



AccessData[®]

FTK 4/5

Additional Analysis

Elements of a Graphics case

Elements of a Email case

Decrypt Files

Decrypt Files

Password:

Confirm Password:

Permanently Mask

Saved Passwords:

- ****
- tooth

Attempt Blank Password

Decrypt File Types

- EFS
- Microsoft Office
- Lotus NSF

Unable to View

Document is encrypted

	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Access
iti...	Microso...	19.00 KB	19.00 KB	E64A6...	340DD...	7AE7A...	2/12/2008 4:53...	2/12/...
io...	EFS En...	28.50 KB	28.36 KB	F64583...	652933...	7A030...	7/25/2007 1:31...	7/25/...
iti...	EFS En...	76.50 KB	76.50 KB	267862...	F6DA9...	287C4...	3/5/2007 6:14:...	3/5/2...
iti...	EFS En...	18.00 KB	18.00 KB	45E4B4...	A52B5...	31A7A...	3/5/2007 6:14:...	3/5/2...
iti...	Microso...	36.95 KB	27.00 KB	018D1...	A2533...	1C0F8...	n/a	n/a
io...	Microso...	27.00 KB	27.00 KB	018D1...	A2533...	1C0F8...	7/25/2007 1:31...	7/25/...
io...	Microso...	36.95 KB	27.00 KB	018D1...	A2533...	1C0F8...	n/a	n/a
iti...	EFS En...	23.50 KB	23.50 KB	20880B...	DB723...	A2AF1...	3/5/2007 6:14:...	3/5/2...

- Open
- Launch in Content Viewer
- Open With... ▶
- Create Bookmark...

File Edit View Evidence Filter Tools Manage Help

Filter: Cerberus Score Filter Manager...

Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile

Case Overview

- db (0 / 29)
- dbb (0 / 2)
- dbx (0 / 8)
- ddb (0 / 1)
- default (0 / 1)
- desklinc (0 / 4)
- dic (0 / 1)
- dll (4 / 4)
- doc (0 / 13)
- dtd (0 / 5)
- enc (0 / 1)
- evt (0 / 3)
- exe (2 / 2)
- gif (0 / 239)
- htm (0 / 145)
- html (0 / 12)
- htt (0 / 3)
- idx (0 / 4)
- ind (0 / 8)

File Content

Hex Text Filtered Natural

Score: 30 EB9ECF568945B60E76396D504AD6094D

+/- Cerberus Score

NETWORK	0
PERSISTENCE	0
PROCESS	+4
CRYPTO	+2
PROTECTED STORAGE	0
REGISTRY	+2
SECURITY	0
OBFUSCATION	+20
PROCESS EXECUTION SPACE	+2
BAD SIGNED	0
EMBEDDED DATA	0
BAD	0
SIGNED	0
Final Score	30

File Content Properties Hex Interpreter

File List

Display Time Zone: W. Europe Daylight Time (From local)

	Name	Item #	Path	Category	C.	Cerberus Sc...	Cerberus - Network	Cerberus - Persistence	Cerberus - Process
<input type="checkbox"/>	Dd5.exe	3668	precious.E01/Partition 1...	Exe	30	N	N	Y	
<input type="checkbox"/>	Dd1.exe	3666	precious.E01/Partition 1...	Exe	30	N	N	Y	

Loaded: 2 Filtered: 2 Total: 2 Highlighted: 1 Checked: 208 Total LSize: 1753 KB

precious.E01/Partition 1/The Precious [NTFS]/[root]/RECYCLER/S-1-5-21-1801674531-1177238915-725345543-1004/Dd5.exe

Ready Overview Tab Filter: [None]

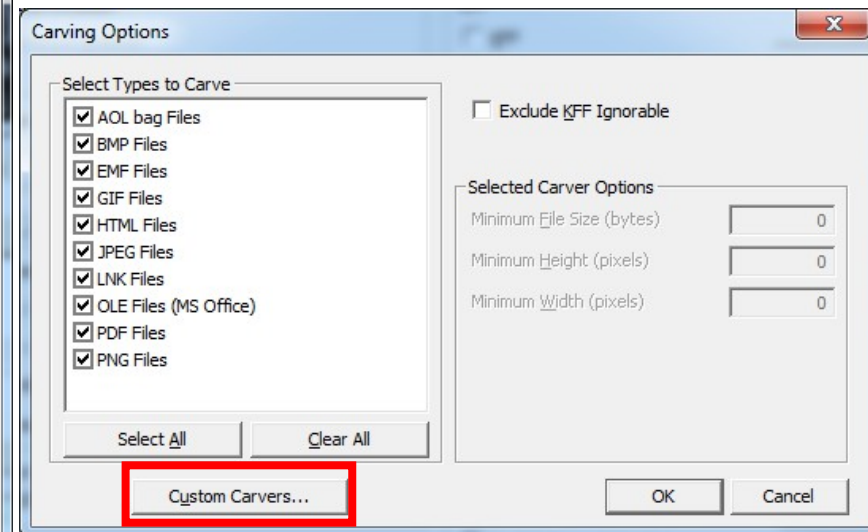
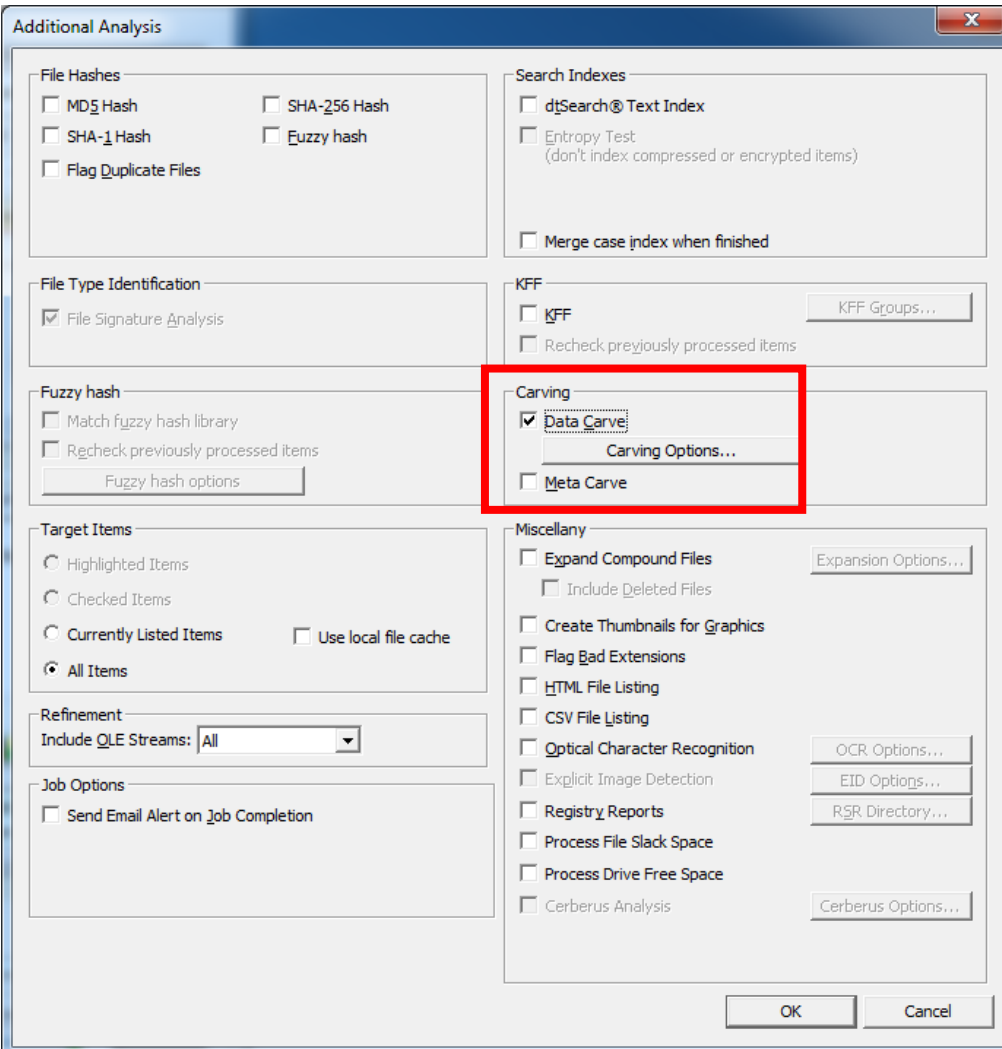
Cerberus Stage 1 Score

Attribute	Threat Score	Description
Network	+1	Imports networking functions.
Persistence	+4	Indicates signs of persistent behavior. For example, the ability to keep a binary running across computer restarts.
Process	+4	Imports functions to programmatically interact with processes. For example, reading or writing into a process's memory, or injecting code into another process.
Crypto	+2	Imports Microsoft Cryptographic Libraries. For example, the ability to encrypt and decrypt data.
Protected Storage	+5	Imports functions used to access protected storage. For example, Internet Explorer stores a database for form-filling in protected storage.
Registry	+2	Imports functions used to access or change values in the registry.
Security	+4	Imports functions used to modify user tokens. For example, attempting to clone a security token to impersonate another logged on user.
Obfuscation	+20	Contains a packer signature, contains sections of high entropy, or imports a low number of functions.
Process Execution Space	+2	Unusual activity in the Process Execution Space header. For example, a zero length raw section, unrealistic linker time, or the file size doesn't match the Process Execution Space header.
Bad Signed	+20	Contains a signature but the signature is bad.
Embedded Data	+5	Contains an embedded executable code.
Bad / Bit-Bad	+20	Contains an IRC or shellcode signature.
Signed / Bit Signed	-20	Contains a valid signature.

