Digital Forensics - Lab 14

Class No :	**CH2021221000516**	Slot :	**L49 + L50**
Course Code :	**CSE4004**	Faculty Name :	**Nagaraj SV**

Aadhitya Swarnesh

- 2 December 2021

Question 1 :

Email forensics

Perform analysis on the attached email header and report your findings.

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

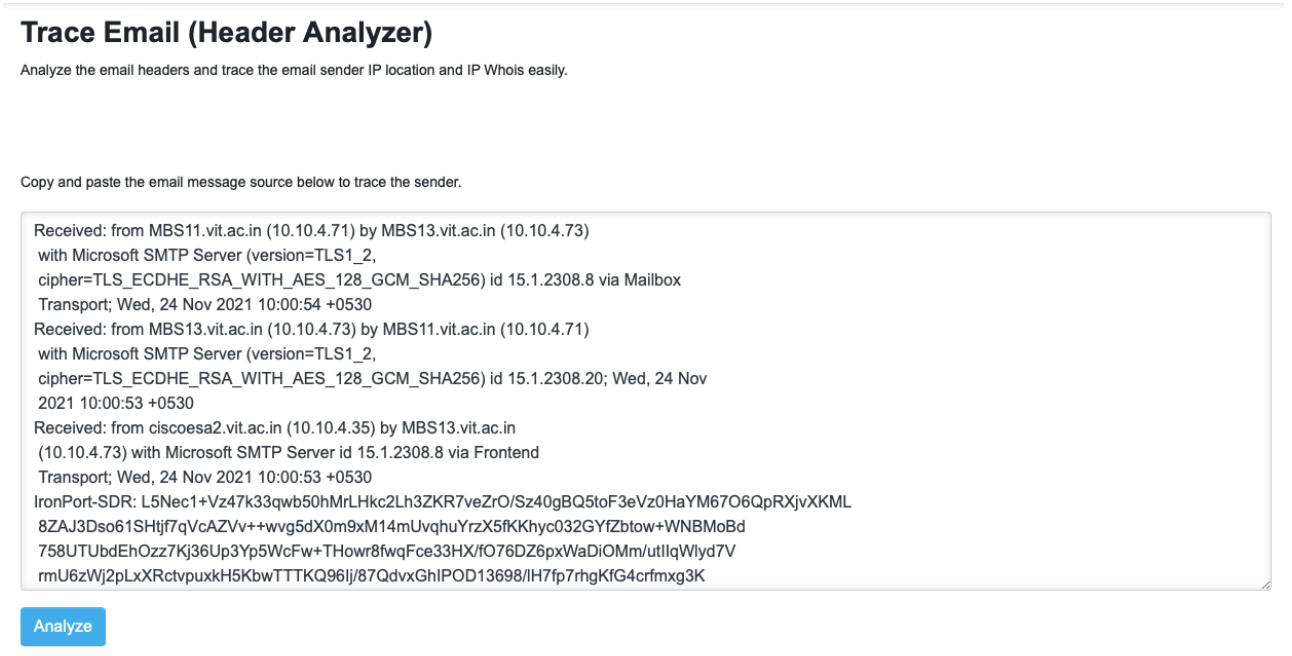
In this lab, we will use the forensic tools available to study emails, especially the headers to gain more information and details about the emails. We can gain knowledge about the sender, the recipient, their email addresses, the time in which the mail was sent, and even the network information of the people involved. These details can prove to be vital to any forensic investigations in this current age of technological advancement.

We have been provided with a email header information in the form of a text file which we will be using to figure out more information on the people involved. We will be using the website mentioned above which helps us to decode the header data and give more overall presentable data in a format which is easily understandable.

