SNS COLLEGE OF TECHNOLOGY

(Autonomous)
COIMBATORE – 35

DEPARTMENT OF COMPUTER SIENCE AND ENGINEERING (UG & PG)

Third Year Computer Science and Engineering, 5th Semester

UNIT II - CYBER FORESENICS

Topic Name : Forensics Analysis of Email

E-mail forensics refers to the study of source and content of e-mail as evidence to identify the actual sender and recipient of a message, data/time of transmission, detailed record of e-mail transaction, intent of the sender, etc. This study involves investigation of metadata, keyword searching, port scanning, etc. for authorship attribution and identification of e-mail scams.

Various approaches that are used for e-mail forensic are:

- Header Analysis – Meta data in the e-mail message in the form of control information i.e. envelope and headers including headers in the message body contain information about the sender and/or the path along which the message has traversed. Some of these may be spoofed to conceal the identity of the sender. A detailed analysis of these headers and their correlation is performed in header analysis.

- Bait Tactics – In bait tactic investigation an e-mail with http: "<imgsrc>" tag having image source at some computer monitored by the investigators is send to the sender of e-mail under investigation containing real (genuine) e-mail address. When the e-mail is opened, a log entry containing the IP address of the recipient (sender of the e-mail under investigation) is recorded on the http server hosting the image and thus sender is tracked. However, if the recipient (sender of the e-mail under investigation) is using a proxy server then IP address of the proxy server is recorded. The log on proxy server can be used to track the sender of the e-mail under investigation. If the proxy server's log is unavailable due to some reason, then investigators may send the tactic e-mail containing a) Embedded Java Applet that runs on receiver's computer or b) HTML page with Active X Object. Both aiming to extract IP address of the receiver's computer and e-mail it to the investigators.

- Server Investigation – In this investigation, copies of delivered e-mails and server logs are investigated to identify source of an e-mail message. E-mails purged from the clients (senders or receivers) whose recovery is impossible may be requested from servers (Proxy or ISP) as most of them store a copy of all e-mails after their deliveries. Further, logs maintained by servers can be studied to trace the address of the computer responsible for making the e-mail transaction. However, servers store the copies of e- mail and server logs only for some limited periods and some may not co-operate with the investigators.

Further, SMTP servers which store data like credit card number and other data pertaining to owner of a mailbox can be used to identify person behind an e- mail address.

- Network Device Investigation – In this form of e-mail investigation, logs maintained by the network devices such as routers, firewalls and switches are used to investigate the source of an e-mail message. This form of investigation is complex and is used only when the logs of servers (Proxy or ISP) are unavailable due to some reason, e.g. when ISP or proxy does not maintain a log or lack of co-operation by ISP's or failure to maintain chain of evidence.

- Software Embedded Identifiers – Some information about the creator of e-mail, attached files or documents may be included with the message by the e-mail software used by the sender for composing e-mail. This information may be included in the form of custom headers or in the form of MIME content as a Transport Neutral Encapsulation Format (TNEF). Investigating the e-mail for these details may reveal some vital information about the senders e-mail preferences and options that could help client side evidence gathering. The investigation can reveal PST file names, Windows logon username, MAC address, etc. of the client computer used to send e-mail message.

- Sender Mailer Fingerprints – Identification of software handling e-mail at server can be revealed from the Received header field and identification of software handling e- mail at client can be ascertained by using different set of headers like "X-Mailer" or equivalent. These headers describe applications and their versions used at the clients to send e-mail. This information about the client computer of the sender can be used to help investigators devise an effective plan and thus prove to be very useful.

EMAIL FORENSICS TOOLS

Erasing or deleting an email doesn't necessarily mean that it is gone forever. Often emails can be forensically extracted even after deletion. Forensic tracing of e-mail is similar to traditional detective work. It is used for retrieving information from mailbox files.

- MiTec Mail Viewer – This is a viewer for Outlook Express, Windows Mail/Windows Live Mail, Mozilla Thunderbird message databases, and single EML files. It displays a list of contained messages with all needed properties, like an ordinary e-mail client. Messages can be viewed in detailed view, including attachments and an HTML preview. It has powerful searching and filtering capability and also allows extracting email addresses from all emails in opened folder to list by one click. Selected messages can be saved to eml files with or without their attachments. Attachments can be extracted from selected messages by one command.

- OST and PST Viewer – Nucleus Technologies' OST and PST viewer tools help you view OST and PST files easily without connecting to an MS Exchange server. These tools allow the user to scan OST and PST files and they display the data saved in it including email messages, contacts, calendars, notes, etc., in a proper folder structure.

- eMailTrackerPro – eMailTrackerPro analyses the headers of an e-mail to detect the IP address of the machine that sent the message so that the sender can be tracked down. It can trace multiple e-mails at the same time and easily keep track of them. The geographical location of an IP address is key information for determining the threat level or validity of an e-mail message.

- EmailTracer – EmailTracer is an Indian effort in cyber forensics by the Resource Centre for Cyber Forensics (RCCF) which is a premier centre for cyber forensics in India. It develops cyber forensic tools based on the requirements of law enforcement agencies.