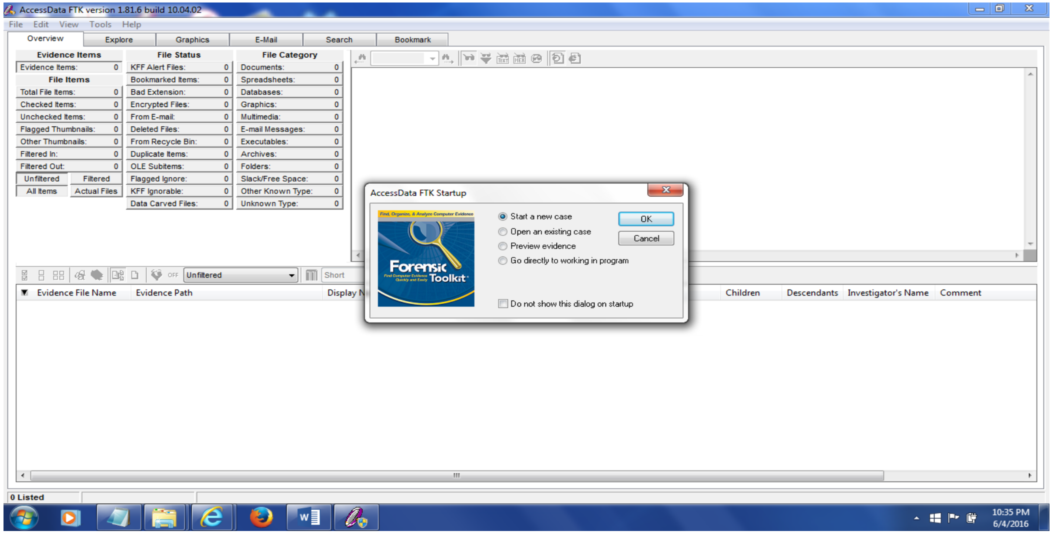
1. Run FTK 1.8.6 on your desktop by double click on the icon


AccessData FTK version 1.81.6 build 10.04.02
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
Evidence Items
File Status
File Category
Evidence File Name
Evidence Path
0 Listed
10:35 PM
6/4/2016

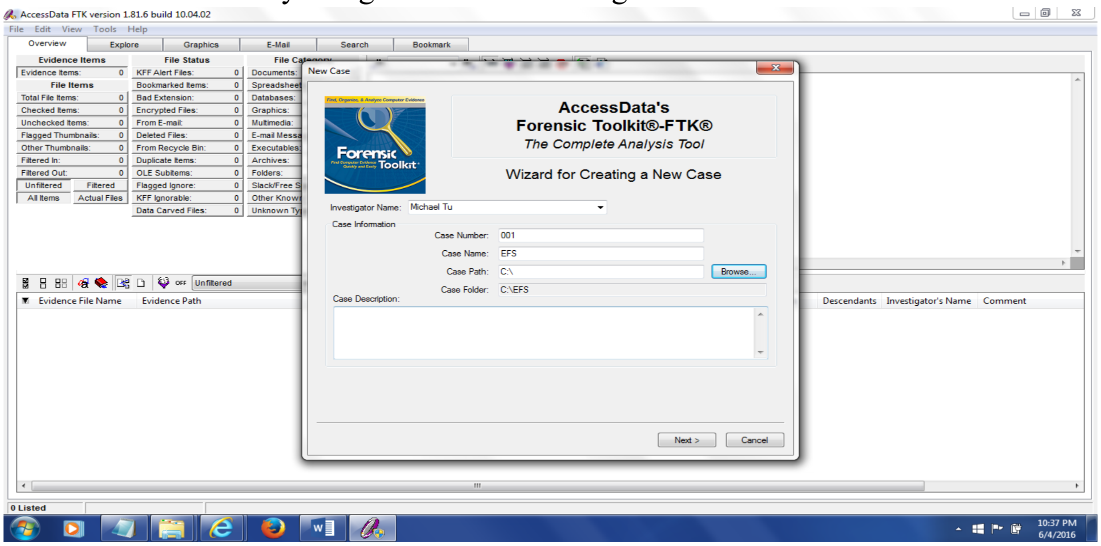
AccessData FTK Startup

● Start a new case
○ Open an existing case
○ Preview evidence
○ Go directly to working in program

