CSE 4004

Digital Forensics

Lab
Session 14

TOPIC: Email forensics

Name: Makesh Srinivasan
Registration number: 19BCE1717
Slot: L49 + L50
Date: 2-December-2021-Thursday
Faculty: Prof. Nagaraj

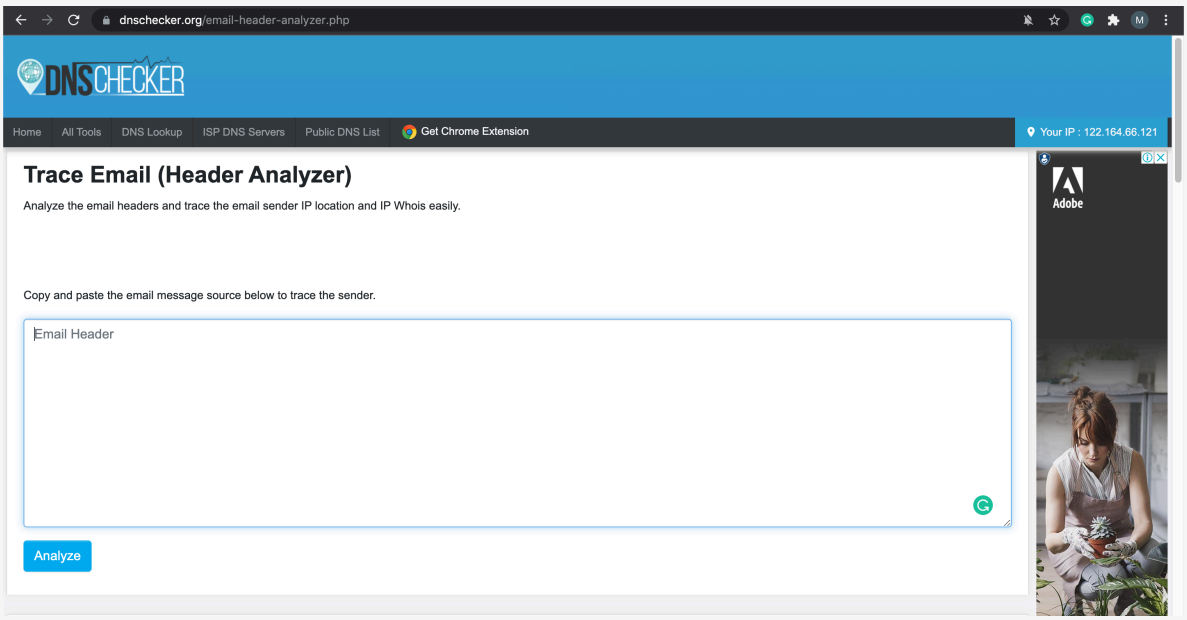
AIM: Analysing the Emails and its contents

Email has become one of the important means of communication in today's world. However, emails can be faked. Analysis of email headers provides useful leads for investigators. There are number of online tools that are useful for email header analysis. For example, https://dnschecker.org/email-header-analyzer.php
Perform analysis on the attached email header and submit screen shots

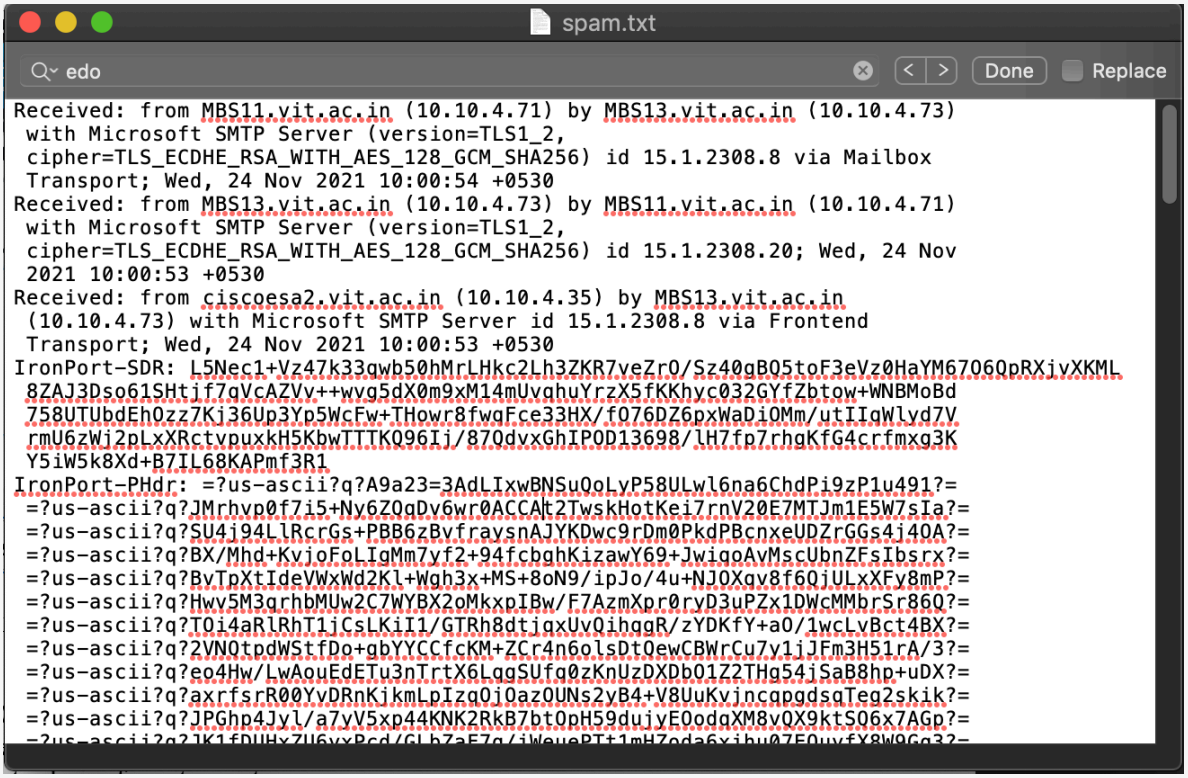
PROCEDURE:

1. Open up a browser and search for email forensics tool. For this exercise, I have used https://dnschecker.org/email-header-analyzer.php
2. Copy and paste the email to be analysed
3. Click on "Analyse"

OBSERVATION:

Email forensics observation
Go to this Webpage: https://dnschecker.org/email-header-analyzer.php

Copy and paste the email from the spam.txt file

Email forensics observation



Paste the email content:

X-MS-Exchange-Organization-AVStamp-Enterprise: 1.0
X-Loop: 1
X-MS-Exchange-Organization-AuthSource: MBS13.vit.ac.in
X-MS-Exchange-Organization-AuthAs: Anonymous
X-MS-Exchange-Transport-EndToEndLatency: 00:00:00.3299808
X-MS-Exchange-Processed-By-BccFoldering: 15.01.2308.008

Analyze

Click on Analyse

Email Source Ip Info	
Source IP Address	102.89.2.124
Source IP Hostname	102.89.2.124
Country	Nigeria
State	Edo
City	Benin City
Zip Code	null
Latitude	6.3381
Longitude	5.6257
ISP	Mtnn-Ojota-Region
Organization	Mtnn-Ojota-Region
Threat Level	low

Email forensics observation

```
% This is the AfriNIC Whois server.
% The AFRINIC whois database is subject to  the following terms of Use. See https://afrinic.net/whois/terms

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '102.89.0.0 - 102.89.31.255'

% No abuse contact registered for 102.89.0.0 - 102.89.31.255

inetnum:        102.89.0.0 - 102.89.31.255
netname:        MTNN-OJOTA-REGION-PREFIXES
descr:          MTNN-OJOTA-REGION-PREFIXES
country:        NG
admin-c:        BRM1-AFRINIC
tech-c:         ISP1-AFRINIC
status:         ASSIGNED PA
mnt-by:         MTNNIGERA1-MNT
source:         AFRINIC # Filtered
parent:         102.88.0.0 - 102.95.255.255

person:         Business Risk Management
address:        Golden Plaza Building, Falomo roundabout, ikoyi
phone:          +08031230141
nic-hdl:        BRM1-AFRINIC
abuse-mailbox:  abuse@mtnnigeria.net
```

```
person:         Business Risk Management
address:        Golden Plaza Building, Falomo roundabout, ikoyi
phone:          +08031230141
nic-hdl:        BRM1-AFRINIC
abuse-mailbox:  abuse@mtnnigeria.net
mnt-by:         GENERATED-5DN7BDIQBRY0JCMBEE6EBZSP56LLR9GU-MNT
source:         AFRINIC # Filtered

person:         Internet Services Planning
nic-hdl:        ISP1-AFRINIC
address:        Yellodrome building, adeola hopewell street, Victoria island
address:        Lagos
address:        Other
phone:          tel:+234-803-123-0141
mnt-by:         MTNNIGERA1-MNT
source:         AFRINIC # Filtered
```

All necessary screenshots are taken

INFERENCE:
According to the online tool, we see that the email has originated from Benin city, Nigeria, and the coordinates and other information are shown in the image above. We can also see the source IP address and the level of threat (Low)

CONCLUSION:
Thus, we have seen email forensics for a sample email given.