



FORENSICS LAB SERIES

Lab 14: Email Forensics

Material in this Lab Aligns to the Following Certification Domains/Objectives		
GIAC Certified Forensics Examiner (GCFE) Domains	Certified Cyber Forensics Professional (CCFP) Objectives	Computer Hacking Forensic Investigator (CHFI) Objectives
7: User Communication Analysis	5: Application Forensics	19: Tracking Emails and Investigating Email Crimes

Document Version: 2016-08-17

Contents

Introduction	3
Objective	3
Pod Topology	4
Lab Settings	5
1 Analyzing & Converting Personal Storage Tables	6
2 Decoding Email Attachments.....	9
3 Analyzing Email Headers	18

Introduction

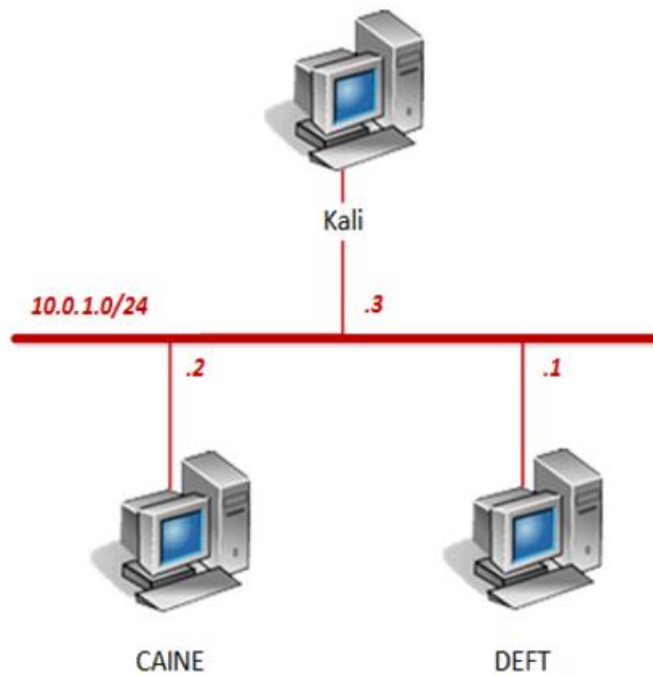
This lab will introduce the concepts of analyzing emails and tracing them through the Internet. The ability to read email boxes and email headers are skills needed by a digital forensics investigator.

Objective

In this lab, you will be conducting forensic practices using various tools. You will be performing the following tasks:

1. Analyzing & Converting Personal Storage Tables
2. Decoding Email Attachments
3. Analyzing Email Headers

Pod Topology



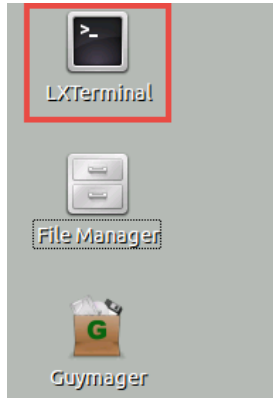
Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
DEFT	10.0.1.1	deft	password
CAINE	10.0.1.2	caine	
Kali	10.0.1.3	root	toor

1 Analyzing & Converting Personal Storage Tables

1. Click on the **DEFT** graphic on the *topology page* to open the VM.
2. Open a new terminal by double-clicking on the **LXTerminal** icon located on the *Desktop*.



3. Using the terminal, navigate to the **/home/deft/Downloads/** directory by typing the command below followed by pressing the **Enter** key.

```
cd Downloads
```

```
deft-virtual-machine ~ % cd Downloads
deft-virtual-machine ~/Downloads %
```

4. Enter the command below to list the files in the current directory.

```
ls
```

```
deft-virtual-machine ~/Downloads % ls
autopsy      outlook.pst  password.txt  pdfcrack-0.15.tar.gz
decoded.txt  password    pdfcrack-0.15
deft-virtual-machine ~/Downloads %
```

Notice the *outlook.pst* file. This file is a personal storage table for email usage. This one is specific for *Microsoft Outlook*.



5. Enter the command below to analyze the contents of the *outlook.pst* file.

```
lspst outlook.pst
```

```
deft-virtual-machine ~/Downloads % lspst outlook.pst
Folder "Deleted Items"
Email From: Google Alerts Subject: Google Alert - m57.biz
Email From: Google Alerts Subject: Google Alert - skin in the office
Email From: alex Subject: FW: Fans ready to stay up all 'Knight' for Batm
an movie
Email From: alex Subject: FW: All In All, I Feel Like Another Brick In th
e Wall
Email From: alex Subject: FW: The CNN Political Ticker AM for Friday, Jul
y 18, 2008
Email From: alex Subject: FW: UFOs Over U.S. Military Sites?
Email From: alex Subject: FW: Making People Sick AND Poor
Email From: alex Subject: FW: Subject line: Missing girl's mom borrowed a
shovel?
Email From: alex Subject: RE: which email address are you using?
Folder "Inbox"
Email
Email From: Microsoft Outlook 2000 Subject: Welcome to Microsoft Outlook 20
```

Notice the list of all the emails contained in the *.pst* file. This file can be converted into a more readable format called "*mbox*". *Mbox* is a file in a text based format so that the content of the emails can be read as well as the headers.

6. Enter the command below to convert the *.pst* file.

```
readpst -C -M outlook.pst
```

```
deft-virtual-machine ~/Downloads % readpst -C -M outlook.pst
Opening PST file and indexes...
Processing Folder "Deleted Items"
Processing Folder "Inbox"
Processing Folder "Outbox"
Processing Folder "Sent Items"
Processing Folder "Calendar"
Processing Folder "Contacts"
Processing Folder "Journal"
    "Journal" - 0 items done, 1 items skipped.
Processing Folder "Notes"
Processing Folder "Tasks"
    "Tasks" - 0 items done, 1 items skipped.
Processing Folder "Drafts"
    "Personal Folders" - 10 items done, 0 items skipped.
    "Calendar" - 0 items done, 2 items skipped.
    "Outbox" - 3 items done, 0 items skipped.
Processing Folder "Google"
    "Sent Items" - 24 items done, 1 items skipped.
    "Inbox" - 224 items done, 2 items skipped.
deft-virtual-machine ~/Downloads %
```

