpEezP
tTdVb56BknAJwdIqeOhrANyCAibQxcB+ggTWjJ53kf65NmFLJaz/TCnQgeyng6udsK
YV8w==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
h=list-id:unsubscribe:feedback-id:reply-to:campaignid:from
:subject:emailidentifer:isdebug:userid:mime-version:date:message-id
:to:dkim-signature;
bh=ZWwcd10ioshBUeNI2m1KBE1b90apEZfbK+URMNBREffY=;
fh=66EGiaowGzfbqyP2TXdeLEOprkCjs6xoRkm+6jMj+3w=;
b=uYU1x1cm8AAQXh/HA0jdpN19G/mkrD8Q3CKQuRrFnMTSGsx0Fkw40oqTnp3su1q4hy
jWtCaND5E4AP2akeBtKRW57H1wnARg5Xkg8TwQ6K+/rcfUzthZ0/9orhNPIdONobPFg
aPDcC1wamSpCOWIdZ3Kv+mKogy9TD5yiH5Psid1dp5musT54xKz9IQnk94d82IuHGg4
p20PC8v1xwBn/LujusEdHfLJvNSxFH3P7t54G708WZTW/ejGKT6EZR2PMa1JcsKLzYY
m/CqFTFhVUOpVxwZVw66bWP6294Kw06TdjIMEaCPn9DI5I+HbnhxCrezke6SVxtjc2
dbTw==
ARC-Authentication-Results: i=1; mx.google.com;
dkim=pass header.i=@growthschool.io header.s=mailmodo header.b=Dk9eZ2TB;
spf=pass (google.com: domain of msprvs1=19550wb5z5iko=bounces-303287-3967@bounce.mailmodo.email designates 156.70.151.37 as permitted sender)
smtp.mailfrom="msprvs1=19550wb5z5iko=bounces-303287-3967@bounce.mailmodo.email";
dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=growthschool.io
```

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=growthschool.io;
s=mailmodo; t=1688550835; i=@growthschool.io;
bh=ZWwcd10ioshBUeNI2m1KBE1b90apEZfbK+URMNBREffY=;
h=To:Message-ID:Date:Content-Type:Subject:From:List-Unsubscribe:
From:To:Cc:Subject;
b=Dk9eZ2TB5fDtQ/IkyQkkWHOGT32XyUQ6euDYIMARdBuFqOpQ8kn9fZnzWnsttmTu
yJSukOp9FZ5CT0J7+V+LMq2/3BxVQ/WP7JPvTxPrYNMq/h3JH1r3jEIdbVgEcVs78P
u51PtWYdKBWP4uMQroFBiItTFYSzE+4i9wPTtKoE=
To: thejayhack@gmail.com
Message-ID: <9D.0D.25130.3BD35A46@in.mta1vrest.cc.prnd.sparkpost>
Date: Wed, 05 Jul 2023 09:53:55 +0000
Content-Type: multipart/alternative; boundary=" _ ---hkbjxdRZRpg4jEkuukVy1g===_7D/0D-25130-3BD35A46"
MIME-Version: 1.0
Userid: db2926df-fb3b-4ccb-9d49-df9a45df1d4c
Isdebug: false
Emailidentifer: 9f278793-8876-4816-93f3-6ffe339afb1b
Subject: =?utf-8?B?8J+SvCBMYW5kIFlvdXIgRHJlYW0gUE0gSm9iO1BtDjHdGVnaWVz?=
=?utf-8?B?ICYgUmVzb3VyY2Vz?=
From: "GrowthSchool" <hi@growthschool.io>
Campaignid: 6765938c-b117-49a4-b676-a76c9bb59007
Reply-To: eila@growthschool.io
Feedback-ID: 6765938c-b117-49a4-b676-a76c9bb59007:db2926df-fb3b-4ccb-9d49-df9a45df1d4c:HTML:9493b7ce-a665-451a-ac87-0d7cab146de9
List-Unsubscribe: <mailto:unsubscribe@gunsub.spmta.com?subject=unsubscribe:YLSuk_u4bMVTfneAR-8GaJ60imjz2gGp-18bU30gHU~|eyAicmNwdF
1c3RvbWVyX21kIjogIjM4NyIsICJzdWJhY2NvdW50X21kIjogIjM5NjciclCAibWVzc2FnZV9pZCI6ICI2ND1jYjMzZGE1NjQ4N2MyZD1kMCIgfQ~~~>
List-Id: <spc.303287.3967.sparkpostmail.com>
```


DomainKeys Identified Mail (DKIM): is an internet standard that allows an entity to assert responsibility for a message in transit. The entity can be the organization of the author of the message, or a relay.

The tags of the above DKIM-Signature are as follows:

“v” = Indicates the version of the DKIM specification. You should expect to see the value “1” in this field as of this writing.

“a” = The algorithm that was used to create the signature. In this case, it is RSA-SHA256.

“c” = Indicates the canonicalization algorithms that were used for the header and the body. The canonicalization algorithm determines how the body and the header are prepared for hashing—especially as it relates to tolerance for in-transit modification. We will discuss this further below.

