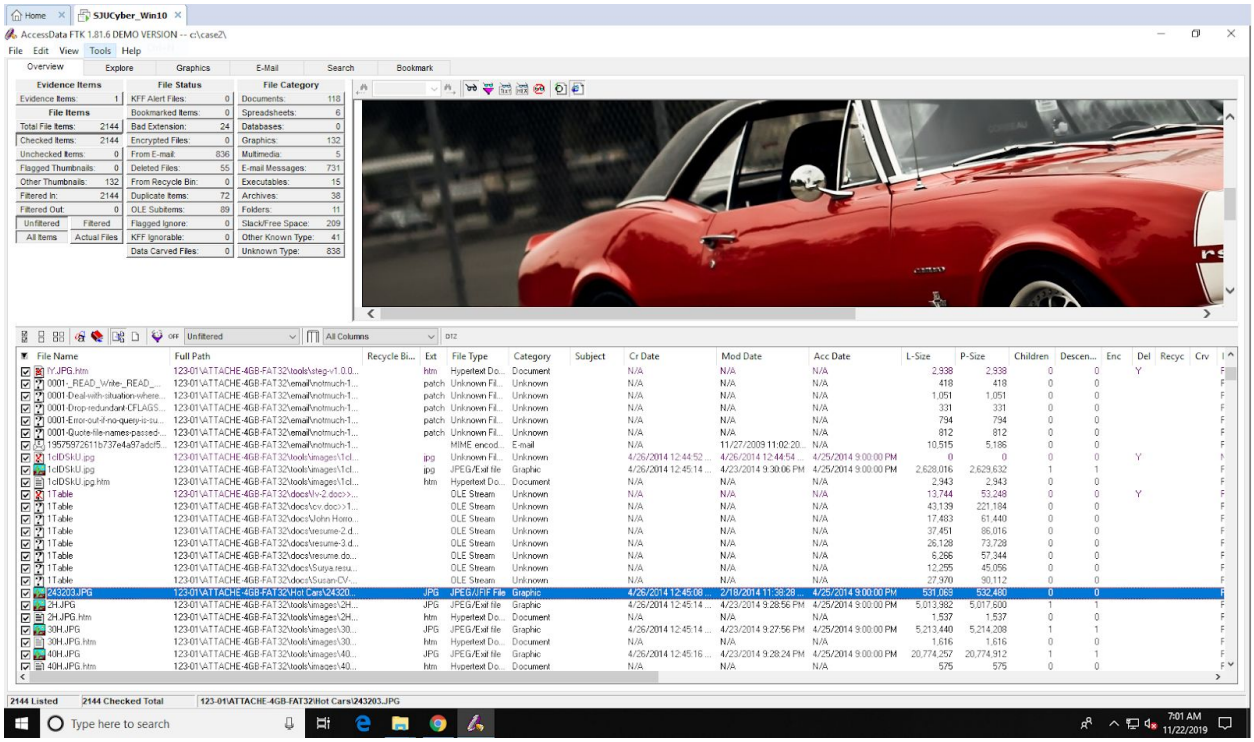
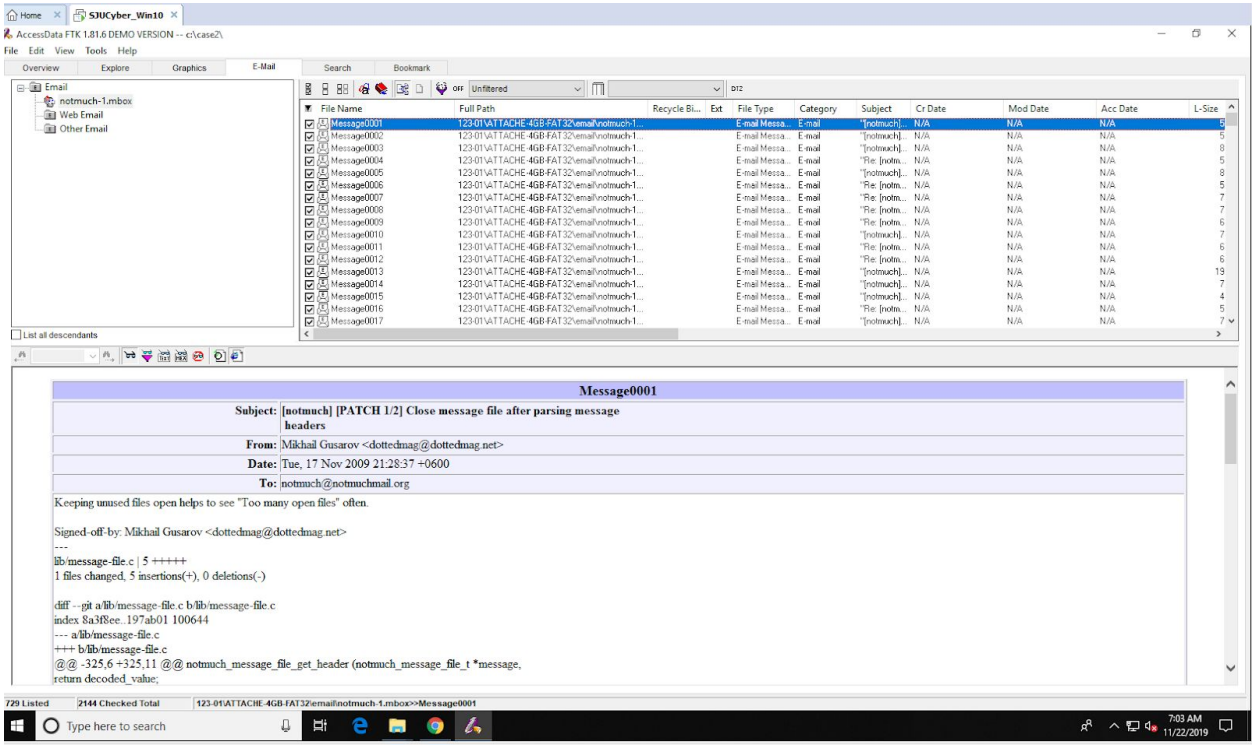
Philip Herman

