Writeup for NCW CSCCTF 2022
Forensic 1st Challenge - “Chitchat”

```
----------------------------- Questions ----------------------------
1. What's the name of suspected person(attacker) that send the malicious brochure?
(fullname all lower case)
>>

2. What is the attacker's phone number?
[Example Format = +62..........] -> +62 is not the flag fragment
>>

3. How many IPv6 address does the mail have to pass-through to get to the
destination email?
[Sample Answer = 3] -> just a digit/number
>>

4. What is the victim's computer hostname?
>>
---------------------------------------------------------------------
```

First, we are given a file named “`Evidence 51.ost`”.
Yes, of course...with `.ost` extension :)))....`another new thing to be learned :D`

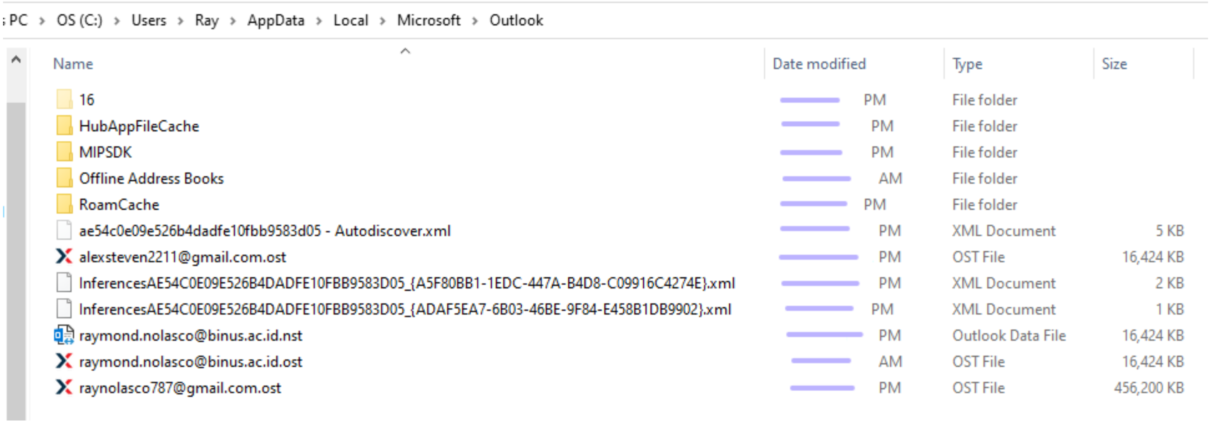
```
---------------------------------------------------------------------
```

[Short explanation]

If any of you didn’t know or never heard about `.ost` extension, you can search it on Google and you will find that it stands for “Offline Storage Table”.

Basically, it is used by Microsoft Outlook to save email messages in a local computer located on *C:\Users\[name]\AppData\Local\Microsoft\Outlook.*

In that directory, if you are using the desktop app for Microsoft Outlook and not through web browser, you will see your `.ost` file along with it's filename which is your account attached to the application. If you're using Outlook from web browser, then there'll be no `.ost` file saved in your local computer.



PC > OS (C:) > Users > Ray > AppData > Local > Microsoft > Outlook

Name	Date modified	Type	Size
16	[redacted] PM	File folder	
HubAppFileCache	[redacted] PM	File folder	
MIPSDK	[redacted] PM	File folder	
Offline Address Books	[redacted] AM	File folder	
RoamCache	[redacted] PM	File folder	
ae54c0e09e526b4dadfe10fbb9583d05 - Autodiscover.xml	[redacted] PM	XML Document	5 KB
alexsteven2211@gmail.com.ost	[redacted] PM	OST File	16,424 KB
InferencesAE54C0E09E526B4DADFE10FBB9583D05_{A5F80BB1-1EDC-447A-B4D8-C09916C4274E}.xml	[redacted] PM	XML Document	2 KB
InferencesAE54C0E09E526B4DADFE10FBB9583D05_{ADAF5EA7-6B03-46BE-9F84-E458B1DB9902}.xml	[redacted] PM	XML Document	1 KB
raymond.nolasco@binus.ac.id.nst	[redacted] PM	Outlook Data File	16,424 KB
raymond.nolasco@binus.ac.id.ost	[redacted] AM	OST File	16,424 KB
raynolasco787@gmail.com.ost	[redacted] PM	OST File	456,200 KB