□ Do not show this dialog on startup

OK Cancel

2. Build a case of EFS by using default case setting


AccessData FTK version 1.81.6 build 10.04.02
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
0 Listed
10:37 PM
6/4/2016

New Case

AccessData's
Forensic Toolkit®-FTK®
The Complete Analysis Tool

Wizard for Creating a New Case

Investigator Name: Michael Tu

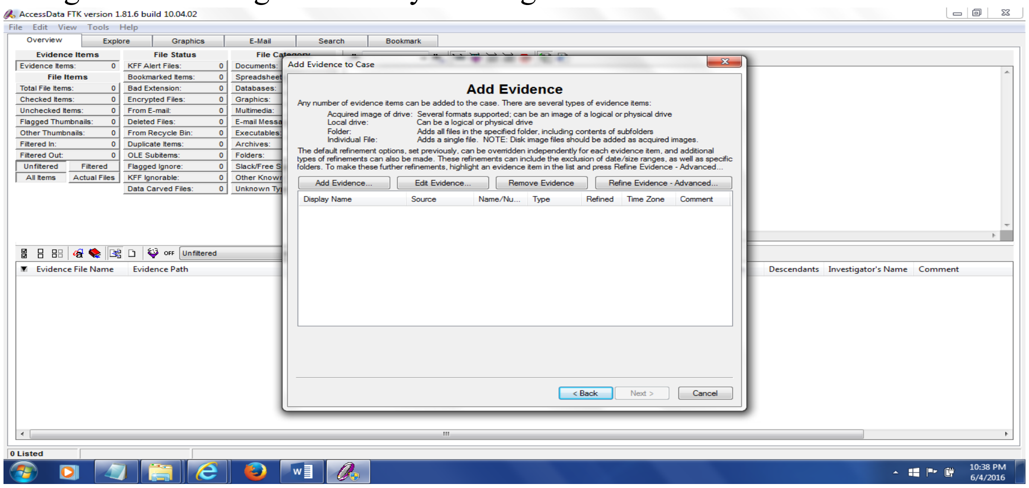
Case Information

Case Number: 001
Case Name: EFS
Case Path: C:\ Browse...
Case Folder: C:\EFS

Case Description:

Next > Cancel

3. Using default settings of FTK by clicking the next button till this “Add Evidence”


AccessData FTK version 1.81.6 build 10.04.02
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
0 Listed
10:38 PM
6/4/2016

Add Evidence to Case

Add Evidence

Any number of evidence items can be added to the case. There are several types of evidence items:

Acquired image of drive: Several formats supported; can be an image of a logical or physical drive
Local drive: Can be a logical or physical drive
Folder: Adds all files in the specified folder, including contents of subfolders
Individual File: Adds a single file. NOTE: Disk image files should be added as acquired images.

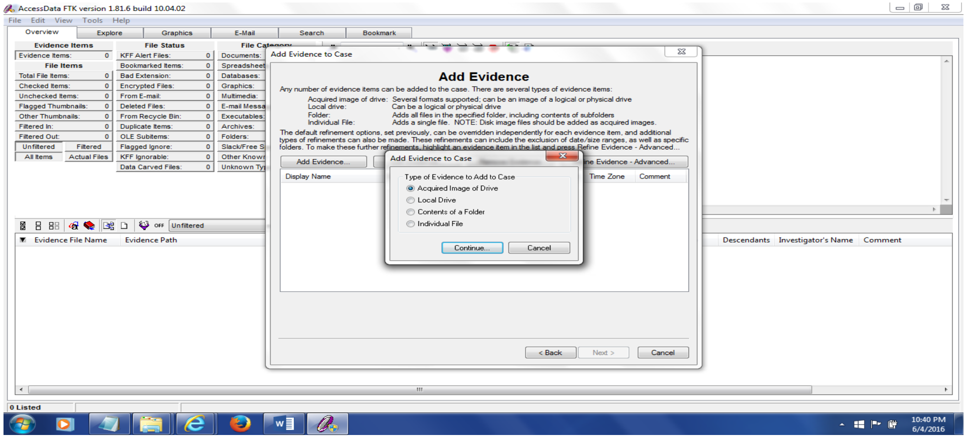
The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced...

Add Evidence... Edit Evidence... Remove Evidence Refine Evidence - Advanced...

