



**AccessData<sup>®</sup>**

Before a disk  
based investigation

Image and tools

Hashes

FTK Imager

# Data Storage Media

## Magnetic

- Floppy Disk
- Hard Drives
- Zip & Tape Drives



## Flash

- SSD, USB, SD/PC cards, etc.



## Optical

- CD
- DVD



## Alternative Media

- MP3 Players
- PDA's, Pagers & Phones
- Who Knows What ...



# Skydda integriteten av originaldata

- Vid forensiska utredningar måste originalets integritet bibehållas
  - Endast kopierat data att arbeta på
  - Processen måste kunna repeteras för att få användas i domstol
  - Multipla forensiska verktyg bör ge samma resultat
    - Ger en validering till resultatet
- Bit-Stream image (bit för bit kopiering) bör skapas, direkt vid en undersöknings start
  - Specialprogramvara för image bör användas
  - UNIX-verktyg är ofta inbyggt i de forensiska verktygen
- Bör användas med en hårdvaru eller mjukvaru skriv-blocker
  - Förhindrar att något ytterligare skrivs på disken

# Hårdvaru insamlingsverktyg



- NoWrite - <http://www.mykeytech.com>
- Forensic pc - <http://www.forensicpc.com>
- PC forensics - <http://www.pcforensics.com>
- Intelligent Computer Solutions (ICS) - <http://www.ics-iq.com>
- Digital Intelligence, FRED, Firefly - <http://www.digitalintelligence.com>
- Forensic computers - <http://www.forensic-computers.com/>
- Lista över tillverkare - [www.e-evidence.info/vendors.html](http://www.e-evidence.info/vendors.html)

# Bygga forensisk boot media

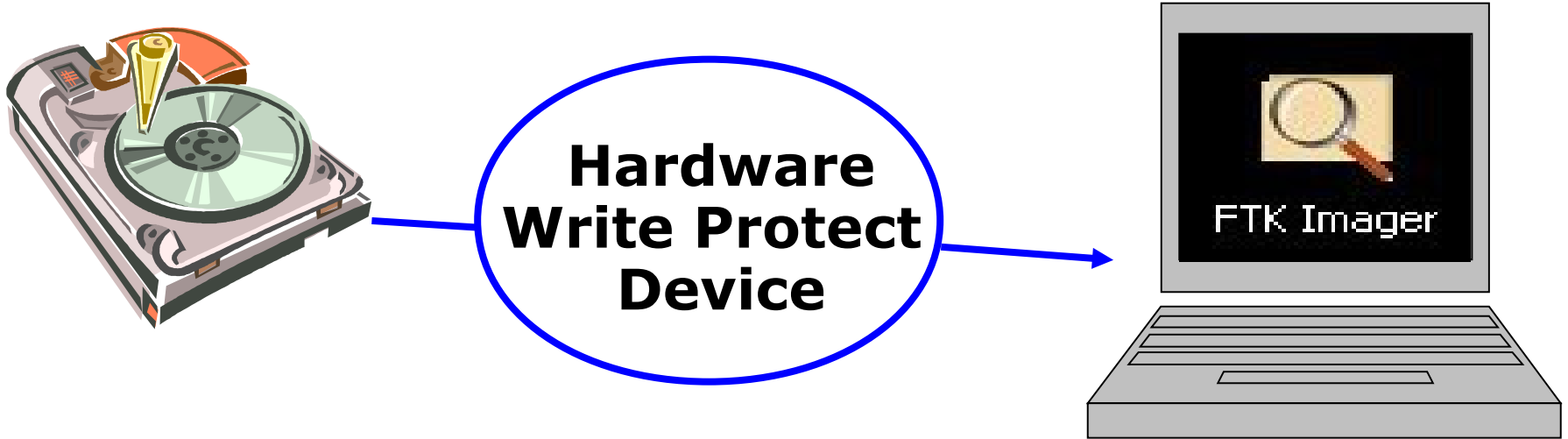
- Ett forensiskt boot-device bootar OS:et utan att accessa hårddisken
  - Floppy, USB-enhet, CD/DVD-ROM etc.
- Vid systemboot så accessas hårddisken vanligen och modifierar datum och tids-stämplor
  - Detta kan påverka undersökningen negativt!
  - Att fastställa när systemet sist var igång kan vara kritiskt
- Boot-mediat kan innehålla DOS/UNIX och Windows OS baserade verktyg
  - Hex editor, någon form av script miljö?
  - Sysinternals.com eller GNU/Linux driver för NTFS montering
  - Skriv-blockering i mjukvara
  - Image mjukvara (dd, FTK Imager, ...)
  - Nätverksmöjlighet, CD/DVD, USB drivrutiner
  - Se till att alla referenser (sökvägar etc. pekar på ditt boot-media)!

# Forensiska verktyg & boot disk

- Det är "vanligen" bäst att boota på ett media som har ett kommersiellt forensiskt verktyg
- Flera open-source live media verktyg finns
  - Linux/UNIX Live – montera media som RO (Read Only)
  - Helix, BackTrack, DEFT, ORION osv.
- Windows Forensic Environment (WinFE builds on WinPE)
  - <http://winfe.wordpress.com/>
- Vissa Windows verktyg kan köras från en bootbar WinPE (Windows Preinstalled Environment) eller BartPE (Bart's Preinstalled Environment) Live CD/Live USB
  - Används vanligen för att rädda filer eller lösenord från en korrupt installation
  - BartPE är freeware och tillåter obegränsat med plugins
  - Se länkar och resurser -> <http://en.wikipedia.org/wiki/BartPE>
  - Bra artikel: <http://www.forensicfocus.com/windows-forensic-environment-boot-cd>



# Skapa Bit-stream image



- DOS - diskcopy
  - a:\>diskcopy [drive1] [drive2] /V
- Linux – dd (disk dumper?), forensiska varianter finns
  - [http://en.wikipedia.org/wiki/Dd\\_\(Unix\)](http://en.wikipedia.org/wiki/Dd_(Unix))
  - dd if=/dev/floppy of=/evidence/floppyImage.dat
  - Parametrar: bs=4096 conv=noerror count=1

