

Chapter 1, Getting Started with Computer Forensics Using FTK

Software	
Operation System	Server 2008 R2 / Windows7 (64-bit)
Hardware	
Processor	Intel® i7, Dual Quad Core Xeon, or AMD equivalent
Memory	32 GB (or more)
OS / Application drive	7200 RPM drive with 64MB cache or SSD drive
Storage for PostgreSQL database	160GB Solid State Drive (SSD) dedicated exclusively to PostgreSQL.
Network Card	Gigabit
HW RAID Controller	Highly recommended if hosting PostgreSQL database. Configure with RAID 5, 6, or 10 avoid RAID0
Temporary Folder Location	SSD drive or RAID0 partition w/ write-through
Drive Configuration	Drive 1: OS Drive 2: PostgreSQL Database (SSD or HW RAID) Drive 3: Case Folder and HD Image Drive 4: Temp Directory (SSD or RAID0)

Find, Organize, & Analyze Computer Evidence



ACCESSDATA

FTK

FORENSIC TOOLKIT™

Database

View User Guide

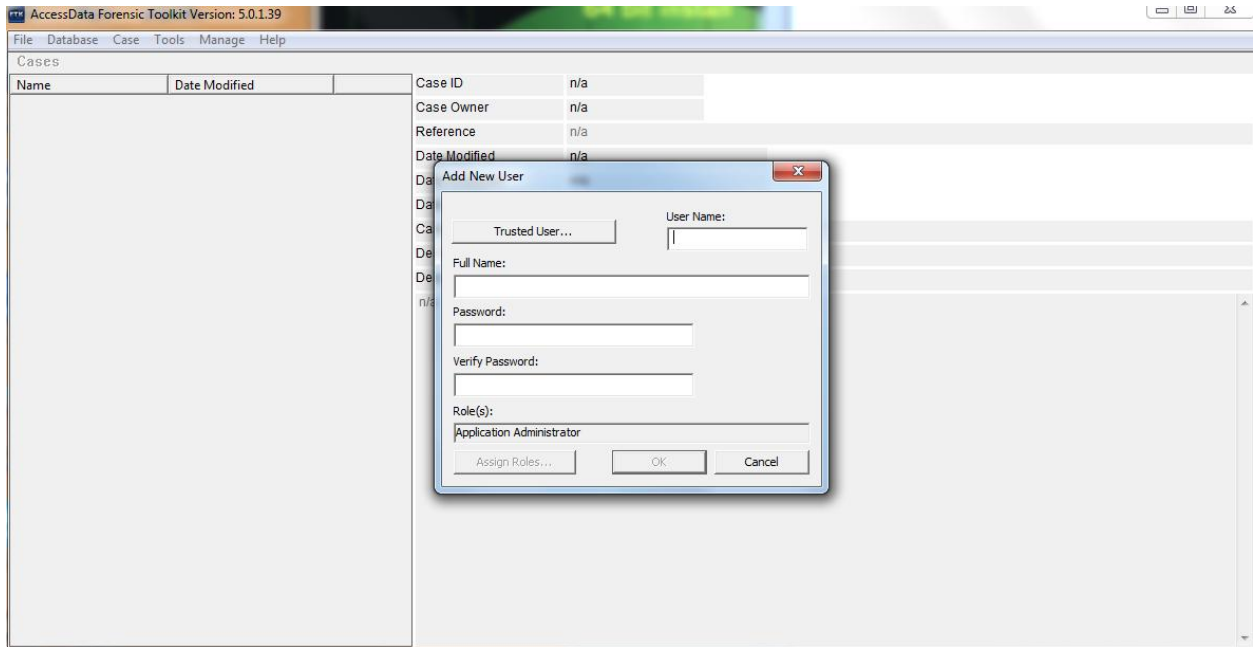
FTK Install

View Readme

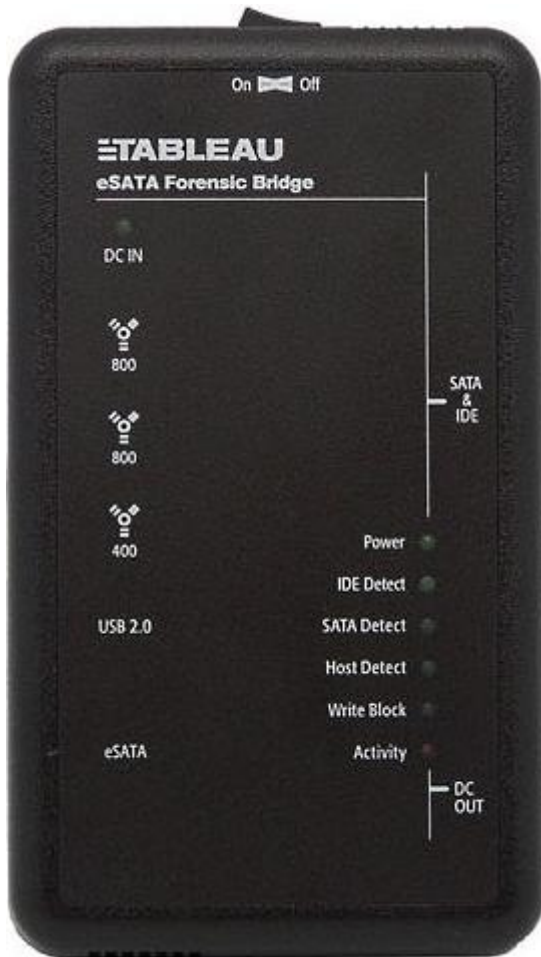
Distributed Engine

Other Products



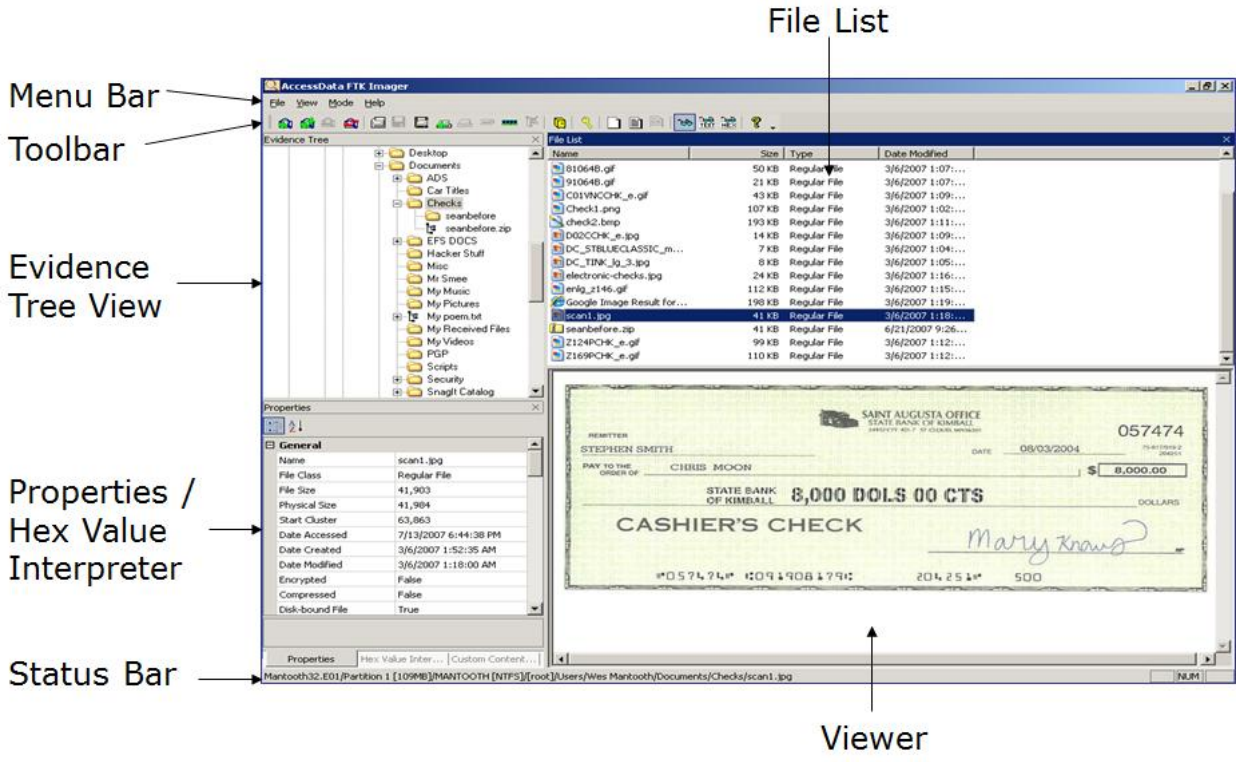


Chapter 2, Working with FTK Imager



All Files (*.*)

E01 Images (*.e01)
SMART Images (*.s01)
Advanced Forensic Format Images (*.aff)
Virtual Hard Disk (*.vhd)
ICS Images (*.I01)
SafeBack / SnapBack Images (*.001)
Tar Archive (*.tar)
Zip Archive (*.zip)
AccessData Logical Image (*.AD1)
VMDK Virtual Drive (*.vmdk)
Ghost Raw Image (*.gho)
Raw CD/DVD image (*.iso; *.img; *.bin; *.tao; *.dao)
Alcohol CD image (*.mds)
DiscJuggler image (*.cdi)
CloneCD image (*.ccd)
Gear CD Image (*.p01)
IsoBuster CD image (*.cue)
Nero CD image (*.nrg)
Philips/OptImage CD image (*.cd)
Pinnacle CD image (*.pdi)
Plextools CD image (*.pxi)
Prassi CD Right Image Plus (*.gcd)
Prassi PrimoDVD Image (*.gi)
Roxio CD Creator Image (*.cif)
Virtual CD image (*.vc4)
WinOnCD image (*.c2d)
Apple Disk Images (*.dmg)



File List

Menu Bar






















Toolbar

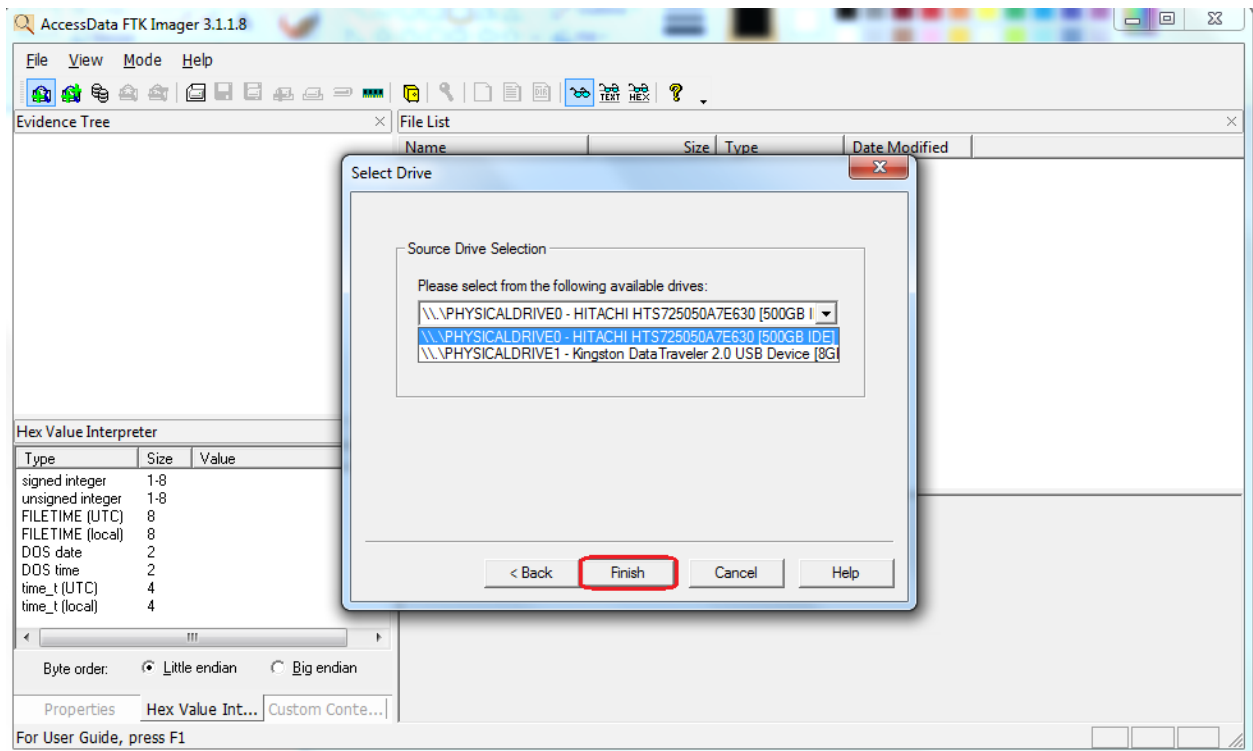
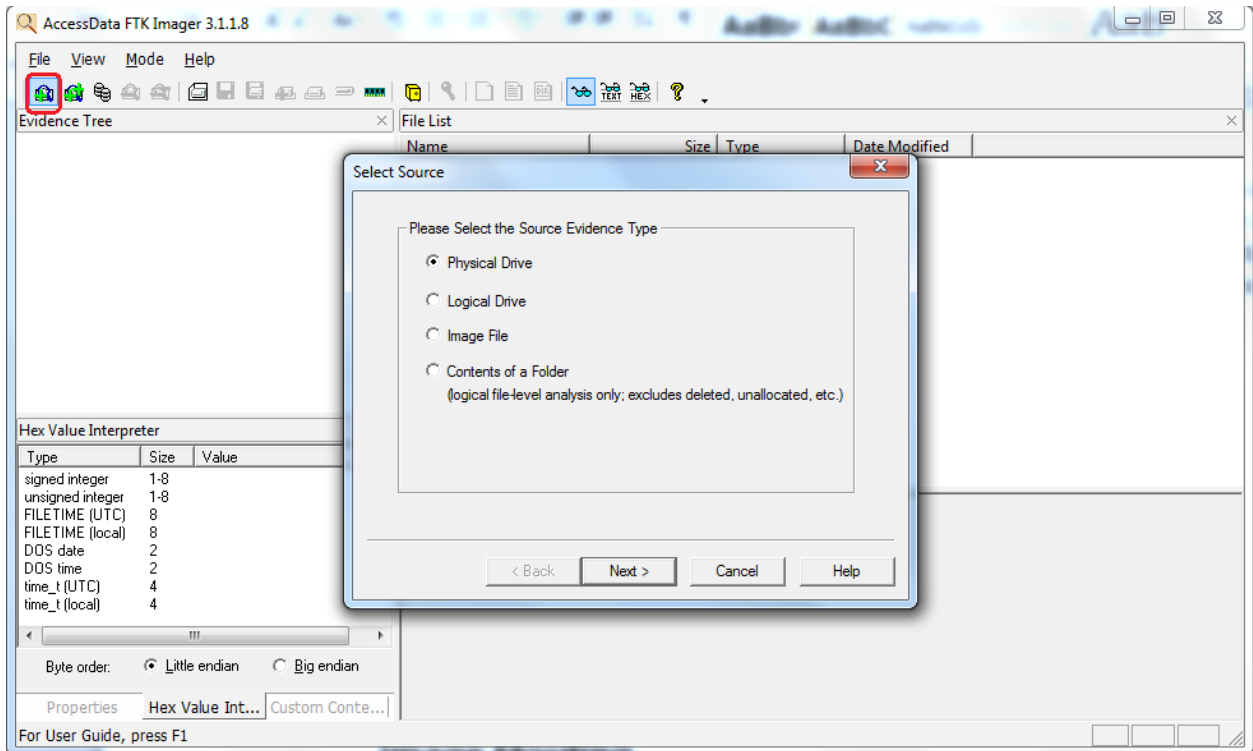
Evidence Tree View