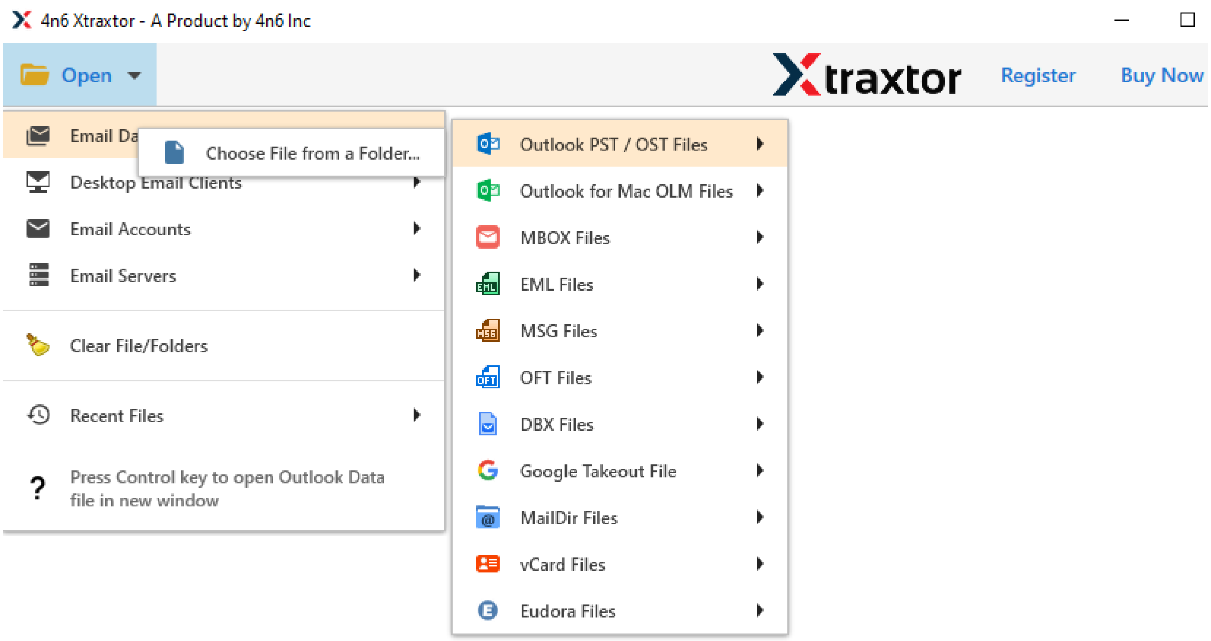
Concerning this .ost file, you might gonna search for online OST viewer or something to view this `.ost` file.

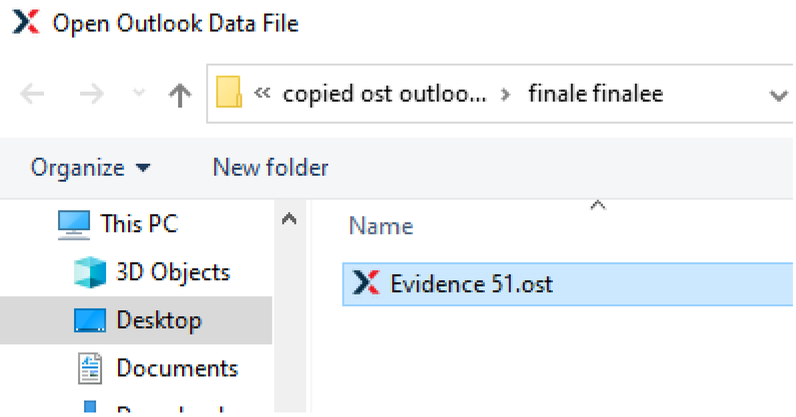
But, if you can take it in a Forensic way, you will think of it like this :

1. I'm given a file with `.ost` extension
2. What is OST? it's an Offline Storage Table specifically for Outlook.
3. It deals with Outlook, now Outlook is with Email thingy.
4. hmm…am i gonna do forensics on email?
5. Is it Email Forensic?
6. Is there a term of Email Forensic either?
7. Oh, yes it is!!!....I am confronted with a challenge of Email Forensic!

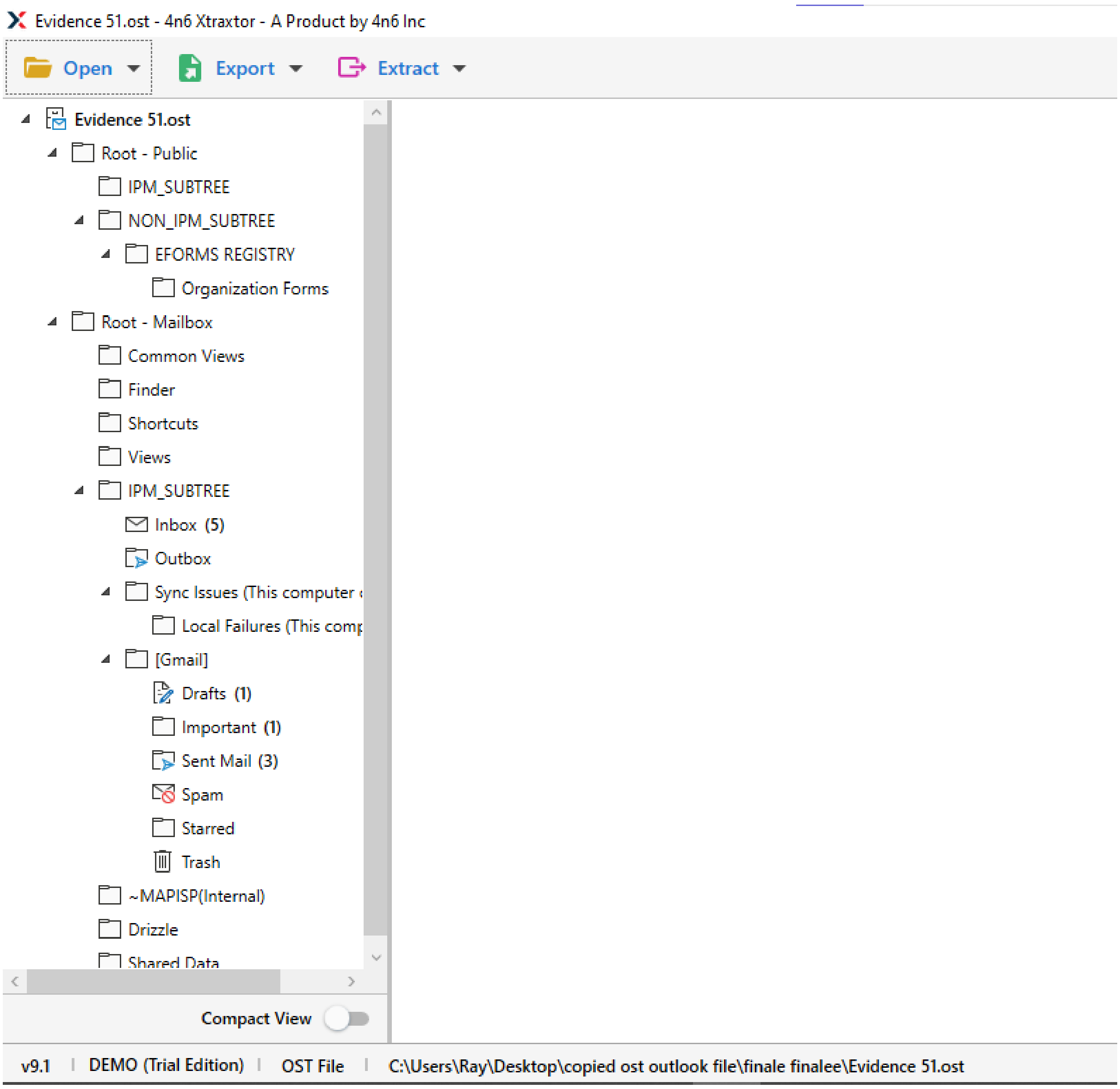
Move on to the next step, now we know that we are dealing with Email Forensic.
So, the first thing we must do is to find a specific email forensic software that can view the .ost file and display all the details of the email for us.
There are many tools out there that you can use. But I prefer to use a software called **"4n6 Xtraxtor"** because it's free and easy to use**.**
→ https://www.xtraxtor.com