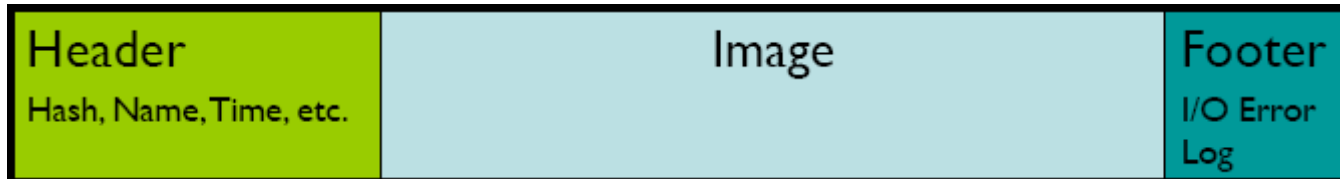
# Mjukvaru insamlingsverktyg och deras native image filformat

- FTK Imager – [www.accessdata.com](http://www.accessdata.com) raw dd, .e01
- Expert Witness Format (EWF), Encase – [www.guidancesoftware.com](http://www.guidancesoftware.com), .e01
- Raw dd (Linux/Unix dd)
- Drivespy - [www.digitalintelligence.com](http://www.digitalintelligence.com), .img
- SMART – [www.linux-forensics.com](http://www.linux-forensics.com) och [www.asrdata.com](http://www.asrdata.com), .s01
- Winimage – [www.winimage.com](http://www.winimage.com), ett antal format
- Symantec Ghost (med forensiska switchar), .gho
- ICS - <http://www.ics-iq.com>
- SafeBack – [www.forensics-intl.com](http://www.forensics-intl.com)
- SnapBack - [www.snapback.com](http://www.snapback.com)
- Advanced Forensic Format (AFF) - [www.afflib.org](http://www.afflib.org)
- Technology Pathways Prodiscover - [www.techpathways.com](http://www.techpathways.com), .pd
- Flera verktyg stöder bin/cue, ISO, NRG, MDS osv. filer



# Image-format

- Format som har extra info, tex. EWF



- Unix/Linux dd (raw) format

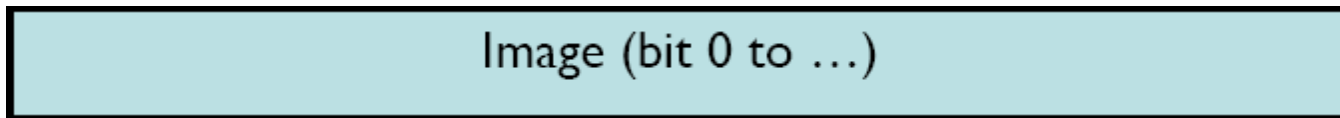
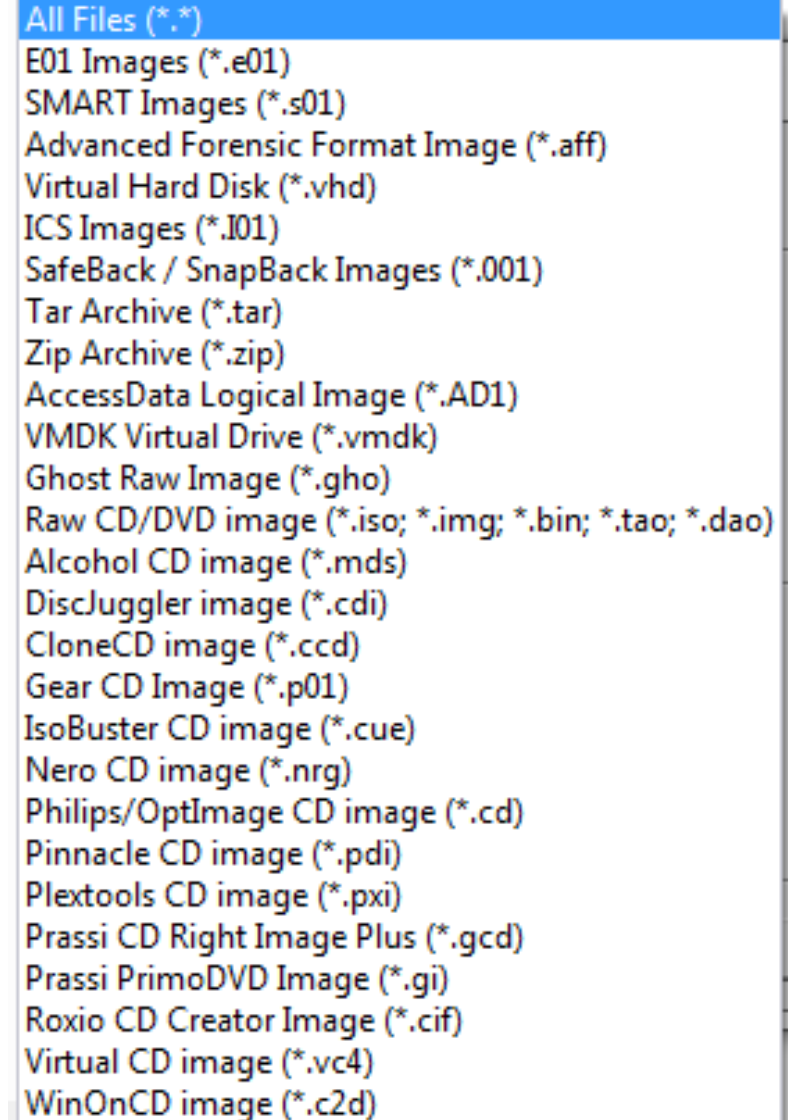
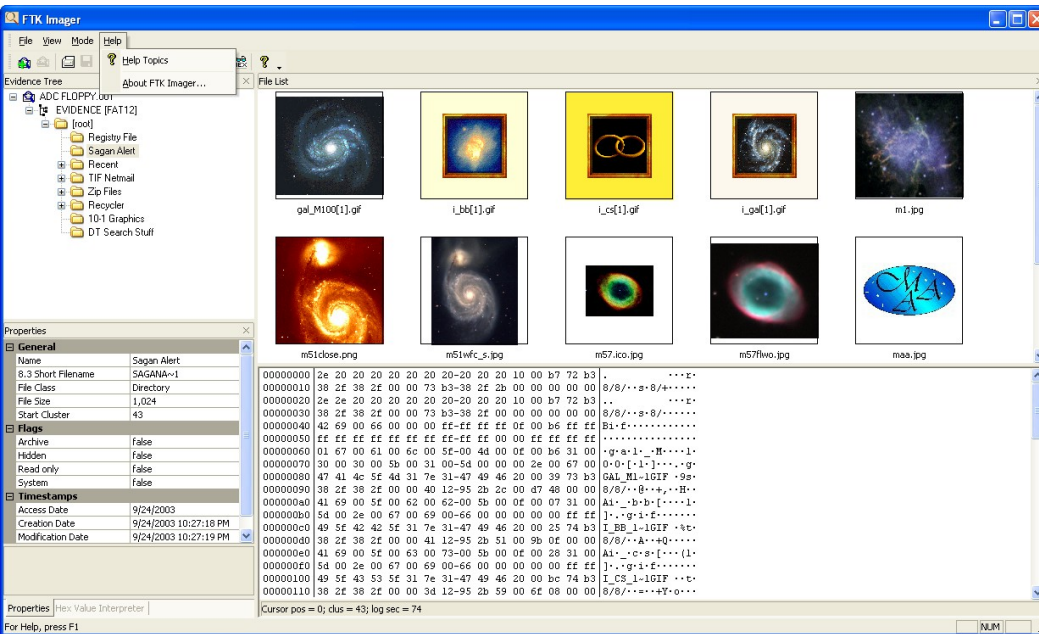


