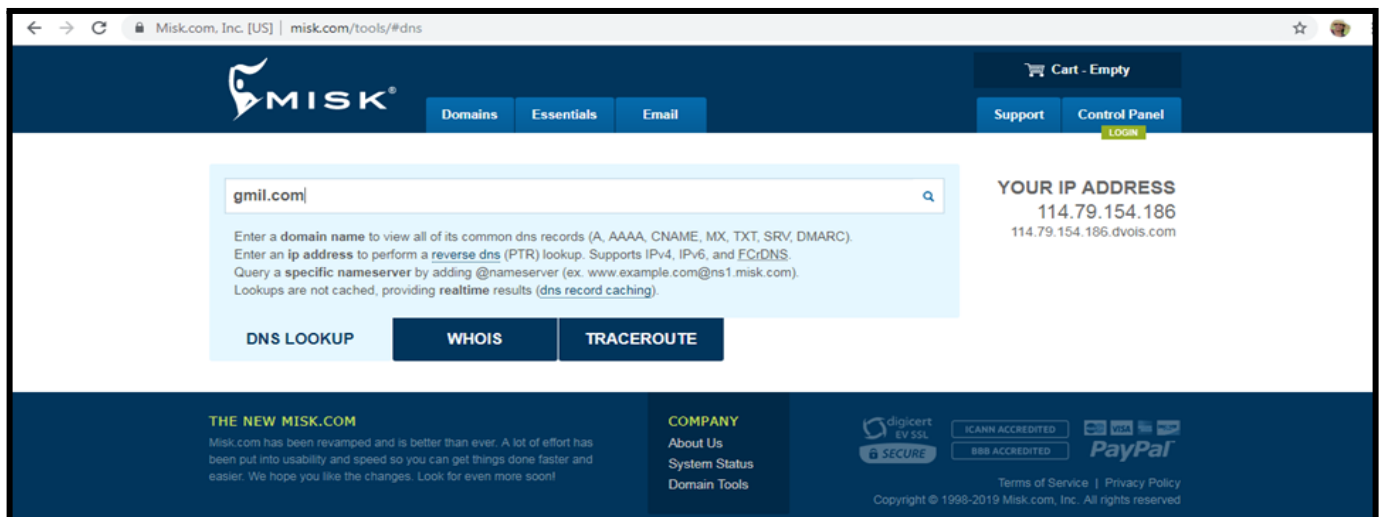


Practical No. 09

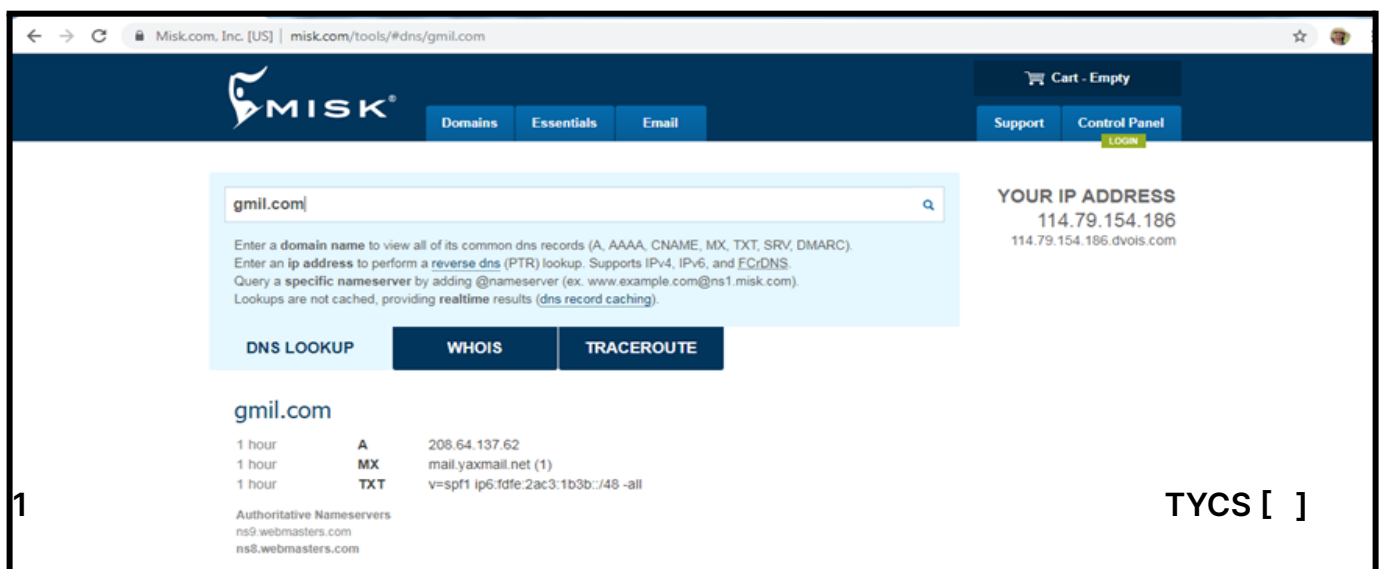
AIM - Email Forensics.