In this case, “relaxed/relaxed” indicates that the relaxed canonicalization algorithm was used for both the header and the body. A single value such as “c=relaxed” would have indicated that “relaxed” was used for the header, and “simple” was used for the body—equivalent to “c=relaxed/simple”.

“d” = Indicates the domain claiming responsibility for transmitting the message. This is the domain whose DNS we query to get the public key. In this case, the domain is “growthschool.io”.

“s” = Indicates the selector for the domain. In this case, “s=mailmodo” indicates that we can query the TXT record for mailmodo.growthschool.io to get the public key.

“h” = This tells us which header fields were included in the signature. In this case, the list is Mime-Version, From, Date, Message-ID, Subject, and To. We will use the same list of header fields when verifying the signature.

“bh” = This is the hash of the body of the message after it was canonicalized, in Base64 form.

Convert epoch to human-readable date and vice versa

[\[batch convert\]](#)

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

Assuming that this timestamp is in **seconds**:

GMT : Wednesday, July 5, 2023 9:53:55 AM


Your time zone : Wednesday, July 5, 2023 3:23:55 PM GMT+05:30

Relative : 10 hours ago

“t” is in epoch timestamp. Here 1688550835 is

“Emailidentifier ” is very useful to check spam mail flooding. Every email has a different email identifier but in spam flooding most of them get the same value and by which we can identify the spam mail.

The next thing we should do is to query the signer’s domain and fetch their public key using <https://mxtoolbox.com/>. We will need the d=growthschool.io and s=mailmodo values for this.

 **DKIM Record Lookup**

Domain Name

growthschool.io

Selector ⓘ

mailmodo

DKIM Lookup

And you can see the result below:

SuperTool Beta7

growthschool.io:mailmodo

DKIM Lookup

dkim:growthschool.io:mailmodo

Find Problems

dkim

v=DKIM1;k=rsa;s=email;h=sha256;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQD1c/R+Ee9cyyGqYJfTrLEBXgKz/6jK7YfGp4AQmdHNR6tYk49/27N9GaY+eYhebX8a8P3qxYsdooEFxH098++oNUMbqoSN0FS7B1TbbUgoDMQc32y4bB4Z3x5TlTioCMFDdh/EwYfbYNu19Ij7GuayPhRsocKvh3mtHE91ES10lwIDAQAB

Tag	TagValue	Name	Description
v	DKIM1	Version	Identifies the record retrieved as a DKIM record. It must be the first tag in the record.
k	rsa (Length: 1024 bits)	Key Type	The type of the key used by tag (p).
s	email	Service Type	A colon-separated list of service types to which this record applies.
h	sha256	Hash Algorithms	A colon-separated list of hash algorithms that might be used.
p	MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQD1c/R+Ee9cyyGqYJfTrLEBXgKz/6jK7YfGp4AQmdHNR6tYk49/27N9GaY+eYhebX8a8P3qxYsdooEFxH098++oNUMbqoSN0FS7B1TbbUgoDMQc32y4bB4Z3x5TlTioCMFDdh/EwYfbYNu19Ij7GuayPhRsocKvh3mtHE91ES10lwIDAQAB	Public Key	The syntax and semantics of this tag value before being encoded in base64 are defined by the (k) tag.

	Test	Result
✓	DKIM Record Published	DKIM Record found
✓	DKIM Syntax Check	The record is valid
✓	DKIM Public Key Check	Public key is present

There are lots of fields inter-connected with DKIM signature and other details of header. Although it is great to know how to do so, verifying DKIM signatures manually can get tedious. You can use a number of open-source tools to add some automation to your DKIM verification workflow. If you use Perl, you can check out Mail::DKIM::Verifier. If Python is more your thing, dkimpy is also a good option—be mindful of how multiple DKIM-Signature headers are handled.

This email was genuine, but if you find email suspicious or spam then you can research more on the DMARC field of mail header. You can find more on <https://dmarc.org/>

Step 3: To do quick analyses of email header we can also use <https://toolbox.googleapps.com/>.

MessageId	9D.0D.25130.38035A46@in.mta1vrest.cc.prd.sparkpost
Created at:	7/5/2023, 3:23:55 PM GMT+5:30 (Delivered after 1 sec)
From:	"GrowthSchool" <hi@growthschool.io>
To:	thejayhack@gmail.com
Subject:	Land Your Dream PM Job: Strategies & Resources
SPF:	pass with IP 156.70.151.37 Learn more
DKIM:	pass with domain growthschool.io Learn more
DMARC:	pass Learn more

#	Delay	From *	To *	Protocol	Time received
0	1 sec	mta-70-151-37.sparkpostmail.com.	→ [Google] mx.google.com	ESMTPS	7/5/2023, 3:23:56 PM GMT+5:30
1			→ [Google] 2002:a17:90a:f00c:b0:262:c9f4:141	SMTP	7/5/2023, 3:23:56 PM GMT+5:30
2			→ [Google] 2002:a05:651c:235:0:0:0:0	SMTP	7/5/2023, 3:23:56 PM GMT+5:30

Conclusion:

Learned about how to perform Email Header Analysis using tools like google Toolbox, whois and mxtoolbox.

Learned about different fields and usage of DomainKeys Identified Mail (DKIM). And how to identify spam and genuine mail.