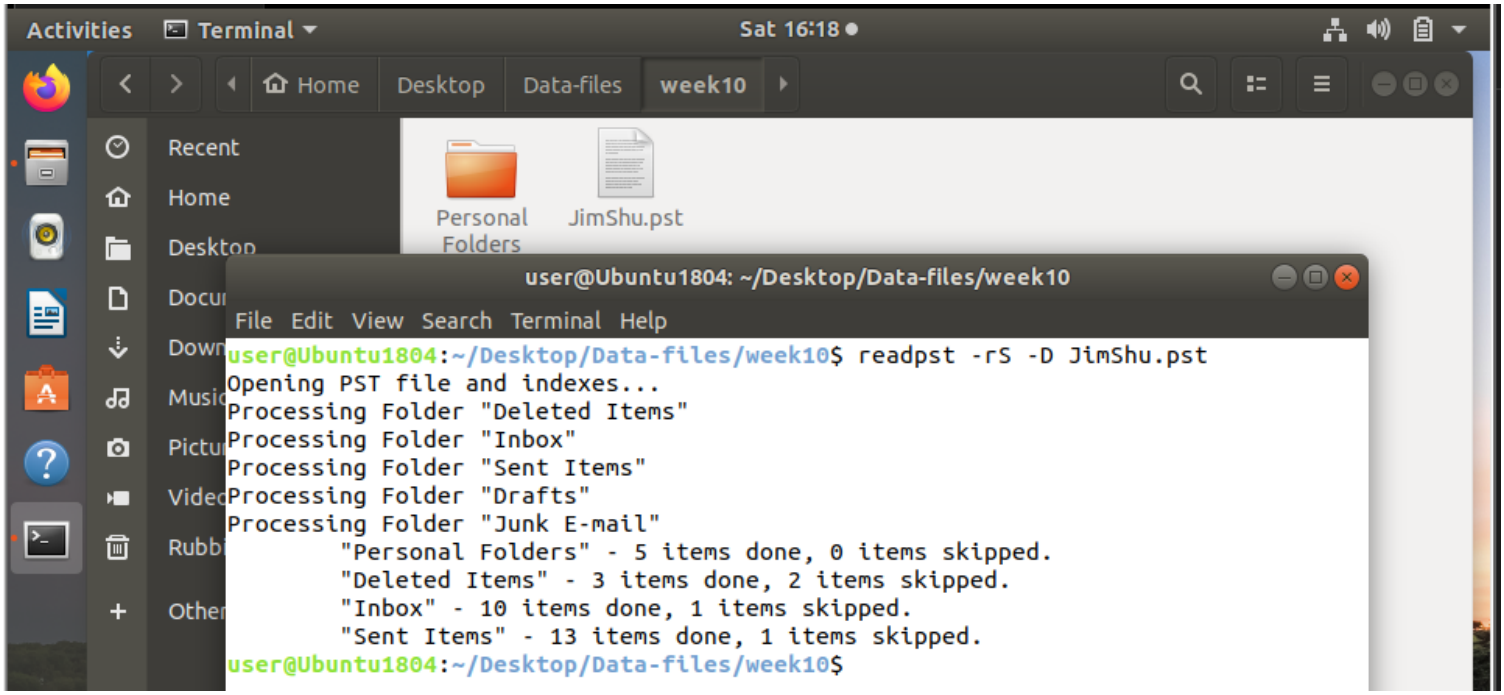
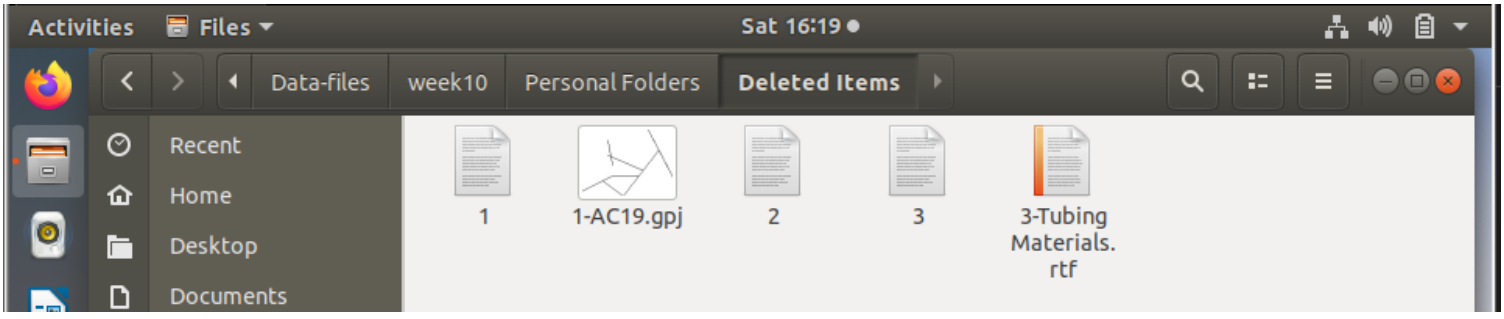
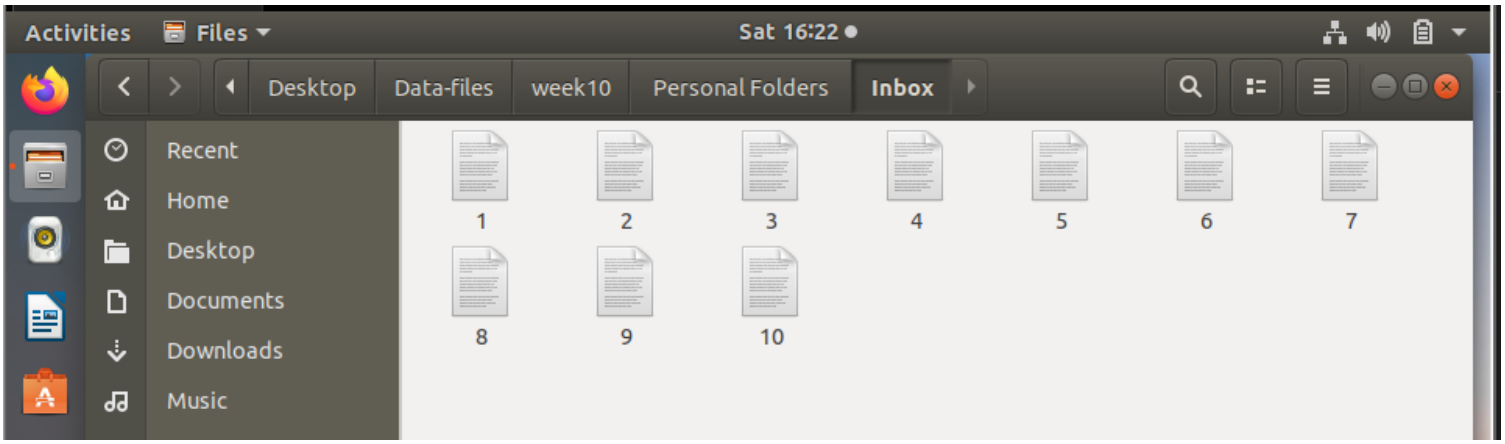
Investigating Outlook PST files with readpst