9.1 Mail Service Providers -

1. Go to “<https://www.misk.com/tools/#dns>” then enter your domain name e.g. gmail.com. Press enter and see the details.

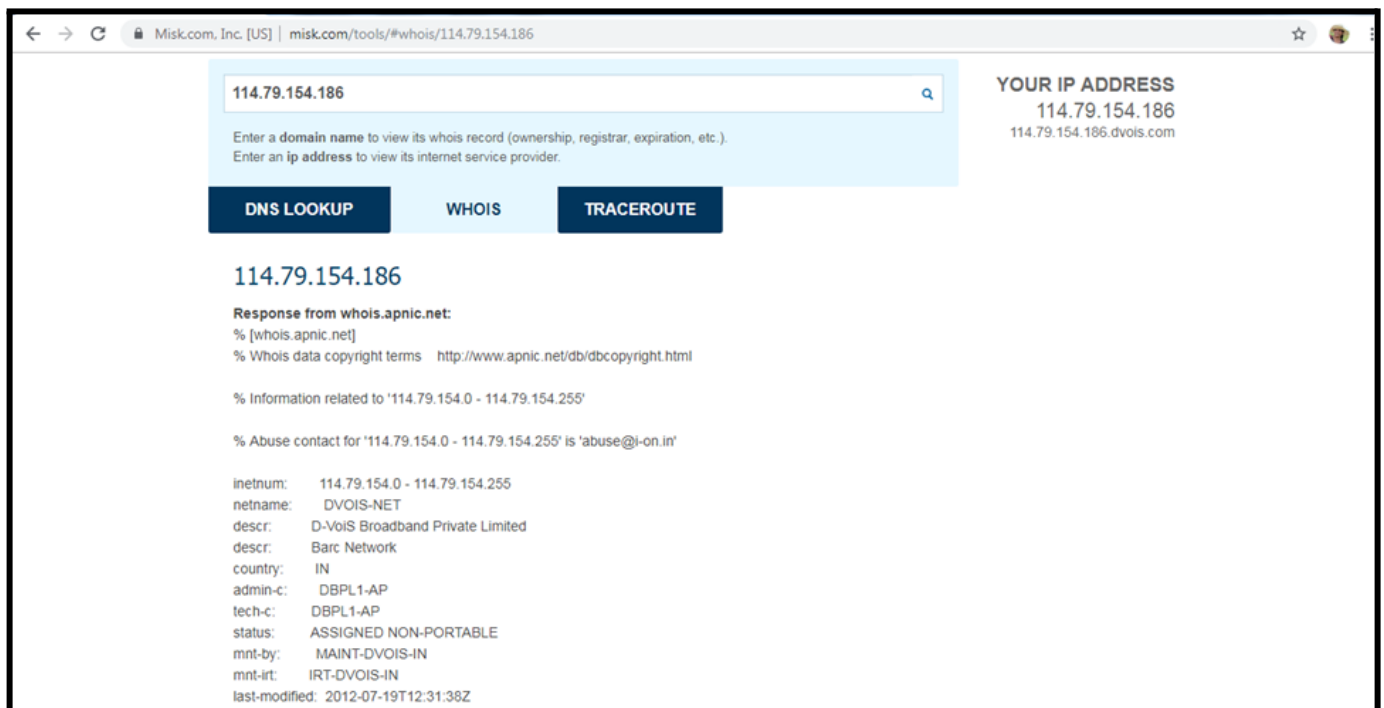


Look for the MX record and observe the name to the right of it, which is the domain's email provider e.g.(mail.yaxmail.net). You can contact this company or one listed as the nameservers in regards to the domain's email.