Display Name	Source	Name/Nu...	Type	Refined	Time Zone	Comment

< Back Next > Cancel

4. Click on “Add Evidence” button to add choose the **acquired image of a drive**


AccessData FTK version 1.81.6 build 10.04.02

Add Evidence to Case

Add Evidence

Any number of evidence items can be added to the case. There are several types of evidence items:

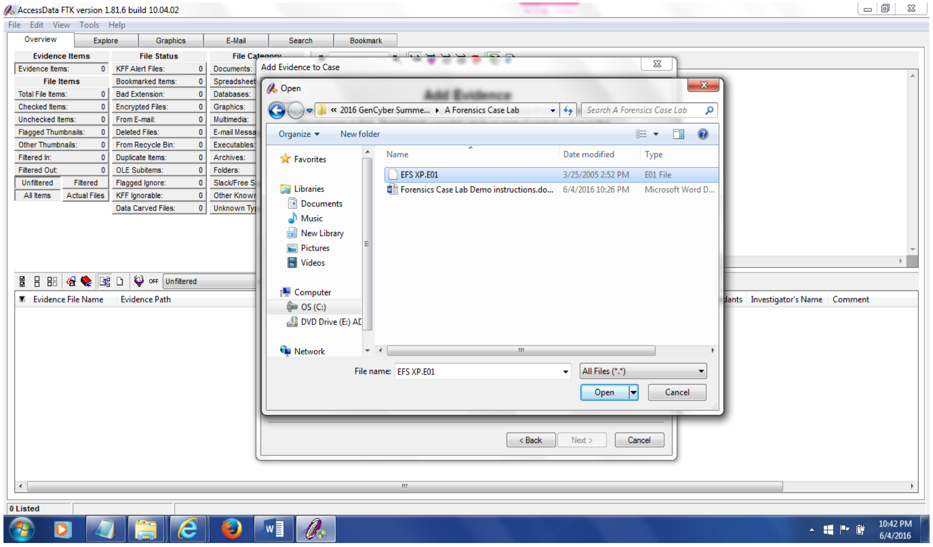
Acquired image of drive:	Several formats supported; can be an image of a logical or physical drive
Local drive:	Can be a logical or physical drive
Folder:	Adds all files in the specified folder, including contents of subfolders
Individual File:	Adds a single file. NOTE: Disk image files should be added as acquired images.

The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced...

Add Evidence to Case

Type of Evidence to Add to Case
- ● Acquired Image of Drive
- ○ Local Drive
- ○ Contents of a Folder
- ○ Individual File

5. Click on continue and next to navigate to the NTFS-EFS-ADS.e01 file on your forensics case lab folder under the 2016 GenCyber Summer Camp folder on your desktop


AccessData FTK version 1.81.6 build 10.04.02

Open

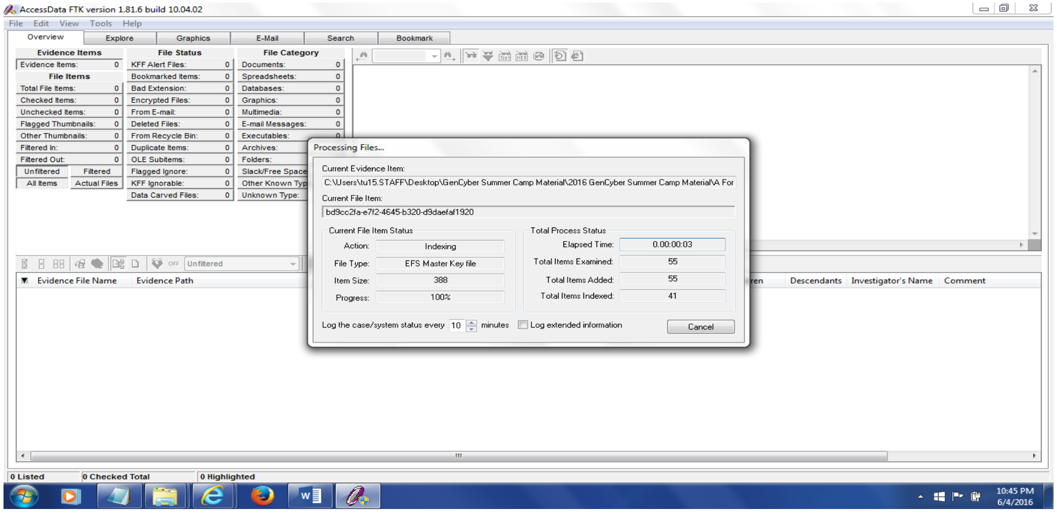
« 2016 GenCyber Summe... ▸ A Forensics Case Lab

Name	Date modified	Type
EFS XP.E01	3/25/2005 2:52 PM	E01 File
Forensics Case Lab Demo instructions.do...	6/4/2016 10:26 PM	Microsoft Word D...

