Kernel PST file viewer for Analysis of outlook email

List of Questions to help with the investigation:

Q 1: What is the return address of the email received by Jeans?

Q 2: When spread sheet was sent to perpetrator?

Q 3: Show the attachment of the spread sheet?

Q 4: Who else was involved ?

Step 1: Open Kernet PST viewer and click select file to open pst file extracted using autopsy

Step 2: Go to inbox and search for an email where Jeans was asked to send over the spread sheet.

Step 3: Click on the email where Jean is asked to send information.

Step 4: Click on advance option and select PR_TRANPORT_MESSAGE_HEADERS as illustrated in figure 22.

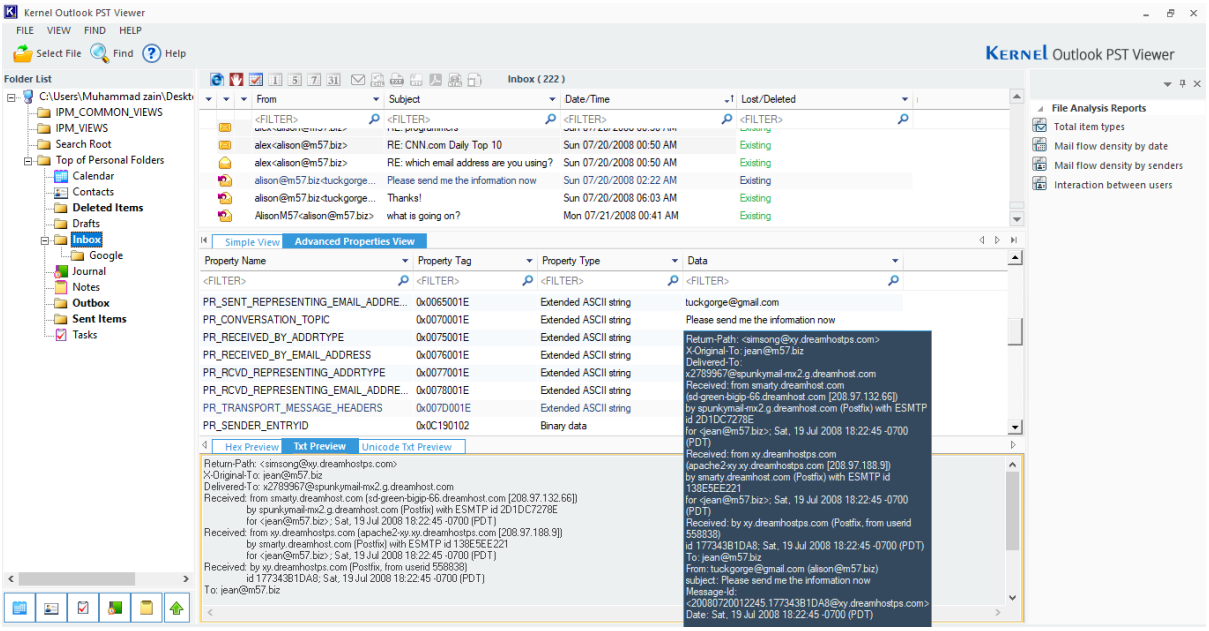

Figure 22: illustration of return address of Alison.

Step 5: Click on text preview to analyse return path and delivery path to investigate the case in-depth. An illustration of return path, sender and receiver information is shown in figure 22 and 23.

```
Return-Path: <simsong@xy.dreamhostps.com>
X-Original-To: jean@m57.biz
Delivered-To: x2789967@spunkymail-mx2.g.dreamhost.com
Received: from smarty.dreamhost.com (sd-green-bigip-66.dreamhost.com [208.97.132.66])
        by spunkymail-mx2.g.dreamhost.com (Postfix) with ESMTP id 2D1DC7278E
        for <jean@m57.biz>; Sat, 19 Jul 2008 18:22:45 -0700 (PDT)
Received: from xy.dreamhostps.com (apache2-xy.xy.dreamhostps.com [208.97.188.9])
        by smarty.dreamhost.com (Postfix) with ESMTP id 138E5EE221
        for <jean@m57.biz>; Sat, 19 Jul 2008 18:22:45 -0700 (PDT)
Received: by xy.dreamhostps.com (Postfix, from userid 558838)
        id 177343B1DA8; Sat, 19 Jul 2008 18:22:45 -0700 (PDT)
To: jean@m57.biz
From: tuckgorge@gmail.com (alison@m57.biz)
subject: Please send me the information now
Message-Id: <20080720012245.177343B1DA8@xy.dreamhostps.com>
Date: Sat, 19 Jul 2008 18:22:45 -0700 (PDT)
```

Figure 23: Shows return path, delivered path, host address, Time and date and sender information with received message.