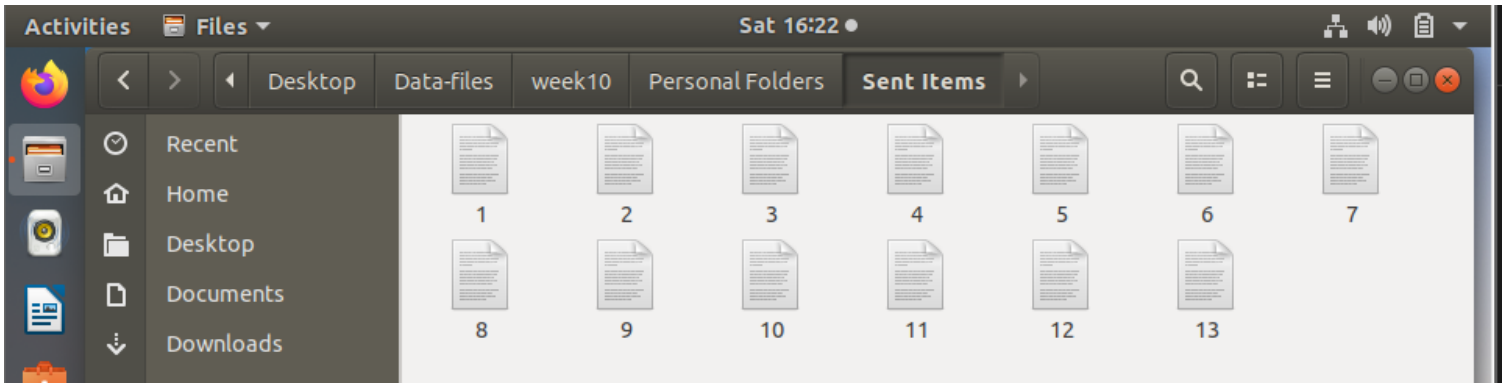
I analyzed emails using a new program called readpst. An introduction to examining Outlook PST files opened the session. It has come to my attention that PST files comprise an organization of attachment objects, message objects, and folder objects, all of which are essential for forensic examination. The presentation focused on the PST file security mechanism, emphasizing how readily crackable the password protection is.