File name: EFS XP.E01

All Files (*.*)

6. Click on open and then click on OK, and then next and finish, till finished.


AccessData FTK version 1.81.6 build 10.04.02

Processing Files...

Current Evidence Item:
C:\Users\tu15.STAFF\Desktop\GenCyber Summer Camp Material\2016 GenCyber Summer Camp Material\A For

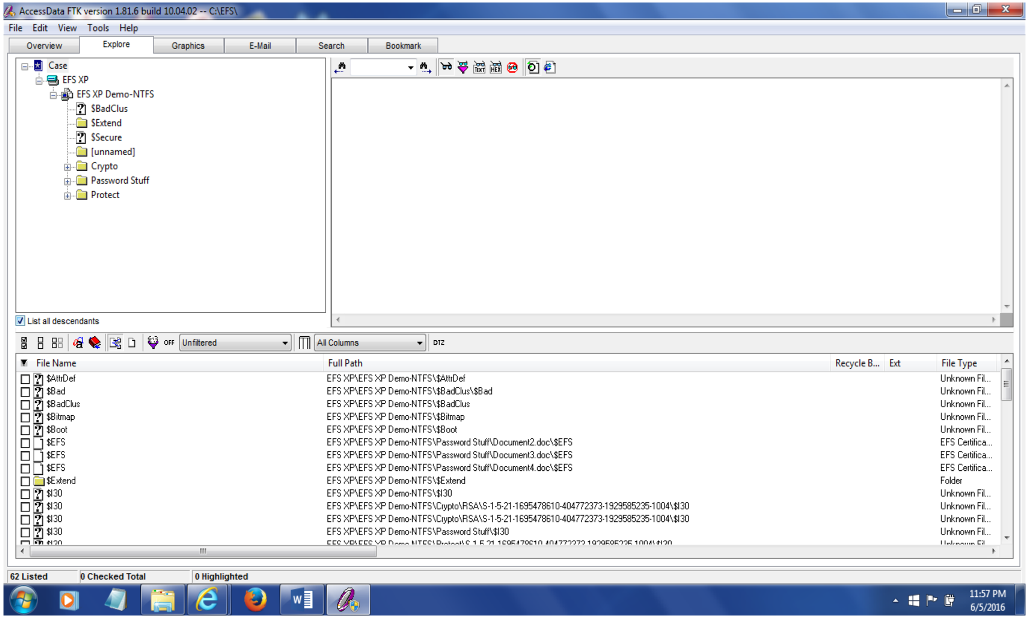
Current File Item:
bd9cc2fa-e7f2-4645-b320-d9daefaf1920

Current File Item Status
- Action: Indexing
- File Type: EFS Master Key file
- Item Size: 388
- Progress: 100%

Total Process Status
- Elapsed Time: 0.00:00:03
- Total Items Examined: 55
- Total Items Added: 55
- Total Items Indexed: 41

