THE UNIVERSITY OF DODOMA

COLLEGE OF INFORMATICS AND VIRTUAL EDUCATION

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (CSE)

LAB ONE: EMAIL FORENSICS

PROGRAM: BSc-CNISE

COURSE: IA 418

SUBMISSION DATE : 12th January 2025

GROUP PARTICIPANTS

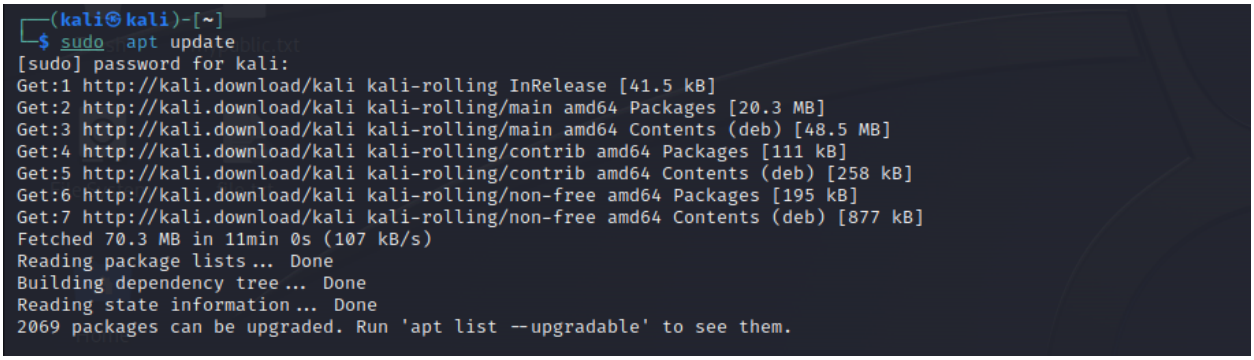
NAME	REGSTRATION NUMBER
NYAMIZI SHIJA	T22-03-02725
PUDENCIANA P. KIYEGA	T22-03-11584
EMMANUEL WOLFGANG	T22-03-09178
GEORGE KALAMU	T22-03-08400

QUESTION:

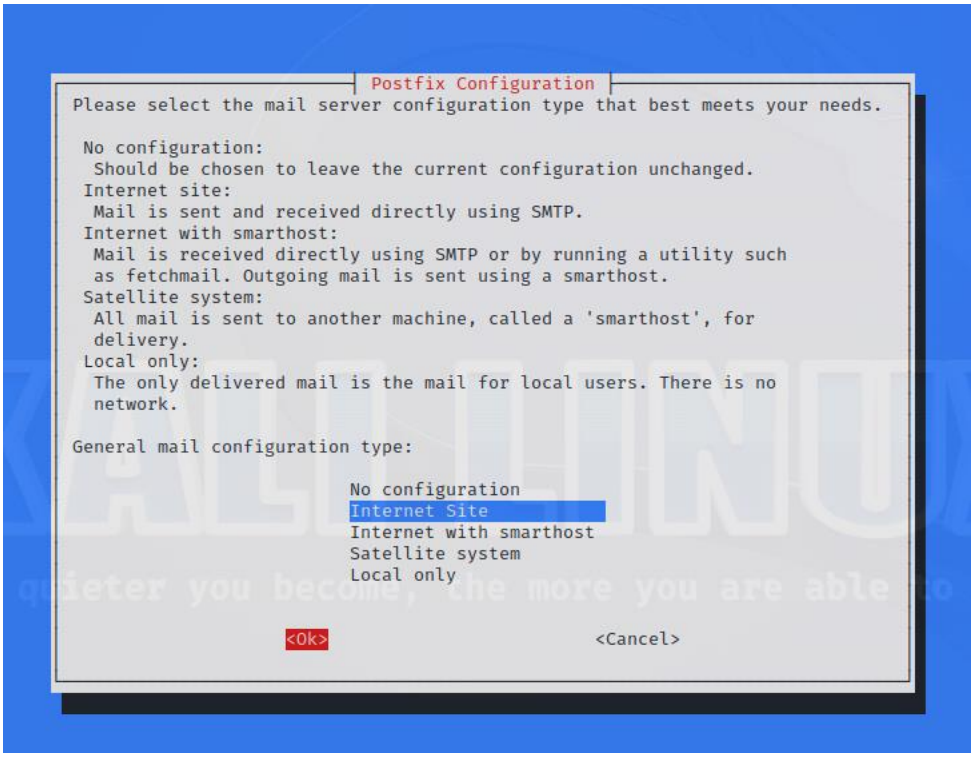
On a Linux Machine (virtual or physical), install and configure a mail server on a specific domain, with a Graphical User Interface to send and receive emails. Create email accounts, send emails from one user to another, and observe email header details associated with the email. Where is the log file associated with email transactions? Can you be able to track email details obtained from email header analysis to the log file?