Open the "*Evidence 51.ost"* file with Xtraxtor.

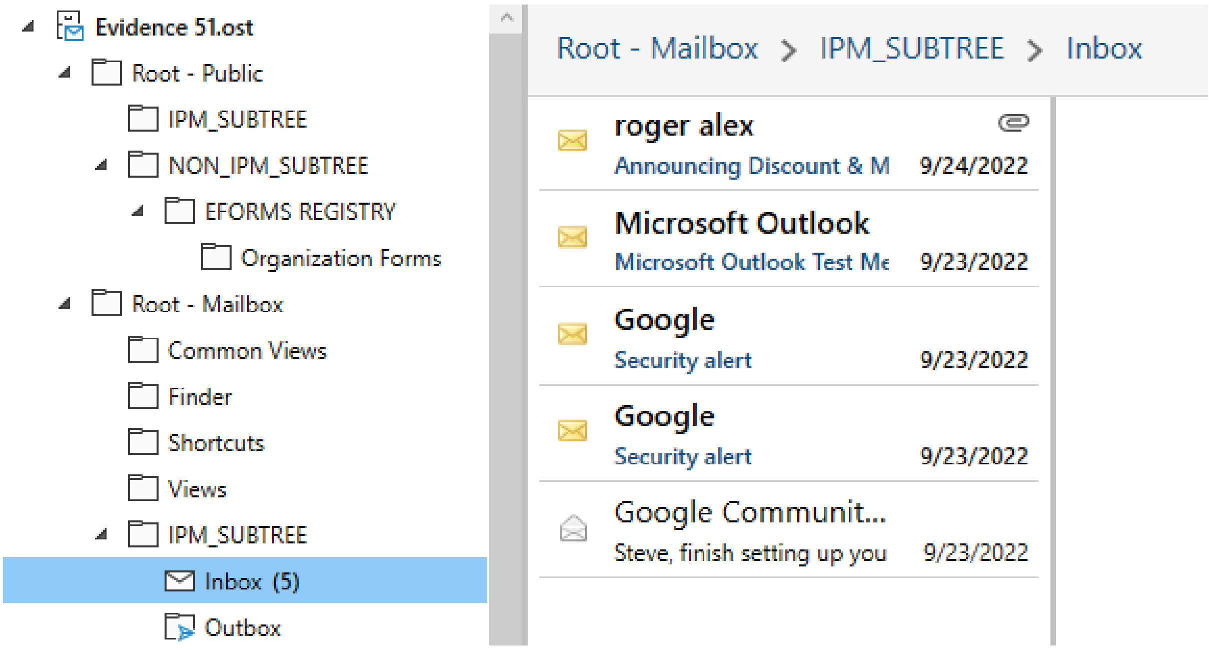




After that, you will see parts of the email’s detail, including the new term like IPM_Subtree and the others, which belongs to Outlook.



Now, because it’s an Email, the basic thing we want to see is obviously the Inbox.