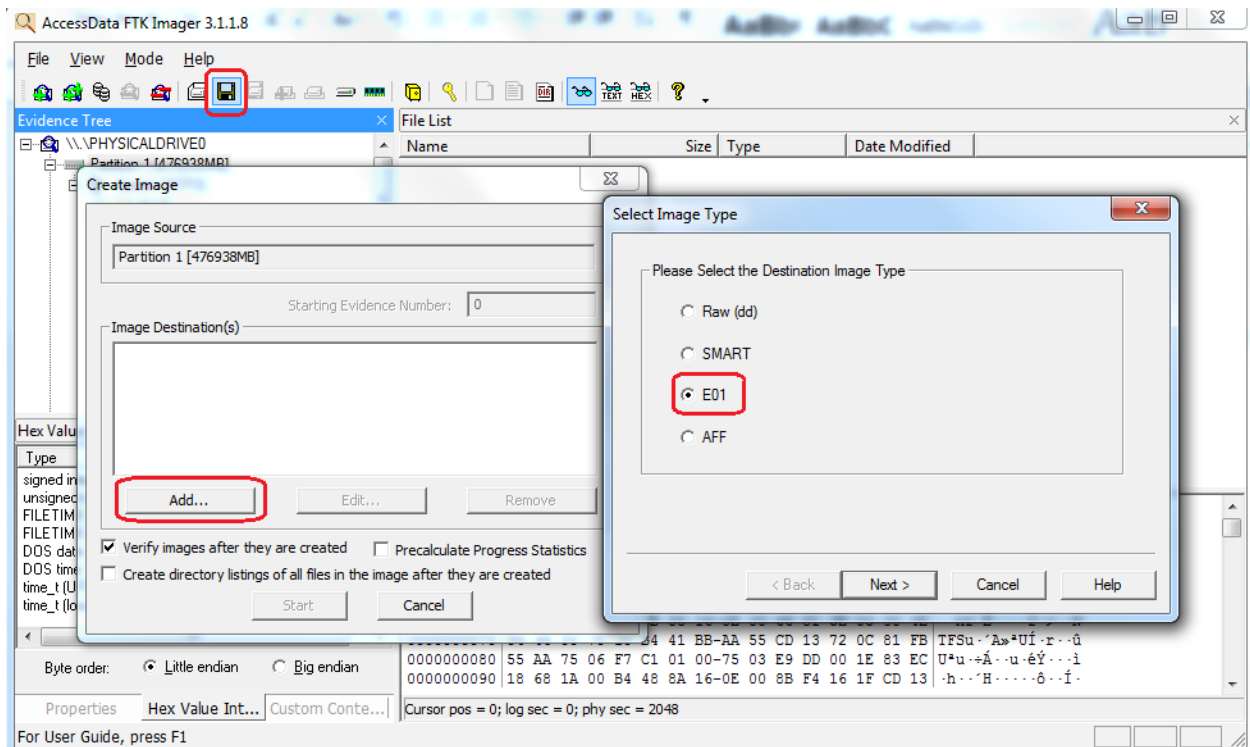
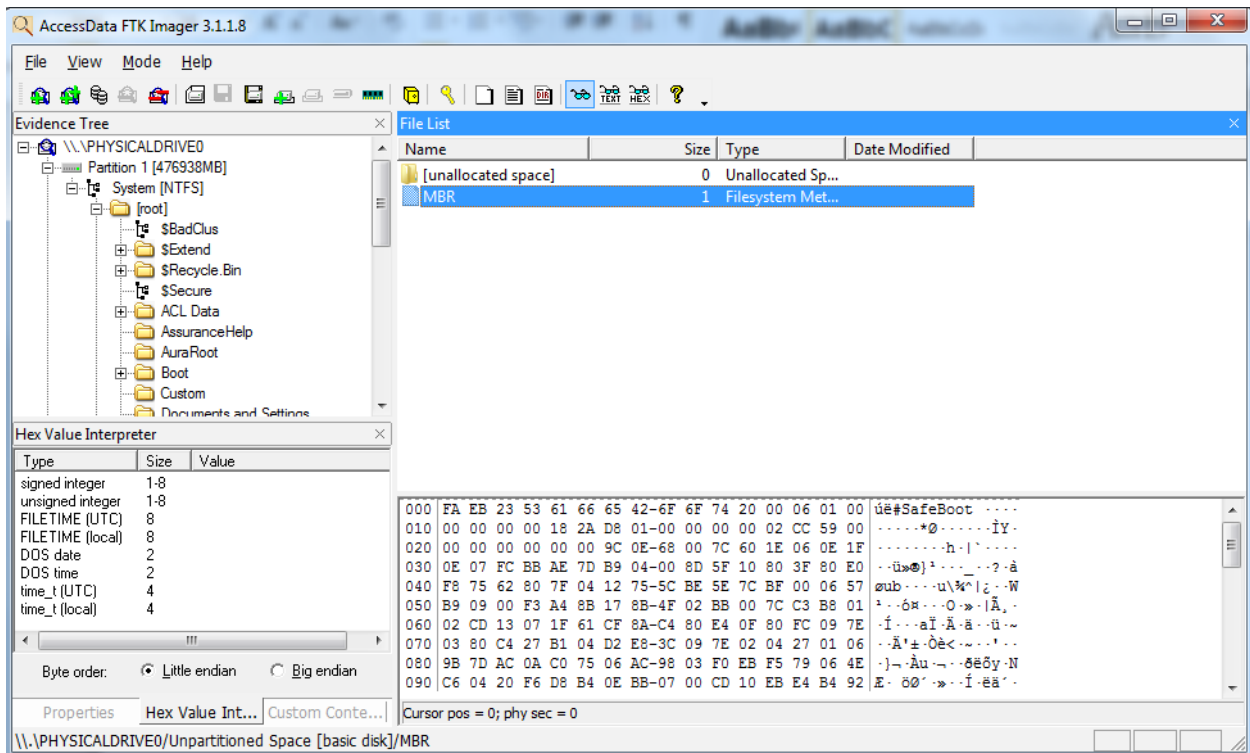
Properties / Hex Value Interpreter

Status Bar

Viewer

-  Add Evidence Item
-  Add All Attached Devices
-  Image Mounting
-  Remove Evidence Item
-  Remove All Evidence Items
-  Create Disk Image
-  Export Disk Image
-  Export Logical Image (AD1)
-  Add to Custom Content Image (AD1)
-  Create Custom Content Image (AD1)
-  Verify Drive/Image
-  Capture Memory
-  Obtain Protected Files
-  Detect EFS Encryption
-  Export Files
-  Export File Hash List
-  Export Directory Listing
-  Choose IE, text, or hex viewer automatically
-  View files in plain text
-  View files in hex format
-  Open FTK Imager User Guide





Evidence Item Information

Case Number:

Evidence Number:

Unique Description:

Examiner:

Notes:

< Back Next > Cancel Help

Select Image Destination

Image Destination Folder

Image Filename (Excluding Extension)

Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment

Compression (0=None, 1=Fastest, ..., 9=Smallest)

Use AD Encryption

< Back Finish Cancel Help

Mount Image To Drive



Add Image

Image File:

C:\Users\304020\Desktop\Mantooth.E01



Mount Type: Physical & Logical



Drive Letter: Next Available (H:)



Mount Method: Block Device / Read Only



Write Cache Folder:

C:\Users\304020\Desktop



Mount

Mapped Image List

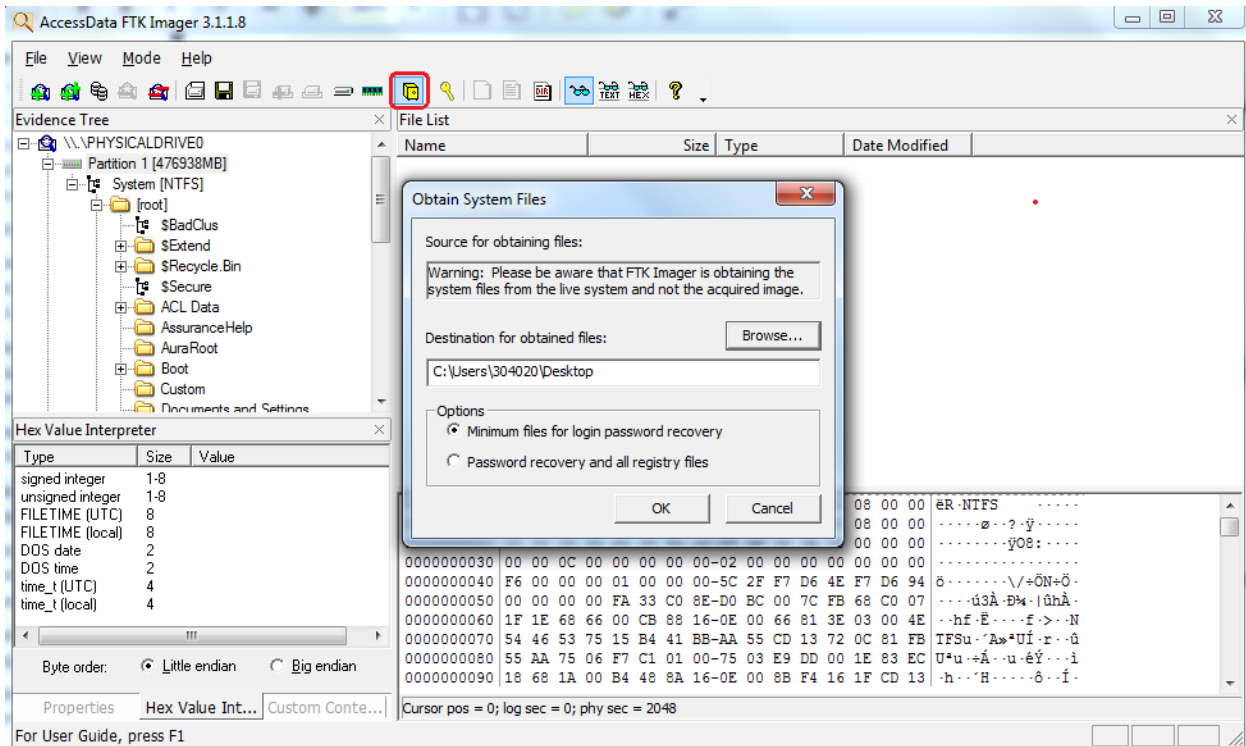
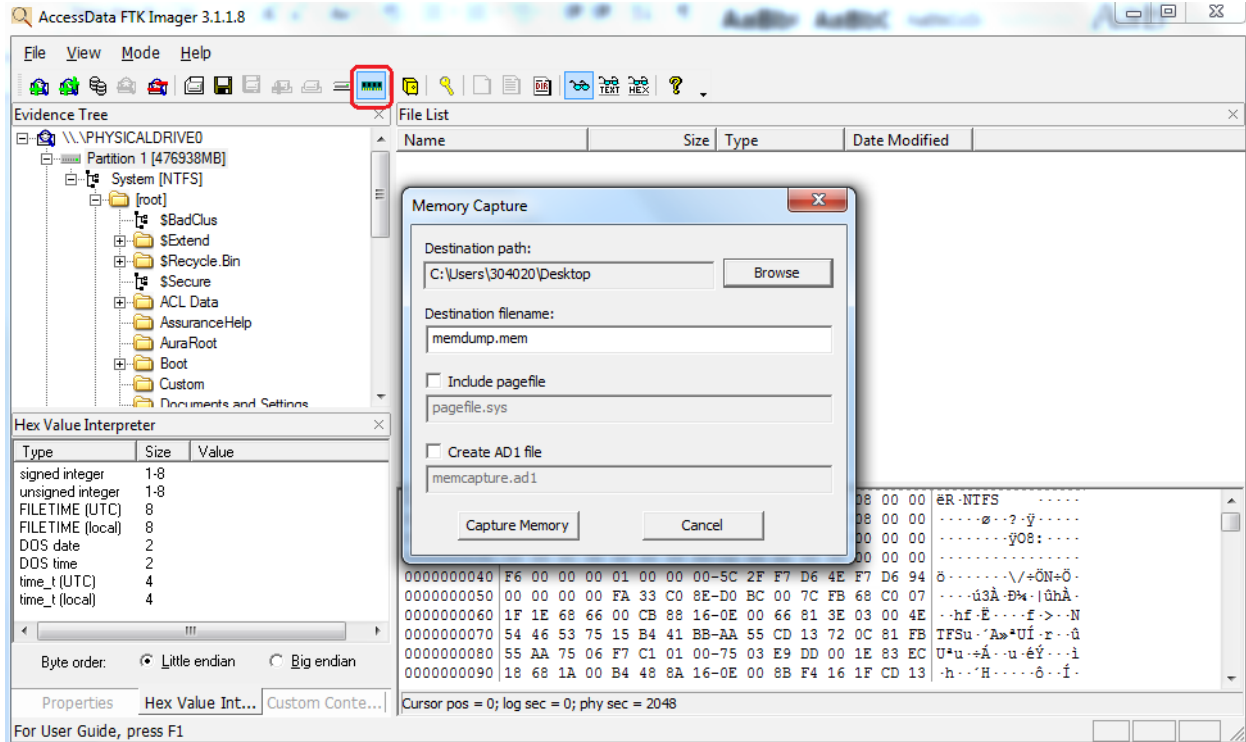
Mapped Images:

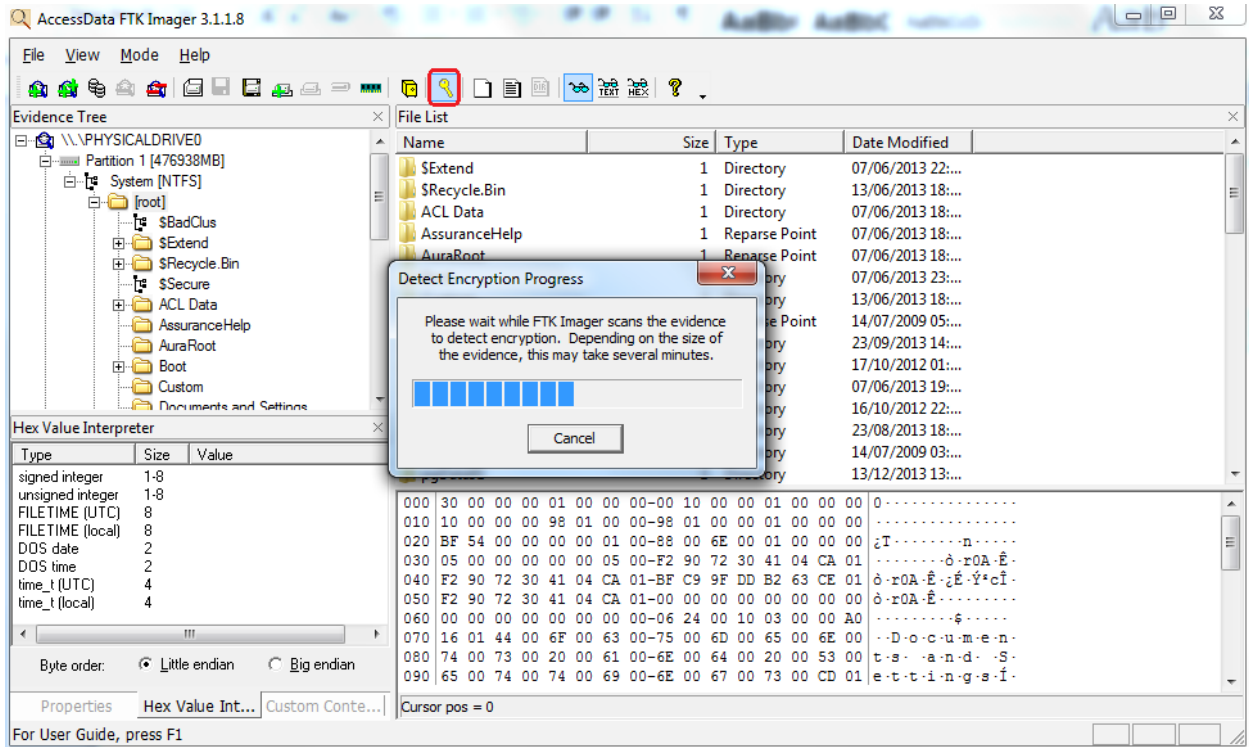
Drive	Method	Partition	Image
PhysicalDrive2	Block Device/Read ...	Image	C:\Users\304020\Desktop\Mantooth.E01
F:	Block Device/Read ...	Partition 1 [109M...	C:\Users\304020\Desktop\Mantooth.E01
G:	Block Device/Read ...	Partition 2 [7MB] ...	C:\Users\304020\Desktop\Mantooth.E01



