D. B. J. COLLEGE, CHIPLUN

Page No. : _____

DEPARTMENT OF COMPUTER SCIENCE

Expt. No.

Name : Piyush Pandurang Burate Class : TYCS Roll No.: 523

Title of Experiment : Email Forensics

Date

Sub titles : Assignment/ Problem Solution, Flow chart/Algorithm, Problem Listing, Input Screen, Output Screen, Comments (If any)

Aim :- To study about Email forensics
- Mail service provider
- Email protocol
- Recovering emails
- Analyzing email header.

Theory :-

• Email Forensic Investigation techniques :

Email techniques refers to the source and content study of email as evidence to identity the actual sender and recipient of msg. data/time transmission detailed record of email transaction, intent of sender etc. This study involves investigation of metadata, keyboard searching, port scanning etc. for authorship and identification of email scans various approaches that are used for email forensics.

1] Header Analysis :-

Metadata in email msg in the form of control info. i.e. envelope and header including headers ~~or~~ in msg body contain info. about sender and the path along

Remark

Signature

Which the msg are traversal some of those may be spoofed to concial the identity of the sender.

2] Bast Tactics :

In bast tactic investigations an email with http: "<Img Src>" tag having source at some computer monitored by investigation contain real email address when the email is opened. A log entry containing the leader of the recipient is recorded on the log on IP server can be used to track the server of email under investigation.

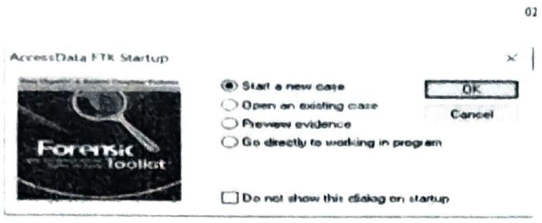
Conclusion :-

We performed email forensic investigation.

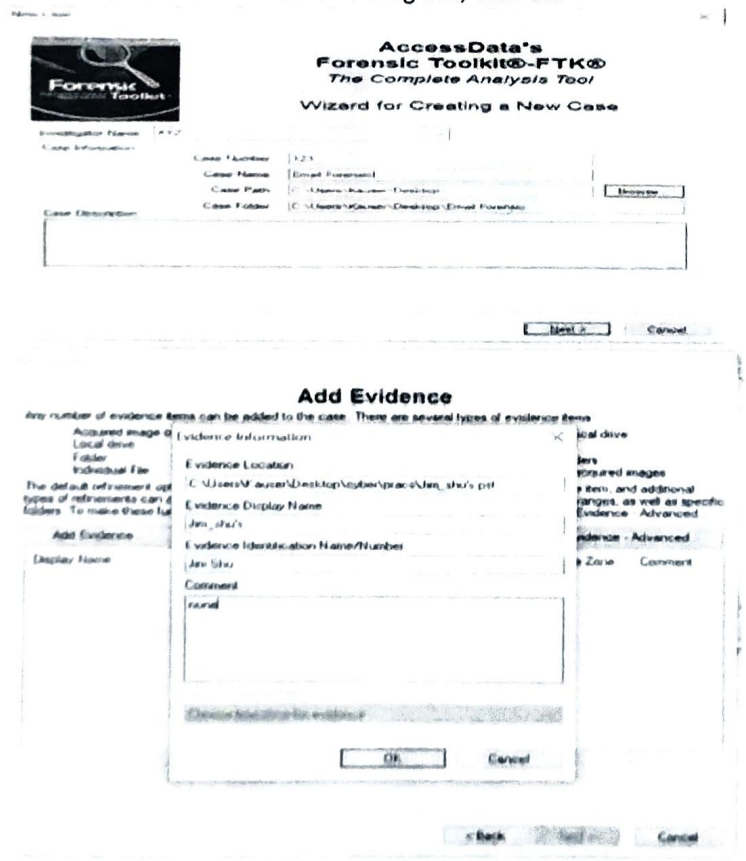
Practical No – 9

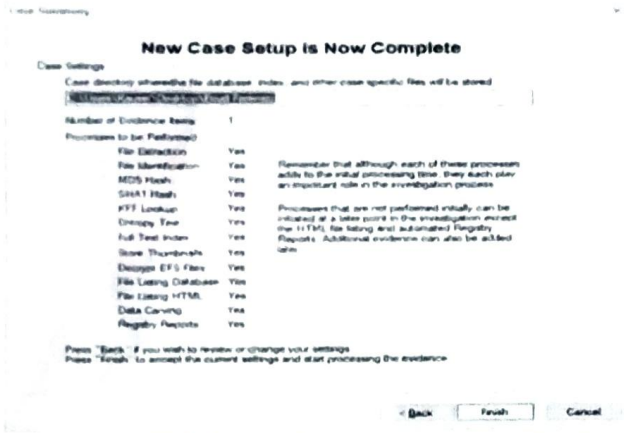
Aim: Email Forensics

- **Mail Service Providers**
- **Email protocols**
- **Recovering emails**
- **Analyzing email header**