roger alex
Announcing Discount & M 9/24/2022

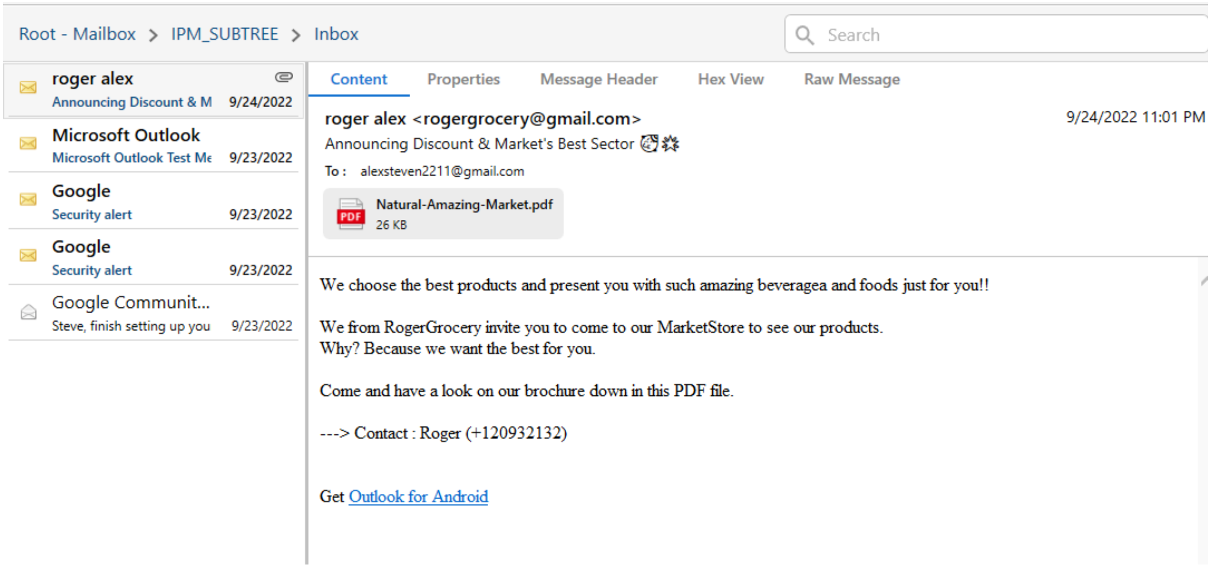
Microsoft Outlook
Microsoft Outlook Test Me 9/23/2022

Google
Security alert 9/23/2022

Google
Security alert 9/23/2022

Google Communit...
Steve, finish setting up you 9/23/2022

There's an email message sent from a person named "roger alex".
Click on it, and the content will be displayed like down below.



roger alex
Announcing Discount & M 9/24/2022

Microsoft Outlook
Microsoft Outlook Test Me 9/23/2022

Google
Security alert 9/23/2022

Google
Security alert 9/23/2022

Google Communit...
Steve, finish setting up you 9/23/2022

roger alex <rogergrocery@gmail.com> 9/24/2022 11:01 PM
Announcing Discount & Market's Best Sector
To : alexsteven2211@gmail.com

Natural-Amazing-Market.pdf
26 KB

We choose the best products and present you with such amazing beveragea and foods just for you!!

We from RogerGrocery invite you to come to our MarketStore to see our products.
Why? Because we want the best for you.

Come and have a look on our brochure down in this PDF file.

---> Contact : Roger (+120932132)

Get Outlook for Android

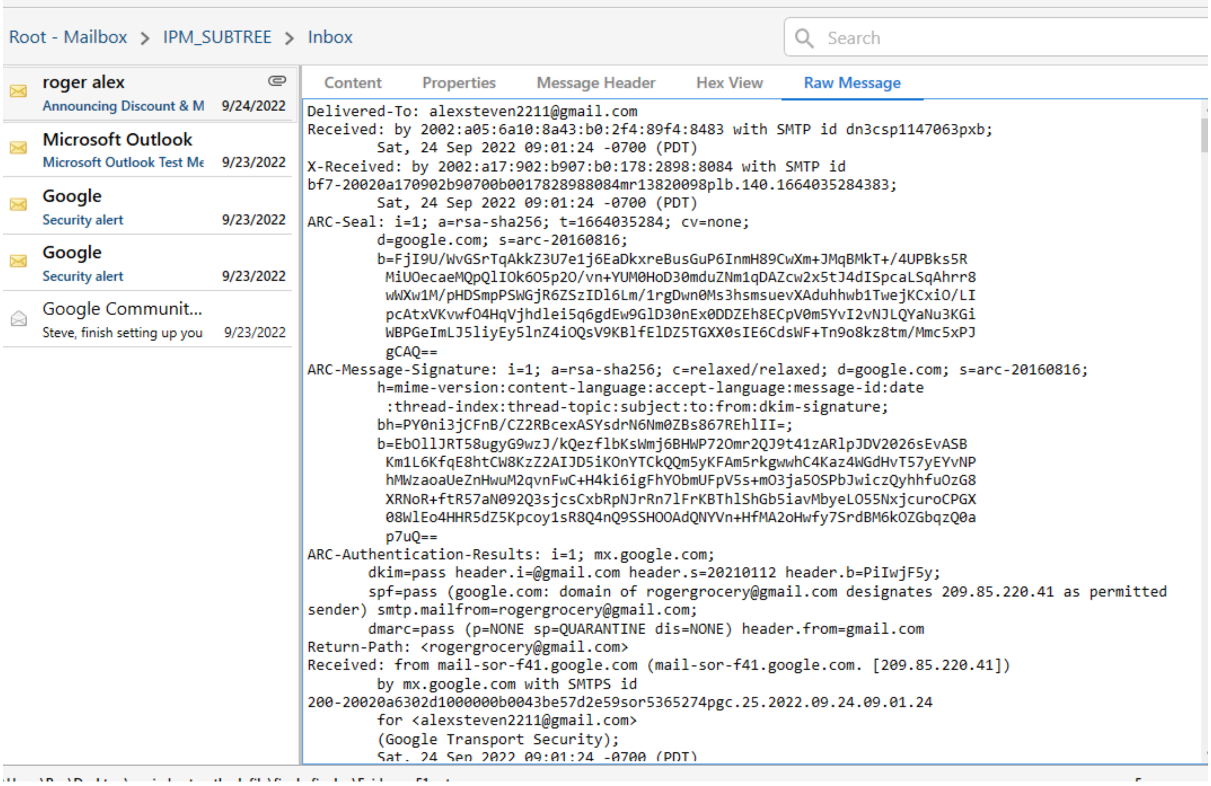
In this challenge, there's only one suspicious message and it's more likely from roger alex with his email "rogergrocery@gmail.com"
But, in real scenario, it will be more difficult because we are faced with .ost file that has thousand and hundreds of thousands of email, like…even my Gmail inbox has more than ten thousands of inbox mail right now :D