Using the command "readpst -rS -D JimShu.pst," I opened the readpst application to begin the inquiry. This extracted every item in every folder—including deleted items—into distinct files. This produced the "Personal Folders" folder, which held all of the emails and attachments from the PST file.






Activities
Files
Sat 16:22
Desktop
Data-files
week10
Personal Folders
Inbox
Recent
Home
Desktop
Documents
Downloads
Music
1
2
3
4
5
6
7
8
9
10


Activities
Files
Sat 16:22
Desktop
Data-files
week10
Personal Folders
Sent Items
Recent
Home
Desktop
Documents
Downloads
1
2
3
4
5
6
7
8
9
10
11
12
13

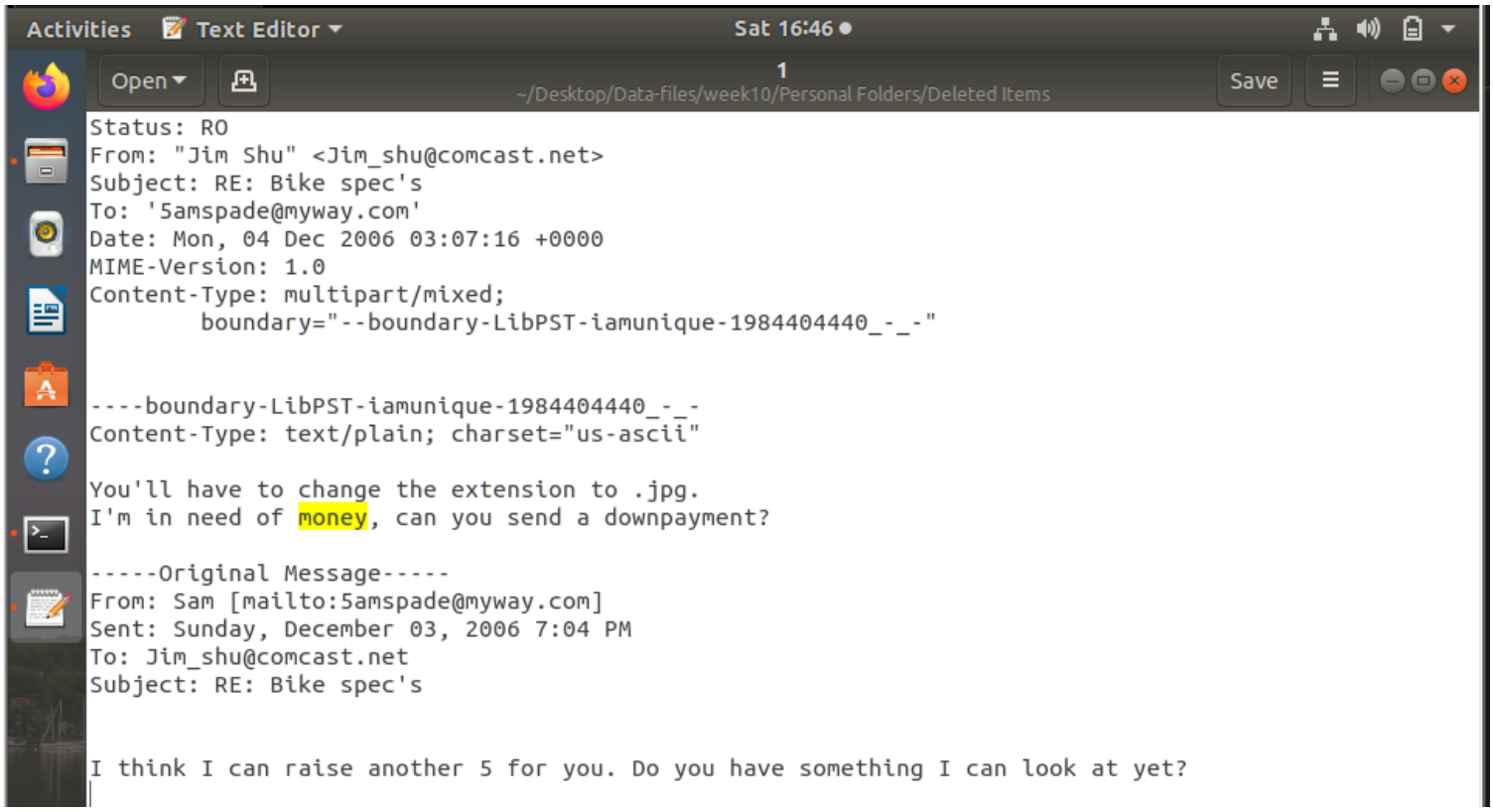
Forensic Tasks

I then conducted keyword searches for "money" and "cash" in the extracted contents to identify the sender and recipient of pertinent emails. In addition, I looked through all of the hits and deleted messages in an effort to locate a certain picture pertaining to bicycle tubing.