Additional Analysis

- From the Case Examiner Interface menu > Evidence > Additional Analysis...

Meta Carve = Filesystem metadata



FTK – Data Carving

- Data Carving finds objects that are not referenced by a directory entry or MFT Record.
- You are adding records, not evidence!
- Carved items become independent items.
- Manually carved items are automatically indexed but not hashed.
- Added records are found in the Overview tab > File Status > Data Carved Files

FTK – Manual Data Carving

The screenshot displays the FTK (Forensic Toolkit) interface. The top menu bar includes File, Edit, View, Evidence, Filter, Tools, and Help. Below the menu is a toolbar with icons for file operations and a search filter set to '- unfiltered -'. The main window is divided into several panes:

- Bookmarks:** A tree view on the left shows a bookmark named 'ndrehel' containing a sub-bookmark 'Carved Credit Card Numbers', which is currently selected.
- Bookmark Information:** A panel on the right provides details for the selected bookmark, including its name ('Carved Credit Card Numbers'), creator ('ndrehel'), and a file comment ('Carved from Pagefile showing credit card numbers.').
- File Content:** The main pane shows the content of the selected file, displaying extracted text for 'visa' and 'Mastercard' cards, including card numbers and expiration dates.
- File List:** A table on the right lists the files in the current view. The table has columns for Name, Label, Item #, Extension, and Path. One file is listed: 'My Carved Data.txt' with an item number of 19436 and extension 'txt'.

At the bottom of the interface, a status bar shows 'Ready' and 'Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/pagefile.sys/My Carved Data.txt'. A 'Bookmarks Tab Filter: [None]' indicator is also present.

Go to offset... Ctrl+G

Save selection as carved file...

FTK – Data Carving

The screenshot shows the FTK (Forensic Toolkit) interface. The 'File Content' window displays the following text:

Guys,
Here are the numbers I was able to purchase online.
We are guaranteed that they are valid for 30 days from 8/1/07.
Do anything you can to use them but DON'T get busted!
Each has a 10K limit!
visa
4805-5555-1234-5566 Exp 10/09
4858.2545.5456.5555 Exp 6/09
4454 5588 5124 2458 Exp 07/08

The 'File List' window shows the following table:

Name	Label	Item #	Extension	Path	Category	Size	MD5	SHA1	SHA256	Content	Access
Carved [374464].jpeg		19449	jpeg	Thumbdrive 05.E01/FA...	JPEG						n/a
Carved [392440].jpeg		19450	jpeg	Thumbdrive 05.E01/FA...	JPEG						n/a
Carved [410021].jpeg		19451	jpeg	Thumbdrive 05.E01/FA...	JPEG						n/a
Carved [428670].jpeg		19452	jpeg	Thumbdrive 05.E01/FA...	JPEG						n/a
Carved [463783].jpeg		19453	jpeg	Thumbdrive 05.E01/FA...	JPEG						n/a
Carved [73257].jpeg		19439	jpeg	Thumbdrive 05.E01/FA...	JPEG						n/a
My Carved Data.txt		19436	txt	Mantooth32.E01/Partiti...	Text	422 B	CB0FF...	969F0...	490A4...		
Test Carved Text.txt		16360	txt	Mantooth32.E01/Partiti...	Text	192 B	710366...	03C27...	F6E241...		

A blue callout box with the text "Every Carved File is found here" is positioned over the 'File List' window, with red arrows pointing to the 'Data Carved Files' folder in the 'Case Overview' pane and the 'My Carved Data.txt' file in the 'File List' table.

FTK – Data Carving

The screenshot shows the FTK (Forensic Toolkit) interface. The main window displays a text file with the following content:

Guys,

Here are the numbers I was able to purchase online.

We are guaranteed that they are valid for 30 days from 8/1/07.

Do anything you can to use them but DON'T get busted!

Each has a 10K limit!

visa

4805-5555-1234-5566 Exp 10/09
4858-2545-5456-5555 Exp 6/09
4454-5588-5124-2458 Exp 07/08

The File List table at the bottom shows the following entries:

Name	Label	Item #	Extension	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Access
MSN.com.url		5729	url	Washer 17.E01/Partiti...	Text	119 B	119 B	919479...	A3FFD...	8EBD3...	8/3/2007 6:19:...	8/3/2
MSN.com.url		5773	url	Washer 17.E01/Partiti...	Text	119 B	119 B	41F409...	379CA...	196C1...	8/3/2007 6:19:...	8/3/2
MSO1033.acd		1986	acd	Mantooth32.E01/Partiti...	Text	37.00 KB	36.93 KB	AEC7E...	D5D0A...	A17A1...	7/7/2007 3:57:...	7/7/2
MSOut11.pip		1987	pip	Mantooth32.E01/Partiti...	Text							
My Carved Data.txt		19436	txt	Mantooth32.E01/Partiti...	Text							
My Confession.txt		1781	txt	Mantooth32.E01/Partiti...	Text							
My poem.txt		1617	txt	Mantooth32.E01/Partiti...	Text							
n2CoreLibs-n2v1-12794...		8694	css	Washer 17.E01/Partiti...	Text							

A red arrow points from the 'Text (1,421 / 1,421)' entry in the file list to the 'My Carved Data.txt' entry in the file list table. A blue callout box contains the text: "Also in the appropriate category".

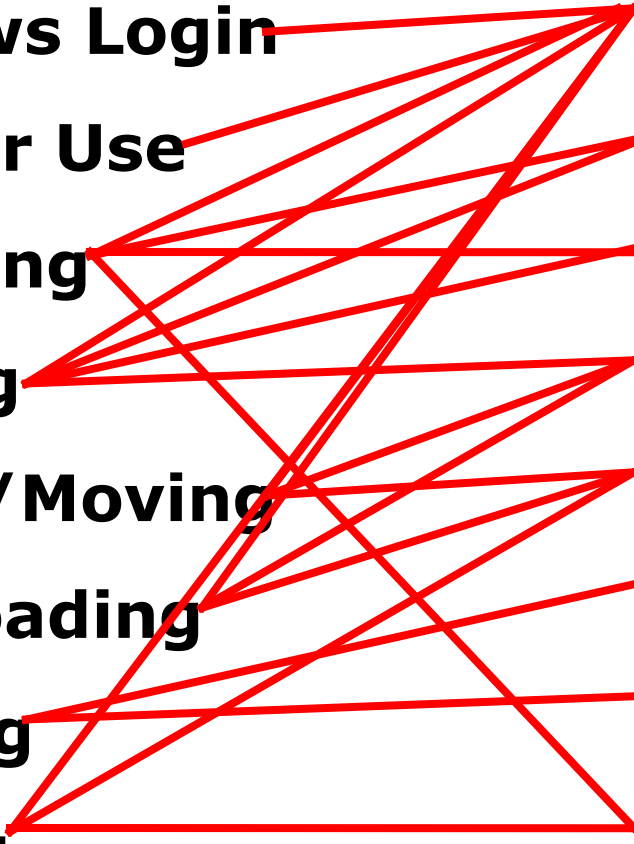
Elements of a Graphics Case

Doing This

- Windows Login
- Browser Use
- Searching
- Viewing
- Saving/Moving
- Downloading
- Deleting
- Sharing

Might leave this

- Registry Entries
- Browser Cache
- Browser History
- Link Files
- Actual Item
- Deleted Item
- Recycle Bin Entry
- Other Artifacts



Graphics Tab

AccessData Forensic Toolkit Version: 4.0.0.35120 Database: localhost Case: precious -Education-

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered- Filter Manager...