Command Breakdown:

-C = standard character set

-M = output messages RFC 822 format (test messages) as separate files

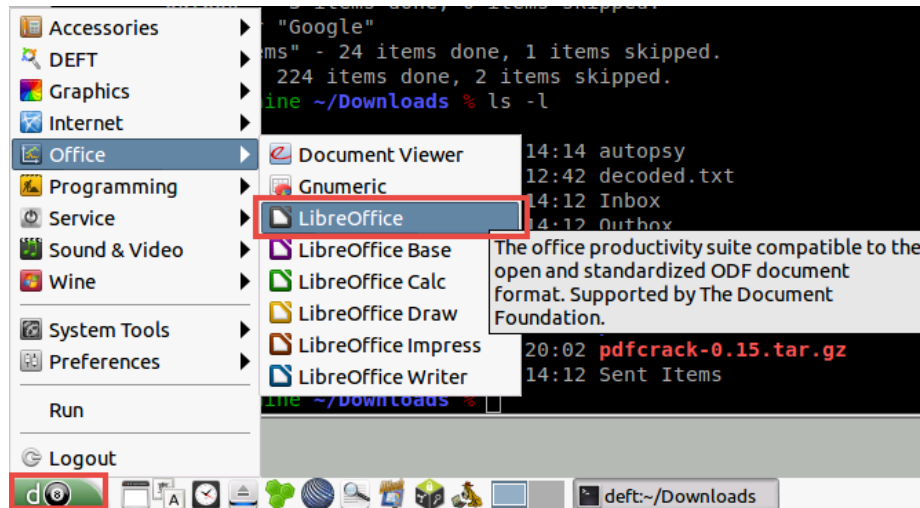
7. List the files in the current directory in a list by entering the command below and verify that *Inbox*, *Outbox*, and *Sent Items* appear in the list.

```
ls -l
```

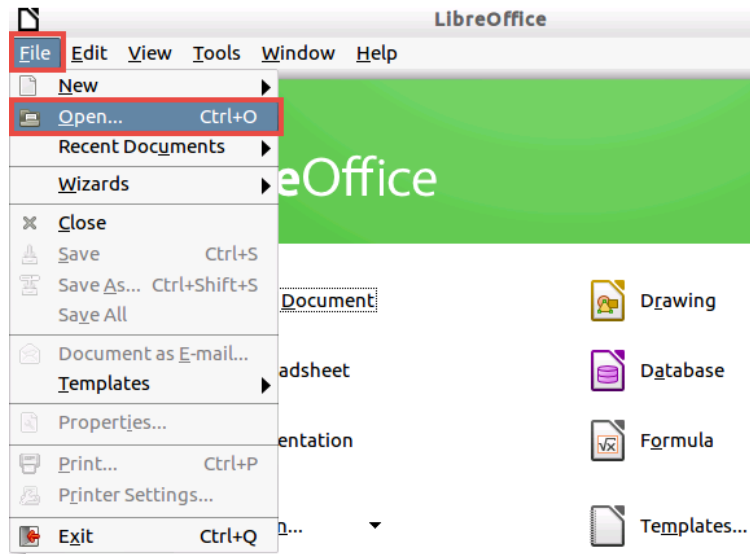
```
deft-virtual-machine ~/Downloads % ls -l
total 6248
-rw-r----- 1 deft deft 2326645 Apr 19 14:14 autopsy
-rw-rw-r-- 1 deft deft 1236 Apr 20 12:42 decoded.txt
-rw-rw-r-- 1 deft deft 1113480 Aug 2 14:12 Inbox
-rw-rw-r-- 1 deft deft 29162 Aug 2 14:12 Outbox
-rw-r----- 1 deft deft 2326528 Apr 19 14:14 outlook.pst
-rw-r--r-- 1 deft deft 25589 May 11 08:47 password
-rw-r--r-- 1 deft deft 26215 May 10 19:52 password.txt
drwxrwxr-x 2 deft deft 4096 May 10 20:12 pdfcrack-0.15
-rw-r--r-- 1 deft deft 34269 May 10 20:02 pdfcrack-0.15.tar.gz
-rw-rw-r-- 1 deft deft 480949 Aug 2 14:12 Sent Items
deft-virtual-machine ~/Downloads %
```


2 Decoding Email Attachments

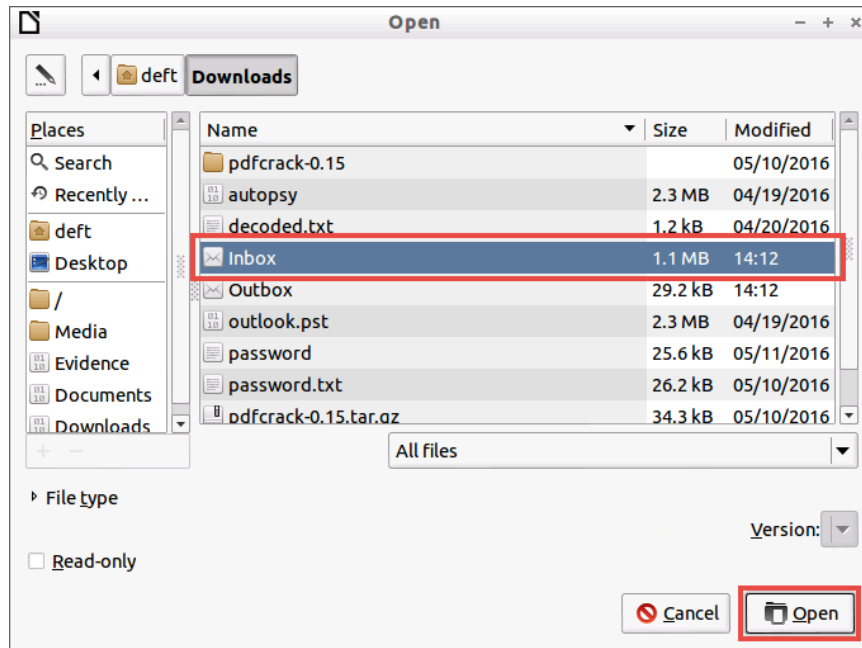
1. Open the *LibreOffice* application by navigating to **Menu > Office > LibreOffice**.