Now, we've got the answer for number one and two.
NCW22{roger alex_+120932132_

The next thing we want to look while doing forensic on email, is to see the Email Header which holds the details of the email such like :

1. Where the email will be sent.
2. From where and to where and what method the email will be sent, which is the domain and the IP Address…to be specific.
3. Who is the person that sent the email.
4. Who is the person that receive the email.
5. What's the content of the email.
6. The victim's computer hostname.
7. And much more :D

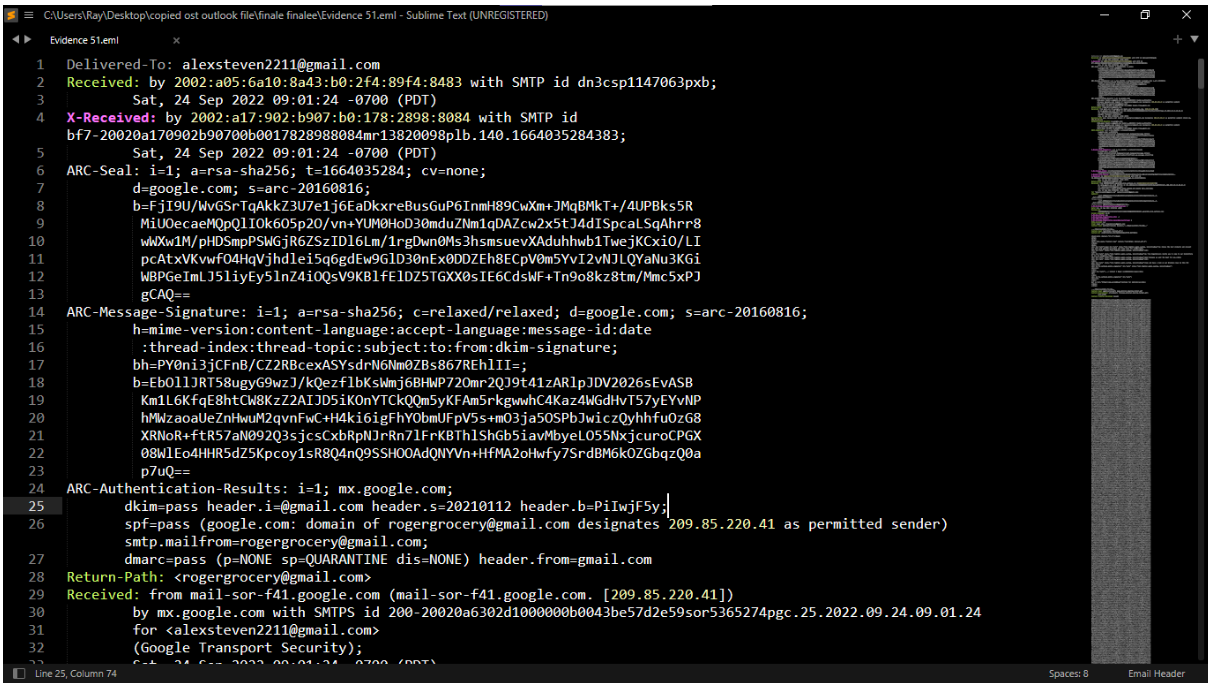
Now we're doing Email Header Analysis, we can go to the right on Xtraxtor app and click on the "`raw message`" tab to see the headers.



```
Delivered-To: alexsteven2211@gmail.com
Received: by 2002:a05:6a10:8a43:b0:2f4:89f4:8483 with SMTP id dn3csp1147063pxb;
        Sat, 24 Sep 2022 09:01:24 -0700 (PDT)
X-Received: by 2002:a17:902:b907:b0:178:2898:8084 with SMTP id
bf7-20020a170902b90700b0017828988084mr13820098plb.140.1664035284383;
        Sat, 24 Sep 2022 09:01:24 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1664035284; cv=none;
        d=google.com; s=arc-20160816;
        b=FjI9U/WvGSrTqAkkZ3U7e1j6EaDkxreBusGuP6InmH89CwXm+JMqBMkT+/4UPBks5R
         MiUOecaeMQpQlIOk6O5p2O/vn+YUM0HoD30mduZNm1qDAZcw2x5tJ4dISpcaLSqAhrr8
         wWXw1M/pHDSmpPSWGjR6ZSzIDl6Lm/1rgDwn0Ms3hsmsuevXAduhhwb1TwejKCxiO/LI
         pcAtxVKvwfO4HqVjhdlei5q6gdEw9GlD30nEx0DDZEh8ECpV0m5YvI2vNJLQYaNu3KGi
         WBPGeImLJ5liyEy5lnZ4iOQsV9KBlfElDZ5TGXX0sIE6CdsWF+Tn9o8kz8tm/Mmc5xPJ
         gCAQ==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=mime-version:content-language:accept-language:message-id:date
         :thread-index:thread-topic:subject:to:from:dkim-signature;
        bh=PY0ni3jCFnB/CZ2RBcexASYsdrN6Nm0ZBs867REhlII=;
        b=EbOllJRT58ugyG9wzJ/kQezflbKsWmj6BHWP72Omr2QJ9t41zARlpJDV2026sEvASB
         Km1L6KfqE8htCW8KzZ2AIJD5iKOnYTCkQQm5yKFAm5rkgwwhC4Kaz4WGdHvT57yEYvNP
         hMWzaoaUeZnHwuM2qvnFwC+H4ki6igFhYObmUFpV5s+mO3ja5OSPbJwiczQyhhfuOzG8
         XRNoR+ftR57aN092Q3sjcsCxbRpNJrRn7lFrKBThlShGb5iavMbyeLO55NxjcuroCPGX
         08WlEo4HHR5dZ5Kpcoy1sR8Q4nQ9SSHOOAdQNYVn+HfMA2oHwfy7SrdBM6kOZGbqzQ0a
         p7uQ==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@gmail.com header.s=20210112 header.b=PiIwjF5y;
       spf=pass (google.com: domain of rogergrocery@gmail.com designates 209.85.220.41 as permitted
sender) smtp.mailfrom=rogergrocery@gmail.com;
       dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
Return-Path: <rogergrocery@gmail.com>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
        by mx.google.com with SMTPS id
200-20020a6302d1000000b0043be57d2e59sor5365274pgc.25.2022.09.24.09.01.24
        for <alexsteven2211@gmail.com>
        (Google Transport Security);
        Sat, 24 Sep 2022 09:01:24 -0700 (PDT)
```