Explore Overview Email **Graphics** Bookmarks Live Search Index Search Volatile

Thumbnails

Loaded: 1 253 Filtered: 1 253 Total: 5 015 Highlighted: 1 Checked: 208 Total LSize: 5467 KB Show Tooltip

Evidence Items File Content

Hex Text Filtered Natural

File Content Properties Hex Interpreter

Quick Picks

File List

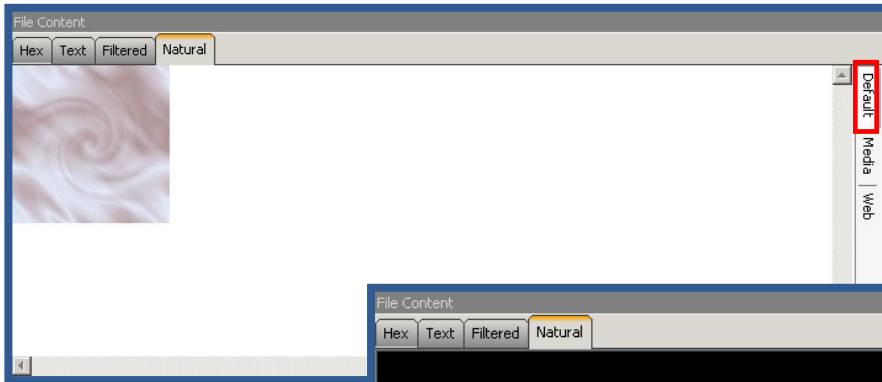
☑	▲	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created
<input type="checkbox"/>		040_fp0993_a[1].jpg		2682	jpg	precious.E01/Partition 1...	JPEG	2048 B	1791 B	F48EEB...	19B318...	AA5F1...	2005-01-01
<input checked="" type="checkbox"/>		040102_alfred.jpg		3038	jpg	precious.E01/Partition 1...	JPEG	20,00 KB	19,52 KB	E56408...	85EDE...	E18B2...	2005-01-01

Loaded: 1 253 Filtered: 1 253 Total: 5 015 Highlighted: 1 Checked: 208 Total LSize: 5467 KB

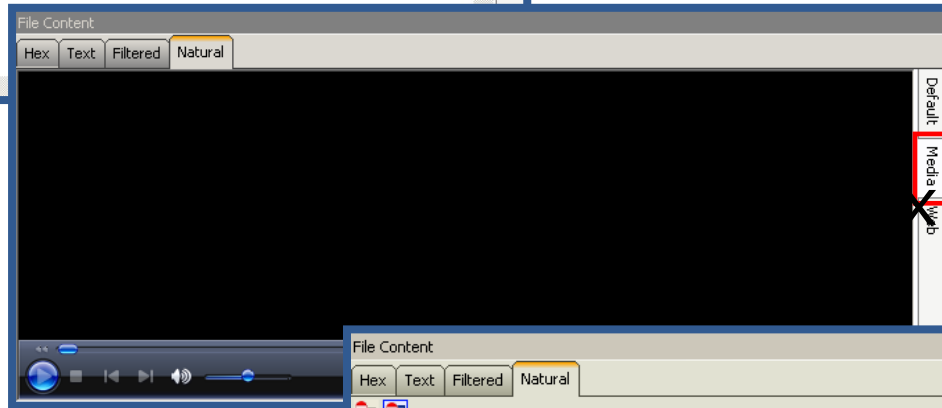
precious.E01/Partition 1/The Precious [NTFS]/[root]/Documents and Settings/Frodo Baggins/My Documents/My Pictures/040102_alfred.jpg