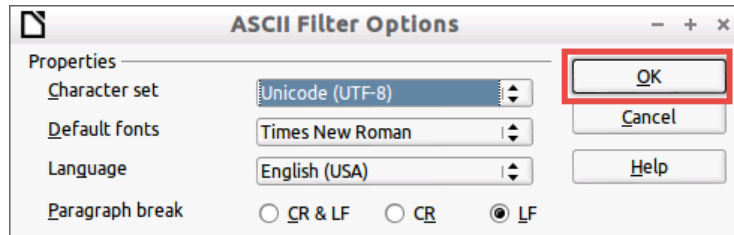
2. Using *LibreOffice*, click on **File** and select **Open**.



3. In the *Open* window, navigate to `/home/deft/Downloads/` and select the **Inbox** file in the middle pane. Click **Open**.

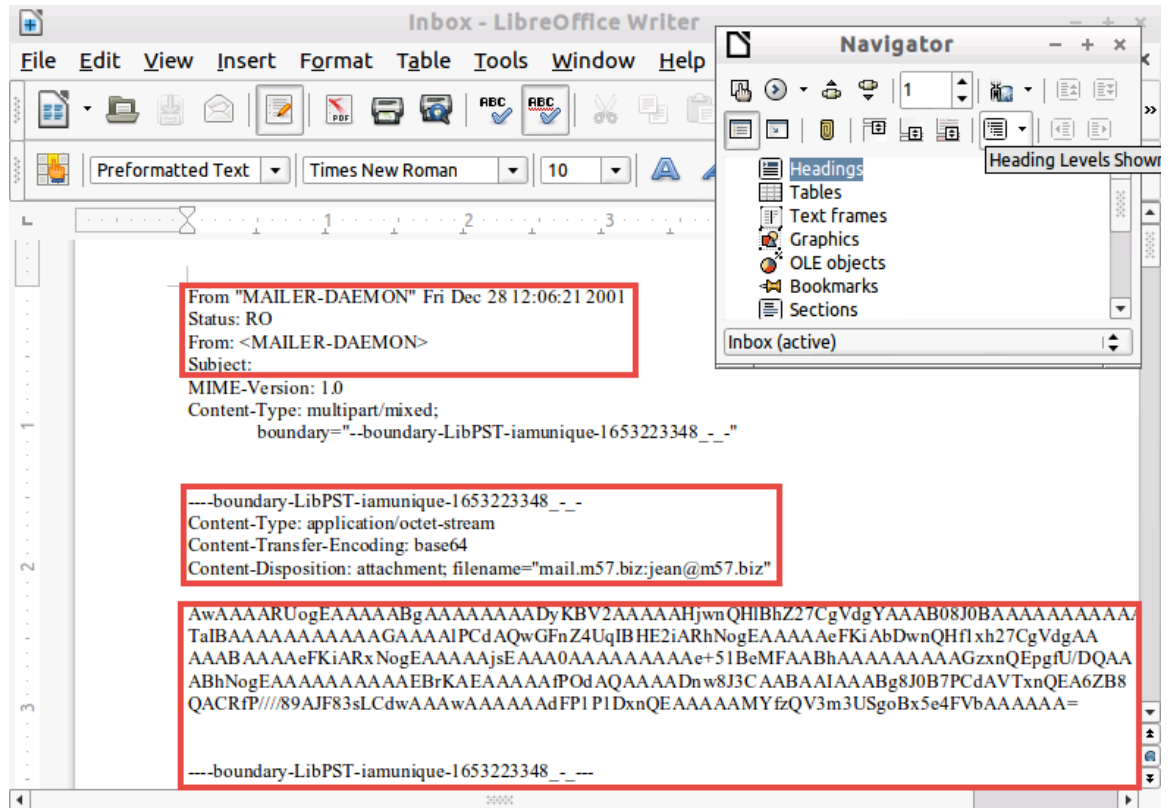


4. In the *ASCII Filter Options* dialog window, leave the defaults and click **OK**.





- Notice that the *Inbox* is now presented in readable format. Briefly analyze the email and take notice of the standard header. The *Multipurpose Internet Mail Extensions (MIME)* and “boundary” lines are also visible followed by hex code.



The “boundary” lines designate the non-ascii attachments. *SMTP* can’t transmit anything other than *ASCII* characters therefore attachments are encoded with *Base64* encoding to translate non-ascii into *ASCII* for transmission.

- Press **CTRL+F** to use the *Find* toolbar. Type `wmt.gif` to find a *GIF* that's encoded with *Base64*. Press the **Enter** key.

```

---boundary-LibPST-iamunique-482615150_--
Content-Type: image/gif
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
    filename*=utf-8"wmt.gif

R0IGODdhWAAfANUAAP/////zMyZAMxmM5nM/5nMzP/M///MzP/MmZnMmZnMZv/MAJmZmZmZZv+Z
mf+ZZv+ZM/+ZAJmZAJlmmWbMzGbmZv9mM2aZzGaZmWaZZmaZM2ZmmWZmZmZmM2YzZmOZzDNmzDNm
ZjNmM/8AAMz//zMzMzMzADMAMzM AAA CZzMz/8zMzACZmQBmzABmZgAzZgAzMwAzAAAAM8yZZgAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACwAAAAAWAAfAAAG/0CacEgsGo/Ip
HLJ
XAKe0Kh0Sq1ar9gsISMERL7gsHhMLpvP6PSYS/Oq33D4aE6v2+/1FdtbKnG+fV8cJQxsaYmIcWh4
j0jel2QiQxCfyU0hUKHmopmclpVc5BtK5SYbH+ahX8cHIV+Xwx9IzSx fa56uK2lure8DJ+gU6J7
X0KyQ5SJhrRDqTTNo7SZtZVcyH3 QhcAjwsOPxSuX45U0rJrjpq6ahkJ6ceVlyvurQz33N5SxJGj
5s0MRomDRs+cITbqBIZz50yhOzDBVICH5ozBE36kSiWLJnBcwVbsNFUa+M7dNEHN/qwltu2enkso
PJgQ0UEEtIvg+hWsZSpRR/+CldTRlPnQFLJaA+9dCriyGwAEvJqhgGDBgwYFGUyUwDnKDUlj5gSh
AxqW1ICHKgtm8snm4ZdgBxAcOPBgxgMaJixU1VBBAYytADB6RQqGsJhqYlyOYapGMUSnec8EQODg
bl4IVhtU0Mo1XMHChsOE7hQnYlwEfh5YgDbAA4oYfWB31snpc+0h9HaOjk2Gpat7DWjBcPFCQAQJ
KAALLpx7obHczUXzThOsglpXJy7BaAGi+IIFnAPnzBh9IW6kiHdOX+SuhPUCHzB8oLGdhXfwHmaT
R+ycefn63niFAUERACBfDR18IH3kUQ3nIAoqeeubtBp0ZFj72xBcEFNC0wgUp0CCDCzAMYUJy
+nkFFm5IZHhYgCyFUMgGgwzRxyvQcBeV2SgRxnLL4GXS3iQQWaLUEA4ABCUwgwiwBSVHKVhC+
KOGVz2H5X3RbpveWU/qk2KNuFxJpJpZa8hckUkqGwaV0hqV5ZpZzbvlim/q86d+aEzo5pI9IEikS
J3h6o2eAakhInSOM0sEjoorUx16jjD4K6aWYhoFKK5x26umnoIYq6qiklhpqE6imquqqqAYBAdS=