You can analyze the headers from there, but I prefer to see those in Sublime Text with specific plugin, just for colorizing the raw message and for better display.

Down here is the look on Sublime.



C:\Users\Ray\Desktop\copied ost outlook file\finale finalee\Evidence 51.eml - Sublime Text (UNREGISTERED)

Evidence 51.eml

```
Delivered-To: alexsteven2211@gmail.com
Received: by 2002:a05:6a10:8a43:b0:2f4:89f4:8483 with SMTP id dn3csp1147063pxb;
        Sat, 24 Sep 2022 09:01:24 -0700 (PDT)
X-Received: by 2002:a17:902:b907:b0:178:2898:8084 with SMTP id
bf7-20020a170902b90700b0017828988084mr13820098plb.140.1664035284383;
        Sat, 24 Sep 2022 09:01:24 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1664035284; cv=none;
        d=google.com; s=arc-20160816;
        b=FjI9U/WvGSrTqAkkZ3U7e1j6EaDkxreBusGuP6InmH89CwXm+JMqBMkT+/4UPBks5R
         MiUOecaeMQpQlIOk6O5p2O/vn+YUM0HoD30mduZNm1qDAZcw2x5tJ4dISpcaLSqAhrr8
         wWXw1M/pHDSmpPSWGjR6ZSzIDl6Lm/1rgDwn0Ms3hsmsuevXAduhhwb1TwejKCxiO/LI
         pcAtxVKvwfO4HqVjhdlei5q6gdEw9GlD30nEx0DDZEh8ECpV0m5YvI2vNJLQYaNu3KGi
         WBPGeImLJ5liyEy5lnZ4iOQsV9KBlfElDZ5TGXX0sIE6CdsWF+Tn9o8kz8tm/Mmc5xPJ
         gCAQ==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=mime-version:content-language:accept-language:message-id:date
         :thread-index:thread-topic:subject:to:from:dkim-signature;
        bh=PY0ni3jCFnB/CZ2RBcexASYsdrN6Nm0ZBs867REhlII=;
        b=EbOllJRT58ugyG9wzJ/kQezflbKsWmj6BHWP72Omr2QJ9t41zARlpJDV2026sEvASB
         Km1L6KfqE8htCW8KzZ2AIJD5iKOnYTCkQQm5yKFAm5rkgwwhC4Kaz4WGdHvT57yEYvNP
         hMWzaoaUeZnHwuM2qvnFwC+H4ki6igFhYObmUFpV5s+mO3ja5OSPbJwiczQyhhfuOzG8
         XRNoR+ftR57aN092Q3sjcsCxbRpNJrRn7lFrKBThlShGb5iavMbyeLO55NxjcuroCPGX
         08WlEo4HHR5dZ5Kpcoy1sR8Q4nQ9SSHOOAdQNYVn+HfMA2oHwfy7SrdBM6kOZGbqzQ0a
         p7uQ==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@gmail.com header.s=20210112 header.b=PiIwjF5y;
       spf=pass (google.com: domain of rogergrocery@gmail.com designates 209.85.220.41 as permitted sender)
       smtp.mailfrom=rogergrocery@gmail.com;
       dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
Return-Path: <rogergrocery@gmail.com>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
        by mx.google.com with SMTPS id 200-20020a6302d1000000b0043be57d2e59sor5365274pgc.25.2022.09.24.09.01.24
        for <alexsteven2211@gmail.com>
        (Google Transport Security);
        Sat, 24 Sep 2022 09:01:24 -0700 (PDT)
```

Line 25, Column 74

For basic analyzation and easy challenge, we are asked about..

`How many IPv6 address does the mail have to pass-through to get to the destination email?`

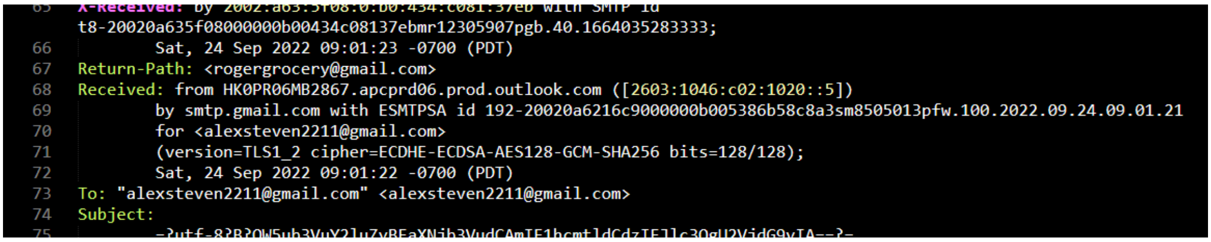
With Sublime Text and plugin called “Email Header” and saving all the raw message into a file with `.eml` extension, we can see the header’s colorization, making us easy to see things like IP Address which is colored with light-yellow.