Table 2. Summary of features supported by various file formats.

	Extensible	Non-Proprietary	Compressed & Seekable
AFF	•	•	•
EnCase			•
ILook	?		•
ProDiscover		•	•
PyFlag		•	•
RAID		•	
SafeBack	?		?
SDi32		•	
SMART		•	

Källa:  
afflib.org

# FTK Imager image-format



- FTK imager kan skapa
  - Raw dd
  - SMART
  - Encase .e01
- FTK imager läser

# FTK Filsystem Support

FTK Imager 3.x stödjer följande filsystem:

- DVD (UDF)
  - CD (ISO / Joliet / CDFS)
  - FAT (12 / 16 / 32)
  - EXT (2 / 3 / 4)
  - NTFS (och NTFS Compressed)
  - HFS/HFS+/HFSX (Server Version)
  - ReiserFS 3
  - ExFAT (Extended File Allocation Table or FAT64)
  - VxFS (called JFS and OnlineJFS in HP-UX)
- 
- Kom ihåg! Det viktiga är att kunna göra en exakt spegelkopia av ALLT!
    - Filer
    - Rå (meta) data – MFT (Master File Table), FAT, MBR osv.
    - Raderade filer
    - Ej allokerad diskyta och slack space

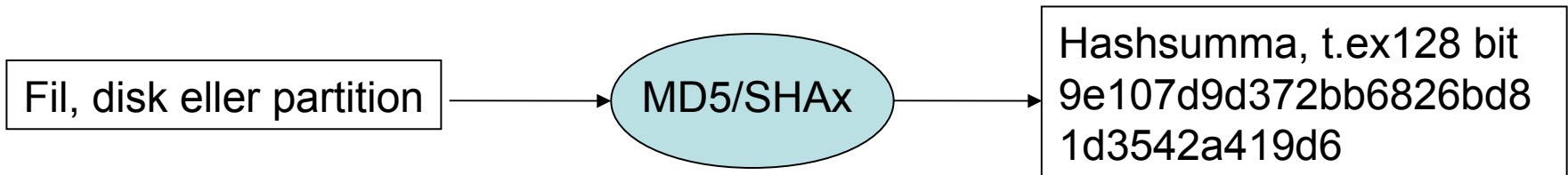
# Mer om image

- Tillverkning av image bör ske i forensiskt lab
- Om operationen är "hemlig" så kan det ske live "on-site" via floppy, USB, CD/DVD etc.
  - Överförs till extern hårddisk via nätverk eller USB/firewire gränssnitt
  - Samla in RAM vid "live" undersökning samt datorns status – nätverk, processer etc. (IR)
- Image-verktyg bör verifiera att en riktig kopia gjorts
  - Hash: ett tal som kan garantera inget ändrats och att kopian unikt kan identifieras
  - Görs "on the fly" av de flesta verktygen



# Mer om image - hashar

- Använd MD5 (16 byte) eller SHAx (Secure Hash Algorithm, SHA1 20 byte) hash-algoritmerna
  - Hårddiskar, partitioner, filer etc.
- Kallas för envägsfunktion (OWF) eller message digest (MD)
  - Genererar ett unikt tal - 128 bitar eller 160 bitar långt oberoende av input,  $2^{128}$  eller  $2^{160}$  kombinationer...
  - Kan även ses som en förbättrad checksumma (CRC)



# Access Data Known File Filter (KFF)

**Kallas även för "Known Good File"**

**KFF är ett databasverktyg som jämför  
kända filers hash-värden mot ditt cases  
filer**

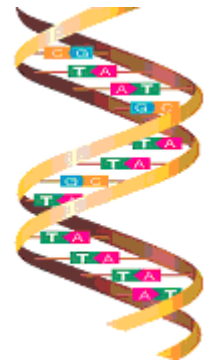
**Genom att använda KFF under analysen:  
(efter en image tagits)**

- Kan man direkt identifiera och ignorera omkring 40-70% av de kända godartade filerna som ej tillför något till utredningen
- Kan man direkt identifiera kända filer som är brottsliga eller på annat bör vara med i utredningen
- Kom ihåg: hashen är baserad på data/innehållet i filen, ej namn eller suffix etc.