Step 6: Click on the send box of outlook and select email where the spread sheet was attached. An illustration is shown below:

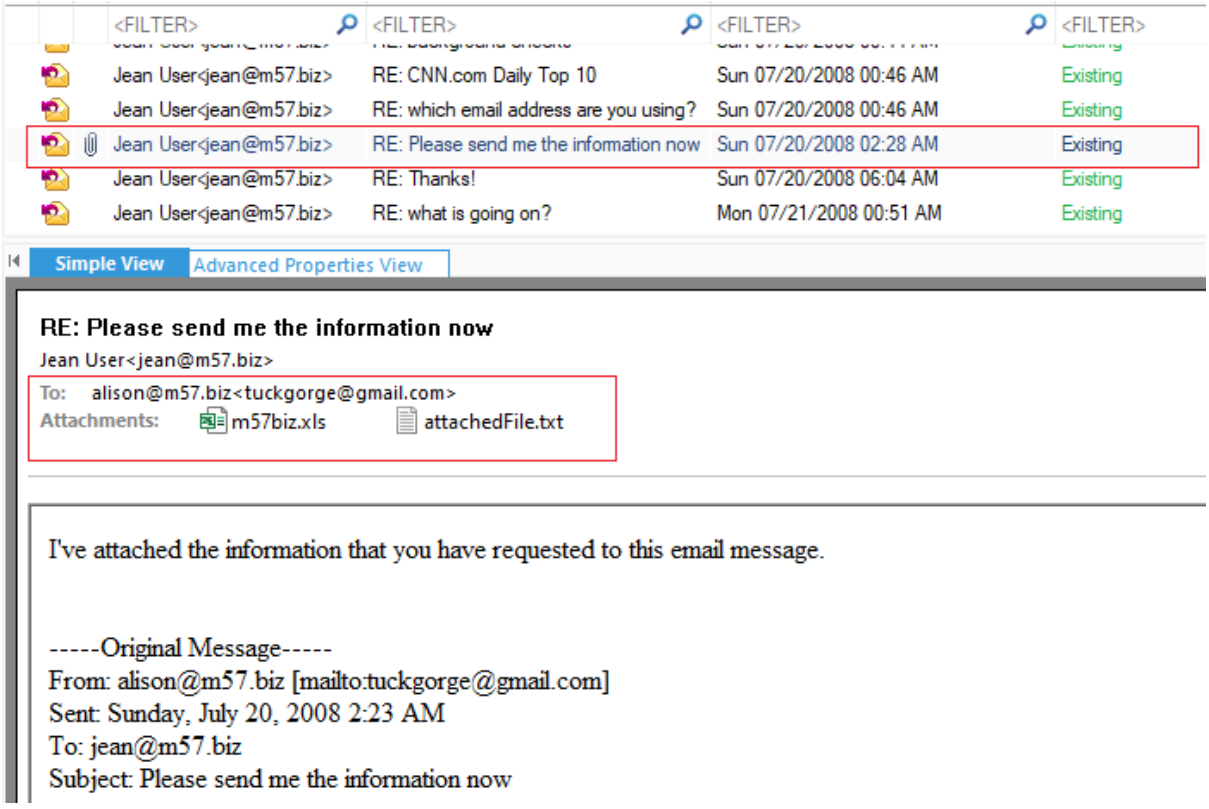

Figure 24: Displays the email where xls and a txt file was attached and was send to Tuckgorge@gmail.com

Step 7: Analyse the interaction activity by clicking on the inbox

Step 8: Click on interaction between users' option on the left side of the pst viewer