Now to see “from where and to where the email has been delivered”, we can **focus on the “Received” header with green color.**

First thing we must know that, **the more upper** the “Received” header is…**the more it’s close to the destination** email. But the **more lower**, **the more it’s close to the source** email.

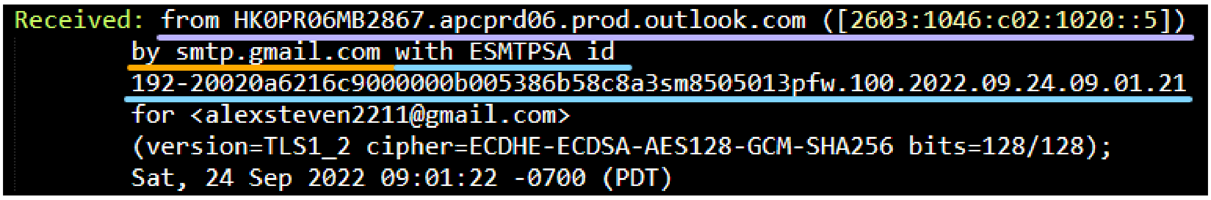
Because of this, we must find the most lowest “Received” header.

Down here is the lowest.



```
X-Received: by 2002:a63:5f08:0:b0:434:c081:37eb with SMTP id
t8-20020a635f08000000b00434c08137ebmr12305907pgb.40.1664035283333;
        Sat, 24 Sep 2022 09:01:23 -0700 (PDT)
Return-Path: <rogergrocery@gmail.com>
Received: from HK0PR06MB2867.apcprd06.prod.outlook.com ([2603:1046:c02:1020::5])
        by smtp.gmail.com with ESMTPSA id 192-20020a6216c9000000b005386b58c8a3sm8505013pfw.100.2022.09.24.09.01.21
        for <alexsteven2211@gmail.com>
        (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
        Sat, 24 Sep 2022 09:01:22 -0700 (PDT)
To: "alexsteven2211@gmail.com" <alexsteven2211@gmail.com>
Subject:
        =?utf-8?B?QW5ub3VuY2luZyBFaXNjb3VudCAmIE1hcmtldCdzIE1lc3QgU2VidG9yIA==?=
```

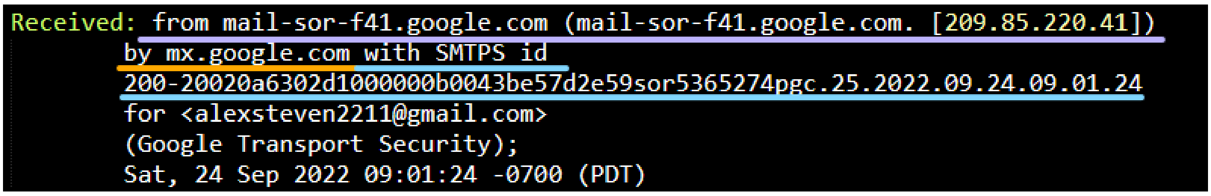
Now that we found the most close to the source email, we must read the Fully-Qualified-Domain-Name with it’s IP Address which stated on the header *(Sometimes, the FQDN is not stated, only the IP Address but that’s okay)*



```
Received: from HK0PR06MB2867.apcprd06.prod.outlook.com ([2603:1046:c02:1020::5])
        by smtp.gmail.com with ESMTPSA id
        192-20020a6216c9000000b005386b58c8a3sm8505013pfw.100.2022.09.24.09.01.21
        for <alexsteven2211@gmail.com>
        (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
        Sat, 24 Sep 2022 09:01:22 -0700 (PDT)
```

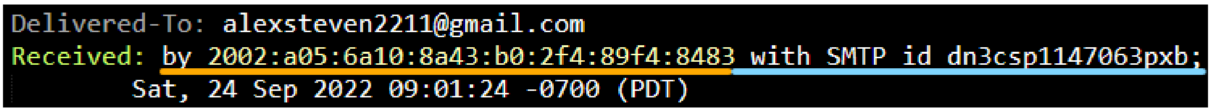
1. `HK0PR06MB2867.apcprd06.prod.outlook.com ([2603:1046:c02:1020::5])`
2. `smtp.gmail.com`

(From here, go to the next “Received” header. Scroll up up up!)



```
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
        by mx.google.com with SMTPS id
        200-20020a6302d1000000b0043be57d2e59sor5365274pgc.25.2022.09.24.09.01.24
        for <alexsteven2211@gmail.com>
        (Google Transport Security);
        Sat, 24 Sep 2022 09:01:24 -0700 (PDT)
```

3. `mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])`
4. `mx.google.com`



```
Delivered-To: alexsteven2211@gmail.com
Received: by 2002:a05:6a10:8a43:b0:2f4:89f4:8483 with SMTP id dn3csp1147063pxb;
        Sat, 24 Sep 2022 09:01:24 -0700 (PDT)
```