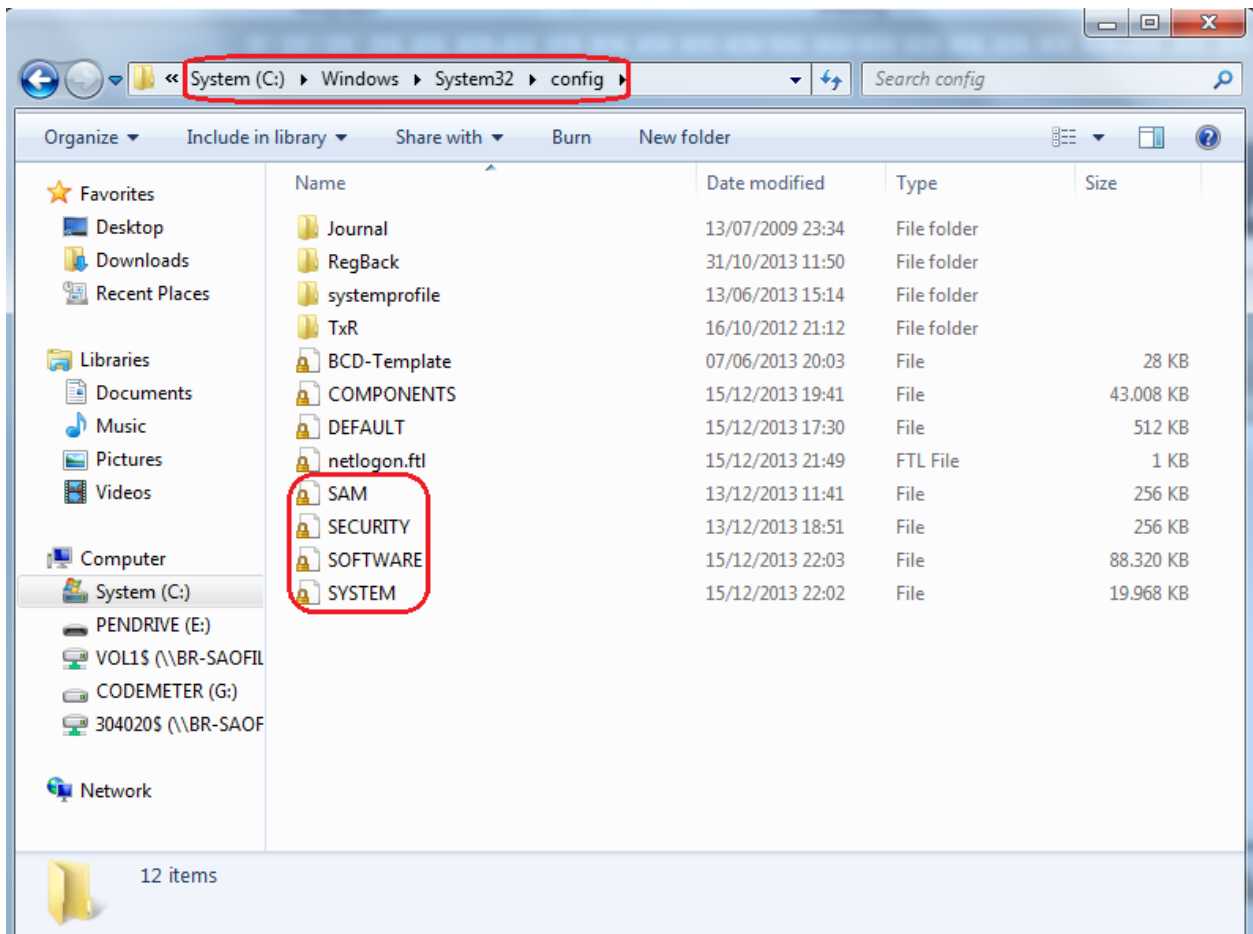
Unmount

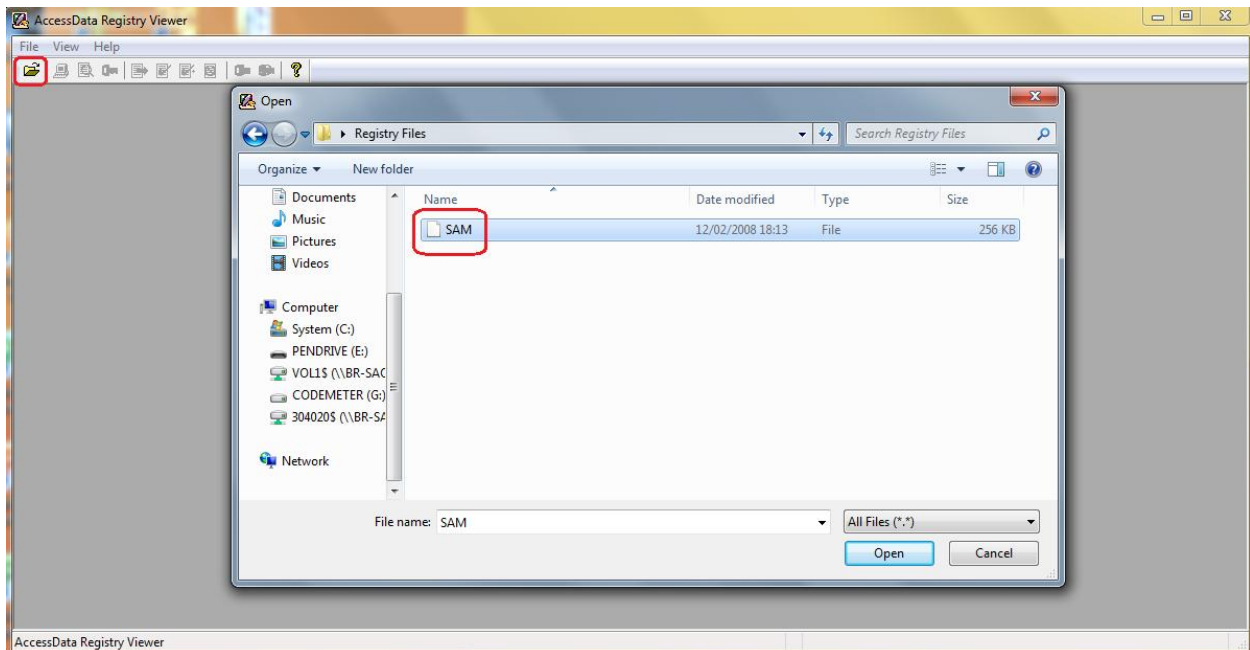
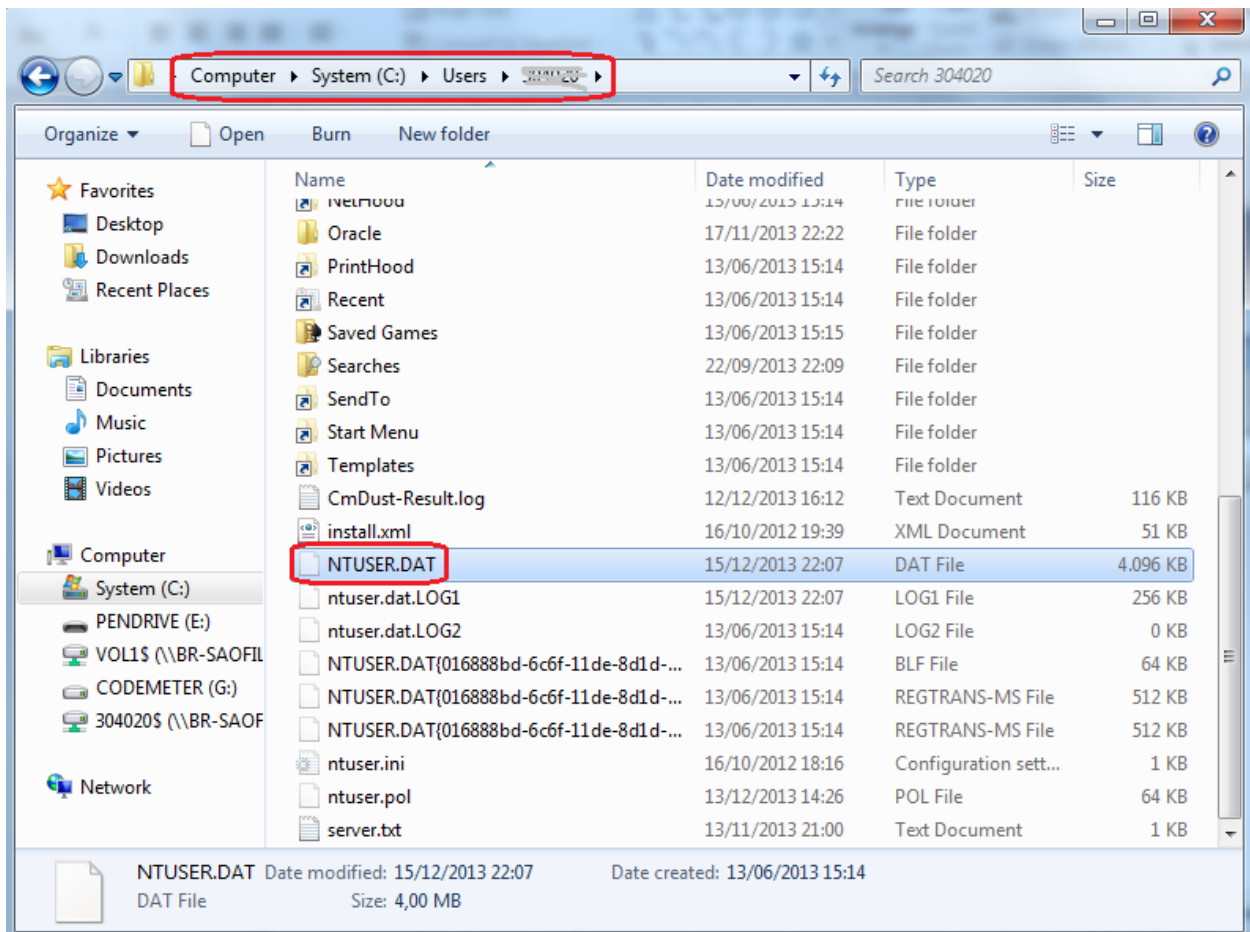
Close

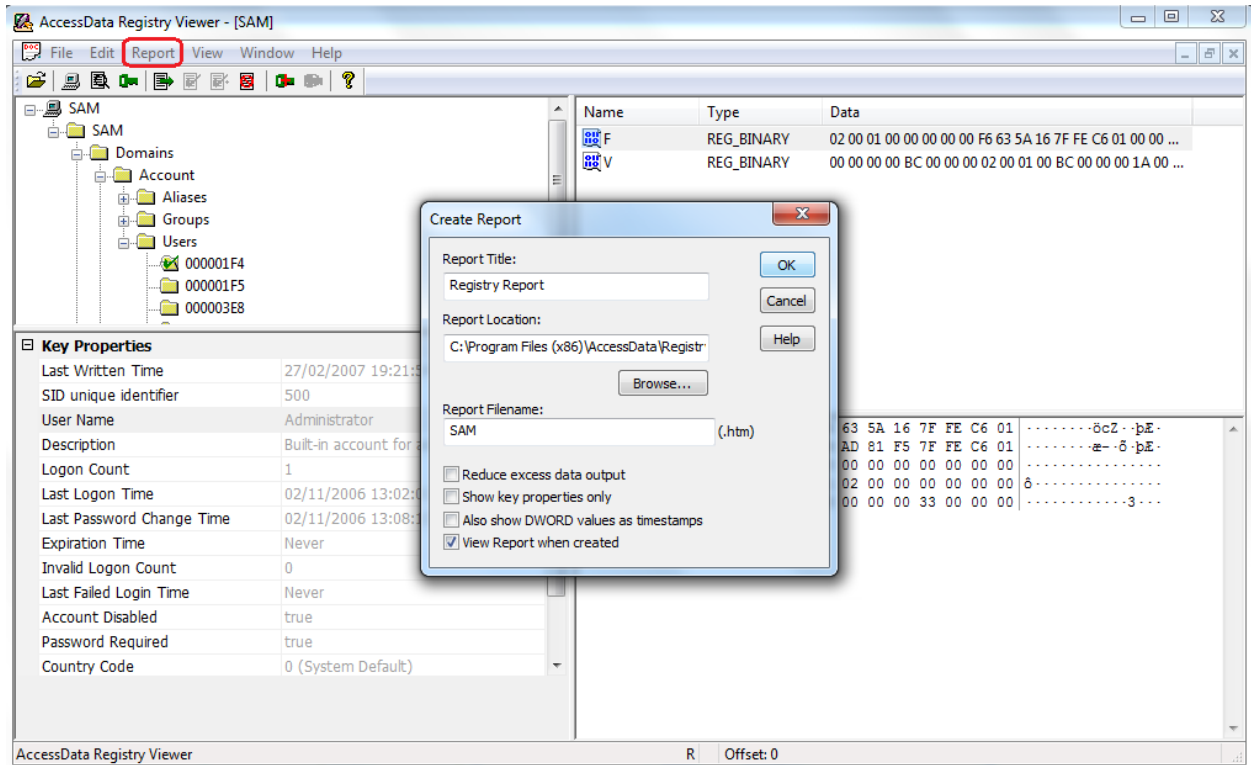
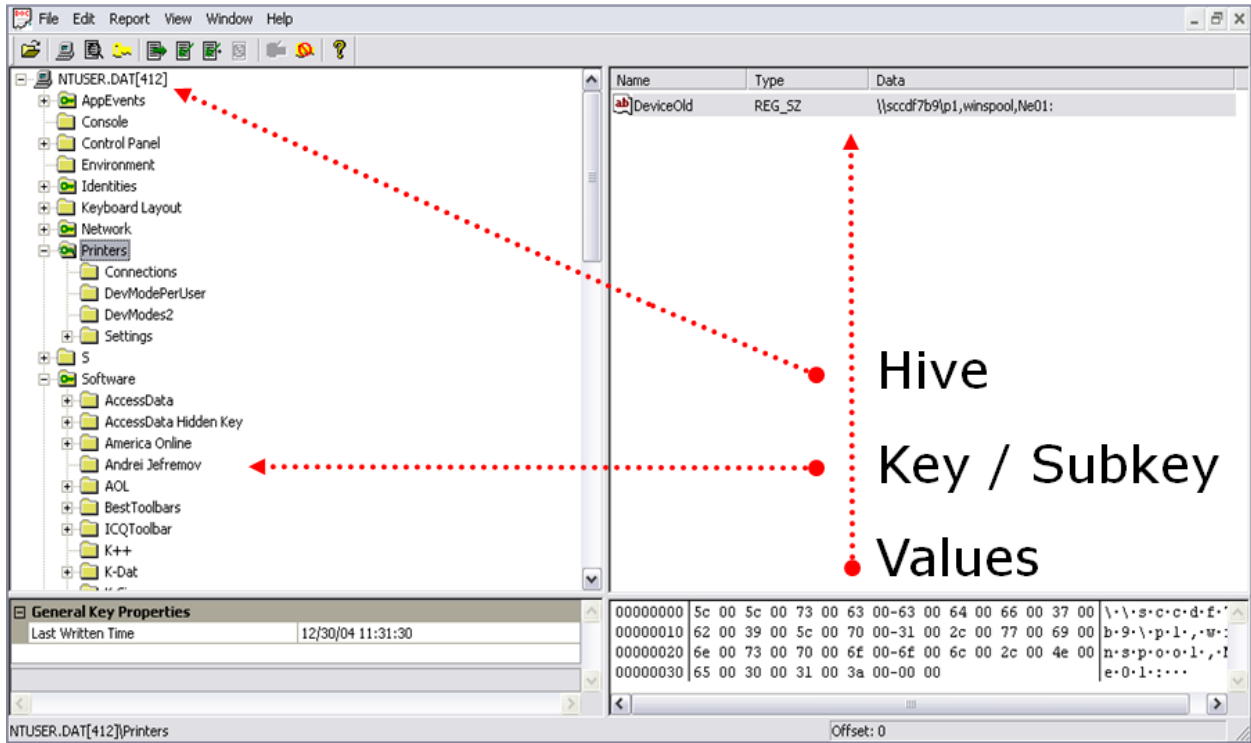


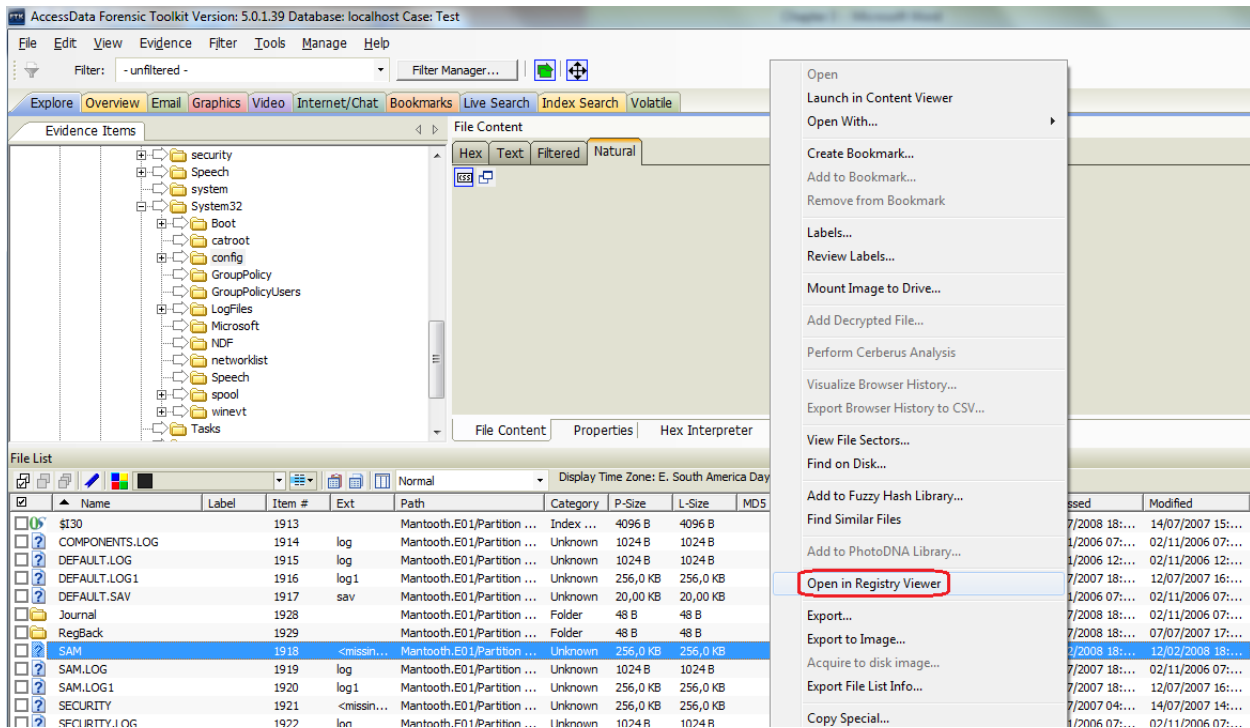
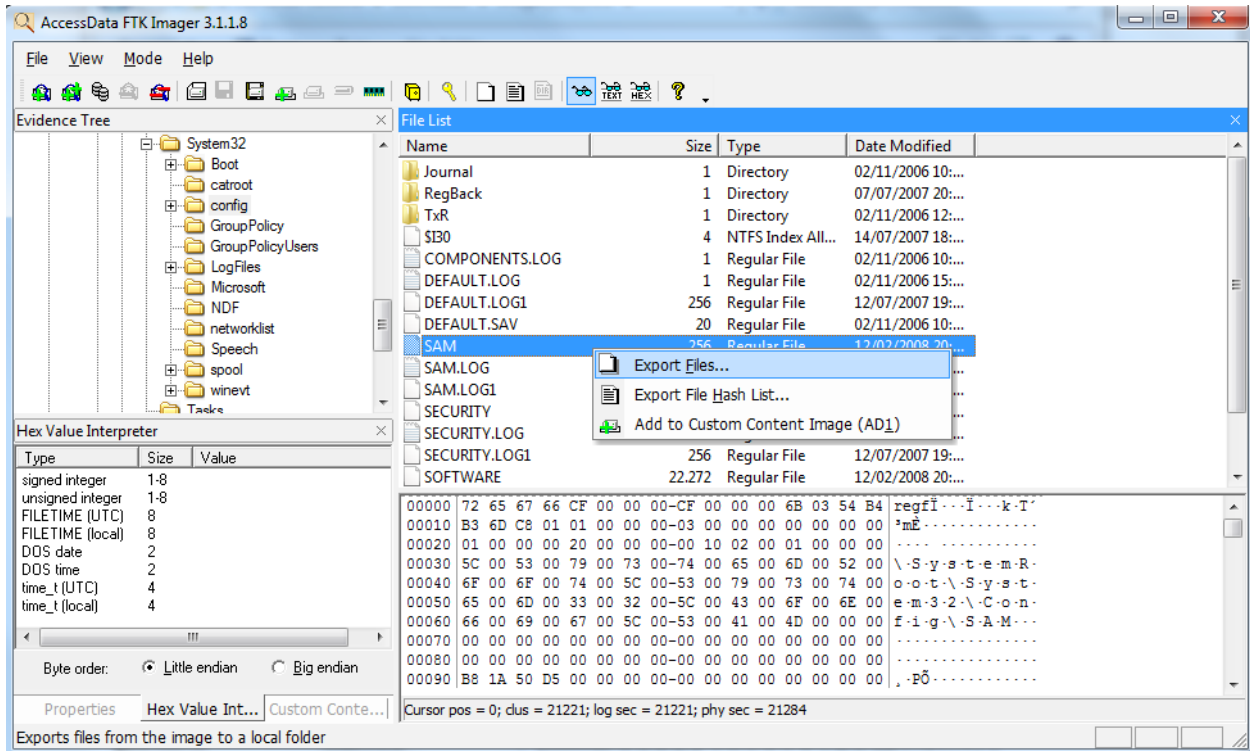