Ready Graphics Tab Filter: Graphic Files

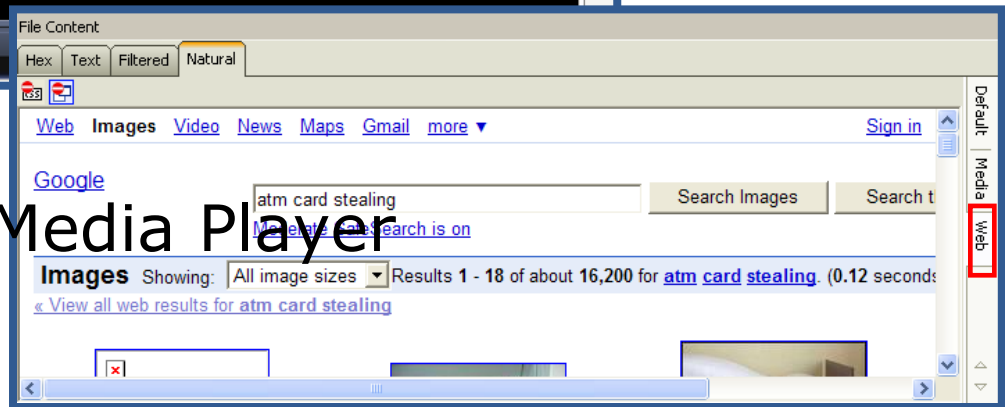
Viewer Options



- Default – INSO (Inside Out) filters

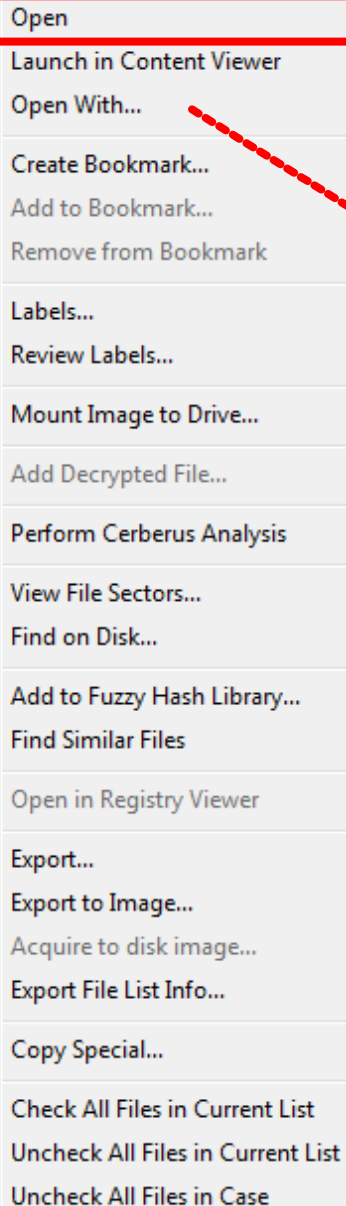


explorer



- Media Player

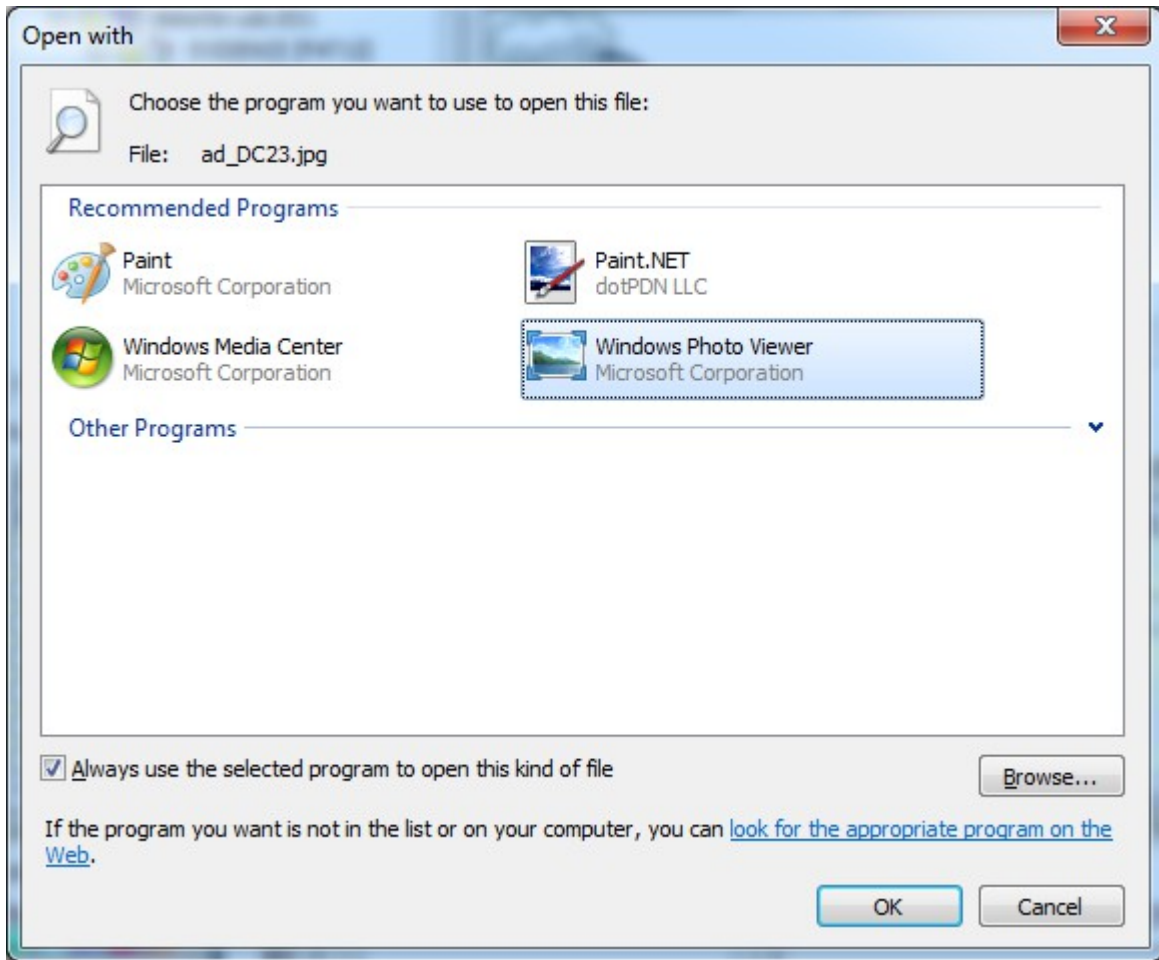
External Programs



A context menu for a file, with the 'Open' option highlighted by a red box. A red dashed arrow points from the 'Open With...' option to the 'Open with' dialog box on the right.

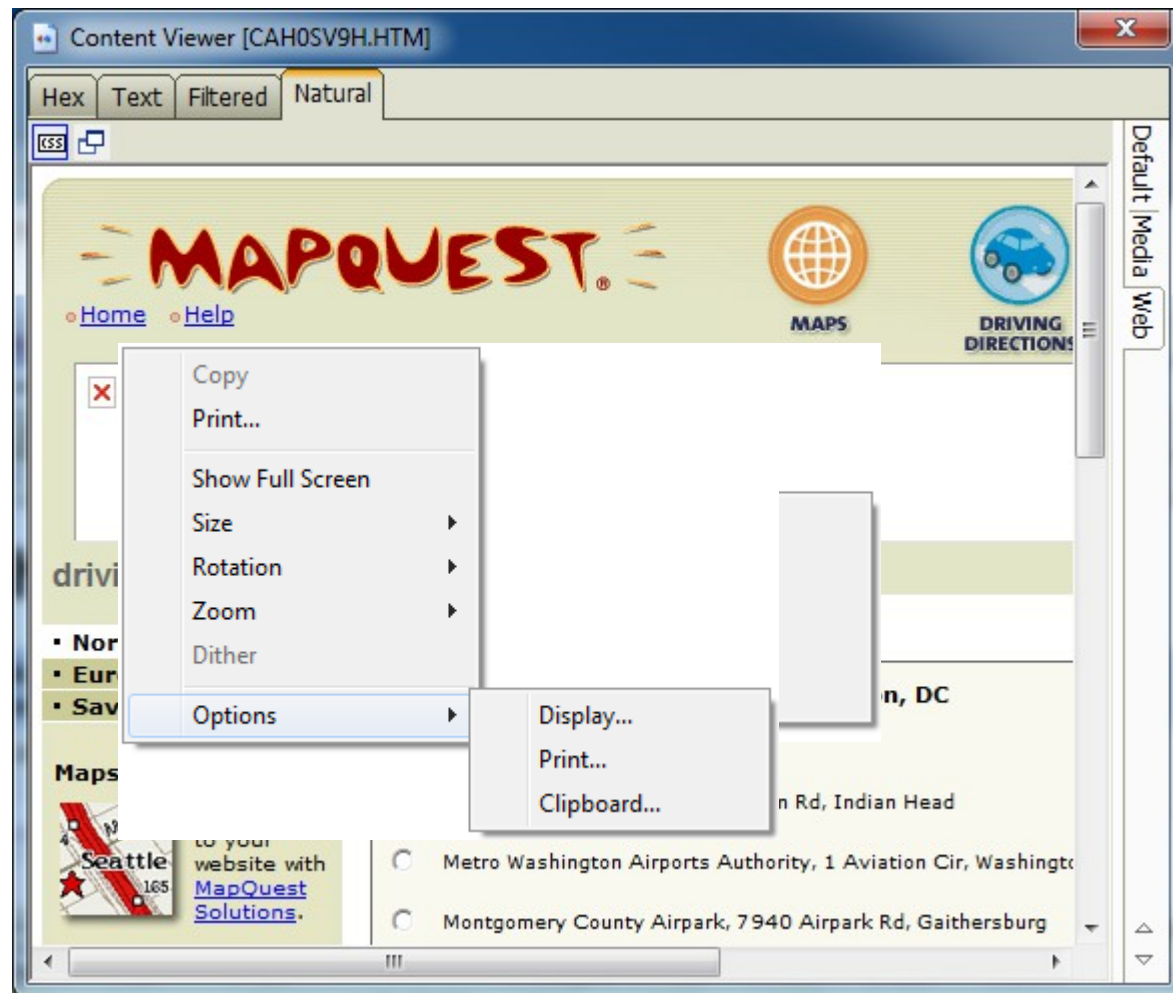
- Open
- Launch in Content Viewer
- Open With...
- Create Bookmark...
- Add to Bookmark...
- Remove from Bookmark
- Labels...
- Review Labels...
- Mount Image to Drive...
- Add Decrypted File...
- Perform Cerberus Analysis
- View File Sectors...
- Find on Disk...
- Add to Fuzzy Hash Library...
- Find Similar Files
- Open in Registry Viewer
- Export...
- Export to Image...
- Acquire to disk image...
- Export File List Info...
- Copy Special...
- Check All Files in Current List
- Uncheck All Files in Current List
- Uncheck All Files in Case

- Open or double-click directly opens the associated program
- Open With...



Detached Content Viewer

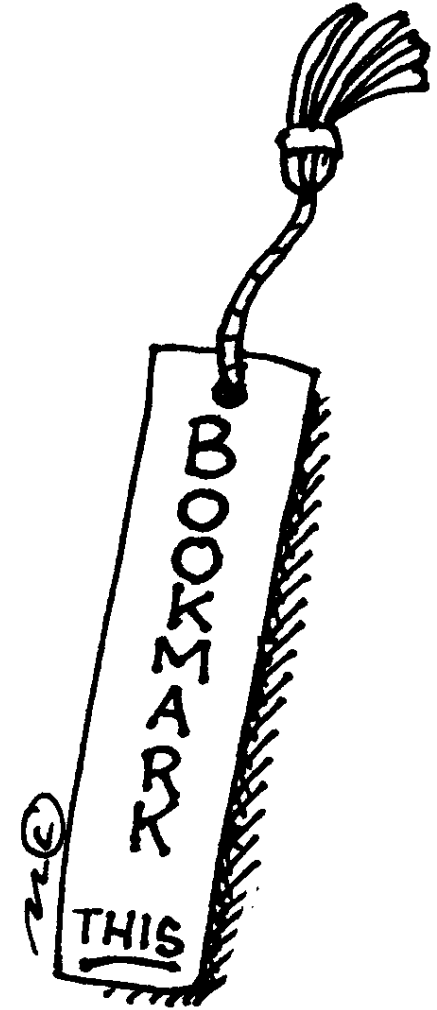
- Open
- Launch in Content Viewer
- Open With...
- Create Bookmark...
- Add to Bookmark...
- Remove from Bookmark
- Labels...
- Review Labels...
- Mount Image to Drive...
- Add Decrypted File...
- Perform Cerberus Analysis
- View File Sectors...
- Find on Disk...
- Add to Fuzzy Hash Library...
- Find Similar Files
- Open in Registry Viewer
- Export...
- Export to Image...
- Acquire to disk image...
- Export File List Info...
- Copy Special...
- Check All Files in Current List
- Uncheck All Files in Current List
- Uncheck All Files in Case