2. IP (Internet Protocol) “whois” →

Copy the IP address and perform “**whois**” search to Find the Company providing service for that IP address.



The screenshot shows a web browser window with the URL `misk.com/tools/#whois/114.79.154.186`. The page features a search bar with the IP address `114.79.154.186` entered. Below the search bar are three tabs: **DNS LOOKUP**, **WHOIS** (selected), and **TRACEROUTE**. The **WHOIS** tab displays the following information:

114.79.154.186

Response from whois.apnic.net:
% [whois.apnic.net]
% Whois data copyright terms <http://www.apnic.net/db/dbcopyright.html>

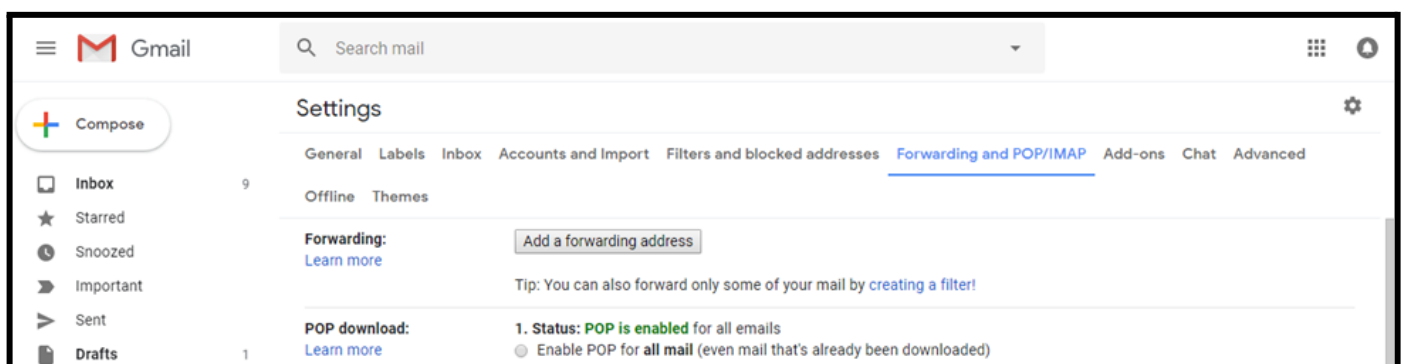
% Information related to '114.79.154.0 - 114.79.154.255'
% Abuse contact for '114.79.154.0 - 114.79.154.255' is 'abuse@i-on.in'

inetnum: 114.79.154.0 - 114.79.154.255
netname: DVOIS-NET
descr: D-VoiS Broadband Private Limited
descr: Barc Network
country: IN
admin-c: DBPL1-AP
tech-c: DBPL1-AP
status: ASSIGNED NON-PORTABLE
mnt-by: MAINT-DVOIS-IN
mnt-irt: IRT-DVOIS-IN
last-modified: 2012-07-19T12:31:38Z

On the right side of the page, it displays **YOUR IP ADDRESS** as `114.79.154.186` with the domain `114.79.154.186.dvois.com`.

9.2 Email Protocols -

On the computer, Open Gmail. In the top right, → Click “**Settings**” → then click the forwarding and “**POP/IMAP**” tab



The screenshot shows the Gmail interface with the **Settings** page open. The **Forwarding and POP/IMAP** tab is selected. The page displays the following settings:

Forwarding: [Learn more](#)

Tip: You can also forward only some of your mail by [creating a filter](#)!

