|  |  |
| --- | --- |
| Course | Computer Forensics |
| Lab | Lab 08 |
| Name of the Student | Maisha Khatoon |
| Student ID | 100899259 |

# **LAB: 08**

This lab focuses on email analysis.

**Objective:**

* **Learn E-mail investigation.**

**Leaning Activities:**

At the end of these activities, you should understand:

* How to apply digital forensics methods to investigating email communications.

**Tools to use:**

-Outlook client

-Aid4Mail

**Note: Please include a screenshot of each step. Corp your screenshot to show relevant information only. Uncropped screenshots will result in a 10% deduction from your marks.**

**Task 1:**

**Install Outlook client**

* 1. Create a test Gmail account or use your existing email account
  2. Configure your Outlook client (Ref#1)
  3. Send/receive test emails
  4. Viewing E-mail headers

Text book page 460, 461 and 462.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Task-2:**

**Using Hex editor to carve email messages**

2.1 Text book page 476, 477 and 478.

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated***Note: Your Winhex editor’s demo license may be expired, you may use other hex editors (Ex: HxD)***

**Task-3:**

Examining Enron employee’s email

3.1 Text book page 488 (Hands-On project 11-1)

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

***Note: I have uploaded eric\_Saibi.pst in DCconnect.***

**Reflective statements (end-of-exercise):**

You should reflect on these questions:

1. Describe how e-mail account names are created on an intranet environment?

In an intranet setting, email account names are made by choosing a distinctive username and adding the domain name of the company. Typically, the format is "username@domain." Typically, the username is derived from the user's name or initials. The accounts have passwords established, and duplicate usernames are checked to prevent conflicts. The accounts give users access to email features on the company's intranet after they are activated.

|  |  |
| --- | --- |
|  |  |

1. Describe the process of examining e-mail messages when you have access to the victim’s computer and when this access is not possible.

Examining Emails with Computer Access from the Victim:

To access saved emails, log into the victim's email program or webmail.

Examine the Sent Items, Deleted Items, and Inbox folders.

To find certain terms or senders, use the search feature.

Verify email attachments for malicious software or sensitive data.

Without Having Access to the Victim's Computer, Examine Email Messages:

To trace emails, use the required permissions to access the email server logs.

To retrieve emails, enlist the assistance of the email service provider.

Examine network traffic and email metadata for hints.

Keep an eye out for emails that have been exposed in public data breach alerts.

1. What is forensic linguistics?

The scientific study of and use of language analysis in legal circumstances is known as forensic linguistics. It entails looking at language-related evidence, including written or spoken communication, in order to support criminal investigations, court cases, and dispute resolution.

1. What kind of information can you find in an e-mail header?

You can discover the following details in an email header:

The email address where undeliverable mails are delivered is known as the return-path.

Timestamps and server information were received. The email was received after travelling.

From: The email address and name of the sender.

The email address where comments should be sent in response.

To: The email address(es) of the recipient.

recipients' email addresses for carbon copying.

Bcc stands for blind carbon copy, and it protects recipients' email addresses from other recipients.

The subject line of the email.

Date: The email's time and date of sending.

Message ID: An email's individual identification number.

The MIME (Multipurpose Internet Mail Extensions) version that was utilised to send the email.

Content-Type: The format of the email's content (for example, text/plain or text/html).

1. Why are network router logs important during an e-mail investigation?

In order to trace an email's path and find unauthorised access or security breaches, network router logs are crucial during an email investigation. They offer crucial information about the source and destination IP addresses, email routing path, timestamps, and potential anomalies in network traffic.

**References**

1. <https://www.nucleustechnologies.com/blog/how-to-configure-gmail-in-ms-outlook/>
2. <https://www.forensicfocus.com/articles/email-forensics-investigation-techniques/>
3. <https://core.ac.uk/download/pdf/56362354.pdf>
4. https://digital-forensics.sans.org/community/papers/gcfa/ids-file-forensics\_9991