```



- Using the mouse, highlight only the hex characters for the `wmt.gif` section.

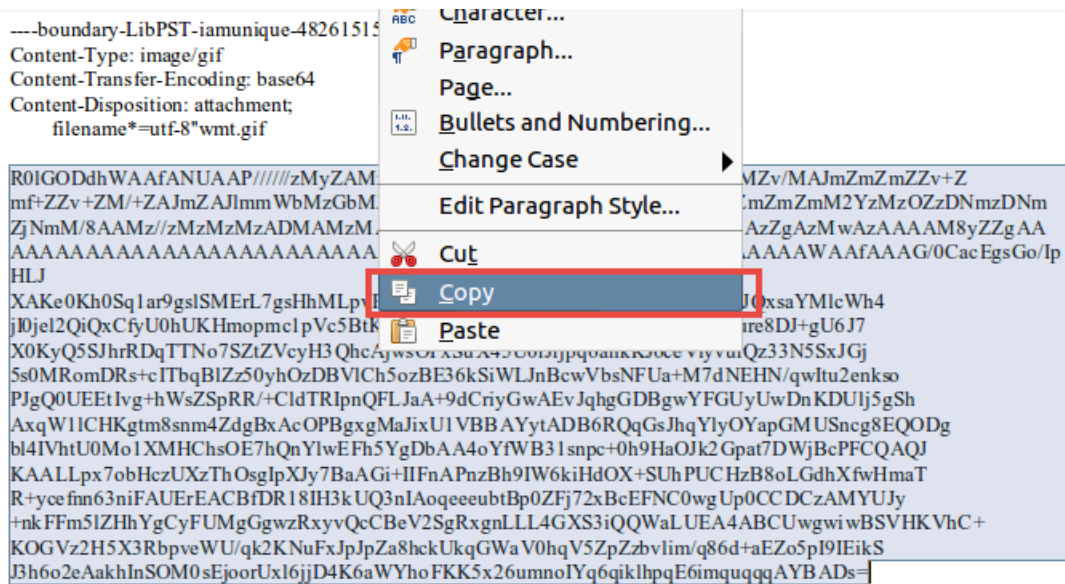
```

---boundary-LibPST-iamunique-482615150_--
Content-Type: image/gif
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
    filename*=utf-8"wmt.gif

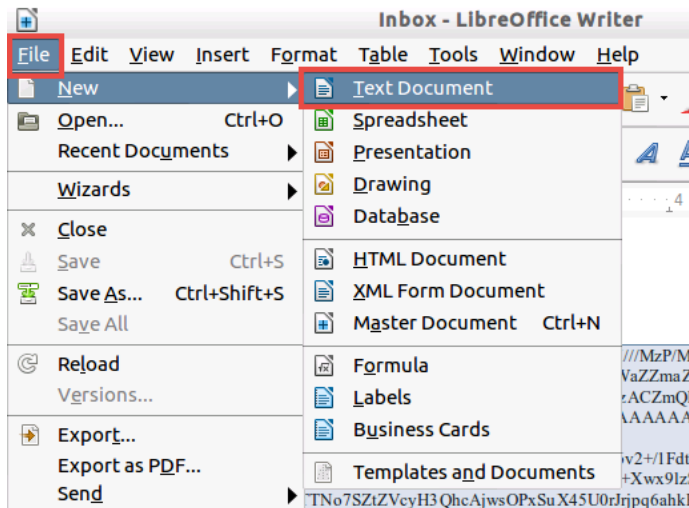
R0IGODdhWAAfANUAAP/////zMyZAMxmM5nM/5nMzP/M///MzP/MmZnMmZnMZv/MAJmZmZmZZv+Z
mf+ZZv+ZM/+ZAJmZAJlmmWbMzGbmZv9mM2aZzGaZmWaZZmaZM2ZmmWZmZmZmM2YzZmOZzDNmzDNm
ZjNmM/8AAMz//zMzMzMzADMAMzM AAA CZzMz/8zMzACZmQBmzABmZgAzZgAzMwAzAAAAM8yZZgAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACwAAAAAWAAfAAAG/0CacEgsGo/Ip
HLJ
XAKe0Kh0Sq1ar9gsISMERL7gsHhMLpvP6PSYS/Oq33D4aE6v2+/1FdtbKnG+fV8cJQxsaYmIcWh4
j0jel2QiQxCfyU0hUKHmopmclpVc5BtK5SYbH+ahX8cHIV+Xwx9IzSx fa56uK2lure8DJ+gU6J7
X0KyQ5SJhrRDqTTNo7SZtZVcyH3 QhcAjwsOPxSuX45U0rJrjpq6ahkJ6ceVlyvurQz33N5SxJGj
5s0MRomDRs+cITbqBIZz50yhOzDBVICH5ozBE36kSiWLJnBcwVbsNFUa+M7dNEHN/qwltu2enkso
PJgQ0UEEtIvg+hWsZSpRR/+CldTRlPnQFLJaA+9dCriyGwAEvJqhgGDBgwYFGUyUwDnKDUlj5gSh
AxqW1ICHKgtm8snm4ZdgBxAcOPBgxgMaJixU1VBBAYytADB6RQqGsJhqYlyOYapGMUSnec8EQODg
bl4IVhtU0Mo1XMHChsOE7hQnYlwEfh5YgDbAA4oYfWB31snpc+0h9HaOjk2Gpat7DWjBcPFCQAQJ
KAALLpx7obHczUXzThOsglpXJy7BaAGi+IIFnAPnzBh9IW6kiHdOX+SuhPUCHzB8oLGdhXfwHmaT
R+ycefn63niFAUERACBfDR18IH3kUQ3nIAoqeeubtBp0ZFj72xBcEFNC0wgUp0CCDCzAMYUJy
+nkFFm5IZHhYgCyFUMgGgwzRxyvQcBeV2SgRxnLL4GXS3iQQWaLUEA4ABCUwgwiwBSVHKVhC+
KOGVz2H5X3RbpveWU/qk2KNuFxJpJpZa8hckUkqGwaV0hqV5ZpZzbvlim/q86d+aEzo5pI9IEikS
J3h6o2eAakhInSOM0sEjoorUx16jjD4K6aWYhoFKK5x26umnoIYq6qiklhpqE6imquqqqAYBAdS=