Log the case/system status every 10 minutes □ Log extended information

7. File export – export SAM and System file for password carcking

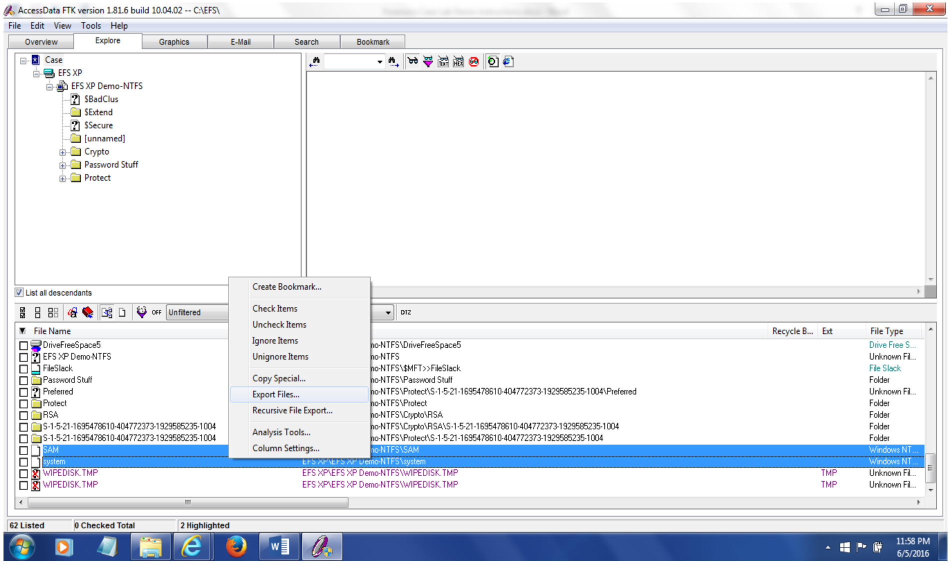

AccessData FTK version 1.81.6 build 10.04.02 -- C:\EFS\
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
Case
EFS XP
EFS XP Demo-NTFS
$BadClus
$Extend
$Secure
[unnamed]
Crypto
Password Stuff
Protect
OFF
DTZ
11:57 PM
6/5/2016

☑ List all descendants

Unfiltered | All Columns

File Name	Full Path	Recycle B...	Ext	File Type
$AttrDef	EFS XP\EFS XP Demo-NTFS\$AttrDef			Unknown Fil...
$Bad	EFS XP\EFS XP Demo-NTFS\$BadClus\$Bad			Unknown Fil...
$BadClus	EFS XP\EFS XP Demo-NTFS\$BadClus			Unknown Fil...
$Bitmap	EFS XP\EFS XP Demo-NTFS\$Bitmap			Unknown Fil...
$Boot	EFS XP\EFS XP Demo-NTFS\$Boot			Unknown Fil...
$EFS	EFS XP\EFS XP Demo-NTFS\Password Stuff\Document2.doc\$EFS			EFS Certifica...
$EFS	EFS XP\EFS XP Demo-NTFS\Password Stuff\Document3.doc\$EFS			EFS Certifica...
$EFS	EFS XP\EFS XP Demo-NTFS\Password Stuff\Document4.doc\$EFS			EFS Certifica...
$Extend	EFS XP\EFS XP Demo-NTFS\$Extend			Folder
$I30	EFS XP\EFS XP Demo-NTFS\$I30			Unknown Fil...
$I30	EFS XP\EFS XP Demo-NTFS\Crypto\RSA\S-1-5-21-1695478610-404772373-1929585235-1004\$I30			Unknown Fil...
$I30	EFS XP\EFS XP Demo-NTFS\Crypto\RSA\S-1-5-21-1695478610-404772373-1929585235-1004\$I30			Unknown Fil...
$I30	EFS XP\EFS XP Demo-NTFS\Password Stuff\$I30			Unknown Fil...