# Andra hash databaser

- NDIC (National Drug Intelligence Center)
  - HashKeeper – Limited availability
  - Gratis, men man måste ansöka om tillstånd
- NIST (National Institute of Standards and Technology)
  - National Software Reference Library (NSRL) Reference Data Set (RDS)
  - \$90 annual subscription (quarterly releases)
  - <http://www.nist.gov/srd/dblist.htm>
- Ovanstående databaser tillåter att man extraherar hashar till en egen DB



# Mer om Image – dokumentation och förvaring

- Dokumentera
  - När, var, hur, verktyg etc.
- Verktyg för för dokumentationen
  - Logga in bevis, journal för notering, bandspelare
- Att förvara media fysiskt säkert bibehåller ”chain of custody”
  - Bra lås, brandsäkert, EMI (ElectroMagnetic Interference), åtkomstlista etc.
  - Digitala bevis är vanligen känsligare än andra bevis – kan lätt modifieras!



# Mer om Image – återställningsverktyg

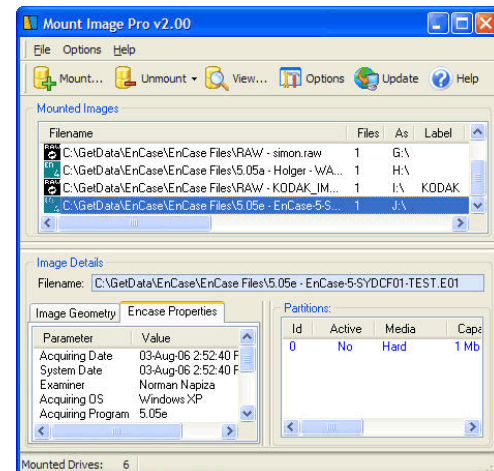
- Din forensiska verktygslåda bör innehålla några dataåterställningsverktyg
  - Är oftast inbyggda i proffsverktygen
  - Använder man andra verktyg måste man förvissa sig om att de fungerar med filsystemet
- Filer som raderats i NTFS behöver specialverktyg på grund av komplexiteten
  - Hitta klusters sekvensnummer
  - Manuellt försöka sätta samman fragmenterade filer
  - Ogiltiga eller borttappade pekare till data
- Exempel på verktyg som återställer filer som raderats ifrån Recycle Bin via tex. WinFE/WinPE/BartPE miljöer
  - GetDataBack – Runtime Software
  - EasyRecovery – Ontrack Data Recovery
  - NTFS Undelete, File-Rescue Plus, NTFS Data Recovery, etc.
- **Windows Vista/7 Shadow Copy, VSS (Volume Snapshot/Shadow Copy Service)** – ShadowExplorer - <http://www.shadowexplorer.com/>

# Mer om Image – återställningsverktyg

- Diskar som drabbats av fysiska fel
  - Byt kabel, kontrollkort (drivelektronik), kortplats, dator, BIOS inställning, drivrutin etc.
  - ”klick döden”, ”bad sectors” på fel ställen, ej bootbara etc. kan ofta det mesta räddas ifrån
    - Disken måste kunna hittas av BIOS
    - Bootsektorn måste vara relativt intakt (diskbeskrivningen)
- Knoppix, Helix, DEFT, BackTrack etc.
  - dd, dd\_rescue, ddrescue
    - dd bs=512 if=/dev/hdxx of=/dir/foo.dd conv=noerror, sync
    - conv=noerror, sync - ignore errors & continue, padda med '0'
    - Kan också skrivas direkt till ny disk
- Disktillverkares utility
  - PowerMax, Drive Fitness Tool, SeaTools etc.

# Mer om Image – montera image

- Linux - montera dd on loopback device
  - [http://wiki.edseek.com/guide:mount\\_loopback](http://wiki.edseek.com/guide:mount_loopback)
- Mount EWF (E01) on Linux (FUSE)
  - <http://stephenventer.blogspot.com/2009/02/mount-ewf-e01-on-linux.html>
- Windows
  - Paraben P2 eXplorer - <http://www.paraben.com/programs/p2x.html>
  - Mount Image Pro - [www.mountimage.com](http://www.mountimage.com) (dd, EWF, SMART, AFF, VMDK, ...)
  - Filedisk - <http://branten.se/nt/> (raw, img etc.)
  - Göra en VMware .vmdk fil och köra i VMware
    - Technology Pathways - ProDiscover Basic: Tools -> Image Conversion -> VMware
    - LiveView - [liveview.sourceforge.net](http://liveview.sourceforge.net)
  - Montera en .vmdk fil
    - VDK och VDKwin - <http://vmxbuilder.com/>
- Fördelar med att kunna montera
  - Man kan undersöka disken som den ser ut "enligt OS"
  - Man kan undersöka disken med olika verktyg
    - Antivirus och anti root-kit program etc.
    - Andra diverse verktyg som används tex. vid live undersökningar, script etc.



# FTK Imager Interface

The screenshot displays the AccessData FTK Imager application window. The interface is divided into several key sections:

- Menu Bar:** Located at the top, containing 'File', 'View', 'Mode', and 'Help' menus.
- Toolbar:** A row of icons below the menu bar for file operations like Open, Save, and Print.
- Evidence Tree View:** A tree structure on the left showing the file system hierarchy, including folders like 'Desktop', 'Documents', and 'Checks'. The 'Checks' folder is expanded to show 'scan1.jpg'.
- File List:** A table on the right showing a list of files with columns for Name, Size, Type, and Date Modified. The file 'scan1.jpg' is selected.
- Properties / Hex Value Interpreter:** A panel at the bottom left showing detailed file properties for 'scan1.jpg', such as Name, File Class, File Size, and Date Modified.
- Viewer:** A large window at the bottom right displaying a scanned image of a cashier's check from the State Bank of Kimball. The check is for \$8,000.00, dated 08/03/2004, and signed by Mary Kraus.
- Status Bar:** Located at the very bottom, showing the current file path and disk information.

Labels with arrows point to these components: Menu Bar, Toolbar, Evidence Tree View, Properties / Hex Value Interpreter, Status Bar, File List, and Viewer.