Marking Graphics

Two procedures:

- Check an Image
- Create a Bookmark
 - Works as usual



Checking Graphics

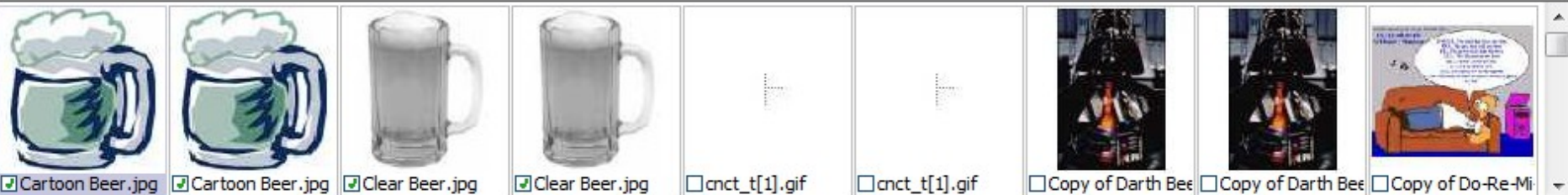
AccessData Forensic Toolkit Version: 4.0.0.35120 Database: localhost Case: lecture -Education-

File Edit View Evidence Filter Tools Manage Help

Filter: Actual Files Filter Manager...

Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile

Thumbnails



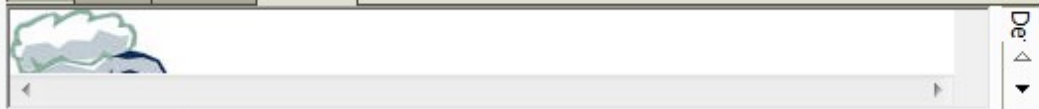
Loaded: 68 Filtered: 68 Total: 382 Highlighted: 1 Checked: 4 Total LSize: 678,0 KB Show Tooltip

Evidence Items

- Evidence
 - diskette-usb.E01
 - EVIDENCE [FAT12]
 - [root]
 - 10-1 Graphics
 - DT Search Stuff

File Content

Hex Text Filtered Natural



File Content Properties Hex Interpreter

File List

Normal Display Time Zone: W. Europe Daylight Time (From local)

☑	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created
☑	Cartoon Beer .jpg		1096	jpg	diskette-usb.E01/Partiti...	JPEG	3584 B	3325 B	E321B...	71A21...	16B9D...	2003-10-01
☑	Cartoon Beer .jpg		1218	jpg	diskette-usb.E01/EVIDE...	JPEG	3584 B	3325 B	E321B...	71A21...	16B9D...	2003-10-01
☑	Clear Beer .jpg		1097	jpg	diskette-usb.E01/Partiti...	JPEG	2048 B	1650 B	60774...	03A35...	C8183...	2003-10-01
☑	Clear Beer .jpg		1219	jpg	diskette-usb.E01/EVIDE...	JPEG	2048 B	1650 B	60774...	03A35...	C8183...	2003-10-01

Loaded: 68 Filtered: 68 Total: 382 Highlighted: 1 Checked: 4 Total LSize: 678,0 KB

diskette-usb.E01/Partition 4/EVIDENCE [FAT12]/[root]/10-1 Graphics/Cartoon Beer.jpg

Ready Graphics Tab Filter: Graphic Files

Change Checked Graphics

AccessData Forensic Toolkit Version: 4.0.0.35120 Database: localhost Case: lecture -Education-

File Edit View Evidence Filter Tools Manage Help

Filter: Actual Files Filter Manager...

Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile

Thumbnails

Loaded: 68 Filtered: 68 Total: 382 Highlighted: 1 Checked: 4 Total LSize: 678,0 KB Show Tooltip

Evidence Items

File List

File List

✓	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created
✓	Cartoon Beer .jpg		1096	jpg	diskette-usb.E01/Partiti...	JPEG	3584 B	3325 B	E321B...	71A21...	16B9D...	2003-10-01
✓	Cartoon Beer .jpg		1218	jpg	diskette-usb.E01/EVIDE...	JPEG	3584 B	3325 B	E321B...	71A21...	16B9D...	2003-10-01
✓	Clear Beer .jpg		1097	jpg	diskette-usb.E01/Partiti...	JPEG	2048 B	1650 B	60774...	03A35...	C8183...	2003-10-01
✓	Clear Beer .jpg		1219	jpg	diskette-usb.E01/EVIDE...	JPEG	2048 B	1650 B	60774...	03A35...	C8183...	2003-10-01

Loaded: 68 Filtered: 68 Total: 382 Highlighted: 1 Checked: 4 Total LSize: 678,0 KB

diskette-usb.E01/Partition 4/EVIDENCE [FAT12]/[root]/10-1 Graphics/Cartoon Beer.jpg

Ready Graphics Tab Filter: Graphic Files

Elements of an Email Case

Doing This

- Reading
- Sending
- Viewing
- Saving
- Renaming/Moving
- Web Mail

Might leave this

- Date and Time
- Status Flag
- User Folders
- Actual File
- Duplicate Files
- Copies in Drafts
- Cache/Swap file
- Link/History Files



Popular Applications

Application	Type of Email File
AOL®	Personal Filing Cabinet (.PFC)
Outlook®	.PST Files
Mozilla Thunderbird	.mbox (plain text file)
Eudora Mail	.mbx (effektivare variant av .mbox)
The Bat!	.MSB, .TBB, TBN
Outlook Express	.DBX like dBase?
Lotus Notes	.NSF
Windows (Vista/7) Mail	plain text .EML (email)
Other?	Cached or POP'ed Messages

- What about Web mail?
- The path to where the email actually is stored varies a lot between different programs and OS versions

Email Tab

AccessData Forensic Toolkit Version: 4.0.0.35120 Database: localhost Case: precious -Education-

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered - Filter Manager...

Explore Overview **Email** Graphics Bookmarks Live Search Index Search Volatile

Email Items

File List

	Subject	Name	To	From	CC	BCC	Submit ...	Deliver...	Unread	Unsent	Has Att...	Created
<input checked="" type="checkbox"/>	frodbaggi, ge...	1/2/2005 eBay...	baggif...	eBay@...			2005-0...	2005-0...	False		False	n/a
<input checked="" type="checkbox"/>	You want it, eB...	12/23/2004 eB...	baggif...	eBay@...			2004-1...	2004-1...	False		False	n/a
<input checked="" type="checkbox"/>	frodbaggi sen...	4/29/2005 bag...	samwiz...	baggif...			2005-0...	2005-0...	False		False	n/a
<input checked="" type="checkbox"/>	RE: HELP!	4/29/2005 jpar...	Baggif...	jparry...			2005-0...	2005-0...	False		False	n/a
<input checked="" type="checkbox"/>	RE: Southeast ...	4/29/2005 swa...	Baggif...	swater...			2005-0...	2005-0...	False		False	n/a

Loaded: 5 Filtered: 5 Total: 5 Highlighted: 0 Checked: 208 Total LSize: 61,15 KB

File Content

Hex Text Filtered Natural

From: swaters@accessdata.com
To: Baggifrodo@aol.com
Subject: RE: Southeast Cybercrime Summit
Sent: 4/29/2005 10:12:08 A.M. Mountain Standard Time
Sent: 2005-04-29 17:12:08 +00:00

I would highly recommend that you participate in the Southeast Cybercrime Summit. They have labs and lectures lead by