According to this email,

Sender – Sam (Samspade@myway.com)

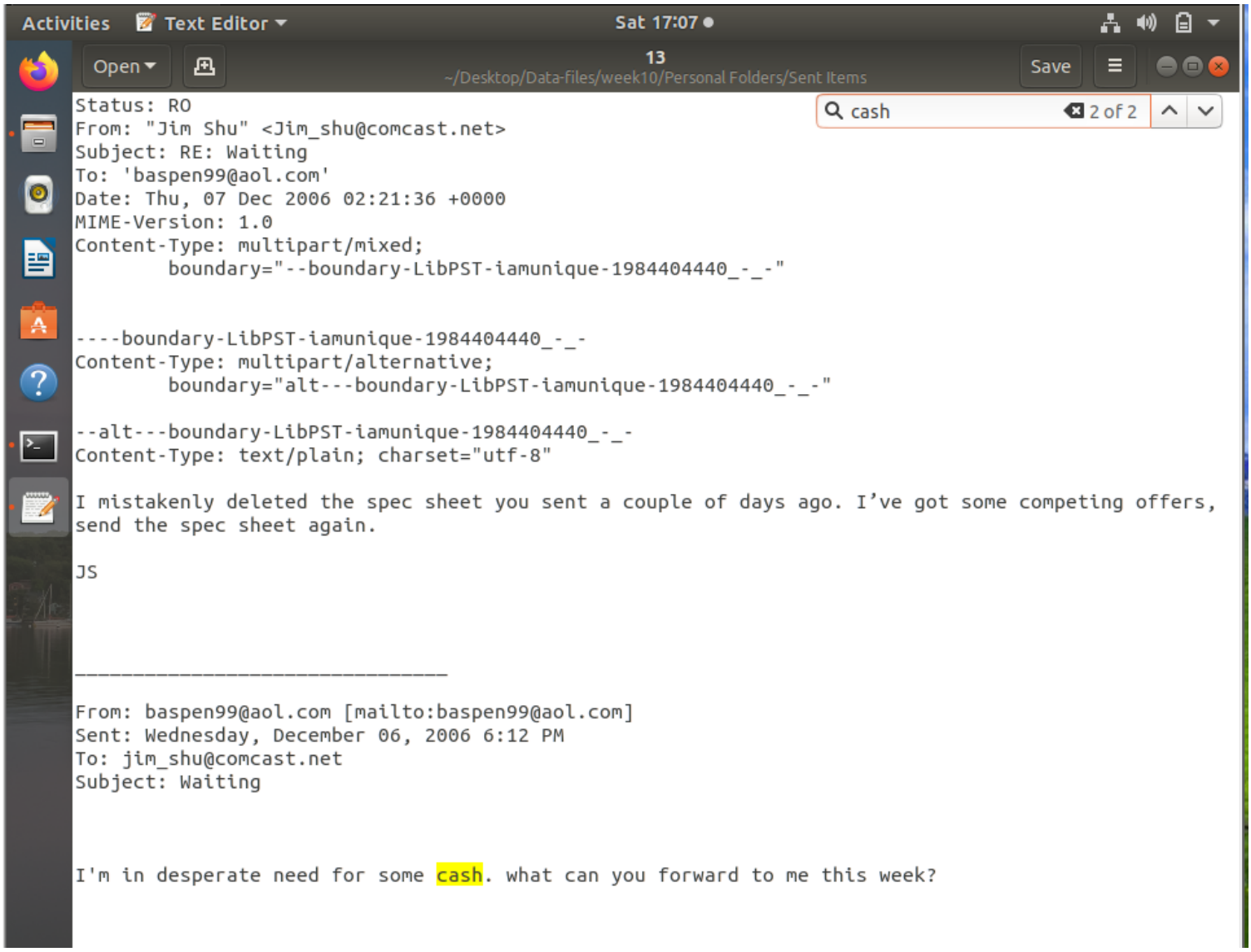
Receiver – Jim Shu (Jim_shiu@comcase.net)