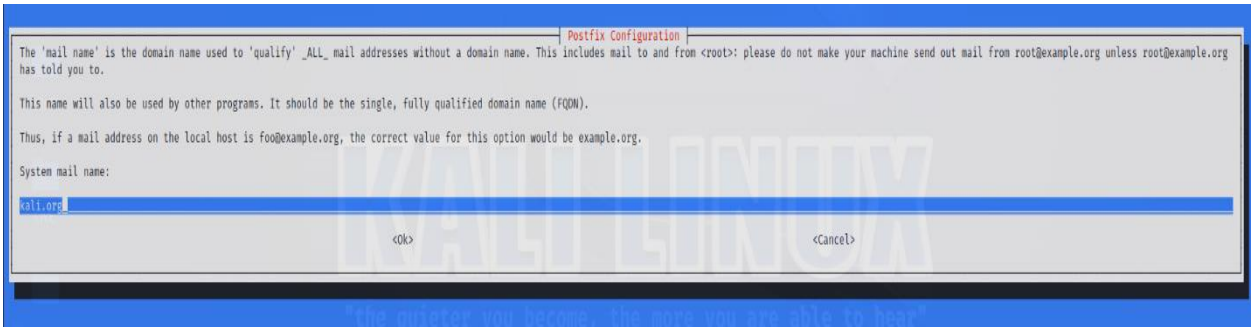
DEMOSTRATIONS.

Step 1: First update the Linux Machine , then install postfix mail server and configure it as shown below.









Step 2: Second is to start postfix in order to make it active also you can enable it so as to make postfix start automatic after rebooting the machine

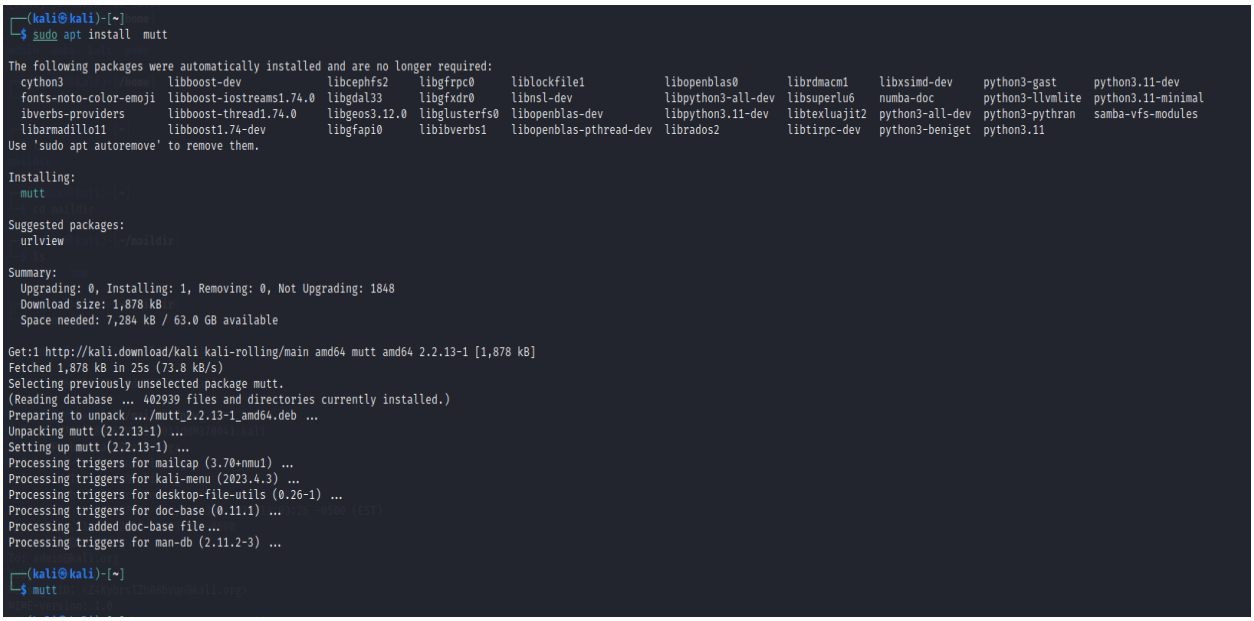
```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start postfix

┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable postfix
Synchronizing state of postfix.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable postfix
```