Email Attachments

4/29/2005 swaters@accessda RE: Southeast Cybercrime Summit

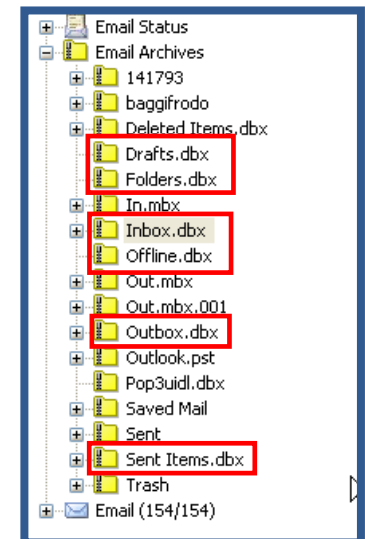
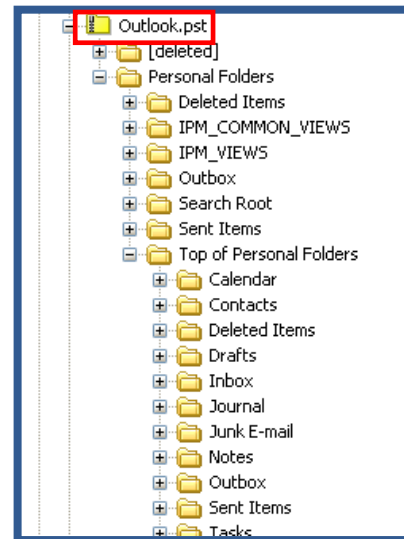
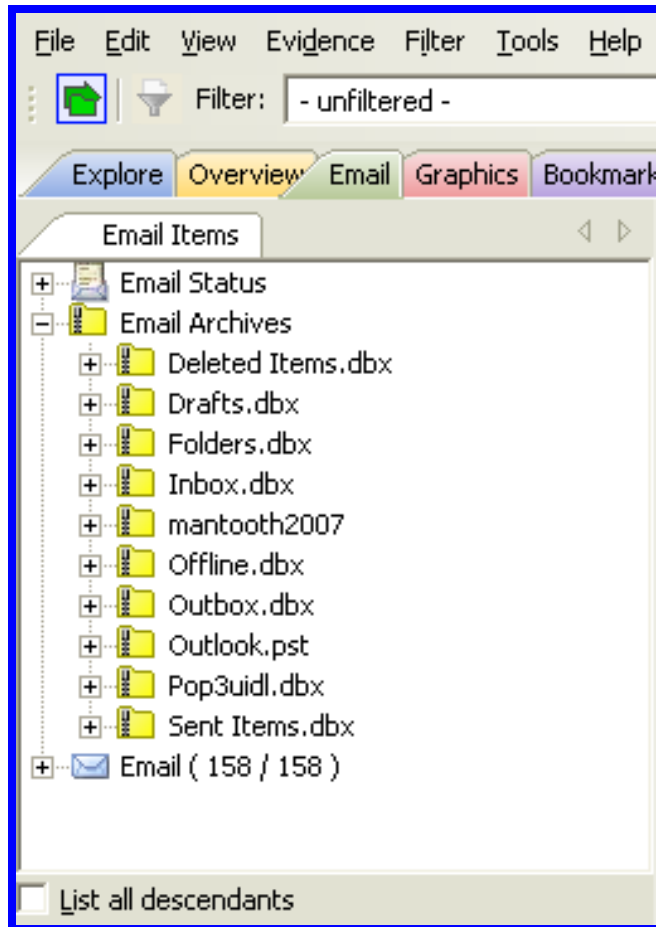
precious.E01/Partition 1/The Precious [NTFS]/[root]/Documents and Settings/All Users/.../baggifrodo»baggifrodo»Mail»IncomingSaved Mail»4-29-2005 swaters@accessda RE: Southeast Cybercrime Summit

Ready

Email Tab Filter: Email Files and Attachments

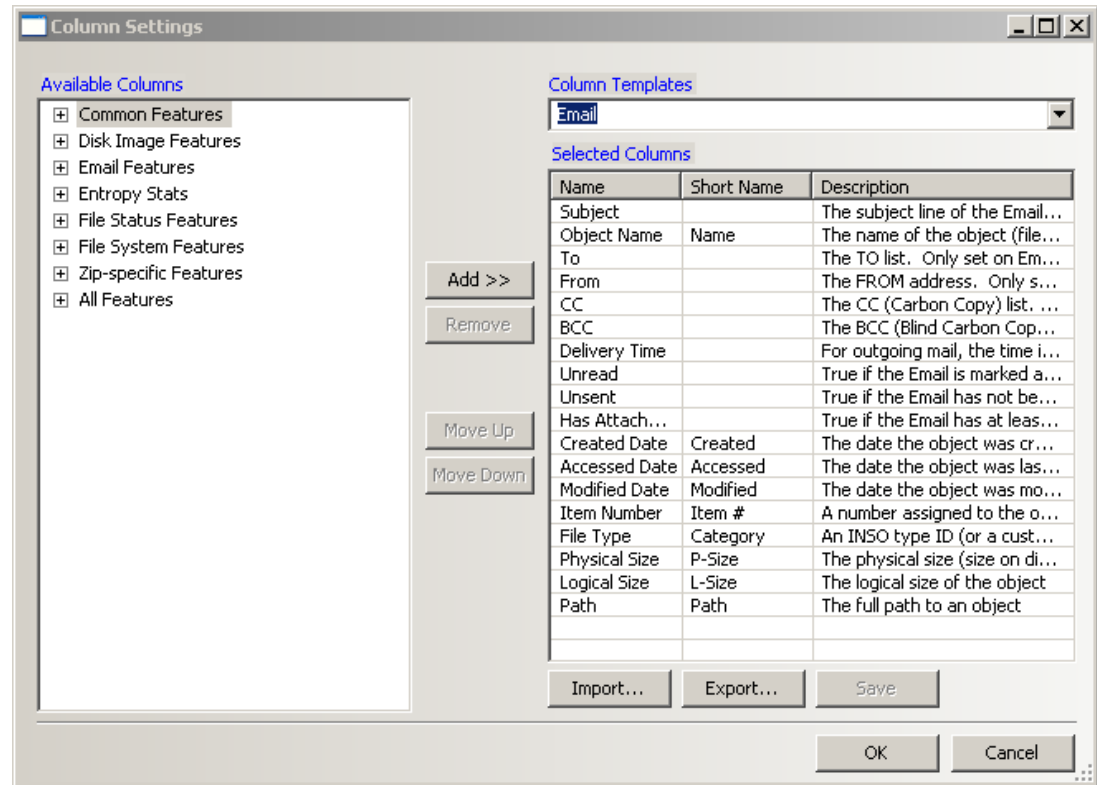
Email Container Formats

CONTAINER -VS- FLAT



Sorting Emails

- **Create Custom Column Settings**
- **Sort By Columns**



Sorting Emails

The screenshot shows a forensic email viewer interface. The main window displays a list of emails sorted by 'Delivery Time'. A red box highlights the 'Delivery Time' column, which shows dates and times in UTC. The selected email is 'RE: Whats up in D town?' from 'Wes Mantooth' to 'John Washer', sent on 6/21/2007 at 6:00:45 PM +00:00. The attachment 'Prescription2.gif' is visible in the 'Email Attachments' pane on the right. The interface includes a menu bar (File, Edit, View, Evidence, Filter, Tools, Help), a toolbar, and a navigation pane on the left showing the folder structure.

Subject	To	From	Delivery Time
Welcome to Mic...	New Outlook User	Outlook 2003 Team	6/20/2007 12:25:36 PM (2007-06-20 17:25:36 UTC)
Welcome to Mic...	New Outlook User	Outlook 2003 Team	6/20/2007 12:25:36 PM (2007-06-20 17:25:36 UTC)
Microsoft Office...	dollarhyde86@comcast.net	dollarhyde86@comcast.net	6/20/2007 12:50:35 PM (2007-06-20 17:50:35 UTC)
Microsoft Office...	dollarhyde86@comcast.net	dollarhyde86@comcast.net	6/20/2007 12:50:35 PM (2007-06-20 17:50:35 UTC)
Whats up in D t...	Mantooth	John Washer	6/20/2007 12:56:25 PM (2007-06-20 17:56:25 UTC)
Re: Whats up i...	Wes Mantooth	John Washer	6/20/2007 1:01:59 PM (2007-06-20 18:01:59 UTC)
Re: Whats up i...	Wes Mantooth	John Washer	6/20/2007 1:09:34 PM (2007-06-20 18:09:34 UTC)
Re: oooh I hav...	Mantooth2007@aol.com	washermeister@gmail.com	6/20/2007 1:16:10 PM (2007-06-20 18:16:10 UTC)
Re: oooh I hav...	Mantooth2007@aol.com	washermeister@gmail.com	6/20/2007 1:24:49 PM (2007-06-20 18:24:49 UTC)
Re: oooh I hav...	Mantooth2007@aol.com	washermeister@gmail.com	6/20/2007 1:24:49 PM (2007-06-20 18:24:49 UTC)
Re: oooh I hav...	Mantooth2007@aol.com	washermeister@gmail.com	6/20/2007 1:38:14 PM (2007-06-20 18:38:14 UTC)

RE: Whats up in D town?