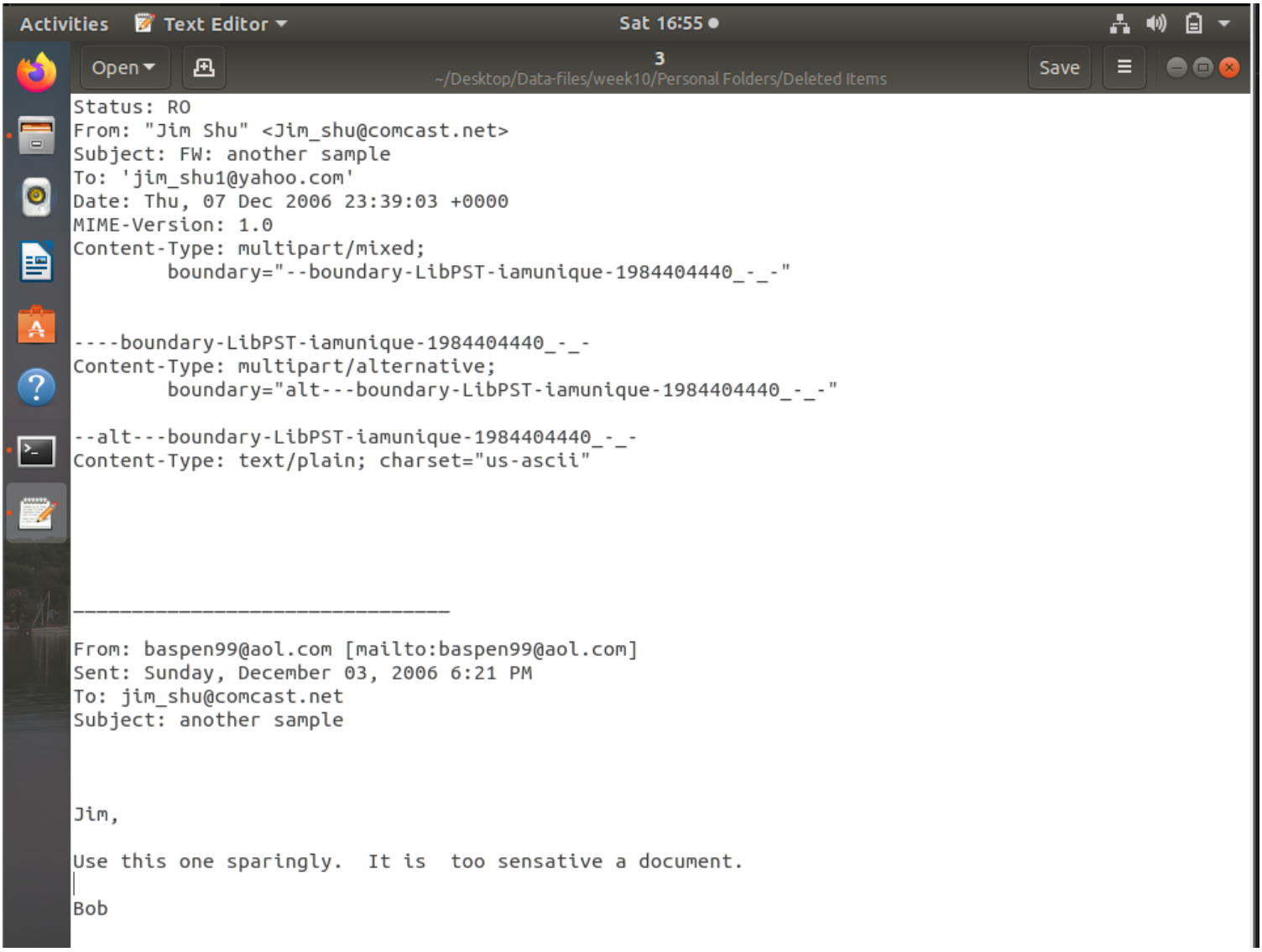


According to this email,

Sender – Bob (baspen99@aol.com)

Receiver – Jim Shu (Jim_shiu@comcase.net)