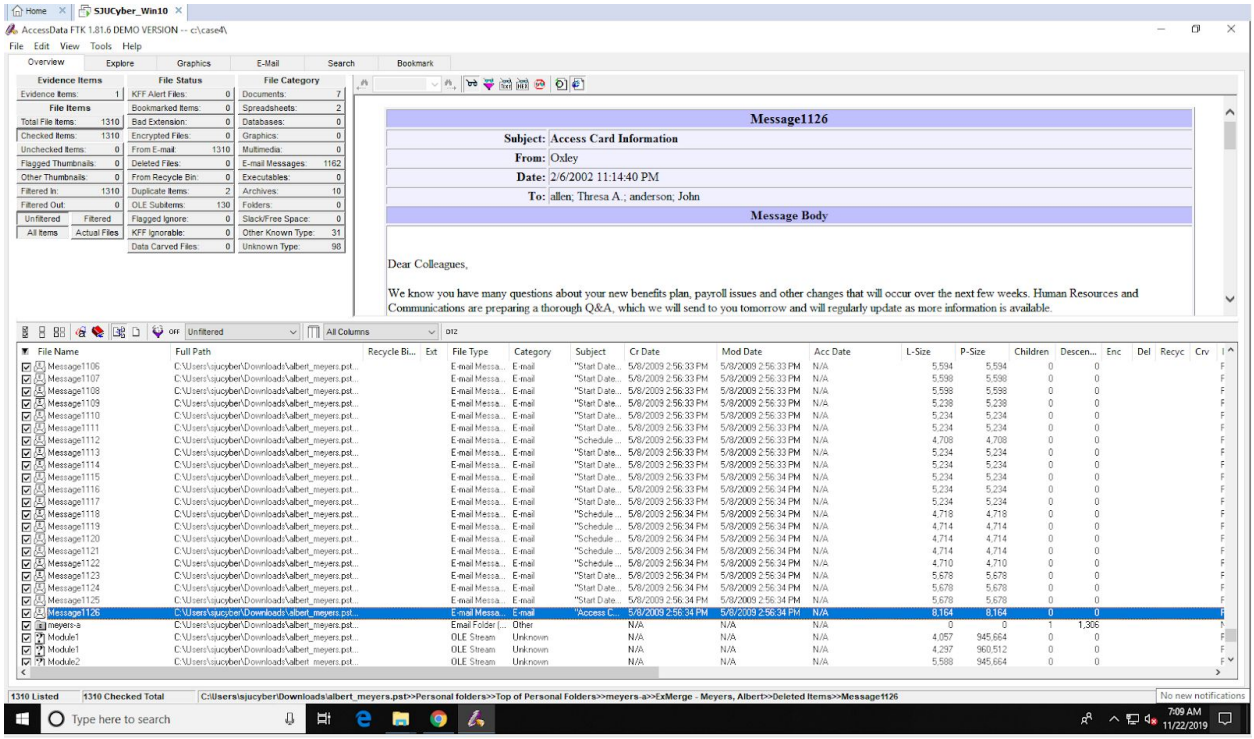
Lab #5 Summary

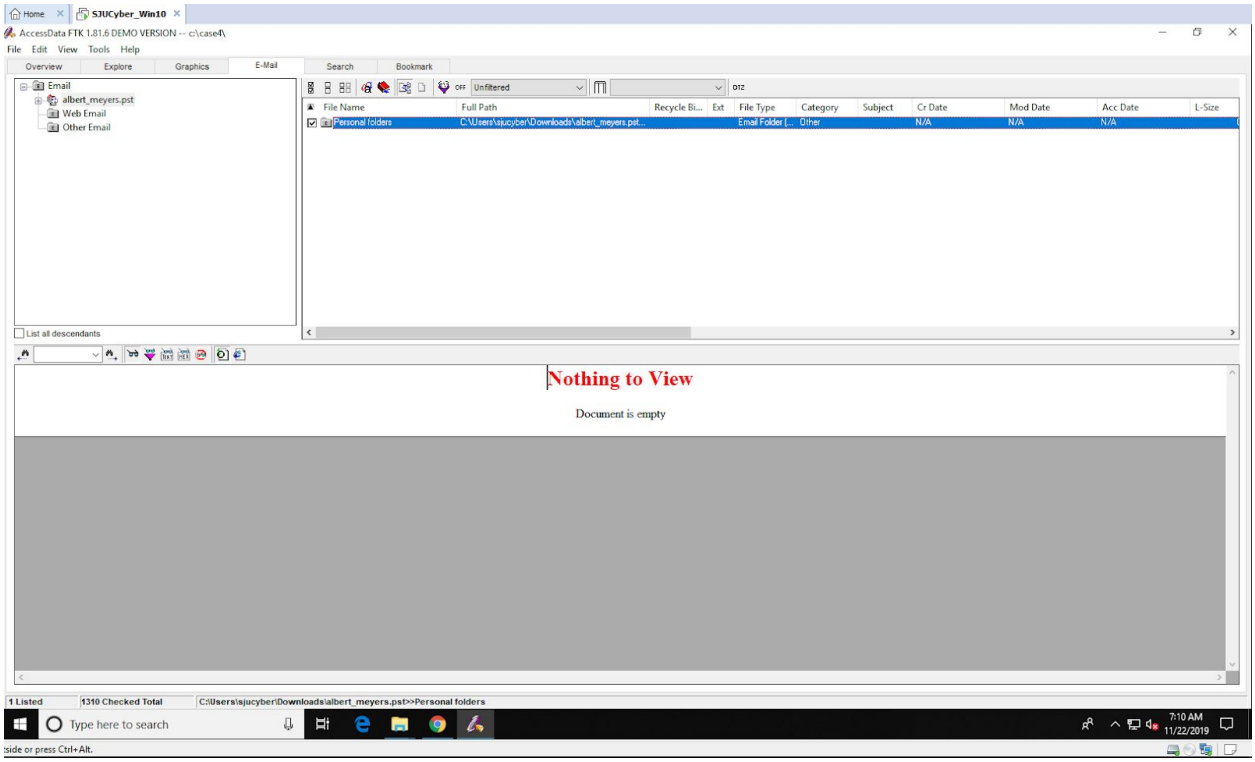
Just as the previous labs, I performed this lab with John Kamen, and we ended up with the same results in the end. We began the lab by opening up FTK on the Virtual Machine and running it as an administrator and when prompted, I ran it in demo mode. After the window stating Security Device Settings popped out and then pressed cancel to save this. After that, I opened up a new case and as per usual, filled out the investigator name, case number and case name with my name, the number one and case one. For the next screen, which displayed Forensic Examiner Information, all of those were left blank on purpose since there was no need to fill them out and I proceeded to the next screen which asked about the different Processes to Perform and I had selected all the options that had been listed. Then, the screens that asked about the Case Refinement and Index Refinement, I left those with the choices that had been checked off and I had then been able to add evidence to the case in FTK. I added the evidence of the *.e01 file by selecting the Acquired Image of Drive and then choosing the time zone as the New York time zone. Next FTK started loading and performing all the required actions by sorting through all the data that could be found in the *.e01 file. After everything loaded, I looked and viewed what was in that file and it was a lot of various different emails files. Next, I followed the same exact steps to create another case and this time I added the individual file called “albert_meyers.pst” however instead of adding it as an Acquired Image of Drive, I selected the individual file option and let FTK sort through everything. I was able to also see email files from this pst file, just as with the *.e01 file. However, with the pst file, the emails were stored in the web email tab under email section but for the *.e01 file, the emails were stored