From: Wes Mantooth
To: 'John Washer'
Subject: RE: Whats up in D town?
Sent: 6/21/2007 6:00:45 PM +00:00
Attachments: Prescription2.gif

File Content | Properties | Hex Interpreter

Ready | Email Tab Filter: Email Files _Attachments

Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/AppData/Local/Microsoft/Outlook/Outlook.pst/Personal Folders/Sent Items/RE: Whats up in D town?

Finding Email Text

The screenshot displays the Outlook 2007 interface. The 'File List' pane shows a search for 'Nigeria' with the following results:

Subject	To	From	Delivery Time
Here is mine	mantooth2007@aol.com	washermeister@gmail.com	6/20/2007 2:12:48 PM (2007-06-20 19:12:48 UTC)
Here is mine	mantooth2007@aol.com	washermeister@gmail.com	6/20/2007 2:12:48 PM (2007-06-20 19:12:48 UTC)
RE: Whats up i...	'John Washer'	Wes Mantooth	6/21/2007 1:00:00 PM (2007-06-21 18:00:00 UTC)
RE: Whats up			18:00:00 UTC
RE: Whats up			21:06:00 UTC
RE: Whats up			21:06:00 UTC
RE: Whats up			23:26:00 UTC
RE: Whats up			23:26:00 UTC
Letter			9:09:08 UTC

A 'Search' dialog box is open, showing the search term 'Nigeria' and the following options:

- Search Term: Nigeria
- Search For: Text, Hex
- Match Case:
- ANSI:
- Unicode:
- Regular Expression:
- Search Up:

The 'File Content' pane shows the email body text:

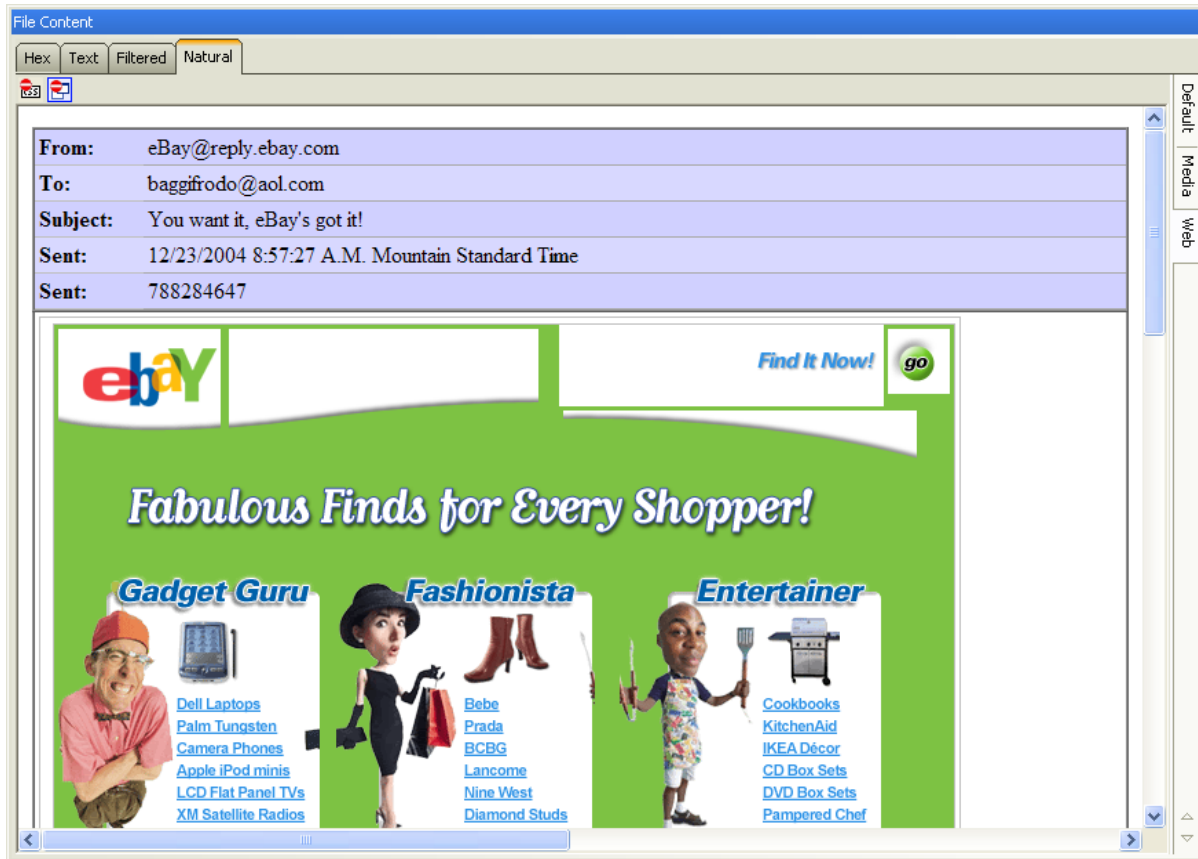
Lagos, Nigeria.
Attention: The President/CEO
Dear Sir,

Confidential Business Proposal

Having consulted with my colleagues and based on the information gathered from the Nigerian Chambers Of Commerce and Industry, I have the privilege to request your assistance to

A callout box with the text 'CTRL-F' has an arrow pointing to the search dialog box.

HTML Mail



Mail containers may contain HTML mail.

Use caution when connected to the Internet!

Bookmarking Emails

The screenshot displays a forensic email viewer interface. The main window is titled "Email Items" and shows a list of email folders on the left, including "Outlook.pst", "Pop3uidl.dbx", "Sent Items.dbx", and "Email (158 / 158)". The "Email" folder is expanded, showing a list of email items. The "File List" pane on the right shows a table of email items with columns for "Subject", "To", "From", and "Delivery Time". The first item is "Here is mine" from "washermeister@gmail.com" to "mantooth2007@aol.com", dated "6/20/2007 2:12:48 PM (2007-06-20 19:12:48 UTC)". A context menu is open over this item, with "Create Bookmark..." selected. The "File Content" pane at the bottom left shows the email's metadata: "From: washermeister@gmail.com", "To: mantooth2007@aol.com", "Subject: Here is mine", "Sent: 6/20/2007 1:12:48 P.M. Mountain Da", "Sent: 6/20/2007 7:12:48 PM +00:00", and "Attachment: 67chev.jpg". The "Email Attachments" pane at the bottom right shows the attachment "6/20/2007 washermeister@gm Here is mine".

File List

Subject	To	From	Delivery Time	
Here is mine	mantooth2007@aol.com	washermeister@gmail.com	6/20/2007 2:12:48 PM (2007-06-20 19:12:48 UTC)	6
Here is mine		washermeister@gmail.com	6/20/2007 2:12:48 PM (2007-06-20 19:12:48 UTC)	6
RE: WH		es Mantooth	6/21/2007 1:00:00 PM (2007-06-21 18:00:00 UTC)	R
RE: WH		es Mantooth	6/21/2007 1:00:00 PM (2007-06-21 18:00:00 UTC)	R
RE: WH		es Mantooth	6/21/2007 4:06:00 PM (2007-06-21 21:06:00 UTC)	R
RE: WH		es Mantooth	6/21/2007 4:06:00 PM (2007-06-21 21:06:00 UTC)	R
RE: WH		es Mantooth	6/21/2007 6:26:00 PM (2007-06-21 23:26:00 UTC)	R
RE: WH		es Mantooth	6/21/2007 6:26:00 PM (2007-06-21 23:26:00 UTC)	R
Letter		asco Badguy	8/1/2007 2:09:08 PM (2007-08-01 19:09:08 UTC)	L
oooh I			6/20/2017 4:16:07 PM (2017-06-20 21:16:07 UTC)	6
Re: ooo			6/20/2017 4:37:56 PM (2017-06-20 21:37:56 UTC)	6

Highlighted: 1 | Checked: 5

File Content

Hex | Text | Filtered | Natural

From: washermeister@gmail.com
To: mantooth2007@aol.com
Subject: Here is mine
Sent: 6/20/2007 1:12:48 P.M. Mountain Da
Sent: 6/20/2007 7:12:48 PM +00:00
Attachment: 67chev.jpg