Then you can check the status of the mail server to look if postfix is active runnig, as shown below.



Step 3: Third is Mutt installation, this is the Graphical User Interface client to send and receive emails. Then Run it to start creating the email accounts, as shown below.



After running the mutt command ,the graphical user interface will be opened as seen below.



Click ‘m’ to start writing your email message, then it will allow you to enter the name of the one you need to sent emails the click enter .



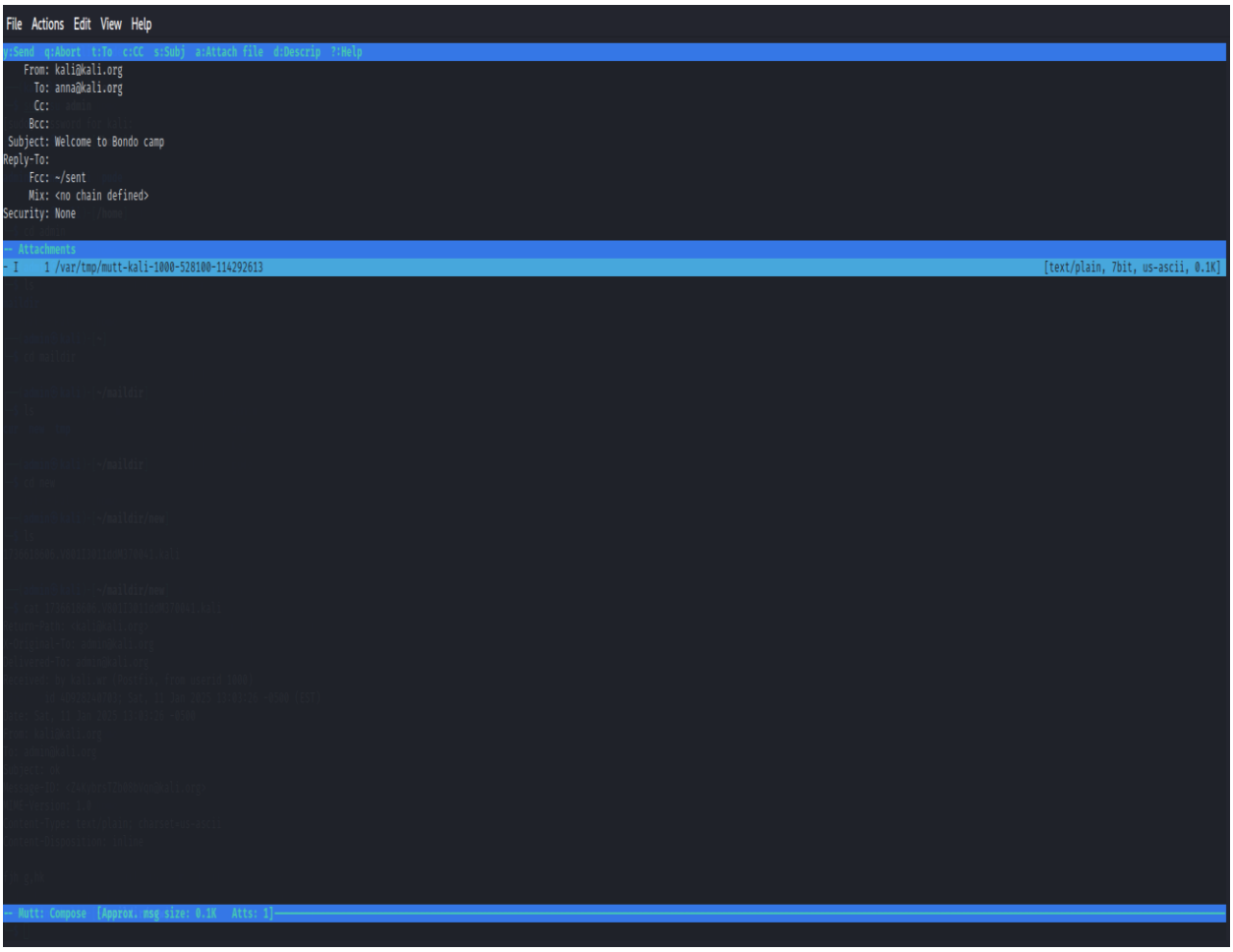
Here you write the message you need to send t your user then click enter