```

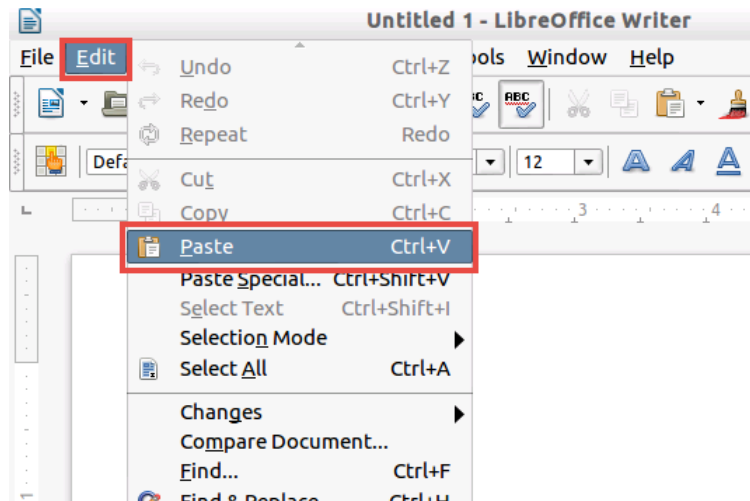
8. Right-click on the highlighted portion and select **Copy**.



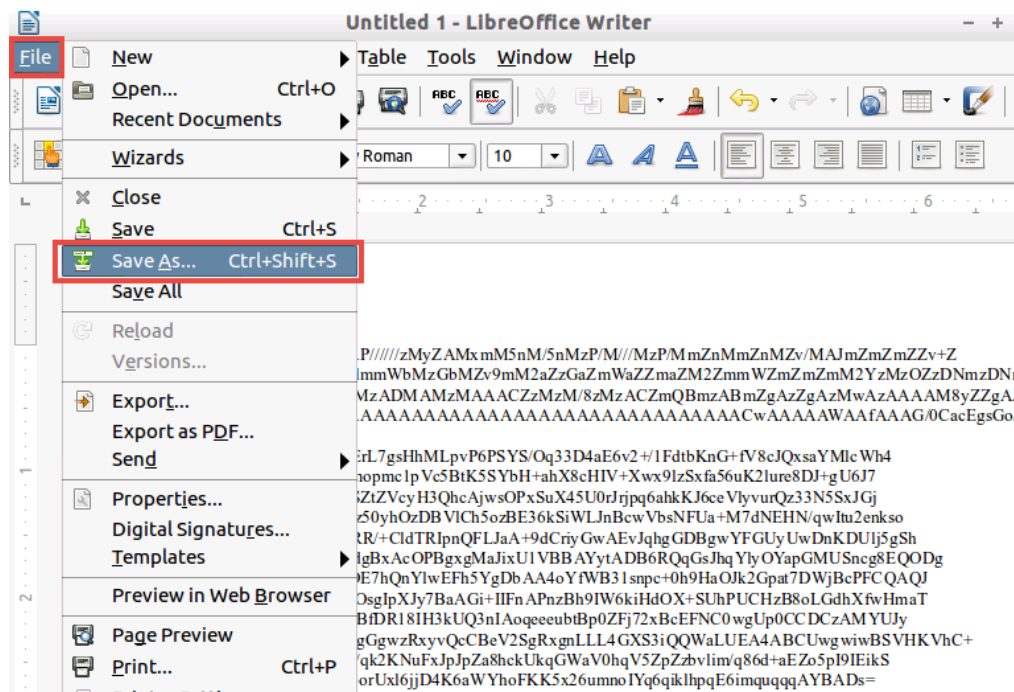
9. Click on **File** and select **New > Text Document**.



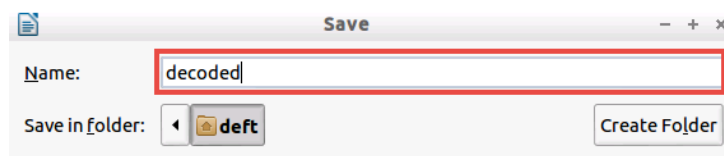
10. Click on **Edit** and select **Paste**.