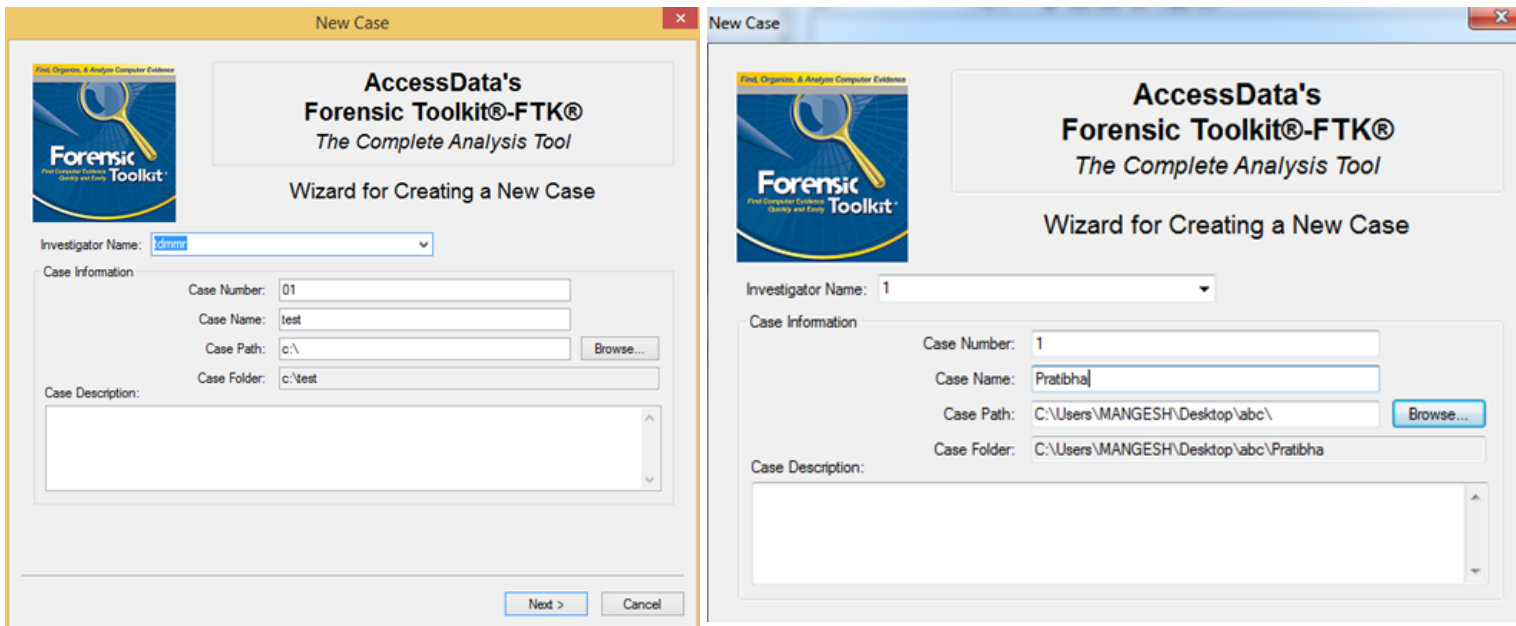
POP download: [Learn more](#)

1. Status: **POP is enabled** for all emails

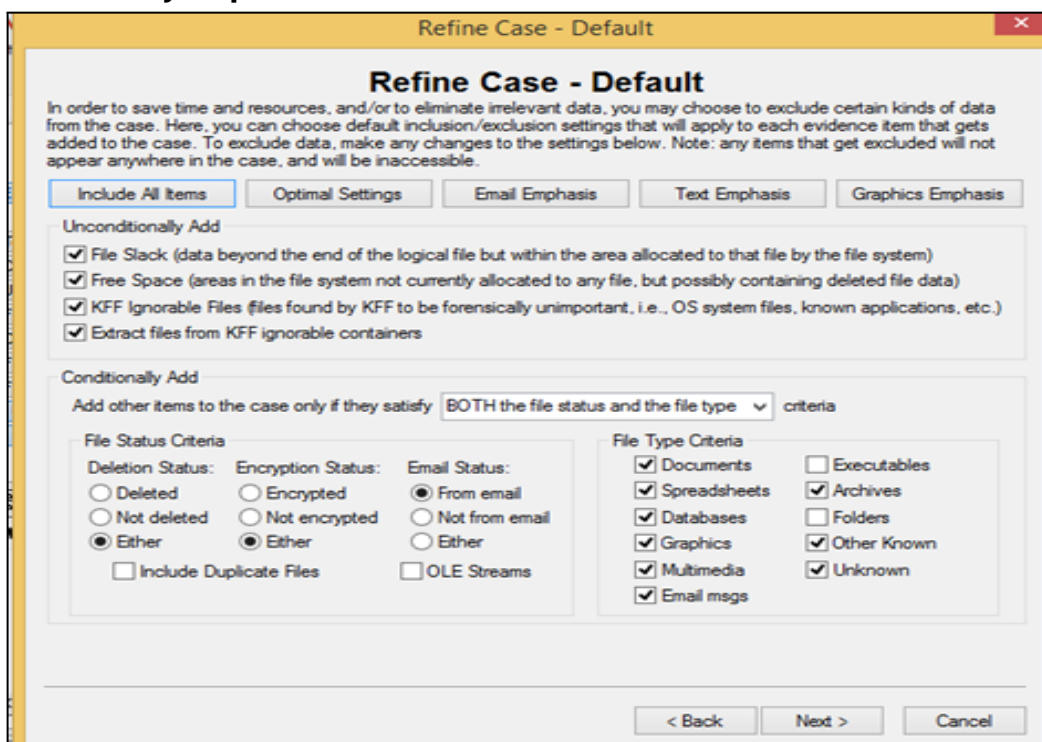
- ☒ Enable POP for all mail (even mail that's already been downloaded)
- ☐ Enable POP for mail that arrives from new email addresses