Step 4: Fourth is to send the email to user Anna, here you need to click “y”. Then automatic mail will be sent as shown below.

Note that: Make sure you create the user before start sending emails, the command to add user is “adduser”.

Example:
$ sudo adduser anna

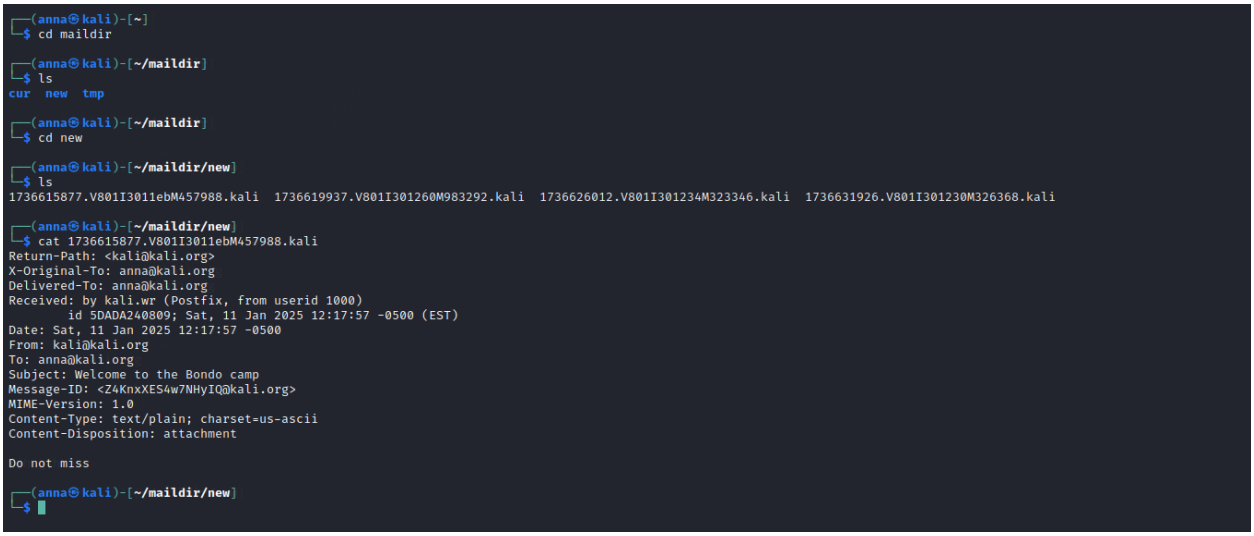

File Actions Edit View Help
y:Send q:Abort t:To c:CC s:Subj a:Attach file d:Descrip ?:Help
From: kali@kali.org
To: anna@kali.org
Cc:
Bcc:
Subject: Welcome to Bondo camp
Reply-To:
Fcc: ~/sent
Mix: <no chain defined>
Security: None
Attachments
I 1 /var/tmp/mutt-kali-1000-528100-114292613 [text/plain, 7bit, us-ascii, 0.1K]
Mutt: Compose [Approx. msg size: 0.1K Atts: 1]


File Actions Edit View Help
q:Quit d:Del u:Undel s:Save m:Mail r:Reply g:Group ?:Help
Mutt: [no mailbox] [Msgs:0]---(threads/date)
Mail sent.

Step 5: The observation of email header details associated with the email, here we give our user anna permission so as we can be able to see the emails sent by kali@kali.org. These are the steps below:



Step 6: The log file associated with the email transactions is founded to the another user Anna as the receiver of the email which is **/home/anna/maildir/new**.



Conclusion: We are able to track email details obtained from email header analysis to the log file since there is no mismatch of any details, all details are correct then no any malicious appears.