# News in FTK Imager 3.x

The screenshot displays the AccessData FTK Imager 3.0.0.1443 application window. The 'File' menu is open, and three items are highlighted with red boxes: 'Image Mounting...', 'Capture Memory...', and 'Detect EFS Encryption'. The 'File List' pane on the right shows a directory structure with files and folders, including 'Docs', 'Pics', 'ARP.EXE', 'FTP.EXE', 'loveletter.virus', 'ouchy.dat', and 'snoof.gz'. The bottom status bar shows the cursor position and log sector information.

AccessData FTK Imager 3.0.0.1443

File View Mode Help

- 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...**
- MetaCarve (Deep Scan)
- Obtain Protected Files...
- Detect EFS Encryption**
- Export Files...
- Export File Hash List...
- Export Directory Listing...
- Exit

File List

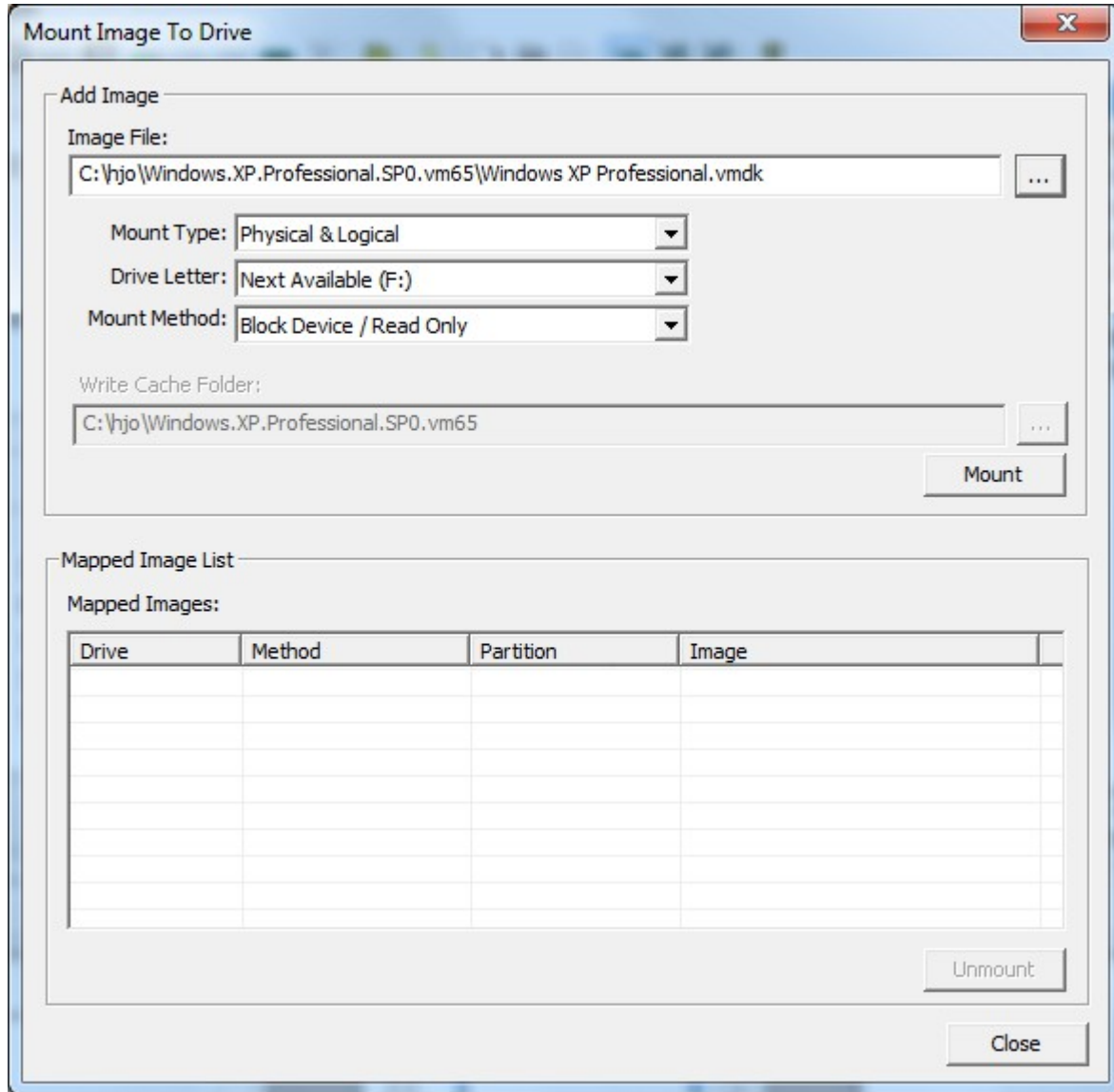
Name	Size	Type	Date Modified
Docs	1 KB	Directory	2000-09-23 15:21:08
Pics	1 KB	Directory	2000-09-23 15:21:16
ARP.EXE	20 KB	Regular File	1996-08-24 11:11:10
FTP.EXE	37 KB	Regular File	1996-08-24 11:11:10
loveletter.virus	16 KB	Regular File	2000-09-21 07:46:24
ouchy.dat	21 KB	Regular File	2000-03-19 19:00:52
snoof.gz	13 KB	Regular File	2000-08-02 07:43:38

0000 41 44 00 6F 00 63 00 73-00 00 00 0F 00 60 FF FF AD-o-c-s-...-yy  
0010 FF FF FF FF FF FF FF FF FF-FF FF 00 00 FF FF FF FF yyyyyyyyyy-yy

Cursor pos = 0; log sec = 19

For User Guide, press F1

# News in FTK Imager 3.x



- All Files (\*.\*)
- E01 Images (\*.e01)
- SMART Images (\*.s01)
- Advanced Forensic Format Image (\*.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)

# Interpreters

The screenshot displays the AccessData FTK Imager interface. The 'Evidence Tree' on the left shows a directory structure for 'Wes Mantooth', including 'AppData', 'Local', 'Microsoft', and 'Windows'. The 'File List' pane on the right shows files like 'index.dat' (80 KB). A 'Hex Value Interpreter' window is open, showing a table of hex values and their corresponding ASCII interpretations. A red box highlights the 'Hex Value Interpreter' window, and a red dashed arrow points to the hex value '01' in the 'Value' column of the table.