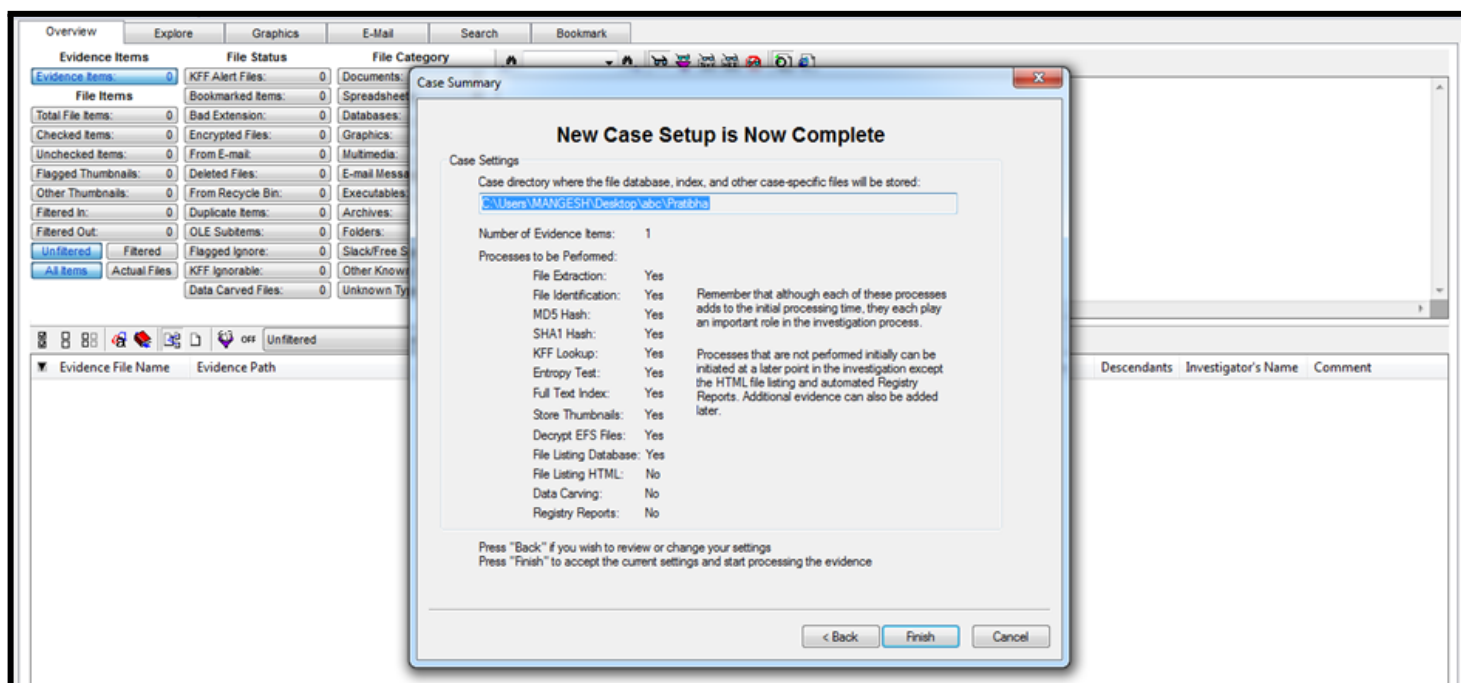