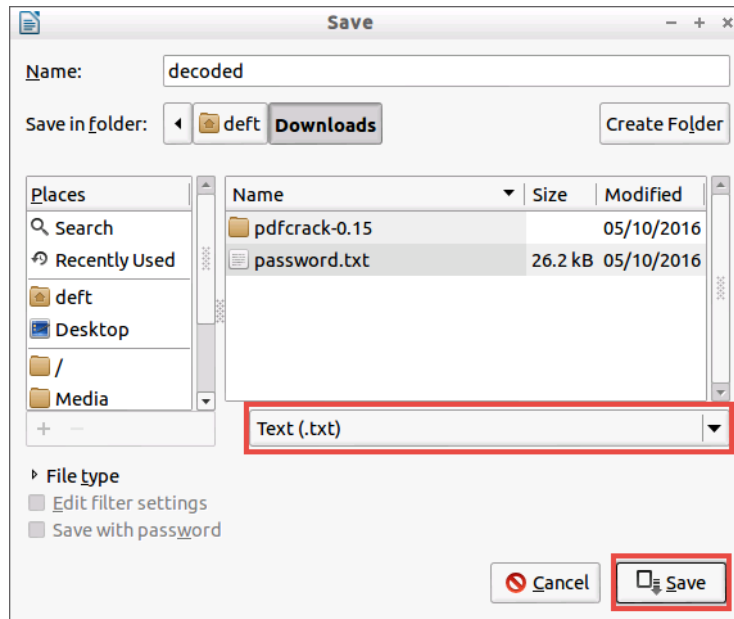
11. Once the information is pasted to a new document, save the file by navigating to **File > Save As**.



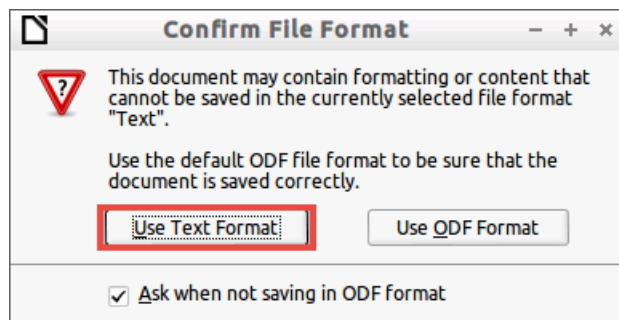
12. In the *Save* dialog window, type **decoded** in the *Name* text field.



13. In the *Save* dialog window, navigate to **/home/deft/Downloads/** and select the file type as **Text (.txt)** from the drop-down menu. Click **Save**.



14. If prompted for file format, click **Use Text Format**.



15. Change focus to the **terminal**.

16. Using the terminal, make sure to be in the `/home/deft/Downloads/` directory and enter the command below to confirm that the `decoded.txt` file is present.

```
ls -l
```

```
deft-virtual-machine ~/Downloads % ls -l
total 6248
-rw-r----- 1 deft deft 2326645 Apr 19 14:14 autopsy
-rw-rw-r-- 1 deft deft 1235 Aug 2 15:03 decoded.txt
-rw-rw-r-- 1 deft deft 1113480 Aug 2 14:12 Inbox
-rw-rw-r-- 1 deft deft 29162 Aug 2 14:12 Outbox
-rw-r----- 1 deft deft 2326528 Apr 19 14:14 outlook.pst
-rw-r--r-- 1 deft deft 25589 May 11 08:47 password
-rw-r--r-- 1 deft deft 26215 May 10 19:52 password.txt
drwxrwxr-x 2 deft deft 4096 May 10 20:12 pdfcrack-0.15
-rw-r--r-- 1 deft deft 34269 May 10 20:02 pdfcrack-0.15.tar.gz
-rw-rw-r-- 1 deft deft 480949 Aug 2 14:12 Sent Items
deft-virtual-machine ~/Downloads %
```

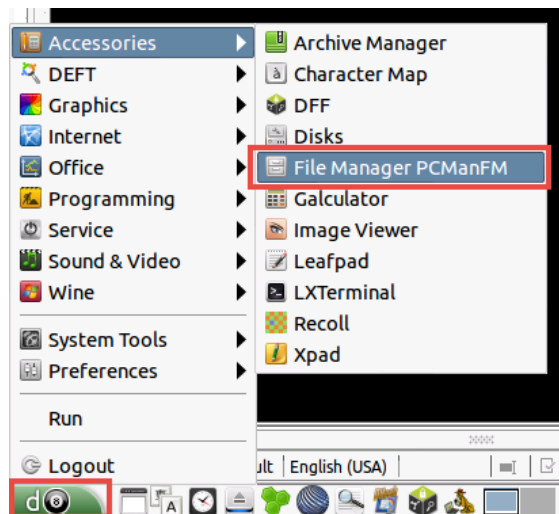
17. Decode the *Base64* encoding in the `decoded.txt` file by entering the command below.

```
dos2unix < decoded.txt | base64 -d > original
```

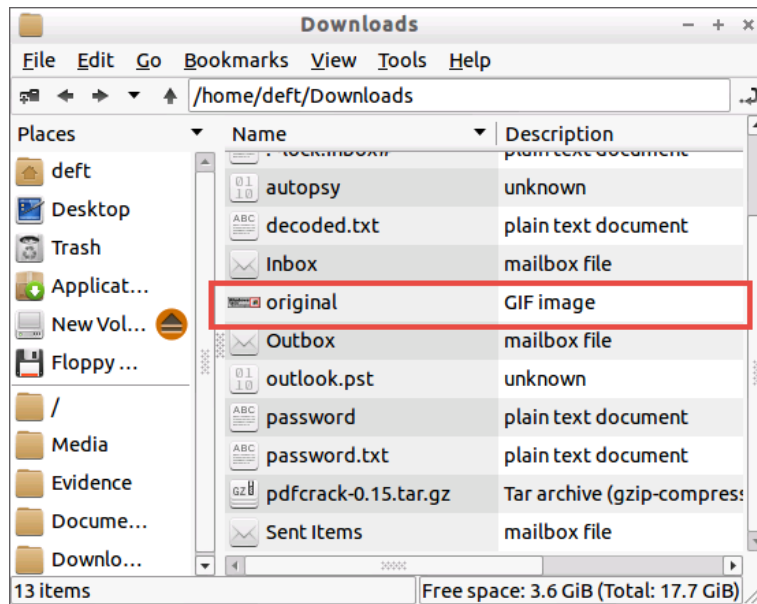
Dos2unix is a command that converts a text to *Unix* format. The *Base64* command with the `-d` argument means “decode” mode and the output will be to “original”.

```
deft-virtual-machine ~/Downloads % dos2unix < decoded.txt | base64 -d > original
deft-virtual-machine ~/Downloads %
```

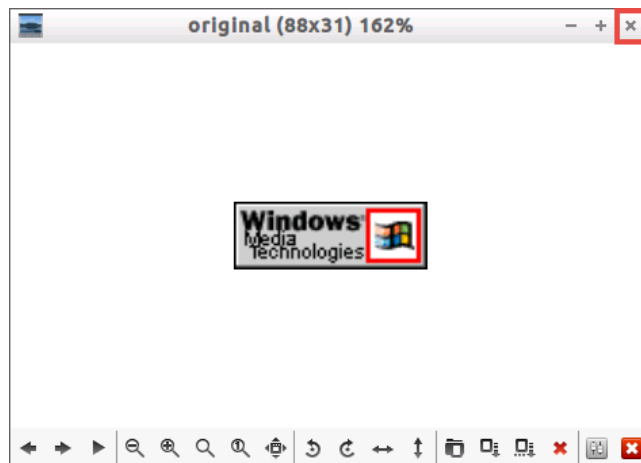
18. Open the file manager by navigating to **Menu > Accessories > File Manager PCManFM**.