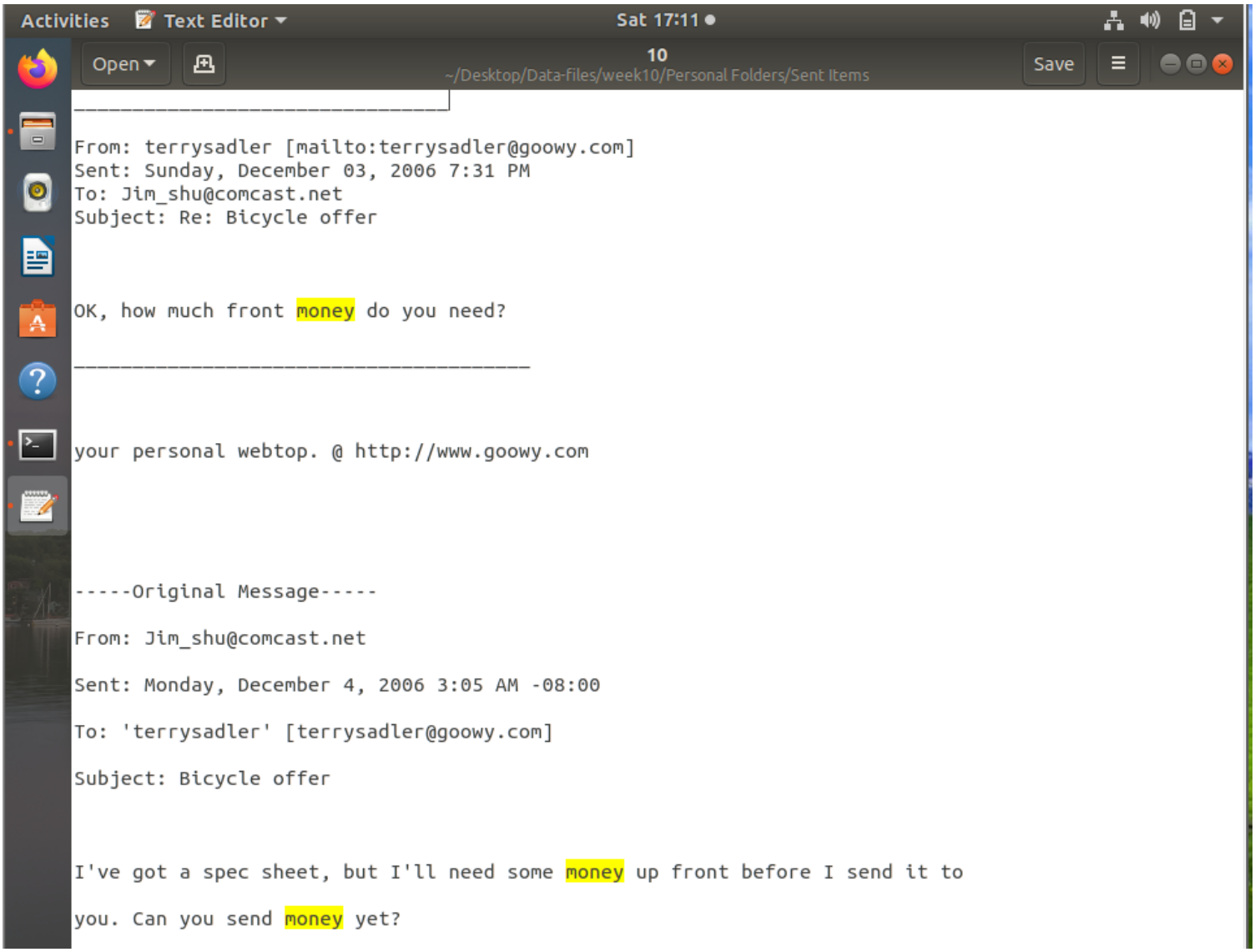


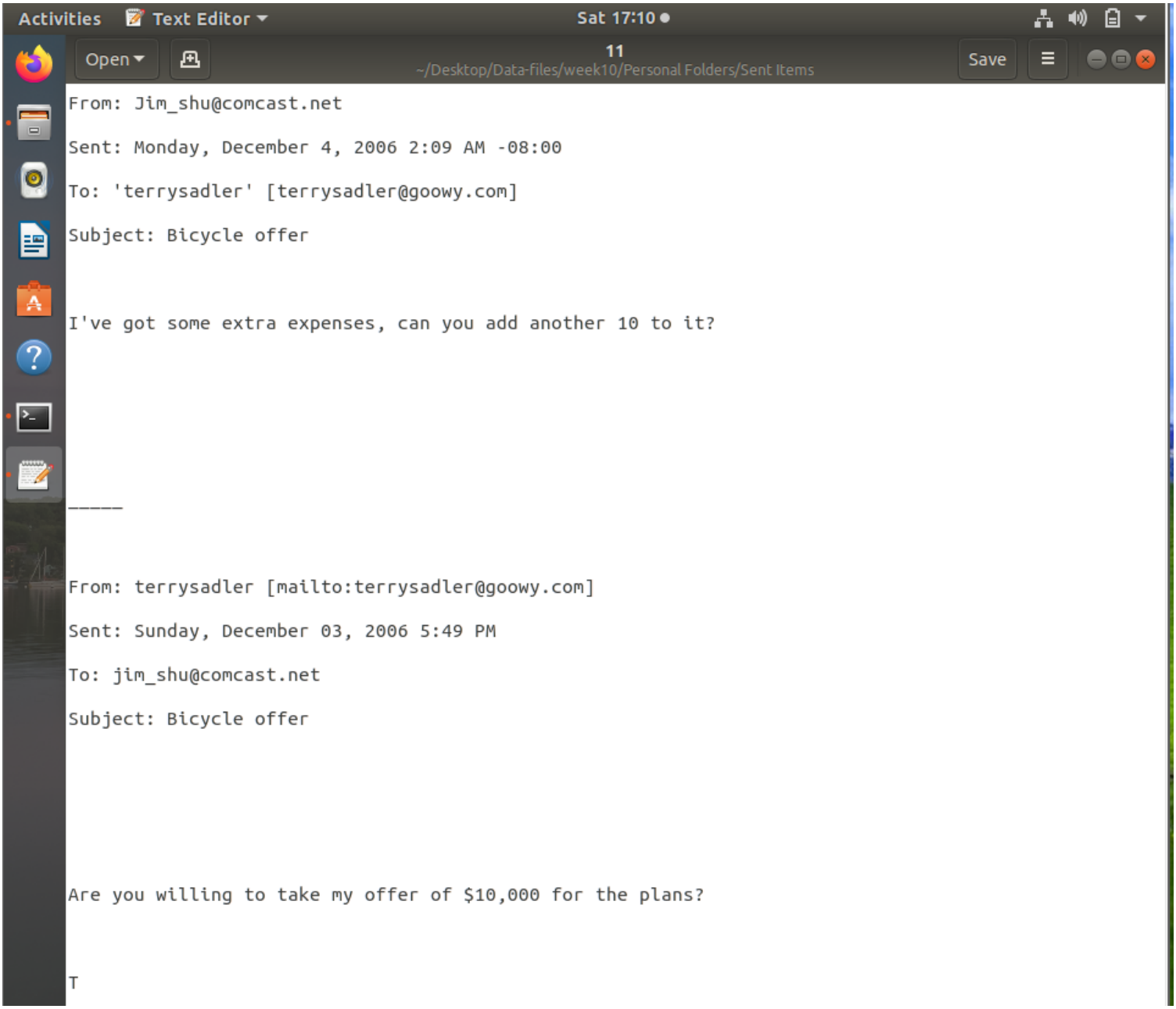

Activities
Text Editor
Sat 16:55
Open
3
~/Desktop/Data-files/week10/Personal Folders/Deleted Items
Save
Status: RO
From: "Jim Shu" <Jim_shu@comcast.net>
Subject: FW: another sample
To: 'jim_shu1@yahoo.com'
Date: Thu, 07 Dec 2006 23:39:03 +0000
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="--boundary-LibPST-iamunique-1984404440_-_-"
----boundary-LibPST-iamunique-1984404440_-_-
Content-Type: multipart/alternative;
boundary="alt---boundary-LibPST-iamunique-1984404440_-_-"
--alt---boundary-LibPST-iamunique-1984404440_-_-
Content-Type: text/plain; charset="us-ascii"
_____
From: baspen99@aol.com [mailto:baspen99@aol.com]
Sent: Sunday, December 03, 2006 6:21 PM
To: jim_shu@comcast.net
Subject: another sample
Jim,
Use this one sparingly. It is too sensative a document.
Bob