Type	Size	Value
signed integer	1-8	128,287,556,571,820,000
unsigned integer	1-8	128,287,556,571,820,000
FILETIME (UTC)	8	7/12/2007 11:14:17 PM
FILETIME (local)	8	7/12/2007 6:14:17 PM
DOS date	2	-
DOS time	2	-
time_t (UTC)	4	-
time_t (local)	4	-

Hex Value Interpreter

Address	Hex	ASCII
053320	ef be ad de ef be ad de ef be ad de ef be ad de	ix~Pik~Pik~Pik~P
053330	ef be ad de ef be ad de ef be ad de ef be ad de	ix~Pik~Pik~Pik~P
053340	ef be ad de ef be ad de ef be ad de ef be ad de	ix~Pik~Pik~Pik~P
053350	ef be ad de ef be ad de ef be ad de ef be ad de	ix~Pik~Pik~Pik~P
053360	ef be ad de ef be ad de ef be ad de ef be ad de	ix~Pik~Pik~Pik~P
053370	ef be ad de ef be ad de ef be ad de ef be ad de	ix~Pik~Pik~Pik~P
053380	55 52 4c 20 02 00 00 00 e0 ef 90 5e da c4 c7 01	URL .....ai^UAC
053390	e0 ef 90 5e da c4 c7 01 07 37 c9 b9 00 00 00 00	ai^UAC...7E^.....
0533a0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0533b0	60 00 00 00 68 00 00 00 fe 00 10 10 00 00 00 00	`...h...p.....
0533c0	01 00 20 00 a8 00 00 00 14 00 00 00 00 00 00 00	.. ..
0533d0	ec 36 c9 b9 01 00 00 00 00 00 00 00 00 00 00 00	i6E^.....
0533e0	00 00 00 00 ef be ad de 56 69 73 69 74 65 64 3a	....ix~Pvisited:
0533f0	20 57 65 73 20 4d 61 6e 74 6f 6f 74 68 40 66 69	_Wes Mantooth@fi
054000	6c 65 3a 2f 2f 2f 45 3a 2f 42 75 73 69 6e 65 73	le:///E:/Busines
054100	73 25 32 30 49 64 65 61 73 2f 75 6e 74 69 74 6c	s%20Ideas/untitl
054200	65 64 2e 62 6d 70 00 de 10 00 02 00 00 00 00 10	ed.bmp~P.....
054300	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....ix~P
054400	ef be ad de ef be ad de ef be ad de ef be ad de	ix~Pik~Pik~Pik~P
054500	ef be ad de ef be ad de ef be ad de ef be ad de	ix~Pik~Pik~Pik~P
054600	ef be ad de ef be ad de ef be ad de ef be ad de	ix~Pik~Pik~Pik~P
054700	ef be ad de ef be ad de ef be ad de ef be ad de	ix~Pik~Pik~Pik~P
054800	55 52 4c 20 02 00 00 00 a0 d2 5f 74 da c4 c7 01	URL ....._tUAC