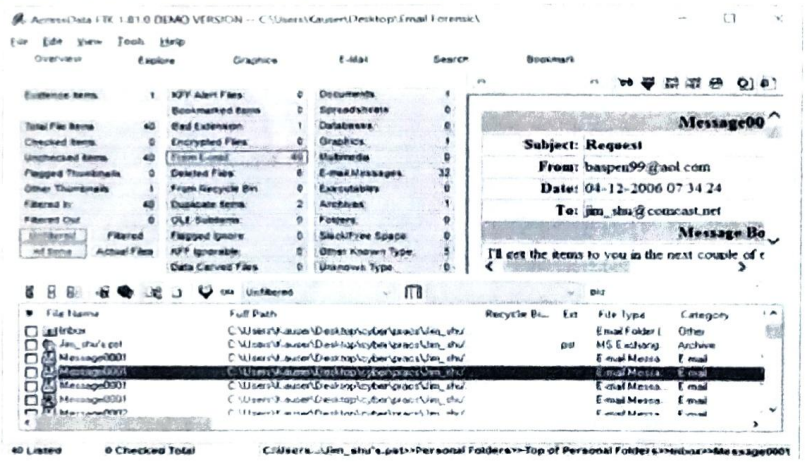


1. Start AccessData FTK by right-clicking the AccessData FTK desktop icon, clicking Run as administrator, and clicking Continue in the UAC message box (if you're using Vista). If you're prompted with a warning message and/or notification (see Figure below), click OK as needed to continue. If asked whether you want to save the existing default case, click Yes.
2. When the AccessData FTK Startup dialog box opens, click Start a new case, and then click OK. 3. In the New Case dialog box, type your name for the investigator name, and type the case number and case name. Click Browse, navigate to and click your work folder, click OK, and then click Next.
4. In the Case Information dialog box, enter your investigator information, and then click Next.
5. Click Next until you reach the Refine Case - Default dialog box, shown in Figure below.
6. Click the Email Emphasis button, and then click Next.
7. Click Next until you reach the Add Evidence to Case dialog box, and then click the Add Evidence button.
8. In the Add Evidence to Case dialog box, click the Individual File option button (see Figure below), and then click Continue.
9. In the Select File dialog box, navigate to your work folder, click the Jim_shu's.pst file, and then click Open.
10. In the Evidence Information dialog box, click OK.





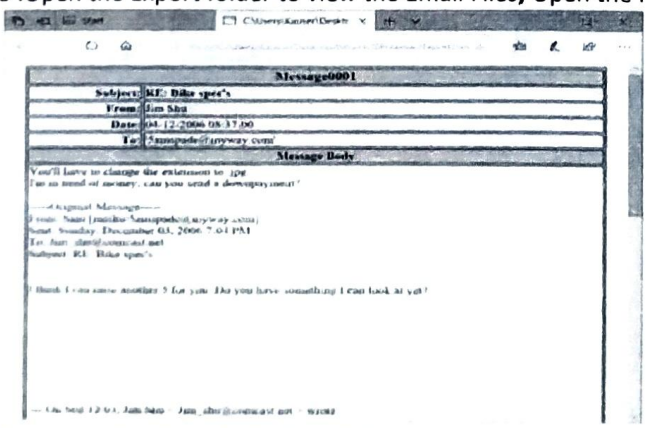
11. When the Add Evidence to Case dialog box opens, click Next. In the Case summary dialog box, click Finish.
12. When FTK finishes processing the file, in the main FTK window, click the E-mail Messages button, and then click the Full Path column header to sort the records



For email recovery follow following steps:¬

1. Click the E-Mail tab. In the tree view, click to expand all folders, and then click the Deleted Items folder
2. Right-click Message0010 in the File List pane and click Export File. In the Export Files dialog box, click OK

3 .Open the Export folder to view the Email Files, Open the HTML file in browser



For analyzing header follow following steps:¬

1. Right Click the file type and Rename it to HTML and open in browser to view header information