Step 9: Tick all pst folder from look in folder

Step 10: Click on analysis button to view the activity

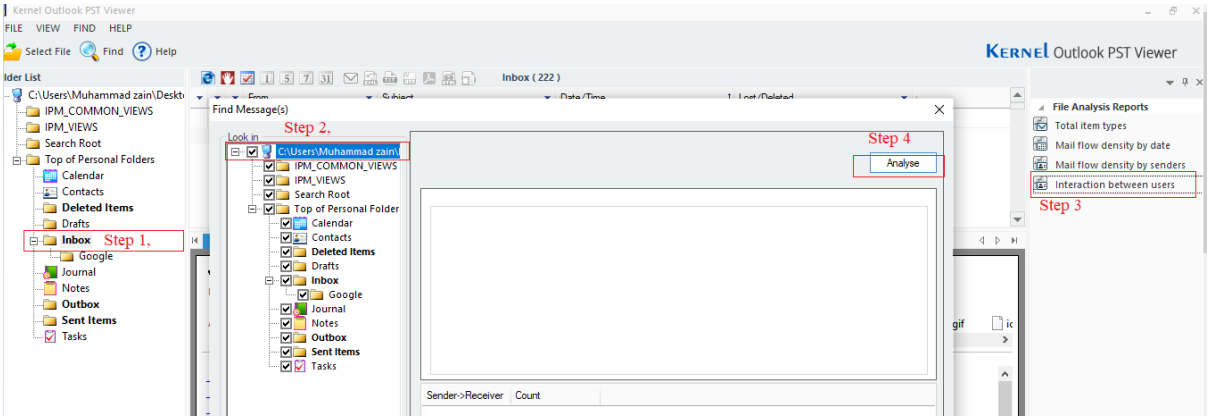

Figure 25: Shows the steps to view the user interaction.

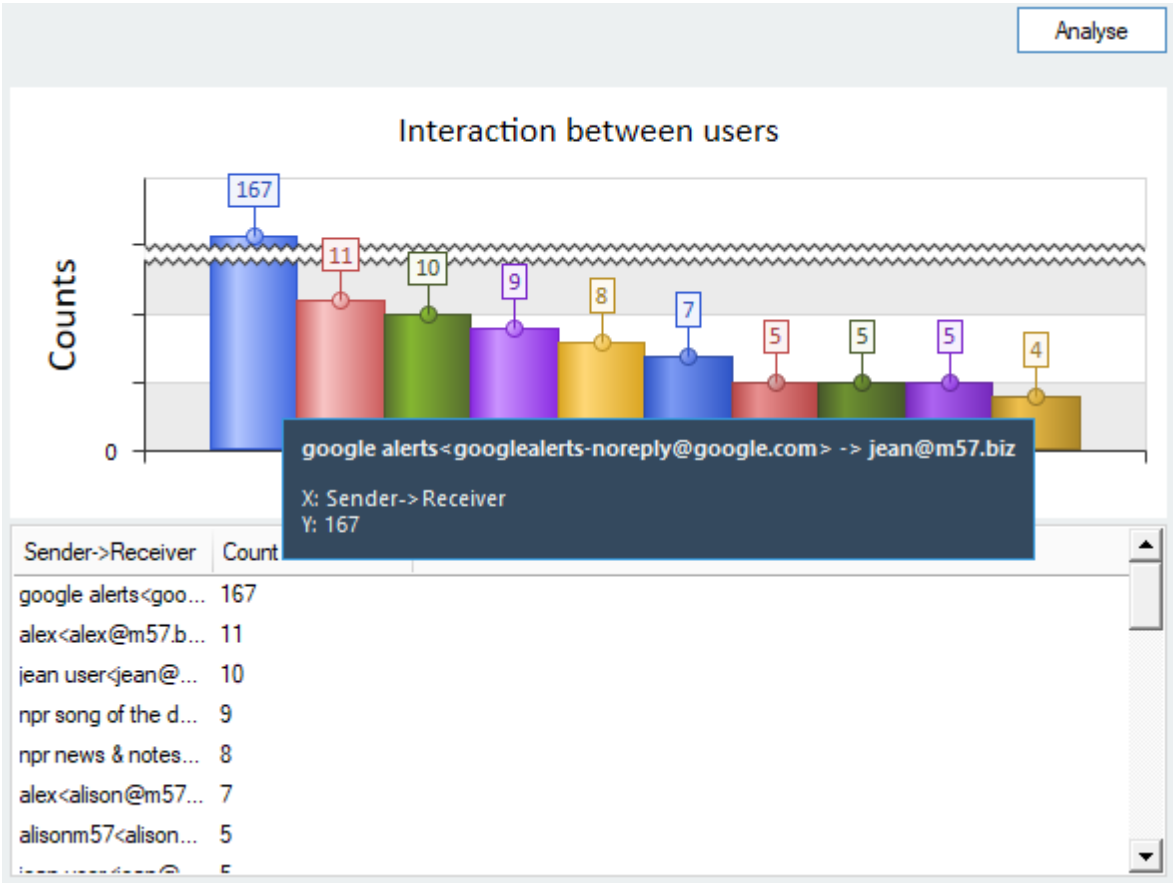

Figure 26: User interaction

Note: Figure 26 highlights the interaction between users and how the data was managed.

Findings from Kernel past viewer are listed below:

Answer 1: Return address was tuckgeorgia@gmail.com with host called dreamhost.com

Answer 2: Jeans was spoofed by tuckgeorge@gmail.com and spread sheet was sent at 2008-07-20 02:28:47.

Answer 3: Figure 24 shows the files being attached

Answer 4: The evidence shows that it was a targeted spear phishing attack which would imply that Alison (boss) was the only intended target.