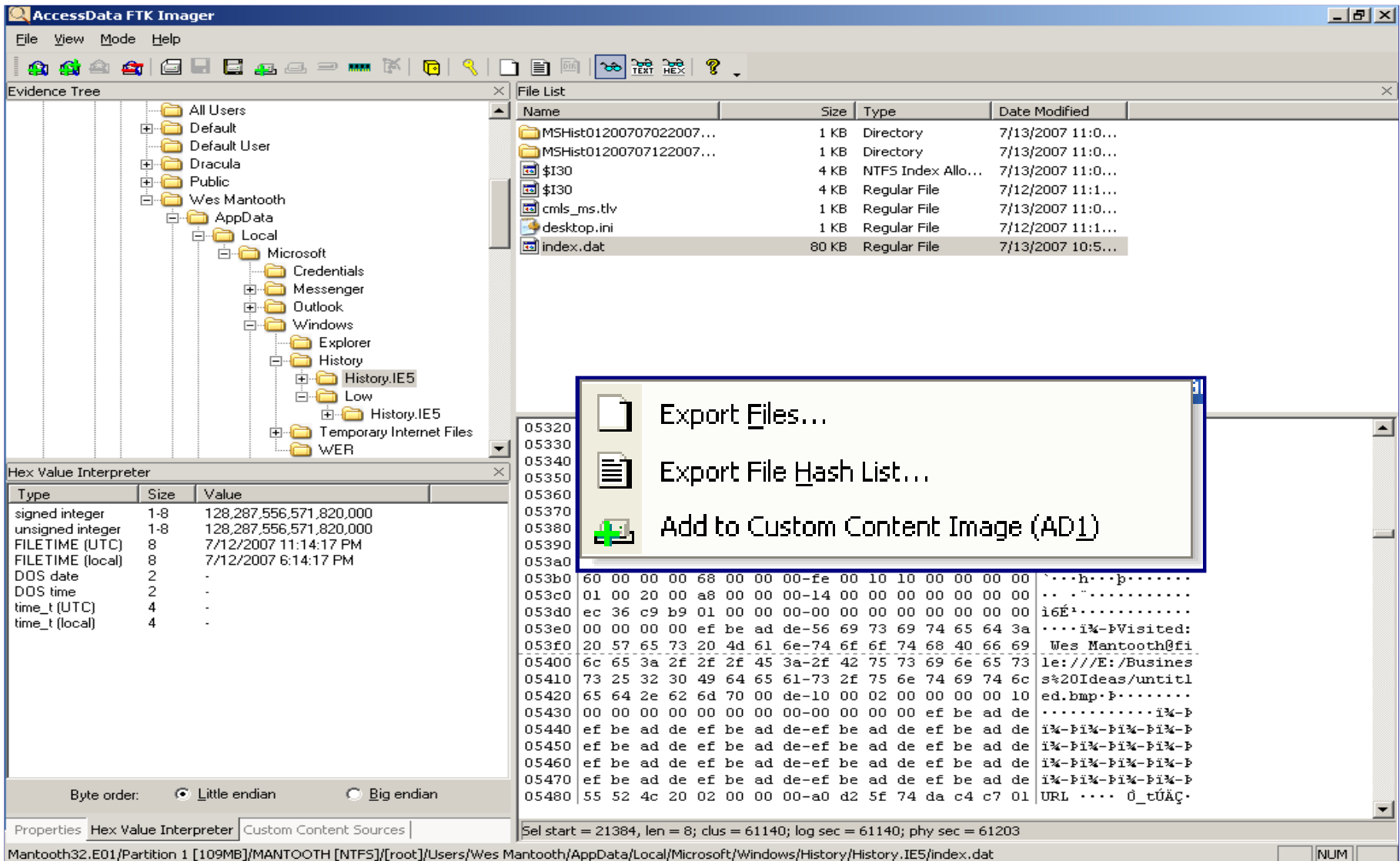
Byte order:  Little endian  Big endian

Properties Hex Value Interpreter Custom Content Sources

Sel start = 21384, len = 8; clus = 61140; log sec = 61140; phy sec = 61203

Mantooth32.E01/Partition 1 [109MB]/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/AppData/Local/Microsoft/Windows/History/History.IE5/index.dat

# Right Click Menu Options





# Drive Freespace

När FTK Imager hittar en kontinuerlig “klump” med ledig diskryta (unallocated space) så namnger den och identifierar ytan med det kluster den börjar med

Nedan kan vi se en 262140 KB klump som börjar på kluster 3 och en annan 2624 KB klump som börjar på kluster 65790 osv.

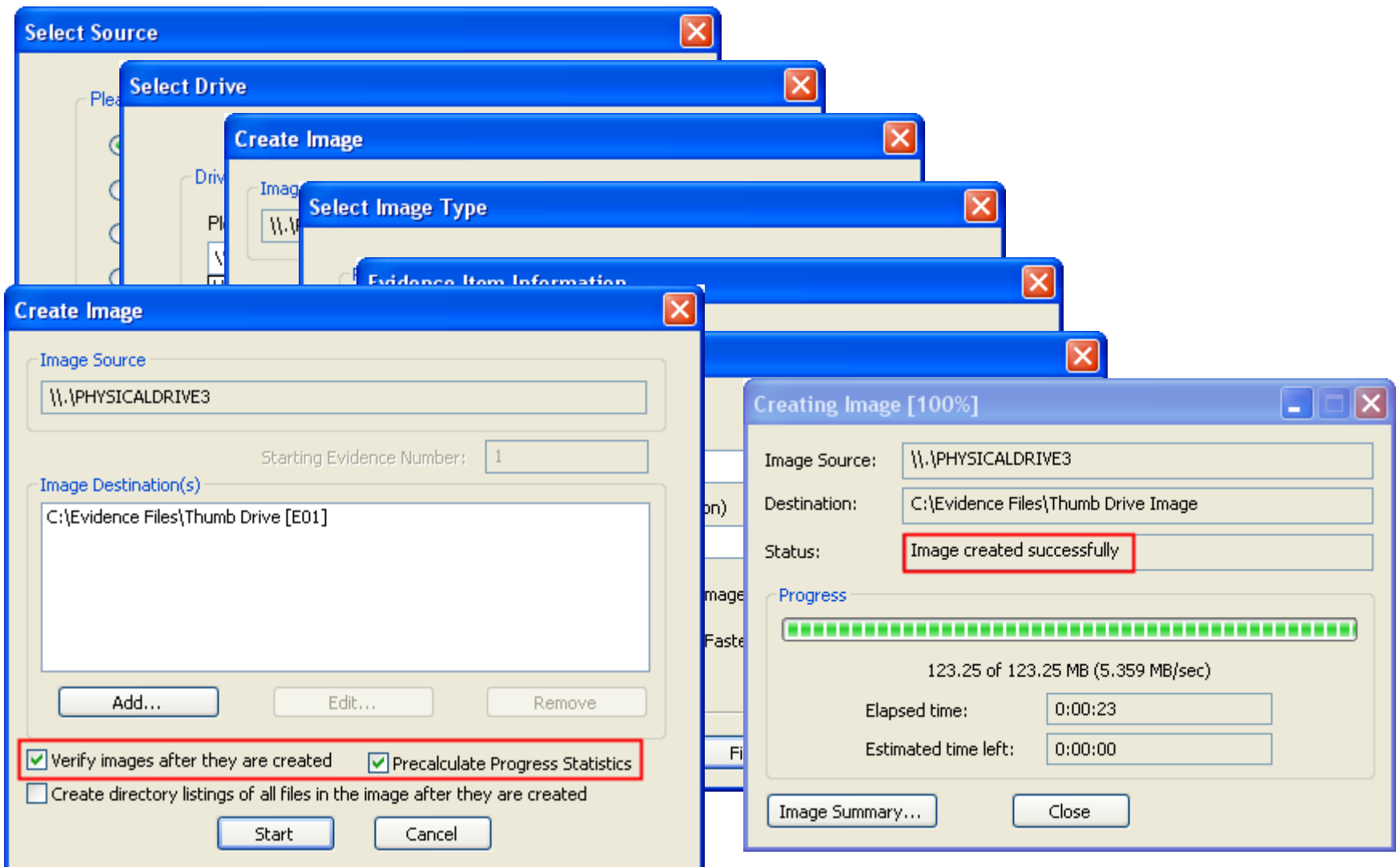
The screenshot shows the FTK Imager interface with the following components:

- Evidence Tree:** Shows a hierarchy for 'MESSIER IMAGE.E01' containing 'Partition 1 [4996MB]' (FAT32), 'Partition 2 [996MB]', and 'Partition 5 [996MB]'. Under 'Partition 1', there is a '[root]' folder and an 'unallocated space' folder.
- File List:** A table listing unallocated space clusters. The first entry is highlighted:

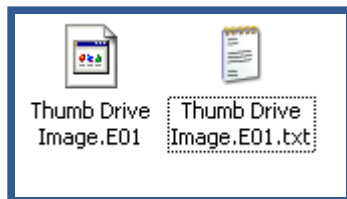
Name	Size	Type	Date Modified
0000003	262,140 KB	Unallocated space	
0066790	2,624 KB	Unallocated space	
0066459	32 KB	Unallocated space	
0066575	64 KB	Unallocated space	
0073147	36 KB	Unallocated space	
0073335	32 KB	Unallocated space	
0073347	4 KB	Unallocated space	
0073349	4 KB	Unallocated space	
0073394	32 KB	Unallocated space	

Below the file list is a hex view showing a continuous sequence of '00' bytes, indicating unallocated space. The status bar at the bottom indicates 'Cursor pos = 0; clus = 3; log sec = 19988; phy sec = 20051'.