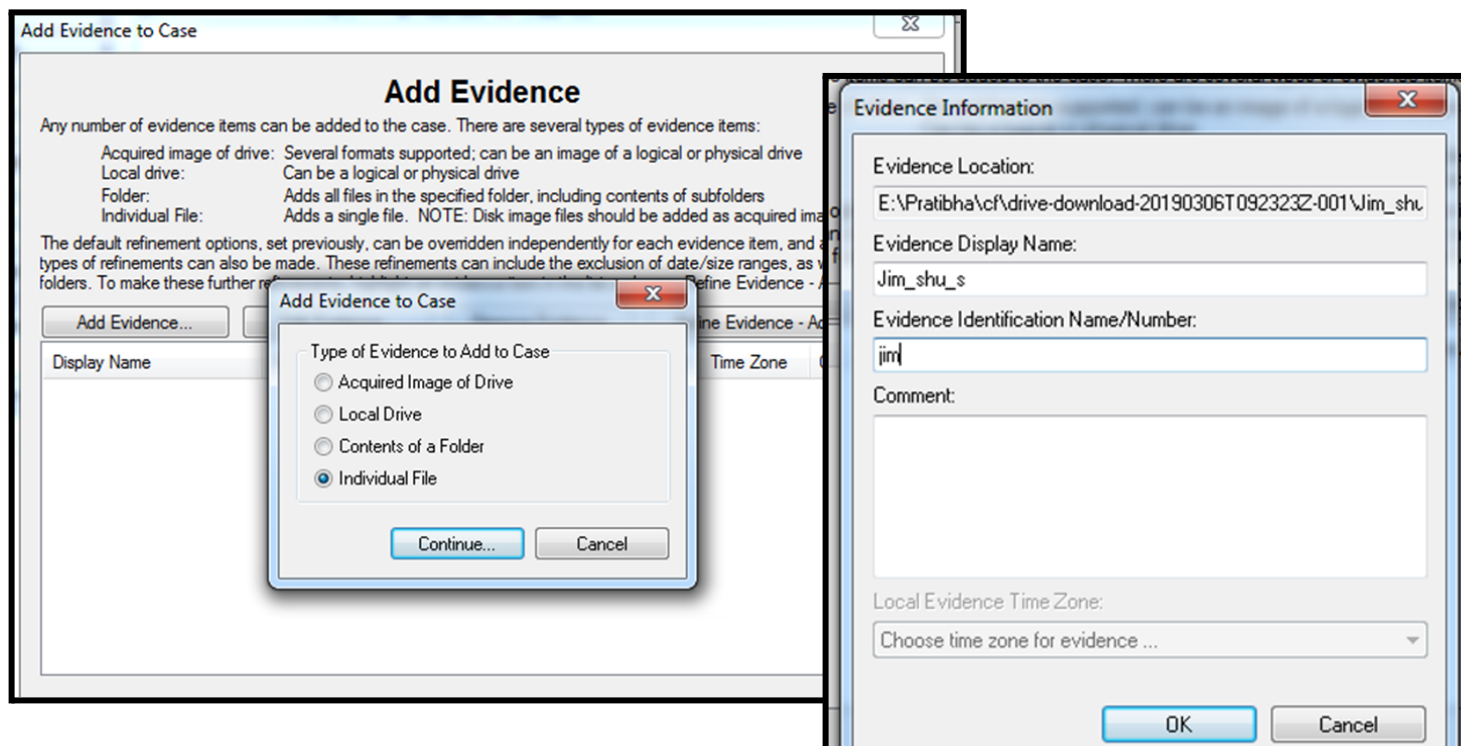
9.3 Recovering Emails -