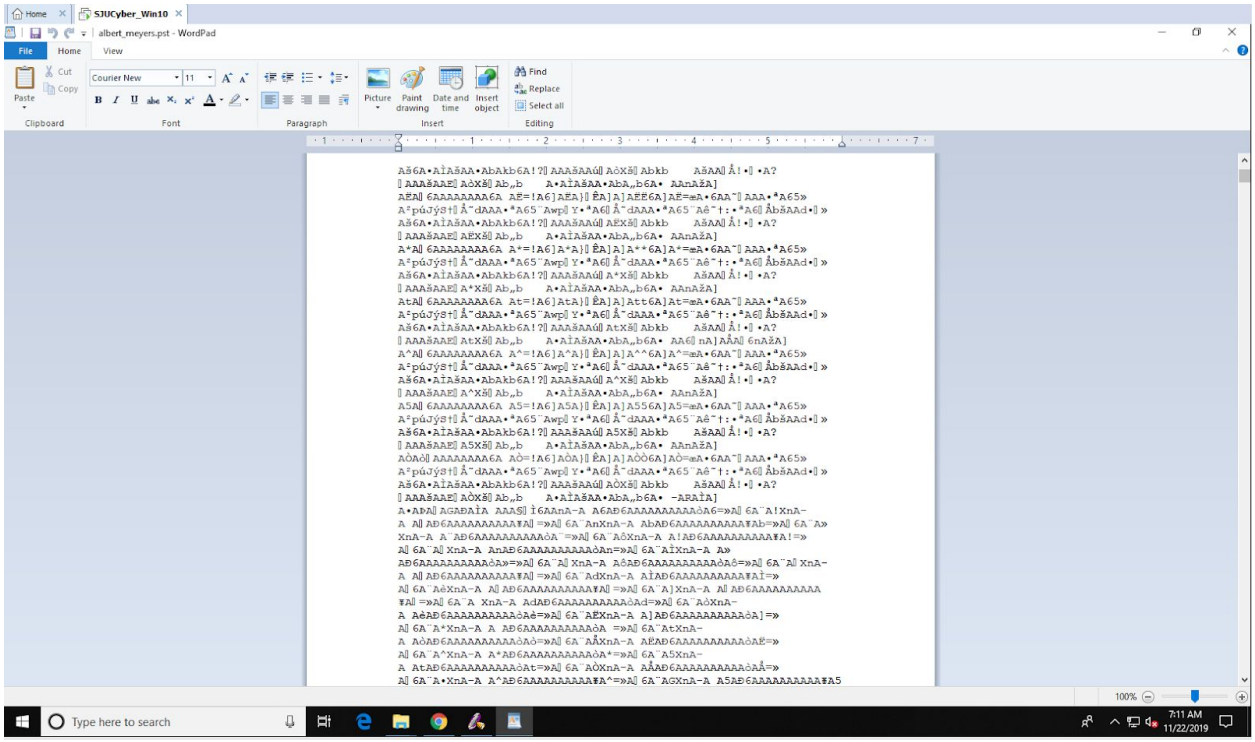
under the notmuch-1.mbox tab in the email section. After that, I opened both the inbox.mbox file and albert_myers.pst file in a enhanced text editor and both displayed a lot of various text that was not legible for me since it was in hex. Next, I downloaded Xiao Steganography from the provided Steg resource website and when prompted to select a target file, I selected the original-zebras.bmp file that I found in the StegTools.zip folder. Then, I chose the file that would be imbedded, which would be the cryptib.dll file and for the Encryption Options, I chose RC2 for the Encryption Algorithms and MD5 for the Hashing Algorithms and the password that we had chosen was password123, as I best remember. After putting in the assigned password, the program completed the steganography, resulting with a new image that I called 1.bmp. After that, we had completed the lab and had created a stegged image to the best of our abilities and below are the screenshots of our lab.

