**Lab 12: Email forensics**

**What You Need for this lab**

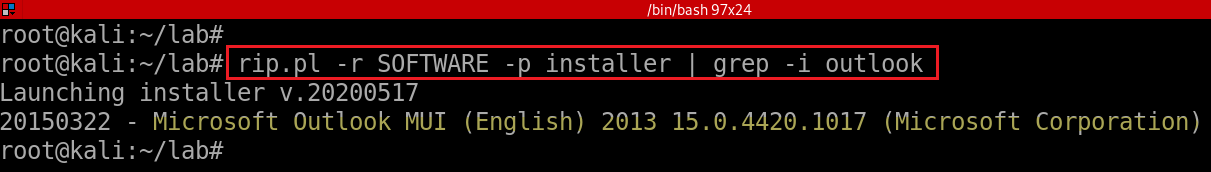
* + Install Virtualbox : <https://www.virtualbox.org/wiki/Downloads>
  + Install Kali 2021.4. : <https://old.kali.org/kali-images/kali-2021.4/>
    - Notes: Suggest You configure the disk size of Kali VM 80G because the size of each leakage cases image is 30G+
  + Image “cfreds\_2015\_data\_leakage\_pc.dd” from Lab 5

**Goals**

* Email forensics (Application Layer)

**Step 1**

What application was used for e-mail communication?



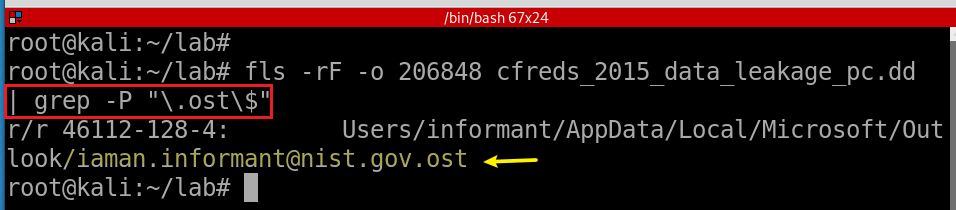
List of email clients

* <https://en.wikipedia.org/wiki/Comparison_of_email_clients>

What was the e-mail account used by the suspect?

*fls -rF -o 206848 cfreds\_2015\_data\_leakage\_pc.dd | grep -P "\.ost\$“*

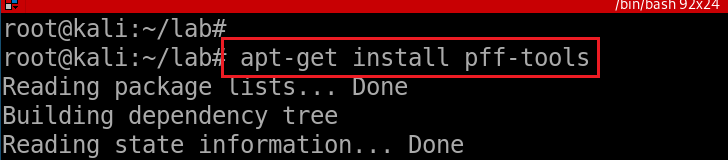
*fls -rF -o 206848 cfreds\_2015\_data\_leakage\_pc.dd | grep -E "\.ost$"*



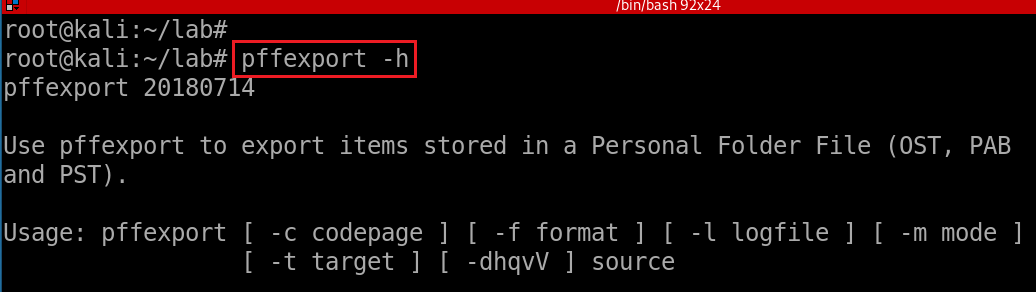
**Step 2.**

List all e-mails of the suspect. If possible, identify deleted e-mails

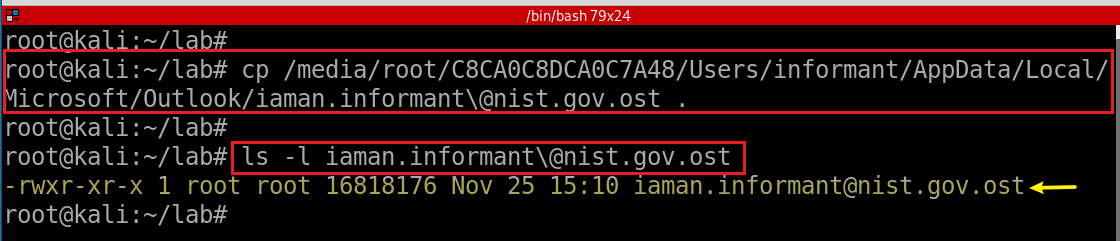
* Install email extracting tool: *libpff*
* Copy .*ost* file from a DD image
* Extract email via *libpff*
* Install *pffexport* tool