Open Forensic Toolkit 1.81 (Run as Administrator) → Start New Case → Fill the Information.

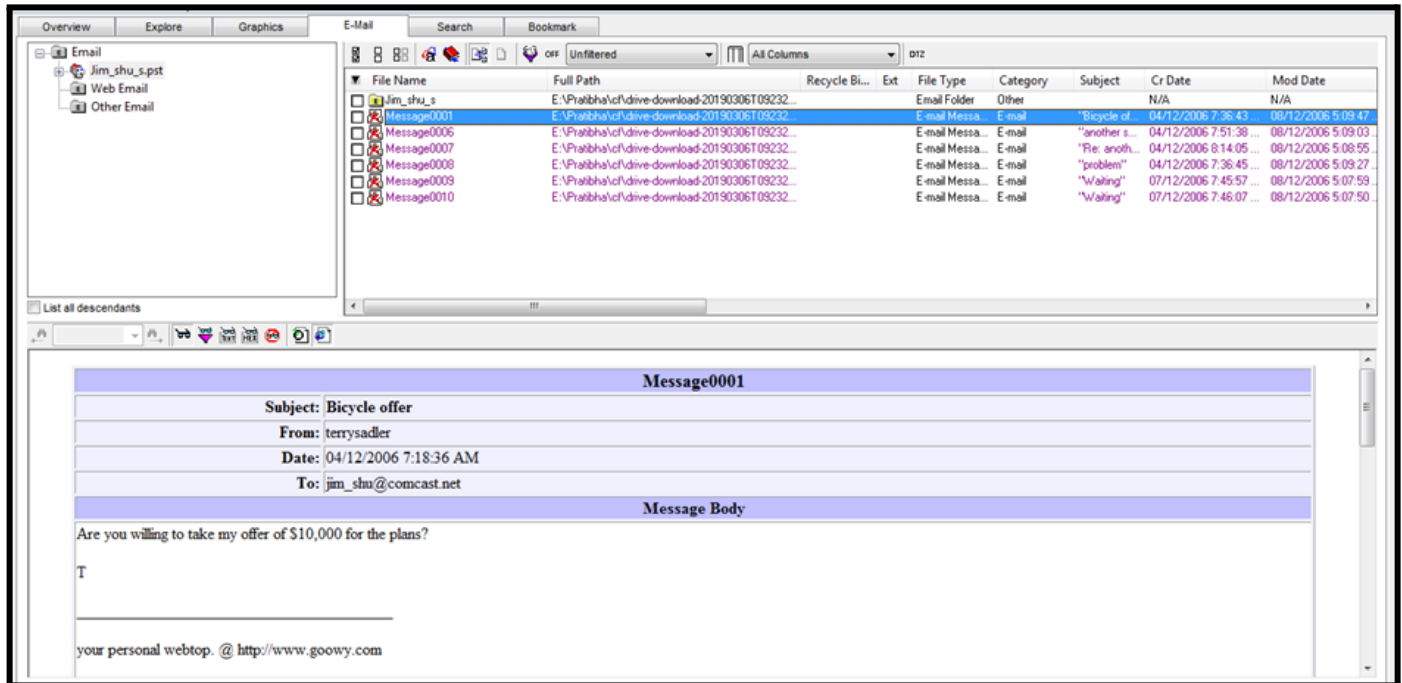


Select Email Emphasis → Select all the CheckBoxes → Add Evidence → Individual File → Browse the “jim.pst” → Finish.