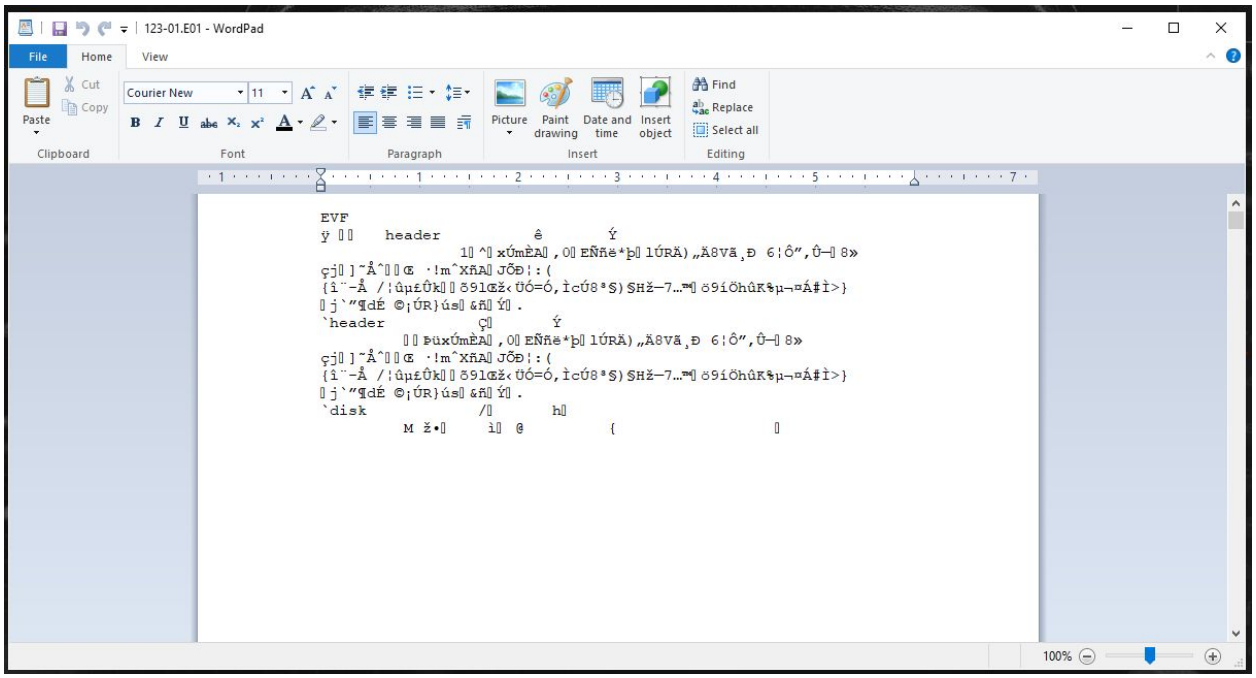

Home
SJUCyber_Win10
AccessData FTK 1.81.6 DEMO VERSION -- c:\case2\
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
Evidence Items
File Status
File Category
File Name
Full Path
Recycle Bi...
Ext
File Type
Category
Subject
Cr Date
Mod Date
Acc Date
L-Size
P-Size
Children
Descen...
Enc
Del
Recyc
Crv
2144 Listed
2144 Checked Total
123-01\ATTACHE-4GB-FAT32\Hot Cars\243203.JPG
Type here to search
7:01 AM
11/22/2019