The following image shows the email header which has been provided to us for analysis :

```
Received: from MBS11.vit.ac.in (10.10.4.71) by MBS13.vit.ac.in (10.10.4.73)
 with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.2308.8 via Mailbox
 Transport; Wed, 24 Nov 2021 10:00:54 +0530
Received: from MBS13.vit.ac.in (10.10.4.73) by MBS11.vit.ac.in (10.10.4.71)
 with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.2308.20; Wed, 24 Nov
 2021 10:00:53 +0530
Received: from ciscoesa2.vit.ac.in (10.10.4.35) by MBS13.vit.ac.in
 (10.10.4.73) with Microsoft SMTP Server id 15.1.2308.8 via Frontend
 Transport; Wed, 24 Nov 2021 10:00:53 +0530
IronPort-SDR: L5Nec1+Vz47k33qwb50hMrLHkc2Lh3ZKR7veZrO/Sz40gBQ5toF3eVz0HaYM67O6QpRXjvXKML
 8ZAJ3Dso61SHtjf7qVcAZVv++wvg5dX0m9xM14mUvqhuYrzX5fKKhyc032GYfZbtow+WNBMoBd
 758UTUbdEhOzz7Kj36Up3Yp5WcFw+THowr8fwqFce33HX/fO76DZ6pxWaDiOMm/utIIqWlyd7V
 rmU6zWj2pLxXRctvpuxkH5KbwTTTKQ96Ij/87QdvxGhIPOD13698/lH7fp7rhgKfG4crfmxg3K
 Y5iW5k8Xd+B7IL68KAPmf3R1
IronPort-PHdr: =?us-ascii?q?A9a23=3AdLIxwBNSuQoLyP58ULwl6na6ChdPi9zP1u491?=
 =?us-ascii?q?JMrhvp0f7i5+Ny6ZQqDv6wr0ACCAt2TwskHotKei7rnV20E7MTJm1E5W7sIa?=
 =?us-ascii?q?SU4j94LlRcrGs+PBB6zBvfraysnAJYKDwc9rDm0PkdPBcnxeUDZrGGs4j4OA?=
 =?us-ascii?q?BX/Mhd+KvjoFoLIgMm7yf2+94fcbghKizawY69+JwiqoAvMscUbnZFsIbsrx?=
 =?us-ascii?q?BvTpXtIdeVWxWd2Kl+Wgh3x+MS+8oN9/ipJo/4u+NJOXqv8f6QjULxXFy8mP?=
 =?us-ascii?q?Hwv5M3qrhbMUw2C7WYBX2oMkxpIBw/F7AzmXpr0ryD3uPZx1DWcMMbrSr86Q?=
 =?us-ascii?q?TOi4aRlRhT1jCsLKiI1/GTRh8dtjqxUvQihqgR/zYDKfY+aO/1wcLvBct4BX?=
 =?us-ascii?q?2VNQtpdWStfDo+gbYYCCfcKM+ZCr4n6olsDtQewCBWrCu7y1jJFm3H51rA/3?=
 =?us-ascii?q?eo4Hw/LwAouEdETu3nTrtX6LqgSUfq0zKnUzDXDbO1Z2THg54jSaB8hp+uDX?=
 =?us-ascii?q?axrfsrR00YvDRnKjkmLpIzqOjOazOUNs2yB4+V8UuKvjncqpgdsqTeg2skik?=
 =?us-ascii?q?JPGhp4Jyl/a7yV5xp44KNK2RkB7btOpH59dujyEOodqXM8vQX9ktSQ6x7AGp?=
 =?us-ascii?q?JK1fDUHxZU6yxPcd/GLbZaF7g/jWeuePTt1mHZoda6xihu07EOuyfX8W9Gq3?=
```

We will now proceed to the aforementioned online tool and insert this header into the space available as shown below :



On clicking the analyst button available there, the tool parses the header for data and then presents them in precise readable format as follows :

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	medium

By this table, we can figure out the key information about the email header which is the IP address of the sender, by which we can approximately track the location from which this mail was sent.

This tool also provides more useful data which is based on the IP address which was extracted from the header. These as shown below :

WHOIS Lookup Info

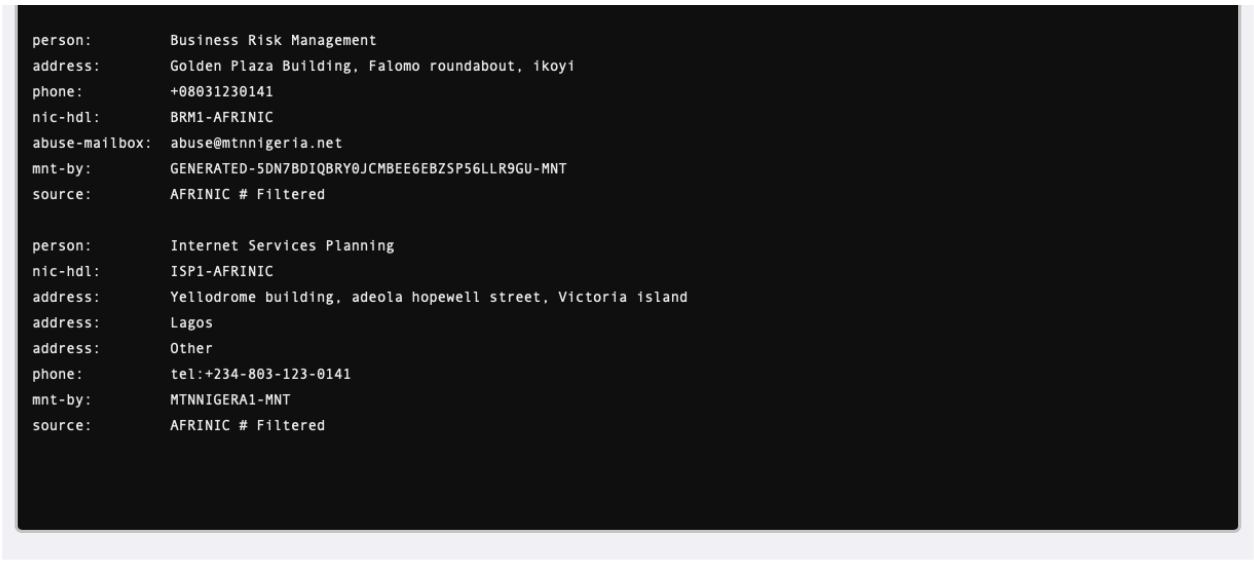
```
% This is the AfriNIC Whois server.
% The AFRINIC whois database is subject to  the following terms of Use. See https://afrinic.net/whois/terms

% 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
```



Thus, we have analyzed the header of this email, and have gotten to the roots of its origination. In this manner this online tool can easily be used to analyze the header of such emails. We have also gotten to know the sender's address, their service providers, and also their geological coordinates for the email's origination.

CONCLUSION

In this lab experiments, we have dealt with and seen email headers which provide useful functionalities for ease of forensic analysis. This is especially a booming field of digital forensics, as we humans rely on emails and other such forms of such communications. Thus it is imperative for forensic investigators to efficiently extract all required details from such email headers which might prove useful in investigations.