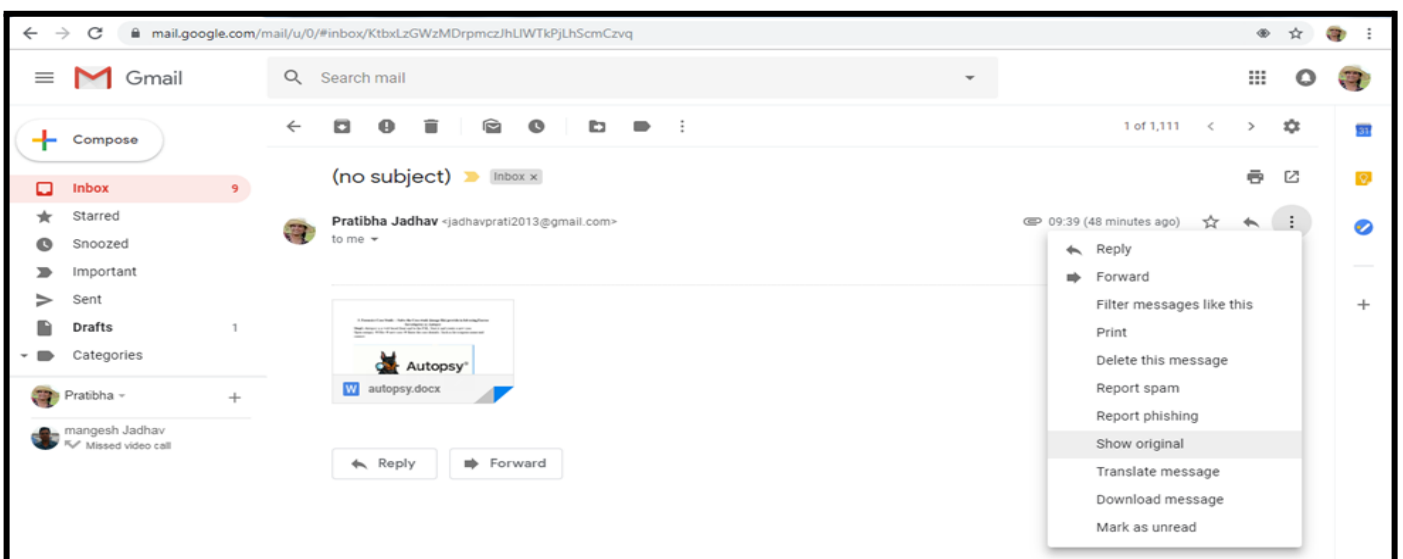


Now, Open the Email Messages tab and select the Email, you want to see the information.



9.3 Analyzing the Email Header-

Open Email you want to check the headers for. Then Next → click the down arrow and click Show original.



Copy the text on the page. And Open the Message header tool. -
→ "<https://toolbox.googleapps.com/apps/messageheader/>"
→ And Paste Email Header.

Delivered-To: jadhavprati2013@gmail.com
Received: by 2002:a2e:5701:0:0:0:0 with SMTP id l1csp141350ljb;
Wed, 20 Feb 2019 18:57:09 -0800 (PST)
X-Goog-Source: AHg13ZV9Td0CzqshyZ1GpGT5l9er6gRb90sY3BZq2M6m16x8paLiPeLRTgD9qxmzsJm18Dauc
X-Received: by 2002:adf1769: with SMTP id a9mr28209749wrq.39.1550717828992;
Wed, 20 Feb 2019 18:57:08 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1550717828; cv=none;
d=google.com; s=arc-20160816;
b=ScCeNRHh4AIUuJMaU5w6DZ9rExF7z5xK9Fplrg0K/b/Vm9hfWNQ+dTkqhxDikgpG
Y/RWhqy683TufjvuttfQQQz/T4utTGwpt5SadRdwf8l1fxgf9sa1XIDN2ppRZ+Btx
dx/EFLJT44SLnrx+6PkLDM9wUDkLcPvIrDta0eCUK9Z17ojoHmskYs95vbXC2N7ZPB
vB4xRD1HiibyRts+Hs11ZRIvQs2rQSFps8PHIMvN23xkYcxZ1PpiS7t+0byFmzR68
C97XcUWXCbMLLIUerpmvC+HAB2cSOzLqEseP54nEyRIA7XkzoZ0Fdd/K6lTbYKsJygg
A+9g==

[ANALYZE THE HEADER ABOVE](#)

Example of what the output may look like

Help

[How do I get email headers?](#)
[Interpreting email headers](#)
What can this tool tell from email headers ?

- Identify delivery delays.
- Identify approximate source of delay.
- Identify who may be responsible.

→ Click Analyze the header Above

Messageid yb3333q.jse1ctzpiapuple@emm.esp99.com

Created at: 2/21/2019, 8:27:08 AM GMT+5:30 (Delivered after 1 sec)

From: Life Insurance India <newsletter@emm.esp99.com> Using eC-Messenger Build 6.90.3856.1

To: jadhavprati2013@gmail.com

Subject: Hi jadhavprati2013@gmail.com : Your Best BackUp Plan For Your Family

SPF: pass

DKIM: pass

#	Delay	From *	To *	Protocol	Time received
0		app61.muc.ec-messenger.com	gp13mtaq111	ESMTP	2/21/2019, 8:27:08 AM GMT+5:30