5. `2002:a05:6a10:8a43:b0:2f4:89f4:8483`

If you don’t understand why that’s the answer, kindly study about Email Forensic and IPv6 Address Format down on these links:
https://www.youtube.com/watch?v=nK5QpGSBR8c&t=1185s
https://www.tutorialspoint.com/ipv6/ipv6_address_types.htm
https://study-ccna.com/ipv6-address-format/

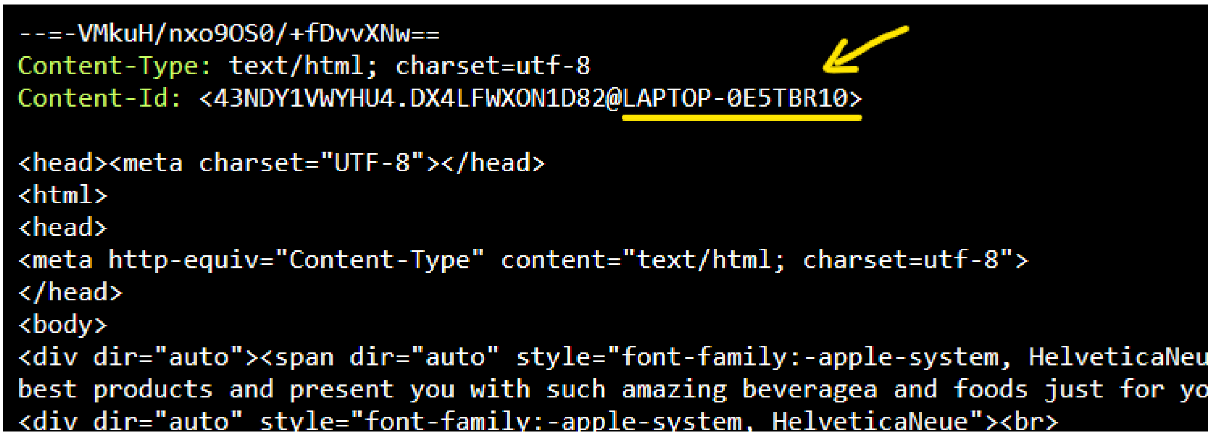
And you can use this website to see the IPv6 details to confirm the domain’s name.
https://nerdiess.com/t/ip-address-check

Now, we’ve got the answer for number three.
NCW22{roger alex_+120932132_5_

For the last answer, we still have to deal with the Email Header.
You can read all the headers even if you don’t understand what it means.

Usually, it’s located on the Content-ID.

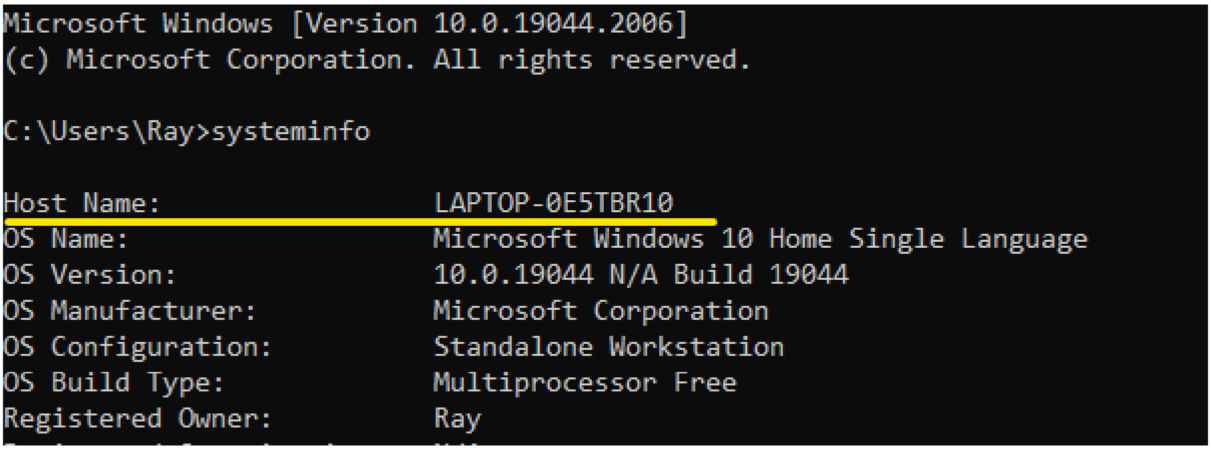
(If you have any idea about the Content-ID which definition is included in MIME, kindly share your thoughts, yes? Because there’s not much sources out there that gives a straight-forward explanation about this)



```
--=-VMkuH/nxo9OS0/+fDvvXNw==
Content-Type: text/html; charset=utf-8
Content-Id: <43NDY1VWYHU4.DX4LFWXON1D82@LAPTOP-0E5TBR10>

<head><meta charset="UTF-8"></head>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
</head>
<body>
<div dir="auto"><span dir="auto" style="font-family:-apple-system, HelveticaNeu
best products and present you with such amazing beveragea and foods just for yo
<div dir="auto" style="font-family:-apple-system, HelveticaNeue"><br>
```

(That’s my computer hostname :D, down below is the confirmation)



```
Microsoft Windows [Version 10.0.19044.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Ray>systeminfo

Host Name:                 LAPTOP-0E5TBR10
OS Name:                   Microsoft Windows 10 Home Single Language
OS Version:                10.0.19044 N/A Build 19044
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Ray
```

Now, we’ve got the last answer, number four.

FLAG = NCW22{roger alex_+120932132_5_LAPTOP-0E5TBR10}

------------------------------ DONE ------------------------------