

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 message source below to trace the sender.

Email Header

Analyze

Your IP : 122.164.66.121

Adobe

Copy and paste the email from the spam.txt file

Email forensics observation

```
spam.txt
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+Vz47k33qwb50hMrLHkc2lh3ZKR7veZr0/Sz40qB05toF3eVz0HaYM67060pRXjvXKML
8ZAJ3Dso61Shtif7gVCAZVv++wvg5dX0m9xM14mUvghuYrzX5fKKhyc032GYfZbtow+WNBMoBd
758UTUbdeH0zz7Kj36Up3WcFwtTHour8fwgFce33HX/f076DZ6pxWaDiOMM+utTIqWlyd7V
rmU6zWj2pLxXRctvpxukH5KbwTTTK096Ij/870dvxGhIP0D13698/lH7fp7rhgKfG4crfmxq3K
Y5iW5k8Xd+B7IL68KAfPmf3R1
IronPort-PHdr: =?us-ascii?q?A9a23=3AdLTixwBNSu0oLyP58ULwl6na6ChdPi9zP1u491?= =?us-ascii?q?JMrvp0f7i5+Ny6ZQoDv6wr0ACCAt2TwskHotKei7rnV20E7MTJm1E5W7sIa?= =?us-ascii?q?SU4j94LlRcrGs+PBB6zBvfraysnAJYKDwc9rPm0PkdBcneUDZrGGs4140A?= =?us-ascii?q?BX/Mhd+KvjoFolIgMm7yf2+94fcbgkhKizawY69+JwigoAvMscUbnZFsTbsrx?= =?us-ascii?q?BvTpXtIdeWxWd2K1+Wgh3x+MS+8oN9/ipJo/4u+Nj0Xqv8f60jULxFv8mP?= =?us-ascii?q?Hwv5M3grhbMUw2CZYBX2oMkxpIBw/F7AzmXpr0ryD3uPZx1DWcMMrSr86Q?= =?us-ascii?q?T0i4aR1RhT1iCsLK1i1/GTRh8dtjqxUv0ihqqr/zYDKfY+a0/1wcLvBct4BX?= =?us-ascii?q?2VN0tpdWStfDo+gbYCCfcKM+ZCr4n6olsDt0ewCBWrCu7y1jJFm3H51rA/3?= =?us-ascii?q?eo4Hw/LwAoqEdETu3nTrtX6LqgSUfq0zKnUzDxDbo1Z2THg54jSaB8hp+uDX?= =?us-ascii?q?axrfssrR00YvDRnKikmlpIzq0i0az0UNs2yB4+V8UuKvincapgdsgTeg2skik?= =?us-ascii?q?JPGhp4jyl/a7yV5xp44KNK2RkB7bt0pH59duijyE0odaXM8v0X9ktS06x7AGp?= =?us-ascii?2g?JK1fDUHx7IU6vxPcd/CLh7aE7g/iWeuePTt1mHzoda6xjhv07E0uvfx8WQg32-
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
```

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.