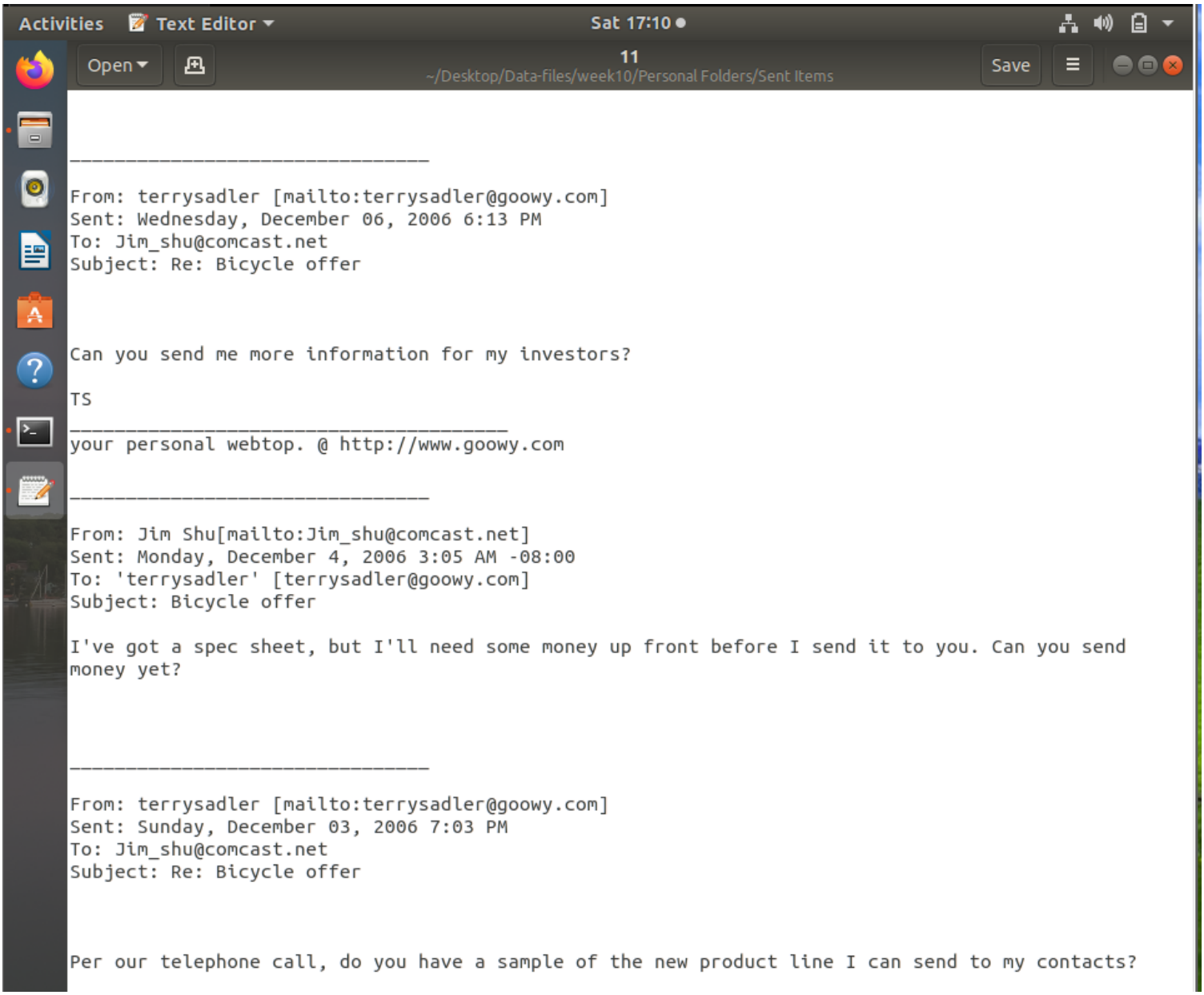
According to this email,

Sender – Terrysadler (terrysadler@goowy.com)

Receiver – Jim Shu (Jim_shiu@comcase.net)




Activities
Text Editor
Sat 17:10
Open
11
~/Desktop/Data-files/week10/Personal Folders/Sent Items
Save
From: Jim_shu@comcast.net
Sent: Monday, December 4, 2006 2:09 AM -08:00
To: 'terrysadler' [terrysadler@goowy.com]
Subject: Bicycle offer
I've got some extra expenses, can you add another 10 to it?
_____
From: terrysadler [mailto:terrysadler@goowy.com]
Sent: Sunday, December 03, 2006 5:49 PM
To: jim_shu@comcast.net
Subject: Bicycle offer
Are you willing to take my offer of $10,000 for the plans?
T



_____

From: terrysadler [mailto:terrysadler@goowy.com]
Sent: Wednesday, December 06, 2006 6:13 PM
To: Jim_shu@comcast.net
Subject: Re: Bicycle offer

Can you send me more information for my investors?

TS

_____
your personal webtop. @ http://www.goowy.com

_____

From: Jim Shu[mailto:Jim_shu@comcast.net]
Sent: Monday, December 4, 2006 3:05 AM -08:00
To: 'terrysadler' [terrysadler@goowy.com]
Subject: Bicycle offer

I've got a spec sheet, but I'll need some money up front before I send it to you. Can you send money yet?

_____

From: terrysadler [mailto:terrysadler@goowy.com]
Sent: Sunday, December 03, 2006 7:03 PM
To: Jim_shu@comcast.net
Subject: Re: Bicycle offer

Per our telephone call, do you have a sample of the new product line I can send to my contacts?

The image I found was: a JPEG file which is related to tubing material for a bicycle.