19. Using the *file manager*, navigate to the **/home/deft/Downloads/** directory and notice the “*original*” file which can be represented as the “*original*” *GIF*. Double-click on the **original** file.

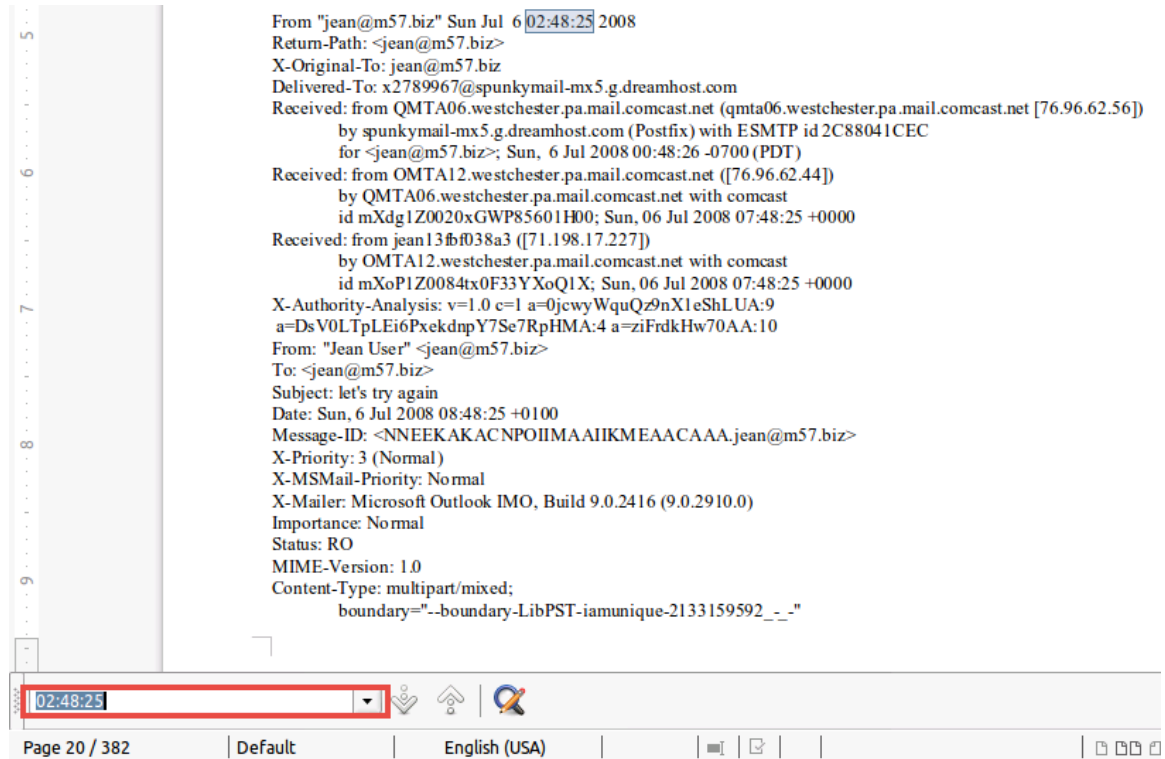


20. In the file preview window, notice the *GIF* contains the *Windows* logo. Close the window.



3 Analyzing Email Headers

1. Change focus to the **LibreOffice** application that has the *Inbox* file opened.
2. Press **CTRL+F** to bring up the *Find* toolbar and type **02:48:25** to search for a specific email. Press the **Enter** key.



From "jean@m57.biz" Sun Jul 6 02:48:25 2008
Return-Path: <jean@m57.biz>
X-Original-To: jean@m57.biz
Delivered-To: x2789967@spunkymail-mx5.g.dreamhost.com
Received: from QMTA06.westchester.pa.mail.comcast.net ([76.96.62.56])
by spunkymail-mx5.g.dreamhost.com (Postfix) with ESMTP id 2C88041CEC
for <jean@m57.biz>; Sun, 6 Jul 2008 00:48:26 -0700 (PDT)
Received: from OMTA12.westchester.pa.mail.comcast.net ([76.96.62.44])
by QMTA06.westchester.pa.mail.comcast.net with comcast
id mXdglZ0020xGWP85601H00; Sun, 06 Jul 2008 07:48:25 +0000
Received: from jean13bf038a3 ([71.198.17.227])
by OMTA12.westchester.pa.mail.comcast.net with comcast
id mXoP1Z0084tx0F33YXoQ1X; Sun, 06 Jul 2008 07:48:25 +0000
X-Authority-Analysis: v=1.0 c=1 a=0jcwYwQuQz9nX1eShLUA:9
a=DsV0LTpLEi6PxeKdnpY7Se7RpHMA:4 a=ziFrdkHw70AA:10
From: "Jean User" <jean@m57.biz>
To: <jean@m57.biz>
Subject: let's try again
Date: Sun, 6 Jul 2008 08:48:25 +0100
Message-ID: <NNEEKAKACNPOIIMAAIIKMEAACAAA.jean@m57.biz>
X-Priority: 3 (Normal)
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook IMO, Build 9.0.2416 (9.0.2910.0)
Importance: Normal
Status: RO
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="--boundary-LibPST-iamunique-2133159592_--"

02:48:25

Page 20 / 382 | Default | English (USA) | [Icons]