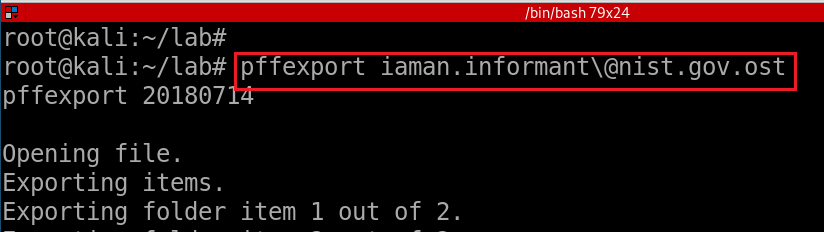
* Verify installation



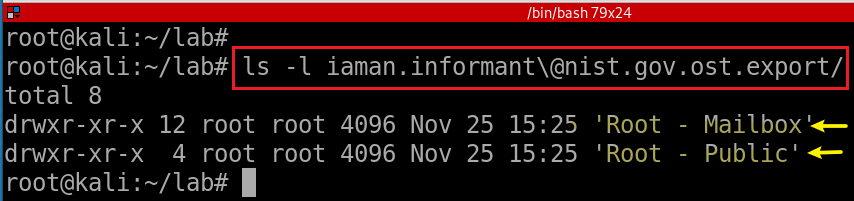
* Copy email to current directory



* Extract emails via *pffexport*

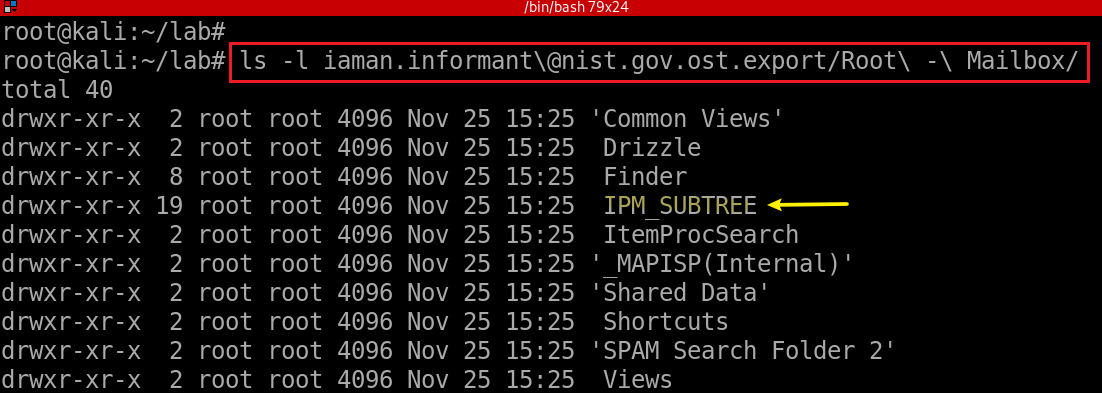


* Verify the default output directory

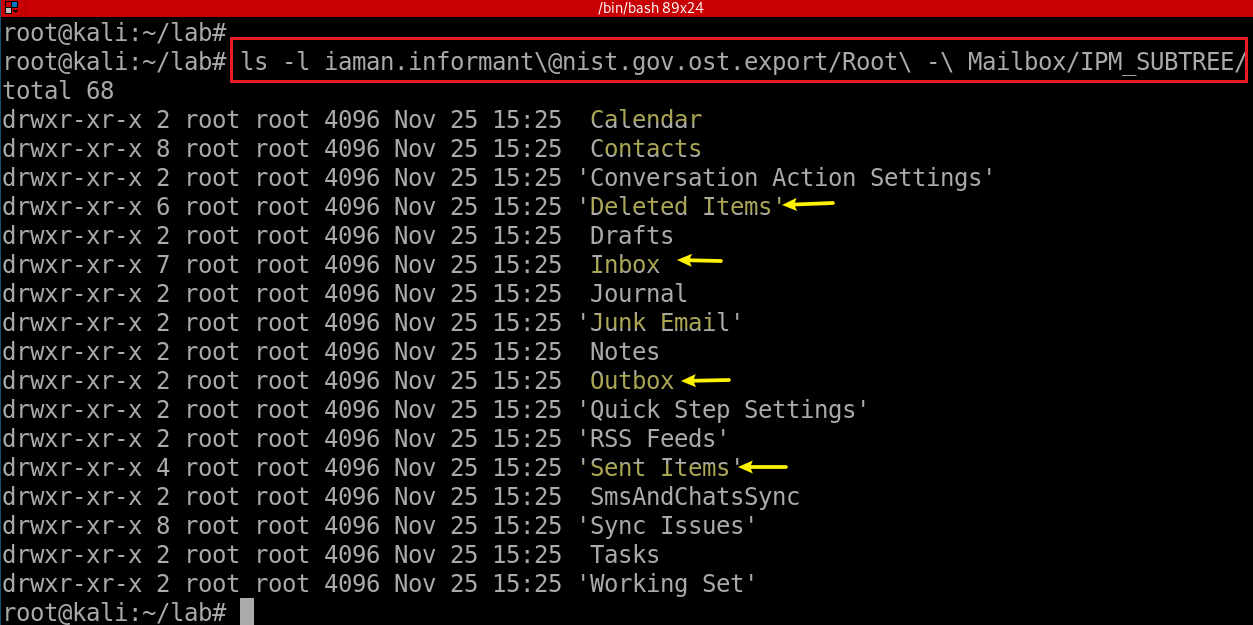


* Access a message in suspect’s Mailbox

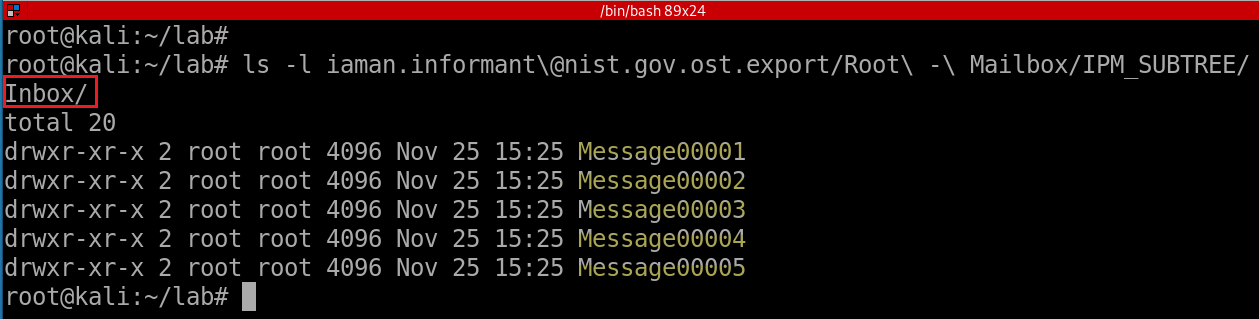
*ls -l iaman.informant\@nist.gov.ost.export/Root\ -\ Mailbox/*



* Access a message in suspect’s *IPM\_SUBTREE*

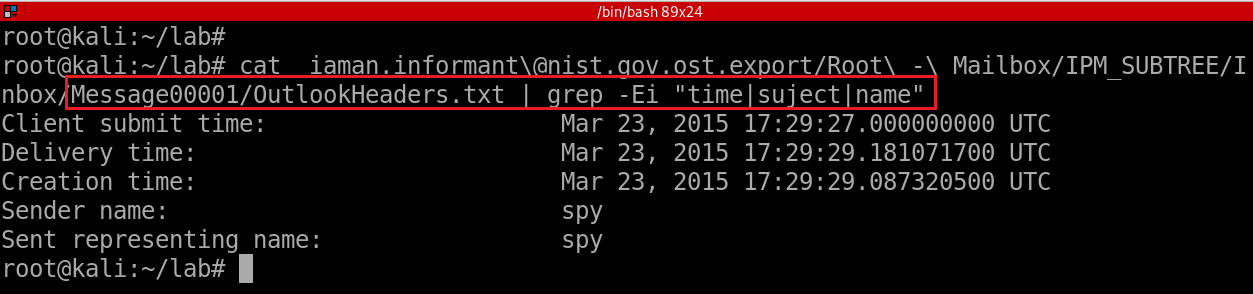


*ls -l iaman.informant\@nist.gov.ost.export/Root\ -\ Mailbox/IPM\_SUBTREE/Inbox/*



*cat iaman.informant\@nist.gov.ost.export/Root\ -\ Mailbox/IPM\_SUBTREE/Inbox/Message00001/OutlookHeaders.txt | grep -Ei "time|suject|name“*

*grep -E ‘strings’ Message\**



**YOU MUST SUBMIT A FULL-SCREEN IMAGE FOR FULL CREDIT!**

Save the document with the filename "**YOUR NAME Lab 12.pdf**", replacing "YOUR NAME" with your real name.

Email the image to the instructor as an attachment to an e-mail message. Send it to: **xxx@fe.edu.vn** with a subject line of "**Lab 12 From YOUR NAME**", replacing "YOUR NAME" with your real name.