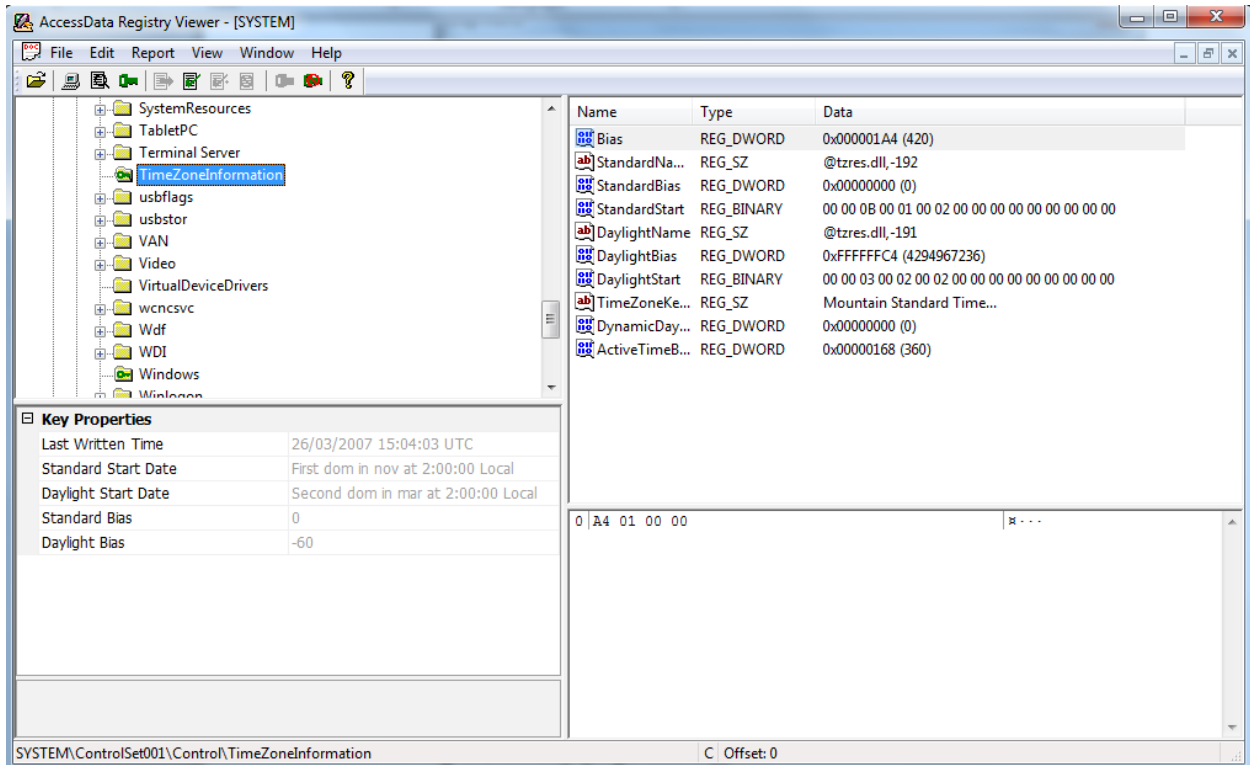
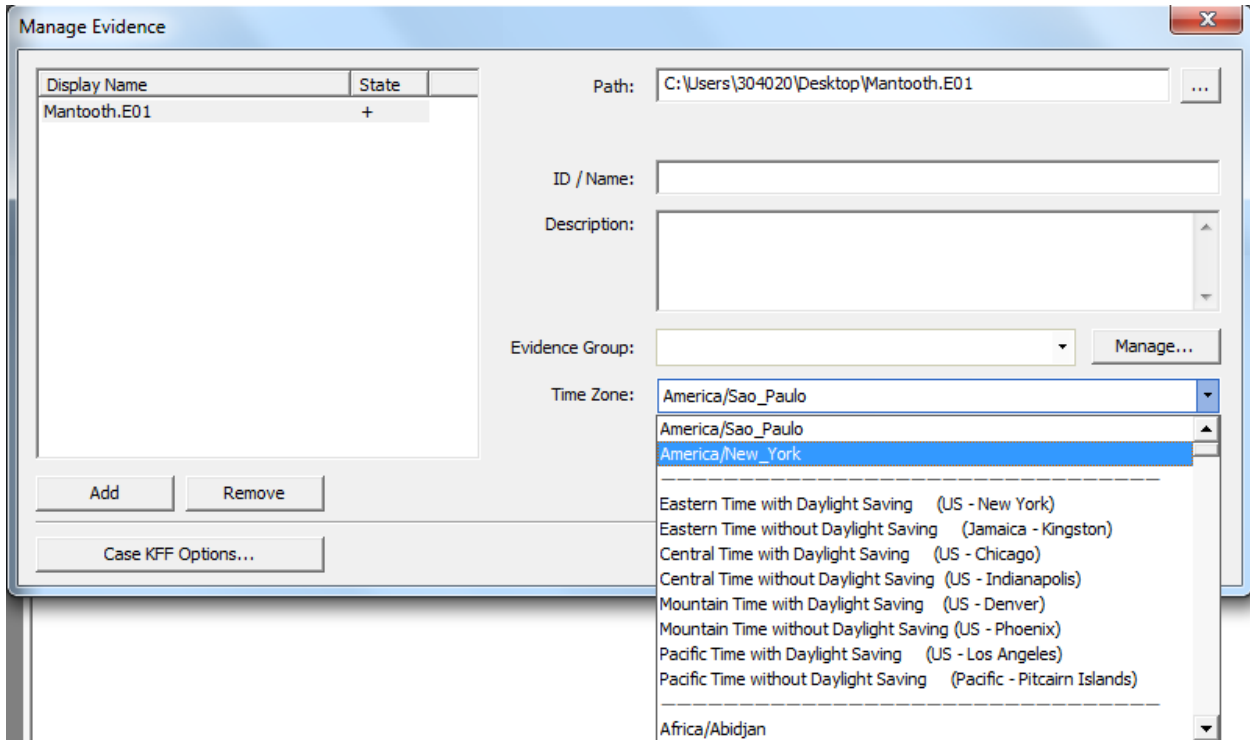
Chapter 3, Working with Registry View

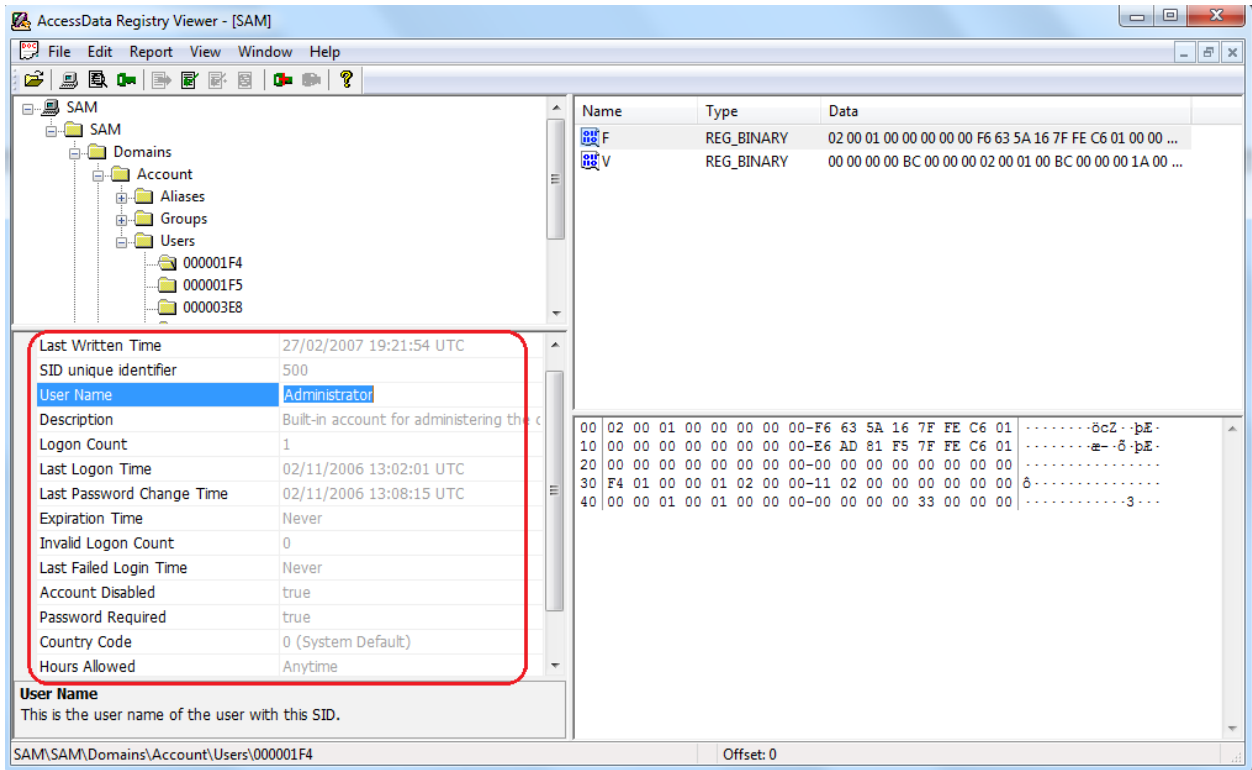




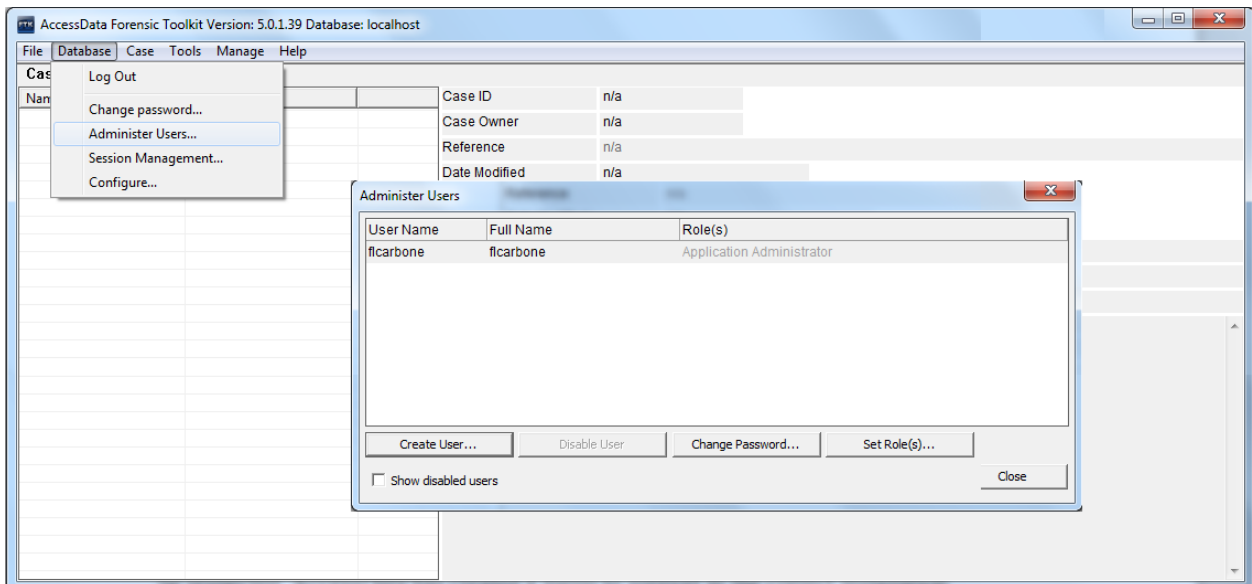
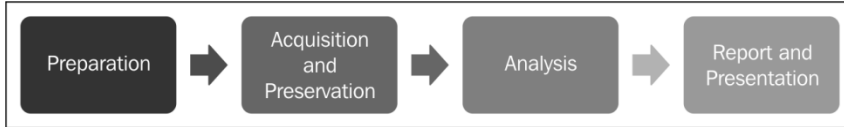








Chapter 4, Working with FTK Forensics



Administer Users

User Name	Full Name	Role(s)
flicarbone	flicarbone	Application Administrator

Add New User

User Name:

Full Name:

Password:

Verify Password:

Role(s):

Show disabled users

Initial Role(s) for:

Roles:

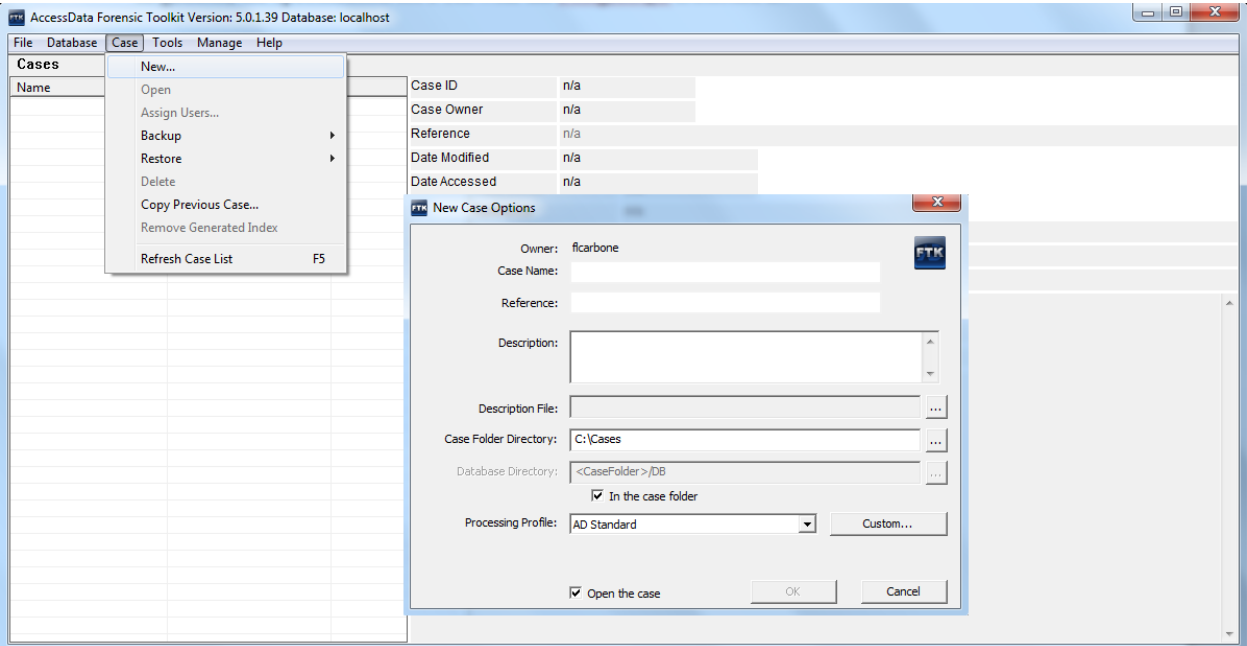
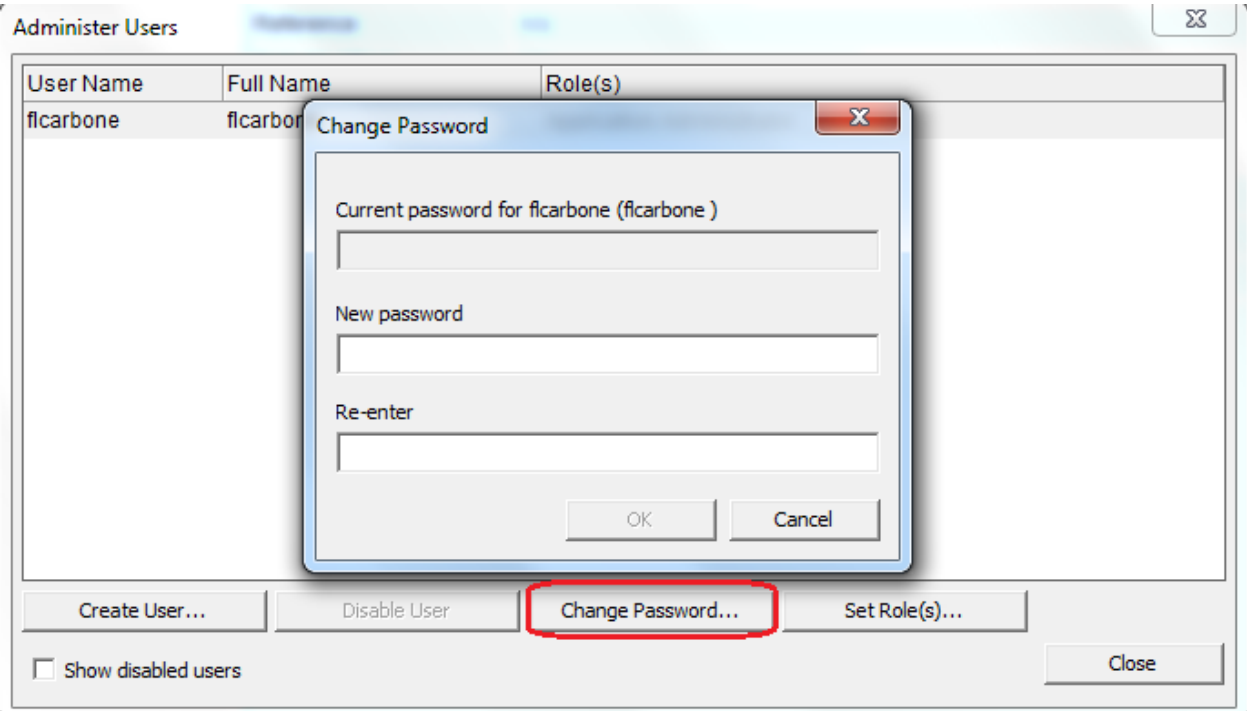
Name	Description
<input type="checkbox"/> Application Administrator	This role has all privileges.
<input type="checkbox"/> Case Administrator	This role has all case privileges.
<input type="checkbox"/> Case Reviewer	This role has review rights only, modification of the evidence data is not permitted

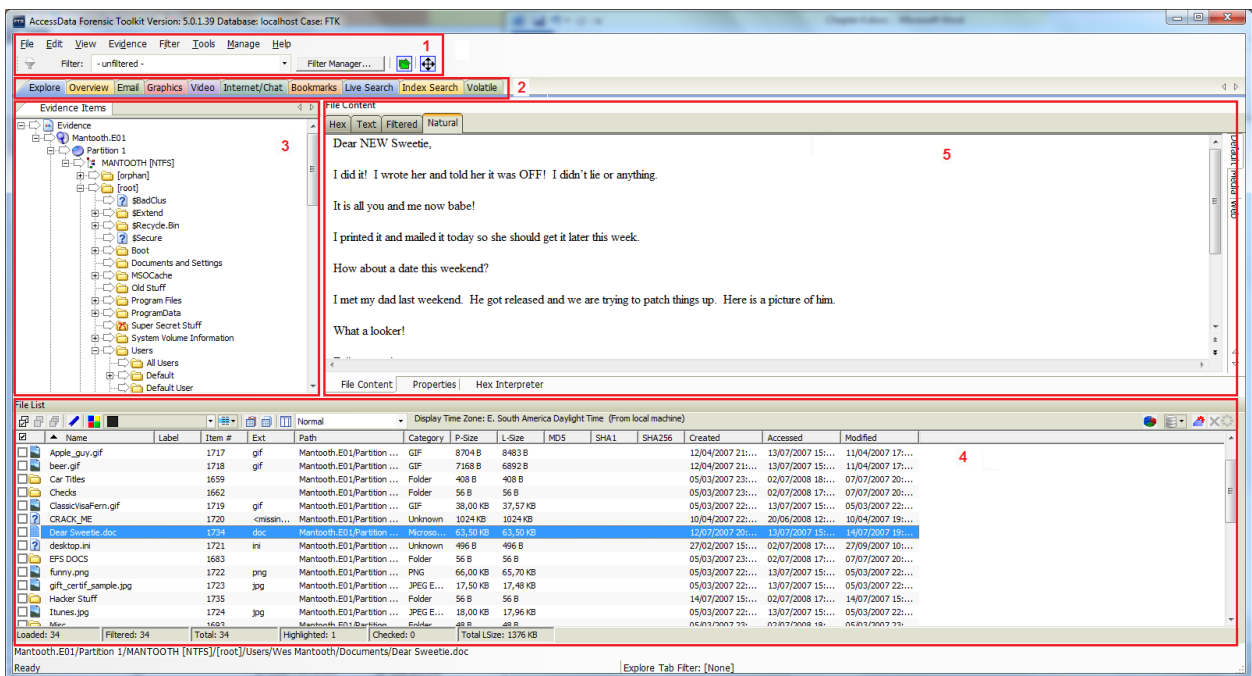
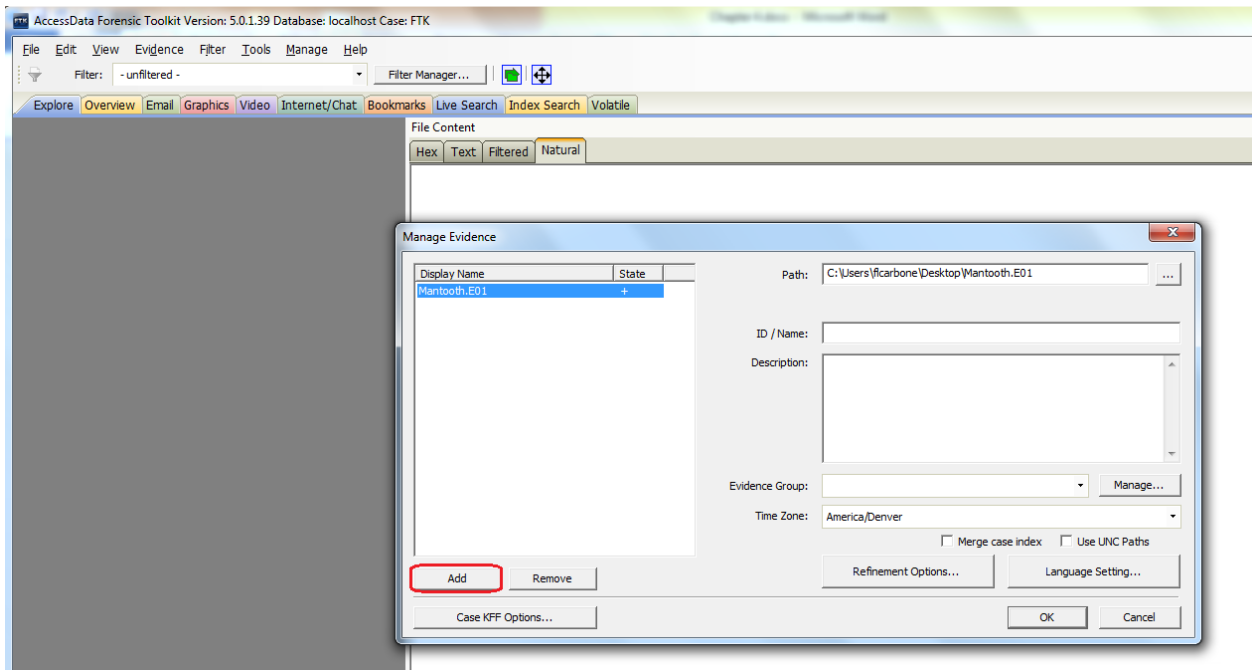
Password:

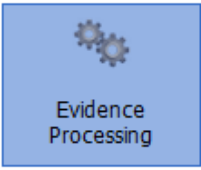
Verify Password:

Role(s):

Show disabled users







Evidence Processing



Evidence Refinement (Advanced)



Index Refinement (Advanced)



Custom File Identification

Evidence Processing

Generate File Hashes (flag duplicates)

- MD5 Hash
- SHA-1 Hash
- SHA-256 Hash
- Fuzzy Hash Fuzzy Hash Options...
- Match Fuzzy Hash Library
- Flag Duplicate Files
- KFF
- PhotoDNA

- Expand Compound Files Expansion Options...

Takes extra time to expand files like email boxes, zips and OLE documents.

- File Signature Analysis
- Flag Bad Extensions
- Entropy Test
- dtSearch® Text Index Indexing Options...
- Create Thumbnails for Graphics Thumbnail Options...
- Create Thumbnails for Videos Video Options...
- Generate Common Video File
- HTML File Listing
- CSV File Listing

- Data Carve Carving Options...

- Meta Carve
- Optical Character Recognition OCR Options...
- Explicit Image Detection EID Options...

C:\Program Files\Acces... \RSR Templates ...

- Registry Reports
- Include Deleted Files Cerberus Options...
- Cerberus Analysis

- Send Email Alert on Job Completion
- Decrypt Credant Files Credant Server Settings...

- Process Internet Browser History for Visualization
- Cache Common Filters
- Perform Automatic Decryption Passwords...
- Language Identification Language ID Options...

Profile: AD Standard

Save to Profile...

OK

Cancel



Evidence Processing



Evidence Refinement (Advanced)



Index Refinement (Advanced)



Custom File Identification

Evidence Refinement (Advanced)

Refine by File Status/Type

Refine by File Date/Size

Inclusion/exclusion settings that will apply to evidence items that are added to the case.

- Include File Slack
- Include Free Space Don't Expand Embedded Graphics
- Include KFF Ignorable Files

Include OLE Streams: All

File Status

- Deleted Ignore status
- Encrypted Ignore status
- From Email Ignore status

File Types

- Documents
- Spreadsheets
- Databases
- Graphics

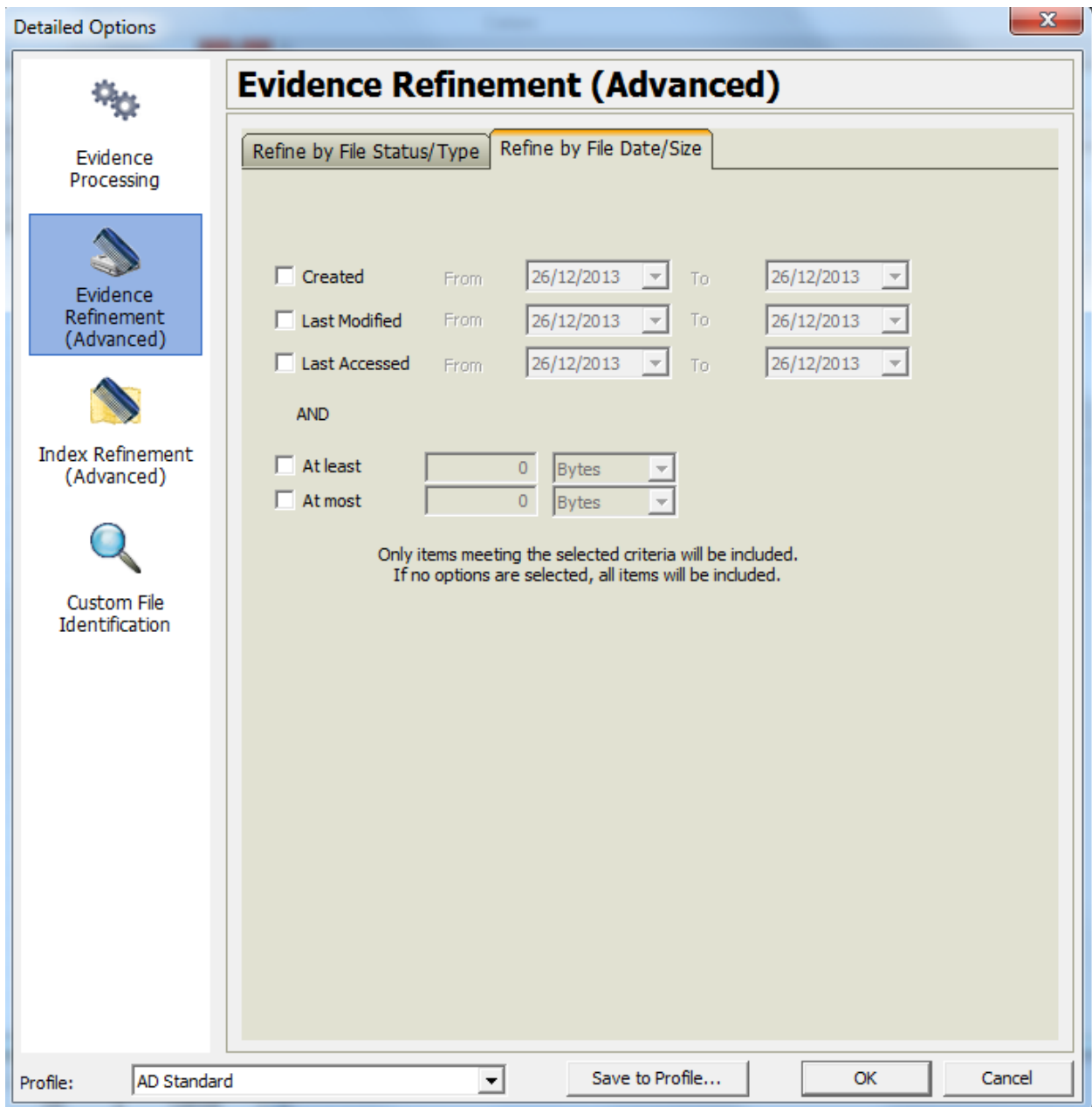
Only add items that match both File Status AND File Types criteria

Profile: AD Standard

Save to Profile...

OK

Cancel



Chapter 5, Processing the Case

Manage Evidence

Display Name	State
Mantooth.E01	
Washer.E01	+

Path: C:\Users\304020\Desktop\Outline preparation kit. Zipped\Washer.i ...

ID / Name:

Description:

Evidence Group: Manage...

Time Zone: America/Denver

Merge case index Use UNC Paths

Refinement Options... Language Setting...

Case KFF Options... OK Cancel

Evidence Processing

Evidence Refinement (Advanced)

Index Refinement (Advanced)

Custom File Identification

Evidence Processing

Generate File Hashes (flag duplicates)

- MD5 Hash
- SHA-1 Hash
- SHA-256 Hash
- Fuzzy Hash
- Match Fuzzy Hash Library
- Flag Duplicate Files
- KFF
- PhotoDNA

Fuzzy Hash Options...

Expand Compound Files

Expansion Options...

Takes extra time to expand files like email boxes, zips and OLE documents.

- File Signature Analysis
- Flag Bad Extensions
- Entropy Test
- dtSearch® Text Index
- Create Thumbnails for Graphics
- Create Thumbnails for Videos
- Generate Common Video File
- HTML File Listing
- CSV File Listing
- Data Carve
- Meta Carve
- Optical Character Recognition
- Explicit Image Detection
- Registry Reports
- Include Deleted Files
- Cerberus Analysis
- Send Email Alert on Job Completion
- Decrypt Credant Files
- Process Internet Browser History for Visualization
- Cache Common Filters
- Perform Automatic Decryption
- Language Identification

Compound File Expansion Options

Only expand office documents with embedded items.