Email Attachments

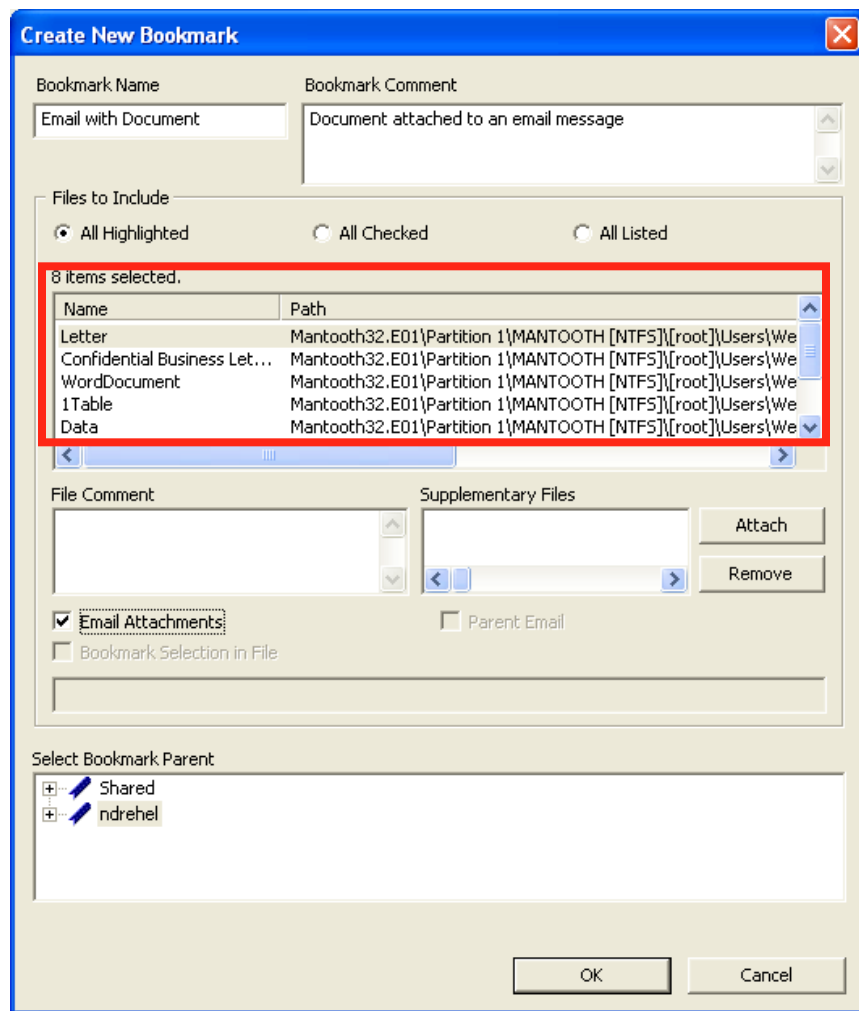
6/20/2007 washermeister@gm Here is mine

File Content | Properties | Hex Interpreter

Ready | Email Tab Filter: Email Files _Attachments

Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/ProgramData/AOL/C AOL 9.0a/organize/mantooth2007/mantooth2007/newmail/6/20/2007 washermeister@qm Here is mine

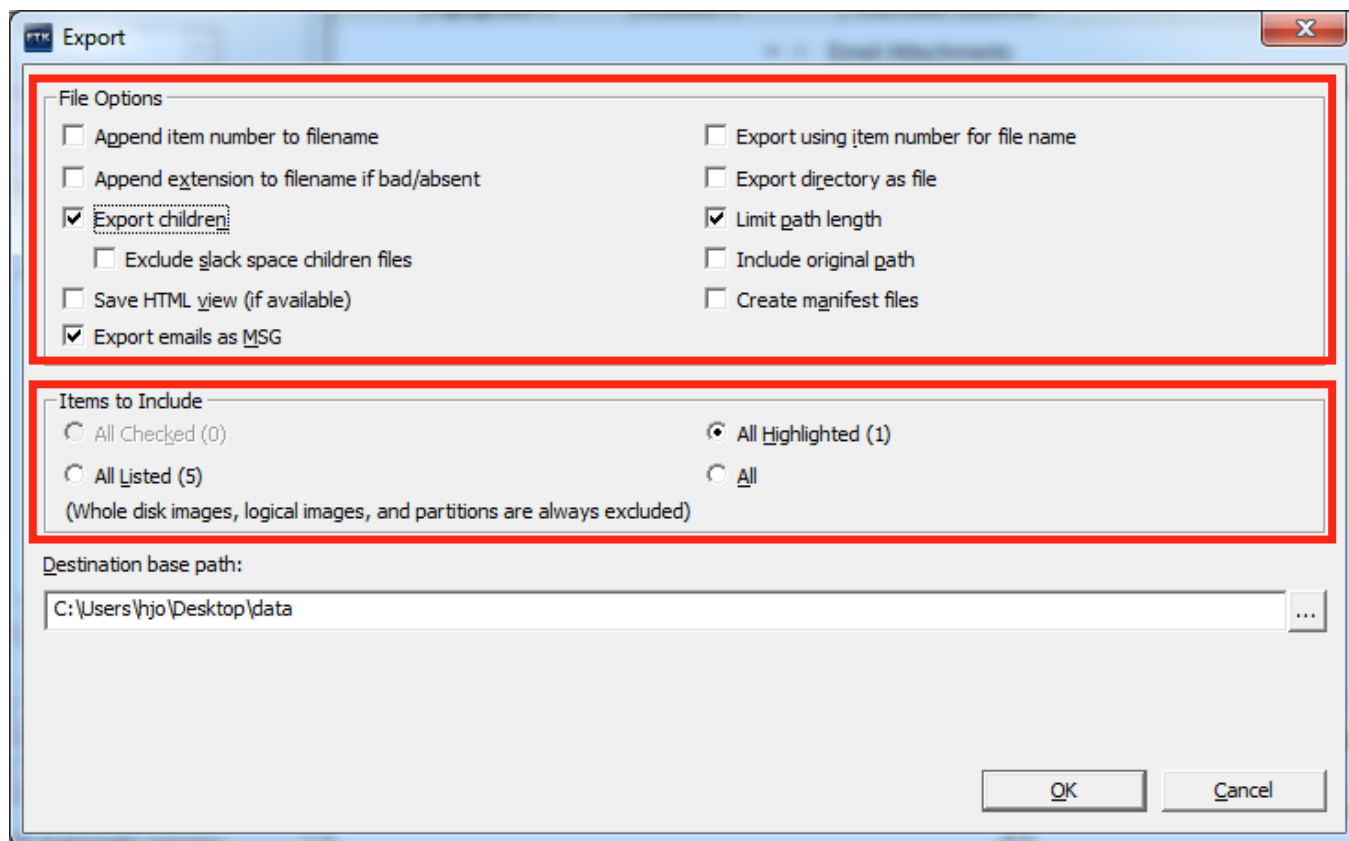
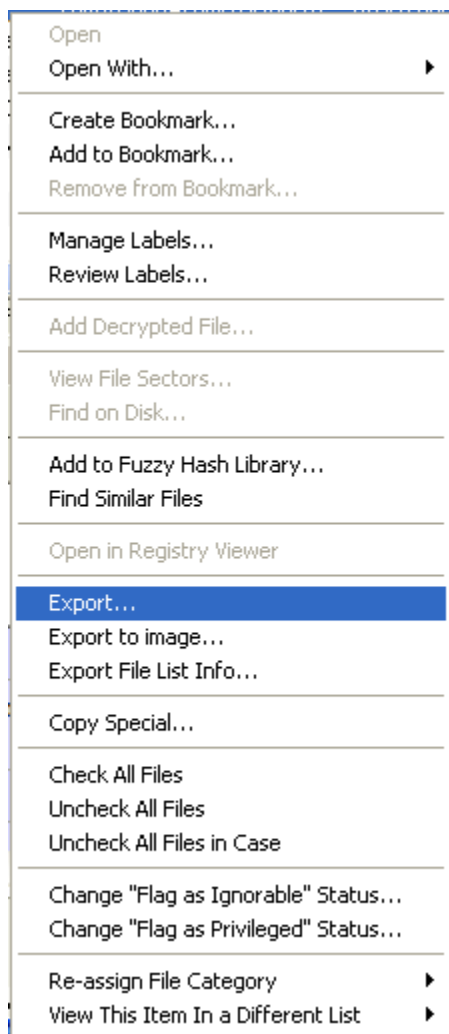
Bookmarking Emails



Options:

- **Email Attachments**
- **Parent Email**

Exporting Email Messages



Export email files into HTML or MSG format for broader compatibility (they look the way they should)