62 Listed | 0 Checked Total | 0 Highlighted

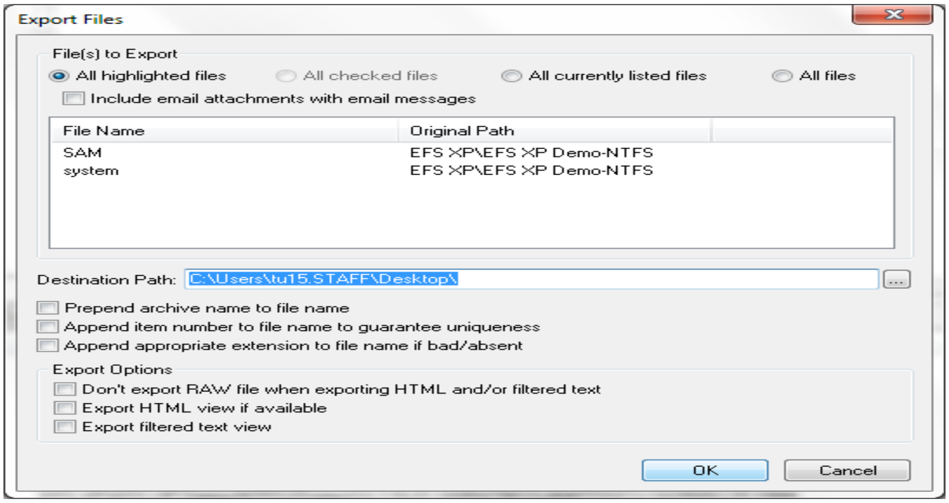


☑ List all descendants

Unfiltered

File Name	Full Path	Recycle B...	Ext	File Type
DriveFreeSpace5	mo-NTFS\DriveFreeSpace5			Drive Free S...
EFS XP Demo-NTFS	mo-NTFS			Unknown Fil...
FileSlack	mo-NTFS\$MFT>>FileSlack			File Slack
Password Stuff	mo-NTFS\Password Stuff			Folder
Preferred	mo-NTFS\Protect\S-1-5-21-1695478610-404772373-1929585235-1004\Preferred			Unknown Fil...
Protect	mo-NTFS\Protect			Folder
RSA	mo-NTFS\Crypto\RSA			Folder
S-1-5-21-1695478610-404772373-1929585235-1004	mo-NTFS\Crypto\RSA\S-1-5-21-1695478610-404772373-1929585235-1004			Folder
S-1-5-21-1695478610-404772373-1929585235-1004	mo-NTFS\Protect\S-1-5-21-1695478610-404772373-1929585235-1004			Folder
SAM	mo-NTFS\SAM			Windows NT...
system	EFS XP\EFS XP Demo-NTFS\system			Windows NT...
WIPEDISK.TMP	EFS XP\EFS XP Demo-NTFS\WIPEDISK.TMP		TMP	Unknown Fil...
WIPEDISK.TMP	EFS XP\EFS XP Demo-NTFS\WIPEDISK.TMP		TMP	Unknown Fil...

62 Listed | 0 Checked Total | 2 Highlighted



Export Files

File(s) to Export

● All highlighted files ○ All checked files ○ All currently listed files ○ All files

□ Include email attachments with email messages

File Name	Original Path
SAM	EFS XP\EFS XP Demo-NTFS
system	EFS XP\EFS XP Demo-NTFS