Select file types to expand

- 7-Zip
- Active Directory
- AOL Files
- Blackberry IPD backup file
- BZIP2
- Chrome Bookmarks
- Chrome SQLite
- DBX
- EMFSPPOOL
- EVTX
- EXIF

Select All Clear All

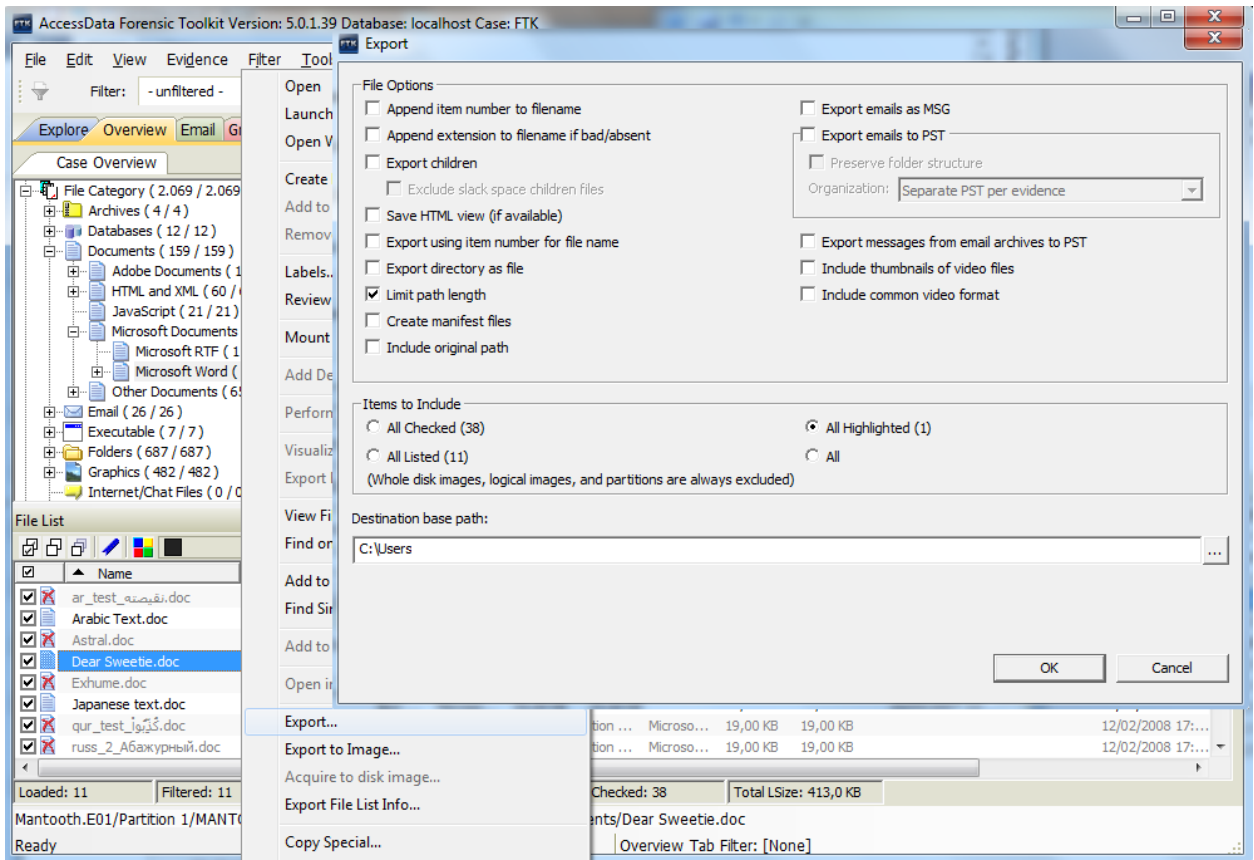
OK Cancel

Profile: AD Standard

Save to Profile...

OK

Cancel



AccessData Forensic Toolkit Version: 5.0.1.39 Database: localhost Case: FTK

Column Settings

Available Columns

- Common Features
- Disk Image Features
- Email Features
- Entropy Stats
- File Status Features
- File System Features
- Zip-specific Features
- Custom Columns
- Office-specific Features
- Cerberus Static Analysis Features
- Microsoft IIS Internet Server
- Log2t
- Internet Data
- All Features

Column Template Name
Normal (1)

Selected Columns

Name	Short Name	Description
Name	Name	The name of the object (f...
Label	Label	Label associated with an ...
Item Number	Item #	A number assigned to the...
Extension	Ext	Extension
Path	Path	The full path to an object
File Type	Category	An INSO type ID (or a cu...
Physical Size	P-Size	The physical size (size on ...
Logical Size	L-Size	The logical size of the obje...
MD5 Hash	MD5	The MD5 hash of the obje...
SHA1 Hash	SHA1	The SHA1 hash of the obj...
SHA256 Hash	SHA256	The SHA256 hash of the ...
Created Date	Created	The date the object was ...
Accessed D...	Accessed	The date the object was l...
Modified Date	Modified	The date the object was ...

File Name	Size	Path	Type	Size	Size
\$Extend	26	Mantooth.E01/Partition ...	Folder	448 B	448 B
\$Recycle.Bin	1813	Mantooth.E01/Partition ...	Folder	56 B	56 B
\$REZFRY8	1830	Mantooth.E01/Partition ...	Folder	56 B	56 B
\$RmMetadata	31	Mantooth.E01/Partition ...	Folder	336 B	336 B
\$Txf	41	Mantooth.E01/Partition ...	Folder	48 B	48 B

Loaded: 687 | Filtered: 687 | Total: 687 | Highlighted: 1 | Checked: 38 | Total LSize: 114,1 KB

Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/\$Extend

Ready | Overview Tab Filter: [None]

adata

Default Media Web

SHA1

Hide

- Name
- Label
- Item #
- Ext
- Path
- Category
- P-Size
- L-Size

Column Settings...

Manage Column Settings

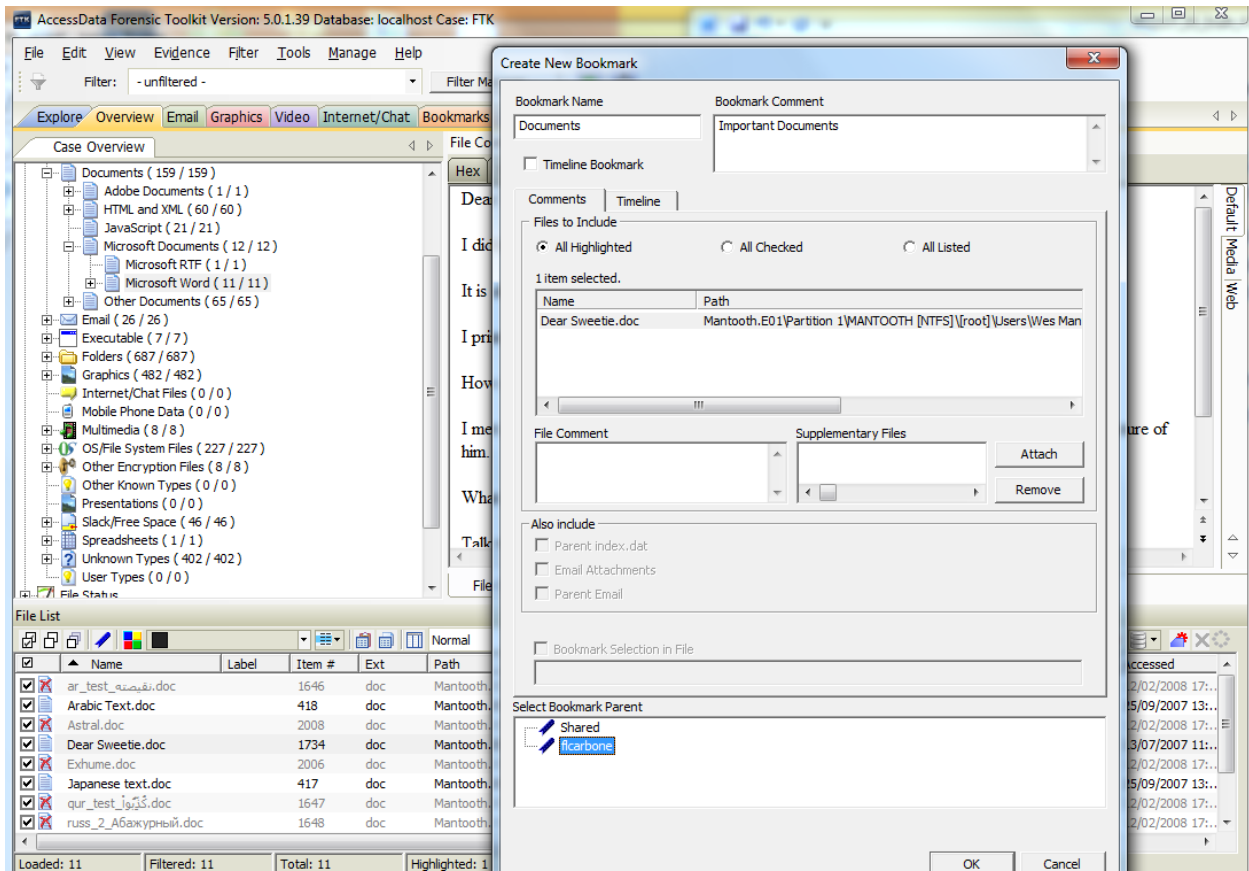


Settings Templates	
Cerberus Results	
EID	
Email	
File Listing	
Internet History	
Normal	
Normal+Filters	
Reports: File Path Section	
Reports: Standard	
eDiscovery	
eDiscovery Email	

New... Edit... Copy Selected... Delete

Import... Export... Make Shared

Apply Close



Additional Analysis

Hashing / Job Options | Indexing / Tools | Miscellaneous

File Hashes

- MD5 Hash
- SHA-1 Hash
- Flag Duplicate Files
- SHA-256 Hash
- Fuzzy hash

KFF

- KFF KFF Groups...
- Recheck previously processed items

Fuzzy hash

- Match fuzzy hash library
- Recheck previously processed items
- Fuzzy hash options

Target Items

- Highlighted Items
- Checked Items
- Currently Listed Items
- All Items

PhotoDNA

- PhotoDNA
-

Refinement


Include OLE Streams: All


Job Options


- Send Email Alert on Job Completion


OK

Cancel


Evidence Processing


Evidence Refinement (Advanced)


Index Refinement (Advanced)


Custom File Identification

Evidence Processing

Generate File Hashes (flag duplicates)

- MD5 Hash
- SHA-1 Hash
- SHA-256 Hash
- Fuzzy Hash
- Match Fuzzy Hash Library
- Flag Duplicate Files
- KFF
- PhotoDNA

Fuzzy Hash Options...

- Expand Compound Files

Expansion Options...

Takes extra time to expand files like email boxes, zips and OLE documents.

- File Signature Analysis

- Flag Bad Extensions

- Entropy Test

- dtSearch® Text Index

Indexing Options...

- Create Thumbnails for Graphics

- Create Thumbnails for Videos

Thumbnail Options...

- Generate Common Video File

Video Options...

- HTML File Listing

- CSV File Listing

- Data Carve

Carving Options...

Carving Options

Select Types to Carve

- AOL bag Files
- BMP Files
- EMF Files
- GIF Files
- HTML Files
- JPEG Files
- LNK Files
- OLE Files (MS Office)
- PDF Files
- PNG Files
- ...

Select All

Clear All

- Exclude KFF Ignorable

Selected Carver Options

- Minimum File Size (bytes)
- Minimum Height (pixels)
- Minimum Width (pixels)

Custom Carvers...

OK

Cancel

Profile: AD S

AccessData Forensic Toolkit Version: 5.0.1.39 Database: localhost Case: FTK

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered- Filter Manager...

Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search Volatile

Case Overview File Content

Evidence Groups (71,468 / 71,468)
File Items
File Extension (1,180 / 1,180)

Hex Text Filtered Natural

北朝鮮のミサイル発射の対抗措置として、日本政府が国民に北朝鮮への渡航自粛を要請したことを受
体として、海上保安庁が自衛隊に警戒態勢を維持する見込みと発表している。

KFF Admin Case: FTK

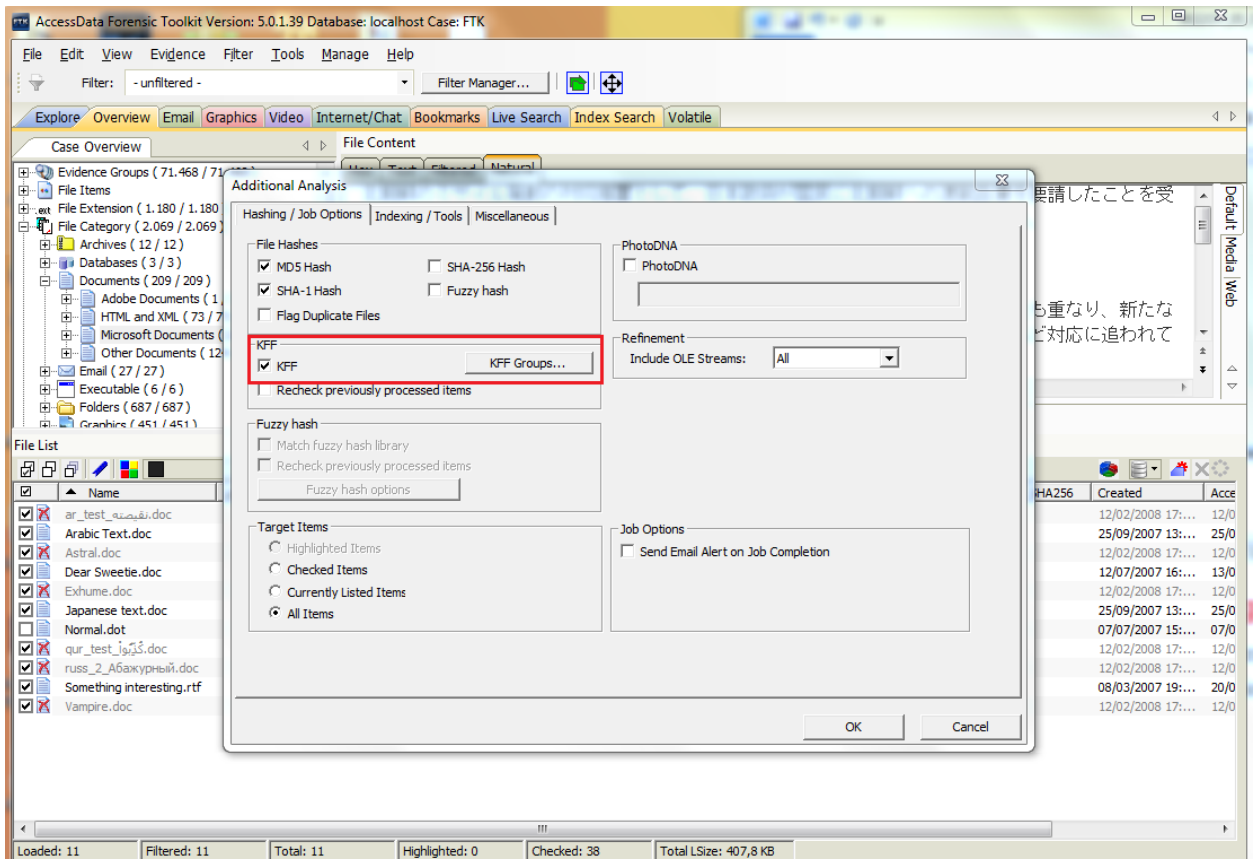
Defined Groups				Defined Sets		
Name	Status	Default	Closed	Name	Status	Source Vendor
				KFF.csv	Alert	In House

Set As Defaults New Edit Delete

Closed KFF groups and sets cannot be edited or deleted.

Import Export Groups Done

Loaded: 11 Filtered: 11 Total: 11 Highlighted: 0 Checked: 38 Total LSize: 407,8 KB



AccessData Forensic Toolkit Version: 5.0.1.39 Database: localhost Case: FTK

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered- Filter Manager...

Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search Volatile

Text Pattern Hex

Search Terms: mantooth Add Clear Export Import

Search Terms Type Code Pages

Mantooth ANSI(Case Insensitive)

Max Hits Per File: 200 Search Filter: -unfiltered- Search

File Content

Hex Text Filtered Natural

No file

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5
SMFT		12	<missin...	Mantooth.E01/Partition ...	Unknown	9344 KB	9344 KB	e17b14...
~ar1730.xar		1566	xar	Mantooth.E01/Partition ...	Unknown	6656 B	6656 B	258af4...
~ar1730.xar.lnk		1499	lnk	Mantooth.E01/Partition ...	Windo...	488 B	488 B	21f68d...
018270		1978		Mantooth.E01/Partition ...	Unalloc...	512,0 KB	512,0 KB	
04f24080836c56509cab...		1294	<missin...	Mantooth.E01/Partition ...	Unknown	512 B	53 B	6a7939...
062746		1981		Mantooth.E01/Partition ...	Unalloc...	32,50 KB	32,50 KB	
08-15-05_arkansas_che...		1430	lnk	Mantooth.E01/Partition ...	Windo...	1024 B	743 B	9a9b8d...