3. Notice that the area in the orange box seen below is the part of the header that indicates the incoming *SMTP* server of the message that it was delivered.

```

From "jean@m57.biz" Sun Jul 6 02:48:25 2008
Return-Path: <jean@m57.biz>
X-Original-To: jean@m57.biz
Delivered-To: x2789967@spunkymail-mx5.g.dreamhost.com
Received: from QMTA06.westchester.pa.mail.comcast.net (qmta06.westchester.pa.mail.comcast.net [76.96.62.56])
    by spunkymail-mx5.g.dreamhost.com (Postfix) with ESMTP id 2C88041CEC
    for <jean@m57.biz>; Sun, 6 Jul 2008 00:48:26 -0700 (PDT)
Received: from OMTA12.westchester.pa.mail.comcast.net ([76.96.62.44])
    by QMTA06.westchester.pa.mail.comcast.net with comcast
    id mXdg1Z0020xGWP85601H00; Sun, 06 Jul 2008 07:48:25 +0000
Received: from jean13fbf038a3 ([71.198.17.227])
    by OMTA12.westchester.pa.mail.comcast.net with comcast
    id mXoPlZ0084tx0F33YXoQ1X; Sun, 06 Jul 2008 07:48:25 +0000
X-Authority-Analysis: v=1.0 c=1 a=0jcwYwQuQz9nX1eShLUA:9
a=DsV0LTpLEi6PxeKdnpY7Se7RpHMA:4 a=ziFrdkHw70AA:10
From: "Jean User" <jean@m57.biz>
To: <jean@m57.biz>
Subject: let's try again
Date: Sun, 6 Jul 2008 08:48:25 +0100
Message-ID: <NNEEKAKACNPOIIMAAIIKMEACAAA.jean@m57.biz>
X-Priority: 3 (Normal)
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook IMO, Build 9.0.2416 (9.0.2910.0)
Importance: Normal
Status: RO
MIME-Version: 1.0
Content-Type: multipart/mixed;
    boundary="--boundary-LibPST-iamunique-2133159592_-_-"

```

4. Notice that the area in the orange box seen below is the part of the header that indicates the originator of the message as well as the *SMTP* server location based by *IP*.

```

From "jean@m57.biz" Sun Jul 6 02:48:25 2008
Return-Path: <jean@m57.biz>
X-Original-To: jean@m57.biz
Delivered-To: x2789967@spunkymail-mx5.g.dreamhost.com
Received: from QMTA06.westchester.pa.mail.comcast.net (qmta06.westchester.pa.mail.comcast.net [76.96.62.56])
    by spunkymail-mx5.g.dreamhost.com (Postfix) with ESMTP id 2C88041CEC
    for <jean@m57.biz>; Sun, 6 Jul 2008 00:48:26 -0700 (PDT)
Received: from OMTA12.westchester.pa.mail.comcast.net ([76.96.62.44])
    by QMTA06.westchester.pa.mail.comcast.net with comcast
    id mXdg1Z0020xGWP85601H00; Sun, 06 Jul 2008 07:48:25 +0000
Received: from jean13fbf038a3 ([71.198.17.227])
    by OMTA12.westchester.pa.mail.comcast.net with comcast
    id mXoPlZ0084tx0F33YXoQ1X; Sun, 06 Jul 2008 07:48:25 +0000
X-Authority-Analysis: v=1.0 c=1 a=0jcwYwQuQz9nX1eShLUA:9
a=DsV0LTpLEi6PxeKdnpY7Se7RpHMA:4 a=ziFrdkHw70AA:10
From: "Jean User" <jean@m57.biz>
To: <jean@m57.biz>
Subject: let's try again
Date: Sun, 6 Jul 2008 08:48:25 +0100
Message-ID: <NNEEKAKACNPOIIMAAIIKMEACAAA.jean@m57.biz>
X-Priority: 3 (Normal)
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook IMO, Build 9.0.2416 (9.0.2910.0)
Importance: Normal
Status: RO
MIME-Version: 1.0
Content-Type: multipart/mixed;
    boundary="--boundary-LibPST-iamunique-2133159592_-_-"

```

5. Notice that the area in the orange box seen below is the part of the message that is the body of the message generated by the client either by using the *POP* or *IMAP* protocol.

```

From "jean@m57.biz" Sun Jul 6 02:48:25 2008
Return-Path: <jean@m57.biz>
X-Original-To: jean@m57.biz
Delivered-To: x2789967@spunkymail-mx5.g.dreamhost.com
Received: from QMTA06.westchester.pa.mail.comcast.net (qmta06.westchester.pa.mail.comcast.net [76.96.62.56])
    by spunkymail-mx5.g.dreamhost.com (Postfix) with ESMTP id 2C88041CEC
    for <jean@m57.biz>; Sun, 6 Jul 2008 00:48:26 -0700 (PDT)
Received: from OMTA12.westchester.pa.mail.comcast.net ([76.96.62.44])
    by QMTA06.westchester.pa.mail.comcast.net with comcast
    id mXdg1Z0020xGWP85601H00; Sun, 06 Jul 2008 07:48:25 +0000
Received: from jean13fbf038a3 ([71.198.17.227])
    by OMTA12.westchester.pa.mail.comcast.net with comcast
    id mXoP1Z0084tx0F33YXoQ1X; Sun, 06 Jul 2008 07:48:25 +0000
X-Authority-Analysis: v=1.0 c=1 a=0jcwYwquQz9nX1eShLUA:9
a=DsV0LTpLEi6PxekdnY7Se7RpHMA:4 a=ziFrdkHw70AA:10
From: "Jean User" <jean@m57.biz>
To: <jean@m57.biz>
Subject: let's try again
Date: Sun, 6 Jul 2008 08:48:25 +0100
Message-ID: <NNEEKAKACNPOIIMAAIHKMEAACAAA.jean@m57.biz>
X-Priority: 3 (Normal)
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook IMO, Build 9.0.2416 (9.0.2910.0)
Importance: Normal
Status: RO
MIME-Version: 1.0
Content-Type: multipart/mixed;
    boundary="-boundary-LibPST-iamunique-2133159592_-_-"
  
```

6. Close all **PC Viewers** and end the reservation to complete the lab.