Destination Path: C:\Users\tu15.STAFF\Desktop\

□ Prepend archive name to file name

□ Append item number to file name to guarantee uniqueness

□ Append appropriate extension to file name if bad/absent

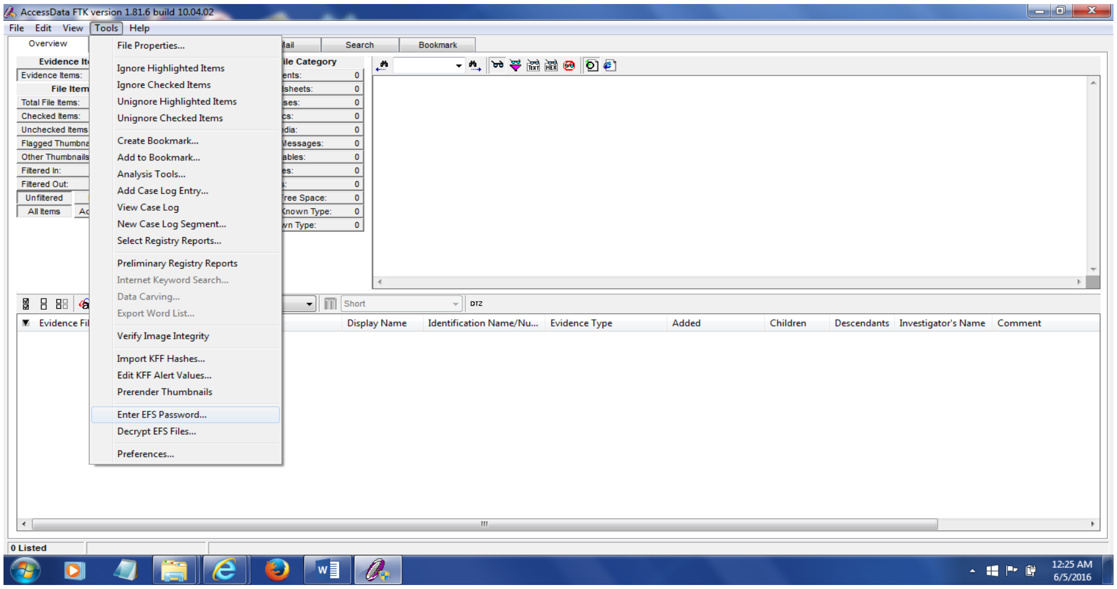
Export Options

□ Don't export RAW file when exporting HTML and/or filtered text

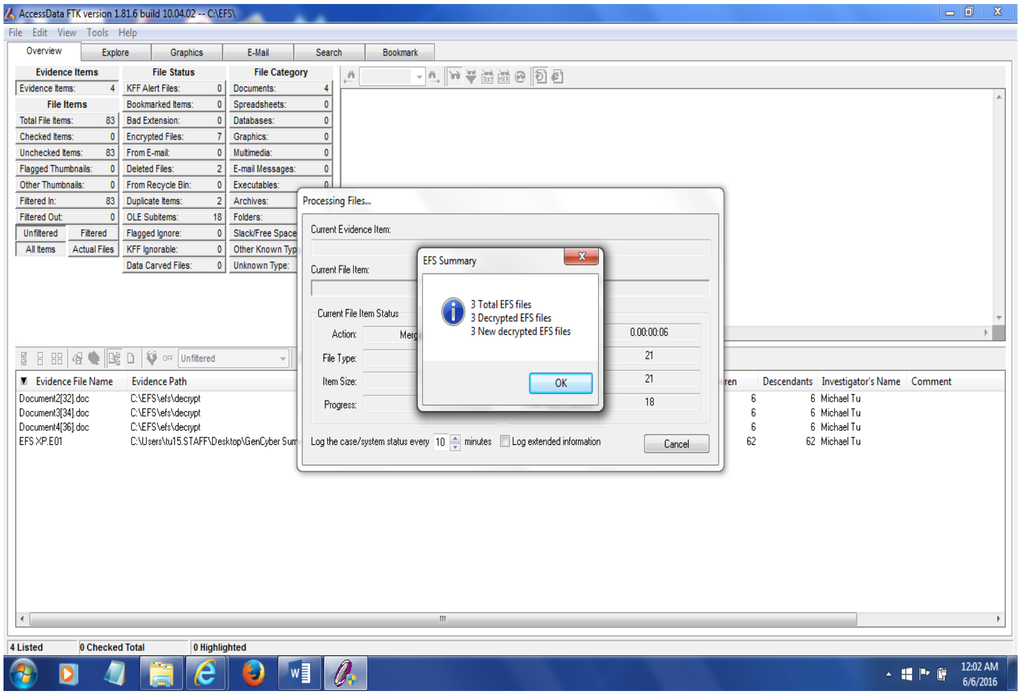
□ Export HTML view if available

□ Export filtered text view

1. *Then go to toos and select the “Enter EFS Password” menu*



2. *Put your password and then it will automatically decrypt the efs files*



Evidence Items		File Status		File Category	
Evidence Items:	4	KFF Alert Files:	0	Documents:	4
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	83	Bad Extension:	0	Databases:	0
Checked Items:	0	Encrypted Files:	7	Graphics:	0
Unchecked Items:	83	From E-mail:	0	Multimedia:	0
Flagged Thumbnails:	0	Deleted Files:	2	E-mail Messages:	0
Other Thumbnails:	0	From Recycle Bin:	0	Executables:	0
Filtered In:	83	Duplicate Items:	2	Archives:	
Filtered Out:	0	OLE Subitems:	18	Folders:	
Unfiltered	Filtered	Flagged Ignore:	0	Slack/Free Space	
All Items	Actual Files	KFF Ignorable:	0	Other Known Typ	
		Data Carved Files:	0	Unknown Type:	

Processing Files...

Current Evidence Item:

Current File Item:

Current File Item Status

Action: Merg

File Type:

Item Size:

Progress:

0.00:00:06

21

21

18

Log the case/system status every 10 minutes □ Log extended information

EFS Summary

3 Total EFS files
3 Decrypted EFS files
3 New decrypted EFS files

Evidence File Name	Evidence Path	ren	Descendants	Investigator's Name	Comment
Document2[32].doc	C:\EFS\efs\decrypt	6	6	Michael Tu	
Document3[34].doc	C:\EFS\efs\decrypt	6	6	Michael Tu	
Document4[36].doc	C:\EFS\efs\decrypt	6	6	Michael Tu	
EFS XP.E01	C:\Users\tu15.STAFF\Desktop\GenCyber Sum	62	62	Michael Tu	

4 Listed | 0 Checked Total | 0 Highlighted

3. *Then you should click the “ overview” tab and go to the document folder to check the decrypted EFS encrypted file*