Loaded: 128 Filtered: 128 Total: 128 Highlighted: 0 Checked: 38 Total LSize: 45,42 MB

Live Search Results

Live Search (Prefilter:(-unfiltered-) Query:(("Mantooth")) (ID: 821)

Text Query: "Mantooth" <ANSI, Case Insensitive> -- 821

Allocated Space -- 814 hit(s) in 125 file(s)

- 200 hit(s) -- Item 839 [index.dat] Mantooth.E01/P
- 89 hit(s) -- Item 586 [index.dat] Mantooth.E01/Pa
- 66 hit(s) -- Item 1393 [index.dat] Mantooth.E01/P
- 56 hit(s) -- Item 12 [SMFT] Mantooth.E01/Partitio
- 38 hit(s) -- Item 1372 [index.dat] Mantooth.E01/P
- 31 hit(s) -- Item 593 [index.dat] Mantooth.E01/Pa
- 27 hit(s) -- Item 588 [index.dat] Mantooth.E01/Pa
- 24 hit(s) -- Item 259 [mantooth2007] Mantooth.E0
- 21 hit(s) -- Item 427 [NTUSER.DAT] Mantooth.E01
- 20 hit(s) -- Item 1936 [SOFTWARE] Mantooth.E01
- 14 hit(s) -- Item 428 [ntuser.dat.LOG1] Mantooth.
- 11 hit(s) -- Item 595 [index.dat] Mantooth.E01/Pa
- 8 hit(s) -- Item 451 [edb000C.log] Mantooth.E01
- 8 hit(s) -- Item 1938 [SOFTWARE.LOG1] Mantooth
- 7 hit(s) -- Item 452 [WindowsMail.MSMMessageStor
- 6 hit(s) -- Item 485 [2A29541D-0000000E.eml] Ma
- 6 hit(s) -- Item 1582 [downloads.rdf] Mantooth.E0
- 4 hit(s) -- Item 446 [edb.chk] Mantooth.E01/Partit
- 4 hit(s) -- Item 489 [3376666D-0000000A.eml] Ma
- 4 hit(s) -- Item 491 [40A511AF-00000008.eml] Ma
- 4 hit(s) -- Item 1360 [2EFD34A0A6COE8EC0672E
- 3 hit(s) -- Item 262 [mantooth2007.ARL] Mantooth
- 3 hit(s) -- Item 460 [165D65F6-00000004.eml] Ma
- 3 hit(s) -- Item 495 [458C76A0-0000000C.eml] Ma
- 3 hit(s) -- Item 508 [09EE4522-00000004.eml] Ma
- 3 hit(s) -- Item 1566 [~ar1730.xar] Mantooth.E01
- 2 hit(s) -- Item 1340 [Templates.LNK] Mantooth.E0
- 2 hit(s) -- Item 1366 [Normal.dot] Mantooth.E01/P
- 2 hit(s) -- Item 1430 [08-15-05_arkansas_check.gi
- 2 hit(s) -- Item 1434 [810648.gif.lnk] Mantooth.E0
- 2 hit(s) -- Item 1435 [910648.gif.lnk] Mantooth.E0
- 2 hit(s) -- Item 1436 [Ape_20shoot.gif.lnk] Mantoc
- 2 hit(s) -- Item 1439 [Bill_Gates.gif.lnk] Mantooth.i
- 2 hit(s) -- Item 1442 [C money plates.lnk] Mantoot
- 2 hit(s) -- Item 1443 [C01VNCCHK_e.gif.lnk] Mant

AccessData Forensic Toolkit Version: 5.0.1.39 Database: localhost Case: FTK

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered- Filter Manager...

Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search Volatile

dtSearch@ Index

Terms

mantooth Add

Indexed Words	Total Hits
maintain	1
mantoo	32
mantooth	6996
mantooth0	6
mantooth1	9
mantooth1_23545...	1
mantooth1_85050...	1
mantooth2000	1
mantooth2007	27
mantooth20071	3
mantooth2007@aol	22

Search Criteria

Operators: And Or

Terms: All Selected Accumulate Results

Search Terms

Search Terms	Total Hits
mantooth	6996

Clear Import... Export... Options... Search Now

Index Search Results

- dtSearch@ Indexed Search (Prefilter:(all files) Qu...
- Allocated Space -- 6966 hit(s) in 1975 file(s)
- Documents -- 736 hit(s) in 207 file(s)
- Spreadsheets -- 10 hit(s) in 2 file(s)
- Databases -- 22 hit(s) in 3 file(s)
- Graphics -- 1398 hit(s) in 447 file(s)
- Multimedia -- 15 hit(s) in 5 file(s)
- Email -- 121 hit(s) in 26 file(s)
- Executable -- 18 hit(s) in 6 file(s)
- Archives -- 36 hit(s) in 12 file(s)
- Folders -- 1591 hit(s) in 657 file(s)
- Other Encryption Files -- 74 hit(s) in 17 file(s)
- Internet/Chat Files -- 354 hit(s) in 19 file(s)
- OS/File System Files -- 1136 hit(s) in 256 file(s)
- Other Known Types -- 8 hit(s) in 2 file(s)
- Unknown Types -- 1447 hit(s) in 316 file(s)
- Unallocated Space -- 30 hit(s) in 30 file(s)