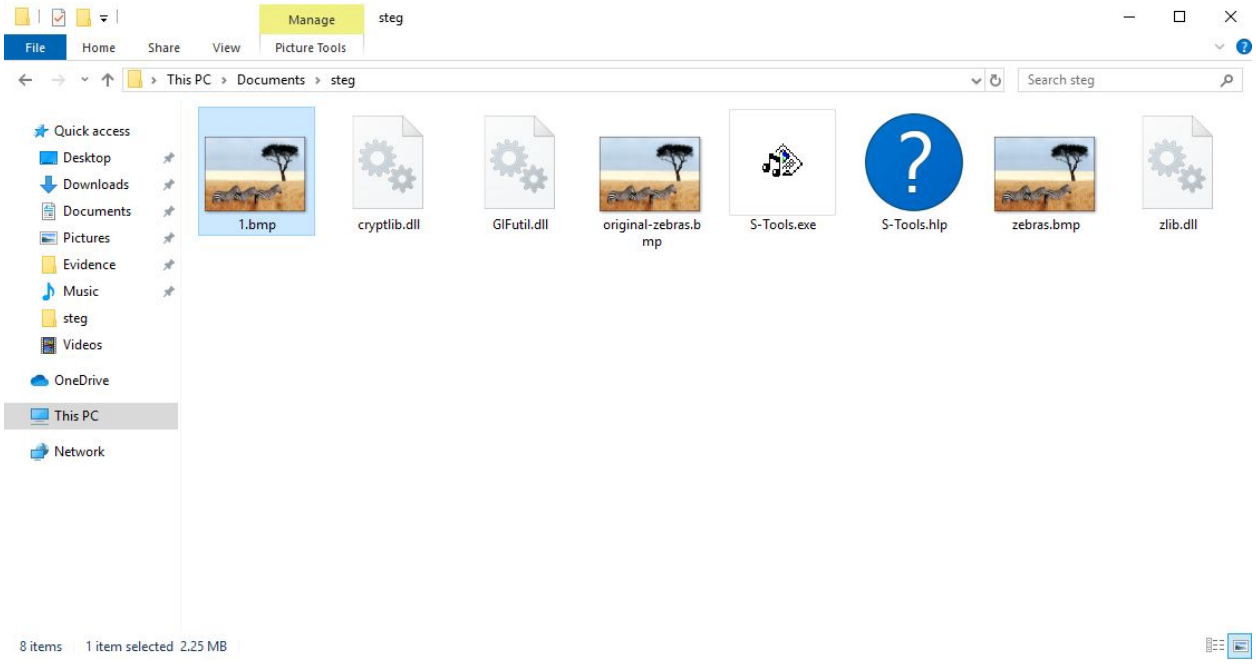

Home
SJUCyber_Win10
AccessData FTK 1.81.6 DEMO VERSION -- c:\case2\
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
Email
notmuch-1.mbox
Web Email
Other Email
List all descendants
Message0001
Subject: [notmuch] [PATCH 1/2] Close message file after parsing message headers
From: Mikhail Gusarov <dottedmag@dottedmag.net>
Date: Tue, 17 Nov 2009 21:28:37 +0600
To: notmuch@notmuchmail.org
Keeping unused files open helps to see "Too many open files" often.
Signed-off-by: Mikhail Gusarov <dottedmag@dottedmag.net>
---
lib/message-file.c | 5 +++++
1 files changed, 5 insertions(+), 0 deletions(-)
diff --git a/lib/message-file.c b/lib/message-file.c
index 8a3f8ee..197ab01 100644
--- a/lib/message-file.c
+++ b/lib/message-file.c
@@ -325,6 +325,11 @@ notmuch_message_file_get_header (notmuch_message_file_t *message,
return decoded_value;
729 Listed
2144 Checked Total
123-01\ATTACHE-4GB-FAT32\email\notmuch-1.mbox>>Message0001
Type here to search
7:03 AM
11/22/2019


Message1126
Subject: Access Card Information
From: Oxley
Date: 2/6/2002 11:14:40 PM
To: allen; Thresa A.; anderson; John
Message Body
Dear Colleagues,
We know you have many questions about your new benefits plan, payroll issues and other changes that will occur over the next few weeks. Human Resources and Communications are preparing a thorough Q&A, which we will send to you tomorrow and will regularly update as more information is available.


Nothing to View
Document is empty


Home
SJUCyber_Win10
albert_meyers.pst - WordPad
File
Home
View
Cut
Copy
Paste
Clipboard
Courier New
11
Font
Paragraph
Picture
Paint drawing
Date and time
Insert object
Insert
Find
Replace
Select all
Editing
100%
Type here to search
7:11 AM
11/22/2019


123-01.E01 - WordPad
File
Home
View
Paste
Cut
Copy
Courier New
11
Clipboard
Font
Paragraph
Picture
Paint drawing
Date and time
Insert object
Insert
Find
Replace
Select all
Editing
EVF
header
header
100%


Manage
steg
File
Home
Share
View
Picture Tools
This PC
Documents
steg
Search steg
Quick access
Desktop
Downloads
Documents
Pictures
Evidence
Music
steg
Videos
OneDrive
This PC
Network
1.bmp
cryptlib.dll
GIFutil.dll
original-zebras.bmp
S-Tools.exe
S-Tools.hlp
zebras.bmp
zlib.dll
8 items
1 item selected 2.25 MB