File Content

Hex Text Filtered Natural

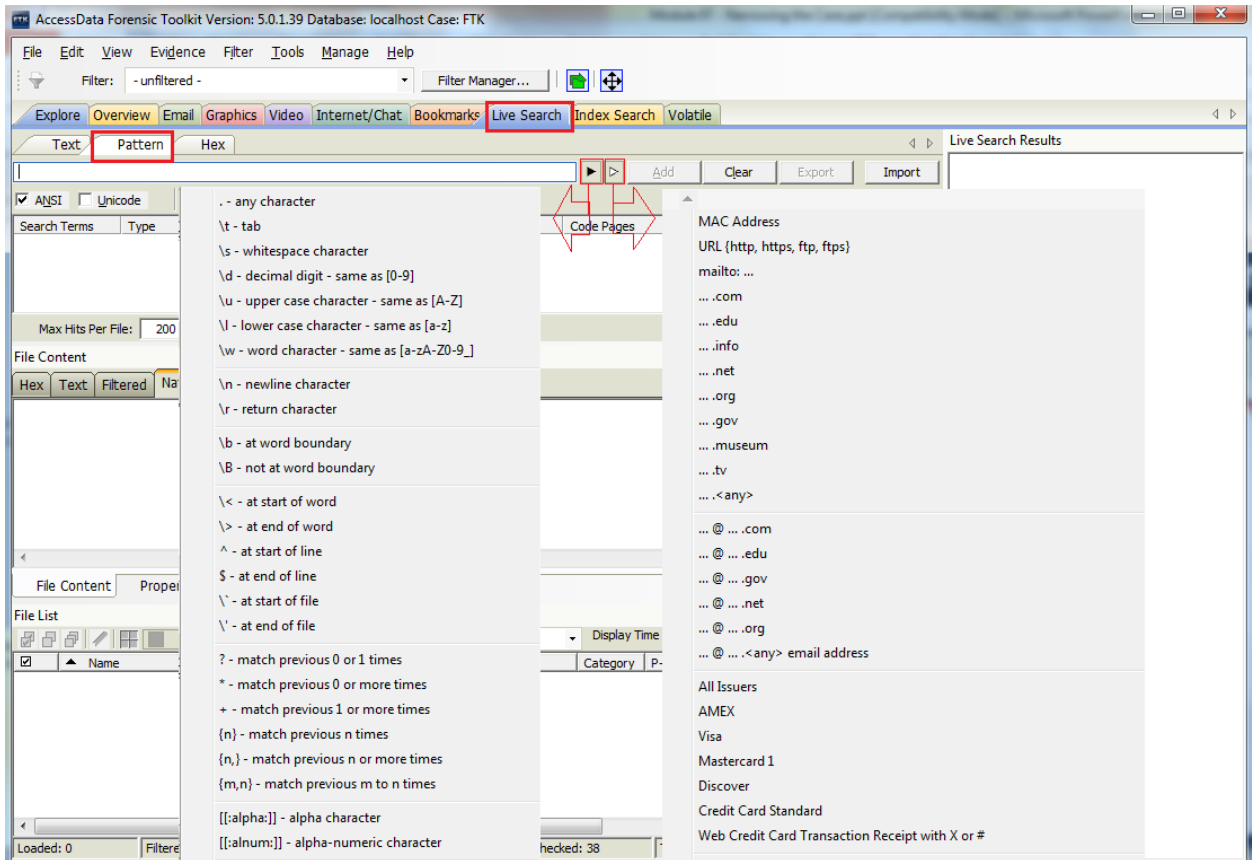
Hit # of Prev Next Go to: Go

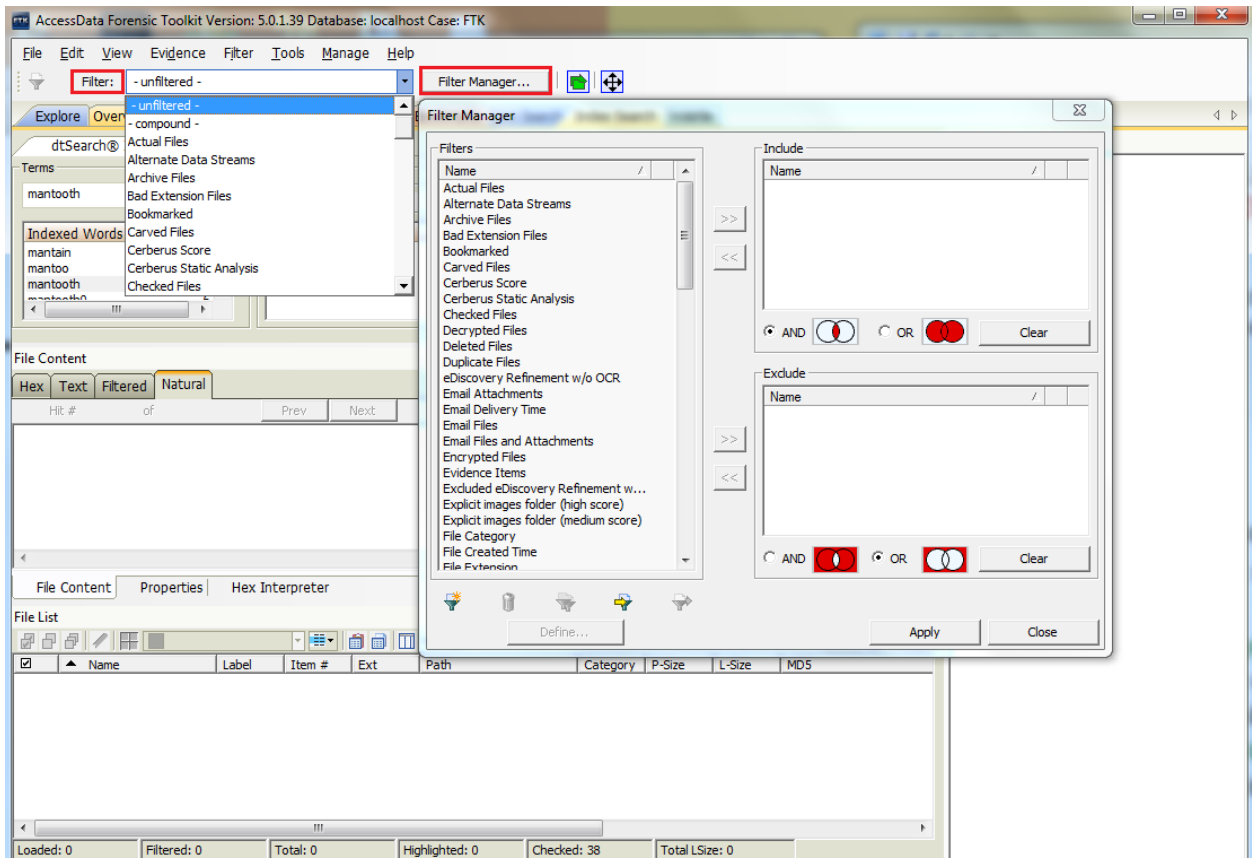
File Content Properties Hex Interpreter

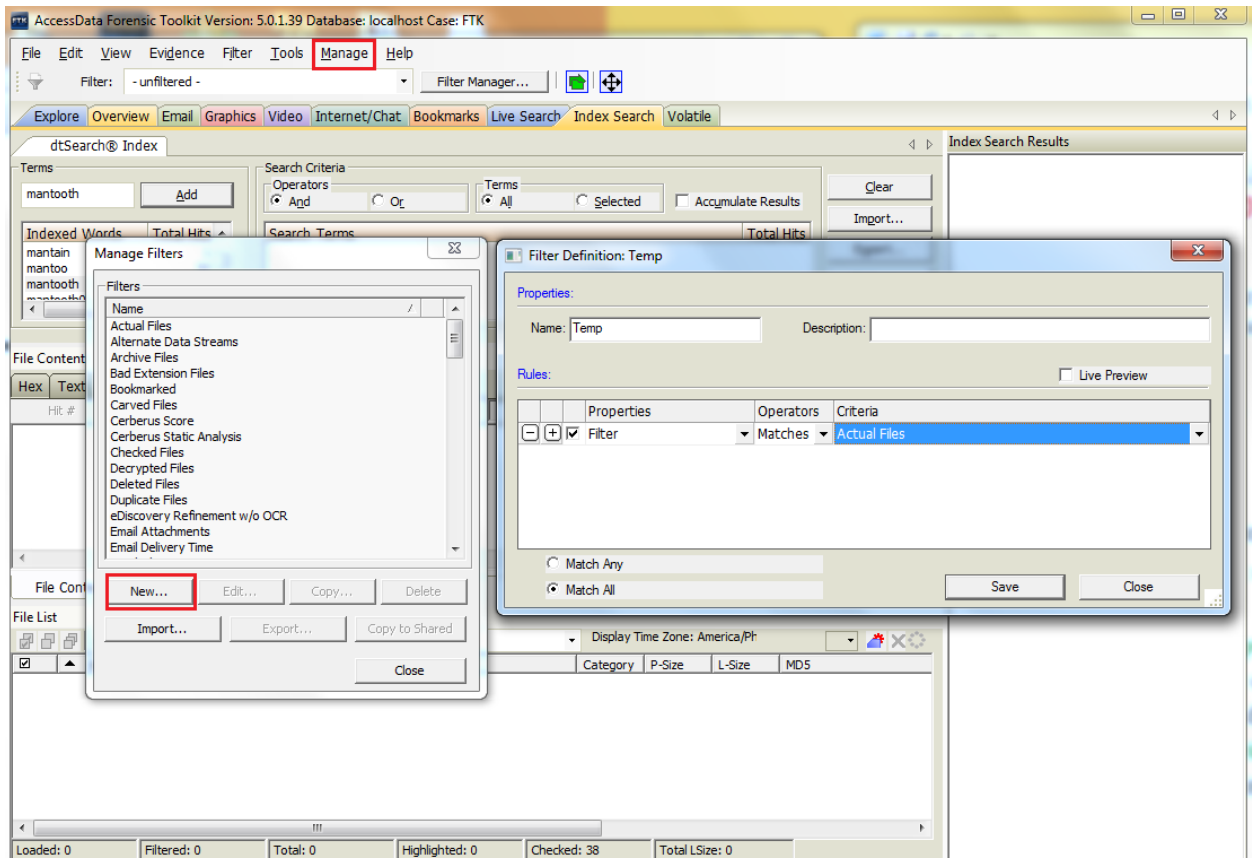
File List

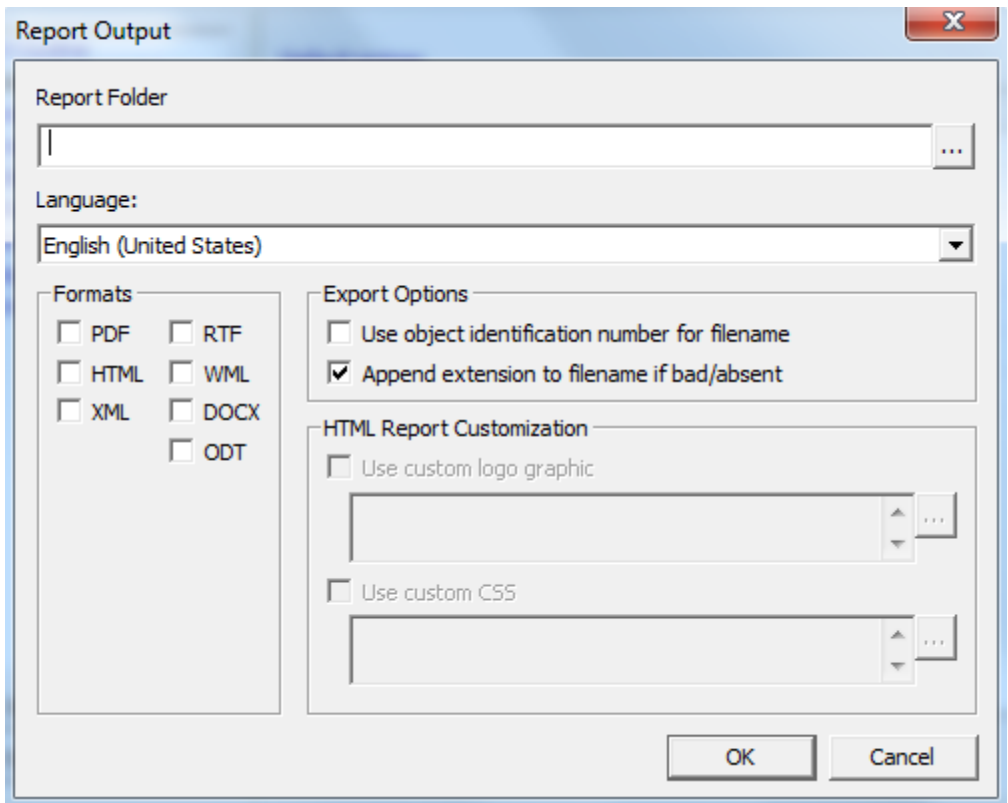
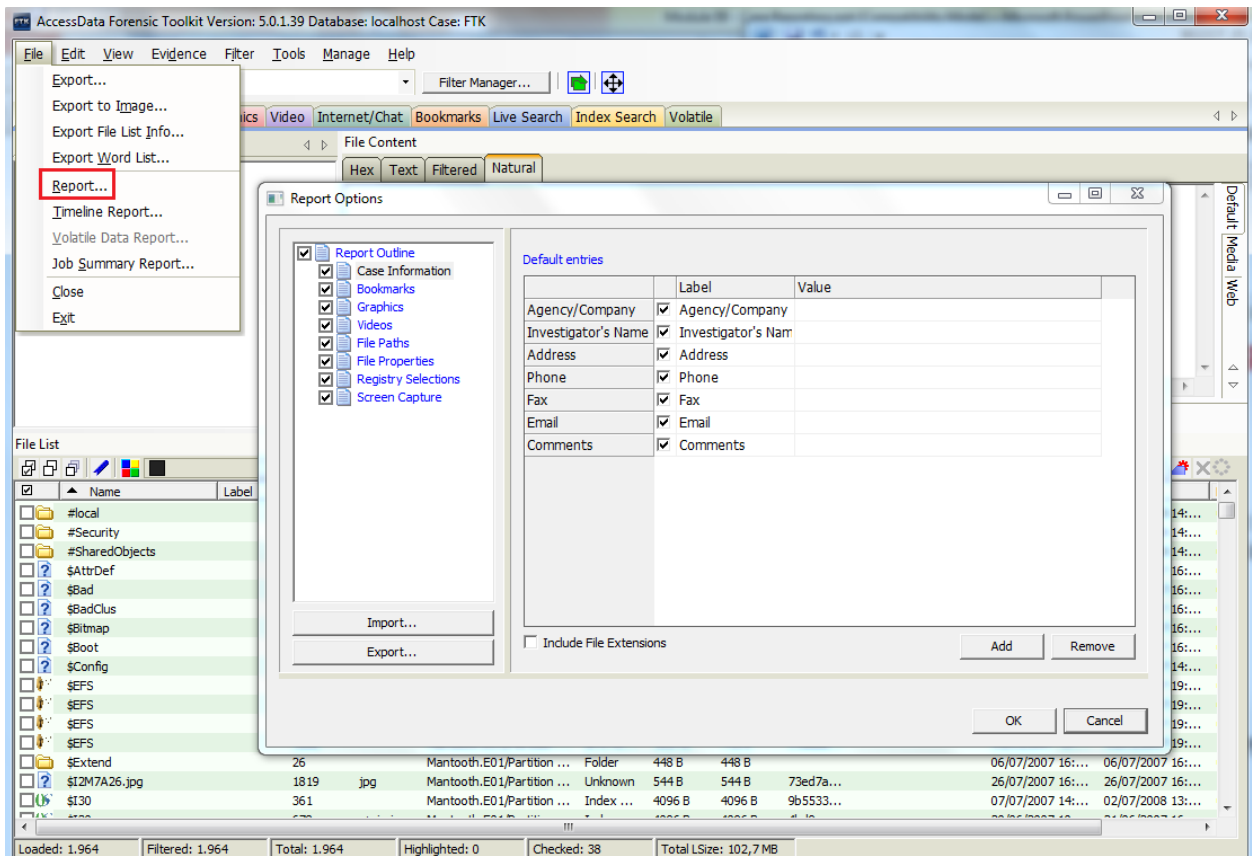
Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5
#local		1283		Mantooth.E01/Partition ...	Folder	160 B	160 B	
#Security		1271		Mantooth.E01/Partition ...	Folder	272 B	272 B	
#SharedObjects		1274		Mantooth.E01/Partition ...	Folder	152 B	152 B	

Loaded: 2.005 Filtered: 2.005 Total: 2.005 Highlighted: 0 Checked: 38 Total LSize: 110,2 MB

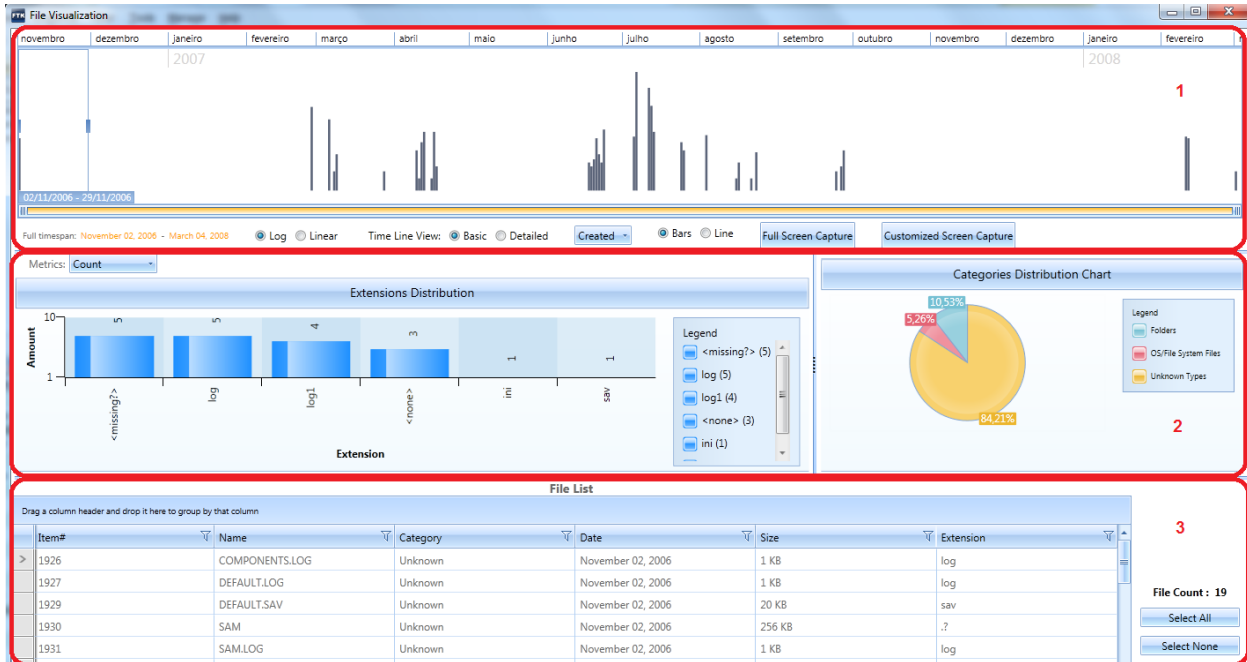








Chapter 6, New Features of FTK 5



Agent Installation

Machines to install

192.168.0.182

Add

Remove Import... Export...

Uninstall agent

Use custom agent name

Service name: AgentService

Executable name: agentcore.exe

Update the agent if it is present

Allow manual uninstall

OK Cancel

AccessData Forensic Toolkit Version: 5.0.1.39 Database: localhost Case: FTK

File Edit View Evidence Filter Tools Manage Help

Filter: unfiltered - Filter Manager...

Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search Volatile

Snapshot Find Difference

Detail List

Name	Path	Start Time	Working Directory	Command Line	PID	Has Search...	Parent PID	User	MDS
SearchProtocol	C:\Program Files\AccessD...	18/01/2014 20:35:...			12792	N	0		00000000000000000000000000000000...
postgres.exe	C:\Program Files\AccessD...	18/01/2014 20:36:...	C:\pgData91\	"C:\Program Fil...	10808	N	0		00000000000000000000000000000000...
explorer.exe	C:\Program Files (x86)\Int...	15/01/2014 17:40:...	C:\WINDOWS\...	"C:\Program Fil...	11188	N	0		00000000000000000000000000000000...
ncsheld.exe	C:\Program Files\Common...	18/01/2014 12:54:...	C:\WINDOWS\...	"C:\Program Fil...	12888	N	0		00000000000000000000000000000000...
AcroRd32.exe	C:\Program Files (x86)\Ad...	18/01/2014 19:15:...	C:\WINDOWS\...	"C:\Program Fil...	11868	N	0		00000000000000000000000000000000...
explorer.exe	C:\Program Files (x86)\Int...	15/01/2014 17:40:...	C:\WINDOWS\...	"C:\Program Fil...	11188	N	0		00000000000000000000000000000000...
splwow64.exe	C:\WINDOWS\syswow64\...	18/01/2014 18:52:...	C:\WINDOWS\...	"C:\WINDOWS\...	8576	N	0		00000000000000000000000000000000...
AcroRd32.exe	C:\Program Files (x86)\Ad...	18/01/2014 19:15:...	C:\WINDOWS\...	"C:\Program Fil...	11868	N	0		00000000000000000000000000000000...
Skype.exe	C:\Program Files (x86)\Sk...	16/01/2014 20:57:...	C:\WINDOWS\...	"C:\Program Fil...	9336	N	0		00000000000000000000000000000000...
AcroRd32.exe	C:\Program Files (x86)\Ad...	18/01/2014 19:15:...	C:\WINDOWS\...	"C:\Program Fil...	1188	N	0		00000000000000000000000000000000...
Skype.exe	C:\Program Files (x86)\Sk...	16/01/2014 20:57:...	C:\WINDOWS\...	"C:\Program Fil...	9336	N	0		00000000000000000000000000000000...
AcroRd32.exe	C:\Program Files (x86)\Ad...	18/01/2014 19:15:...	C:\WINDOWS\...	"C:\Program Fil...	1188	N	0		00000000000000000000000000000000...
Skype.exe	C:\Program Files (x86)\Sk...	16/01/2014 20:57:...	C:\WINDOWS\...	"C:\Program Fil...	9336	N	0		00000000000000000000000000000000...
real Sched.exe	C:\Program Files (x86)\Re...	18/01/2014 12:52:...	C:\WINDOWS\...	"C:\Program Fil...	12988	N	0		00000000000000000000000000000000...

Total: 149 Highlighted: 1 Checked: 0 KFF: Unlisted,Important,Unimportant

Detailed Information

Name	TCP/IP	Handles	Fuzzy Hash	Search Hits	SDT	VAD	Has Search...	Version	Creation Time	Process Name	PID	MDS
explorer.exe							N		15/01/2014 17:40:...	explorer.exe	11188	00000000000000000000000000000000...
ntldr.dll							N		15/01/2014 17:40:...	explorer.exe	11188	00000000000000000000000000000000...
wow64.dll							N		15/01/2014 17:40:...	explorer.exe	11188	00000000000000000000000000000000...
wow64win.dll							N		15/01/2014 17:40:...	explorer.exe	11188	00000000000000000000000000000000...
wow64cpu.dll							N		15/01/2014 17:40:...	explorer.exe	11188	00000000000000000000000000000000...
explorer.exe							N		15/01/2014 17:40:...	explorer.exe	11188	00000000000000000000000000000000...
ntldr.dll							N		15/01/2014 17:40:...	explorer.exe	11188	00000000000000000000000000000000...
kernel32.dll							N		15/01/2014 17:40:...	explorer.exe	11188	00000000000000000000000000000000...
KERNELBASE.dll							N		15/01/2014 17:40:...	explorer.exe	11188	00000000000000000000000000000000...
ADVAPI32.dll							N		15/01/2014 17:40:...	explorer.exe	11188	00000000000000000000000000000000...
msvrt.dll							N		15/01/2014 17:40:...	explorer.exe	11188	00000000000000000000000000000000...
sechost.dll							N		15/01/2014 17:40:...	explorer.exe	11188	00000000000000000000000000000000...
RPCRT4.dll							N		15/01/2014 17:40:...	explorer.exe	11188	00000000000000000000000000000000...
user32.dll							N		15/01/2014 17:40:...	explorer.exe	11188	00000000000000000000000000000000...

Additional Analysis

Hashing / Job Options | Indexing / Tools | Miscellaneous

Indexed Search

dtSearch® Text Index

Process File Slack Space

Process Drive Free Space

Entropy Test
(do not index compressed or encrypted items)

Do not include document metadata in filtered text

Merge case index when finished

Decryption

Decrypt Credant Files Credant Server Settings...

Perform Automatic Decryption Passwords...

Other Tools

Optical Character Recognition OCR Options...

Explicit Image Detection EID Options...

Registry Reports RSR Directory...

Cerberus Analysis Cerberus Options...

Language Identification Lang ID Options...

Explicit Image Detection Options

X-DFT (default)

X-FST (faster)

X-ZFN (more accurate)

OK Cancel

OK Cancel

Additional Analysis



Hashing / Job Options | Indexing / Tools | Miscellaneous

Indexed Search

- dtSearch® Text Index
 - Process File Slack Space
 - Process Drive Free Space
- Entropy Test
(do not index compressed or encrypted items)
- Do not include document metadata in filtered text
- Merge case index when finished

Decryption

- Decrypt Credant Files
- Perform Automatic Decryption

Other Tools

- Optical Character Recognition
- Explicit Image Detection
- Registry Reports
- Cerberus Analysis
- Language Identification

OK

Cancel

File Content

Hex Text Filtered **Natural**

CS3

EXAMPLE.EXE

Score: **49** CA9E66C592100D3BD7D0B47BF3F9D4C1

+/- Cerberus Score

Function Call Summary

+/- **File Access**

- [DeleteFileA\(<unknown>\)](#)
- [CreateFileA\(<unknown>, <unknown>, <unknown>, 00000000, <unknown>, 80, 00000000\)](#)
- [CreateFileA\(<unknown>, <unknown>, <unknown>, <unknown>, 3, 4000000, <unknown>\)](#)

Loads a driver
 Low-Level Access
 Network Functionality
 Process Manipulation
 Security Access

+/- **Subverts API**
 Surveillance
 Uses Cryptography
 Windows Registry

Function Call Detail

Function	Location	Argument(s)		
		Name	Type	Value
ContinueDebugEvent	5488498	dwProcessId	DWORD	<unknown>
		dwThreadId	DWORD	<unknown>
		dwContinueStatus	DWORD	<unknown>
DebugActiveProcess	5488474			

File Content Properties Hex Interpreter

Default Web

File System	Application Data										
Dropbox (dropbox)			20333	245	Fri Mar 04 21:23:11 +0000 2011	0	545	1	Welcome to official twitter page for United. We look forward to connecting with you.	260907612	
Google Voice (googlevoice)											
LinkedIn (linkedin)											
Osfoora (twitter)			2116	280	Thu Apr 30 11:28:02 +0000 2009	0	430	0	ForensicFocus.com - computer forensics portal for digital forensics and ediscovery practitioners	36641167	
accounts											
drafts											
friends	Southern California	654	107	Mon Aug 31 14:59:57 +0000 2009	7	3818	0	Police/Medical Technical Advisor for The Mentalist	70412647		
storedDMs											
storedDMsSent	NY	205	31	Tue May 25 16:59:09 +0000 2010	0	115	0	Apple OS X & iOS Digital Forensics	148025431		
storedtweets											
storedmentions	Lindon, UT	1660	567	Fri Sep 04 15:09:57 +0000 2009	0	1954	0	See new videos, resources & industry news from AccessData, a leading provider of E-Discovery, Forensics & Cyber Security software.	71557070		
Skype (skype)											
Accounts	m Oxford	312237	0	Fri Sep 11 14:57:38 +0000 2009	0	474	0	C. S. Lewis Quotes Everyday	73402979		
CallMembers											
Calls	Dallas, TX	1617240	15	Tue Jan 30 22:14:50 +0000 2007	3114	3781	0	Woot : One Day, One Deal. See followers for additional Woot feeds.	734493		
ChatMembers											
Chats											
Contacts											
Conversations	For USA customers	1589818	35	Tue May 01 15:46:16 +0000 2007	35	1544	1	Refurbished Dell™ computers, electronics. Questions/comments? Contact Chris Beutnagel @ChrisCBATDell or Elise Osborn @EliseATDell.	5688592		
Messages	wilson Los Angeles-ish	2384295	225	Wed Jan 28 05:28:45 +0000 2009	1226	5515	1	I am an actor and a writer and I co-created SoulPancake and my son, Walter.	19637934		
SMSes	ices.shtml NYC - On tour this summer	590958	455	Sun Jun 03 11:09:19 +0000 2007	35	1673	1	Husband to hot wife, father of 4, comedian, actor, writer, former sleeper http://favstar.fm/users/JimGaffigan Itunes = http://tinyurl.com/65z4dfy	6539592		

Chapter 7, Working with PRTK

Module Name	Display Name	Attack Types	Supported Products
ABICoder	ABICoder Password Module	dictionary	Product Name: ABI Coder Versions supported: 3.5.7.4 - 3.6.1.4
Access	MS Access Password Module	decryption dictionary	Product Name: Microsoft Access Versions supported: Through 2013
ACT	ACT! Password Module	decryption	Product Name: ACT! Versions supported: 1 - 4 2000 5 - 6
AdvancedFileLock	AdvancedFileLock Password Module	dictionary	Product Name: Advanced File Lock Versions supported: 6 - 7.1
AIM	AIM Password Module	decryption dictionary	Product Name: AOL Instant Messenger Versions supported: Through 7.5 Product Name: AIM Triton Versions supported: Through 1.5 Product Name: AIM For Windows Versions supported: Through
AmiPro	AmiPro Password Module	dictionary	Product Name: Ami Pro Versions supported: <i>Unknown</i>