# Acquisition



# Acquisition



```
Thumb Drive Image.E01.txt - Notepad
File Edit Format View Help
Created By AccessData® FTK® Imager 2.5.3.14 071018

Case Information:
Case Number: 07-12345
Evidence Number: AD-54321
Unique Description: Trek Thumb Drive
Examiner: R. Maddox
Notes: From Desk Drawer

-----

Information for C:\Evidence Files\Thumb Drive Image:

Physical Evidentiary Item (Source) Information:
[Drive Geometry]
Cylinders: 15
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 252,416
[Physical Drive Information]
Drive Model: TREK TD2SMART G3M USB Device
Drive Interface Type: USB
Source data size: 123 MB
Sector count: 252416
[Computed Hashes]
MD5 checksum: c3f3494f1c9fa5d255e7fd8aa823a708
SHA1 checksum: 19c11c0f359393c56f9ee26302637799bda796e8

Image Information:
Acquisition started: Wed Jan 09 15:31:37 2008
Acquisition finished: Wed Jan 09 15:32:01 2008
Segment list:
C:\Evidence Files\Thumb Drive Image.E01

Image Verification Results:
Verification started: Wed Jan 09 15:32:01 2008
Verification finished: Wed Jan 09 15:32:03 2008
MD5 checksum: c3f3494f1c9fa5d255e7fd8aa823a708 : verified
SHA1 checksum: 19c11c0f359393c56f9ee26302637799bda796e8 : verified
```

# Conversion – Image and Image

The screenshot displays the AccessData FTK Imager interface. The 'Evidence Tree' on the left shows a drive with a 'FAMIL' folder. A context menu is open over the drive, with 'Export Disk Image...' selected. The 'File List' pane is empty. The main hex view shows data starting at address 00000000. The hex values are: eb 58 90 4d 53 44 4f 53-35 2e 30 00 02 02 26 00. The corresponding ASCII characters are: èX·MSDOS5.0...ã·. The 'Hex Value Interpreter' window is open, showing a table of data types and their sizes.

Type	Size	Value
signed integer	1-8	
unsigned integer	1-8	
FILETIME (UTC)	8	
FILETIME (local)	8	
DOS date	2	
DOS time	2	
time_t (UTC)	4	
time_t (local)	4	

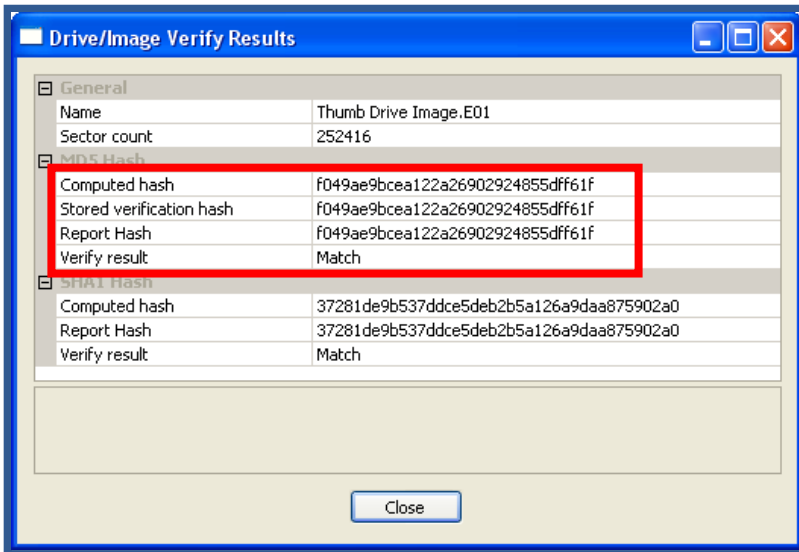
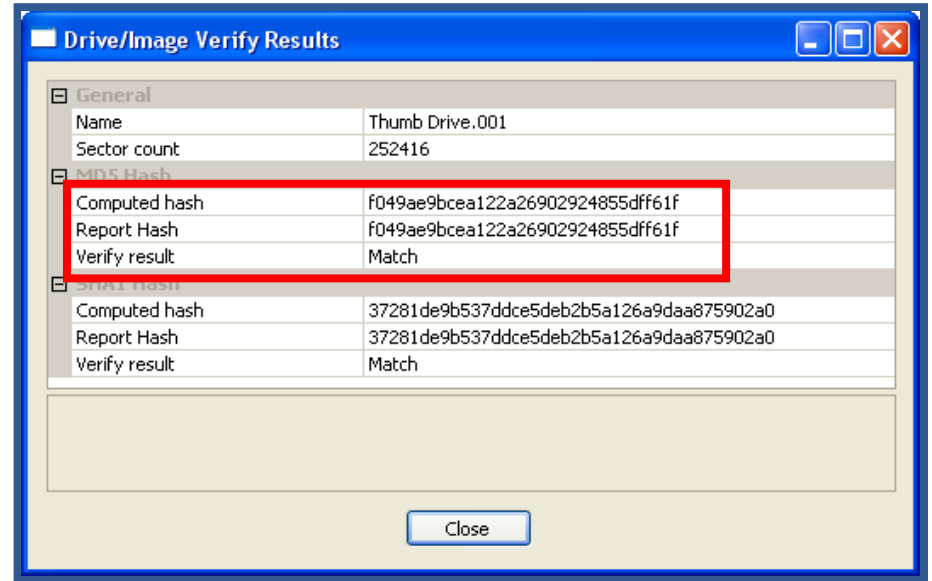
Byte order:  Little endian  Big endian

Cursor pos = 0; log sec = 0

Exports a forensic image of the selected drive or partition

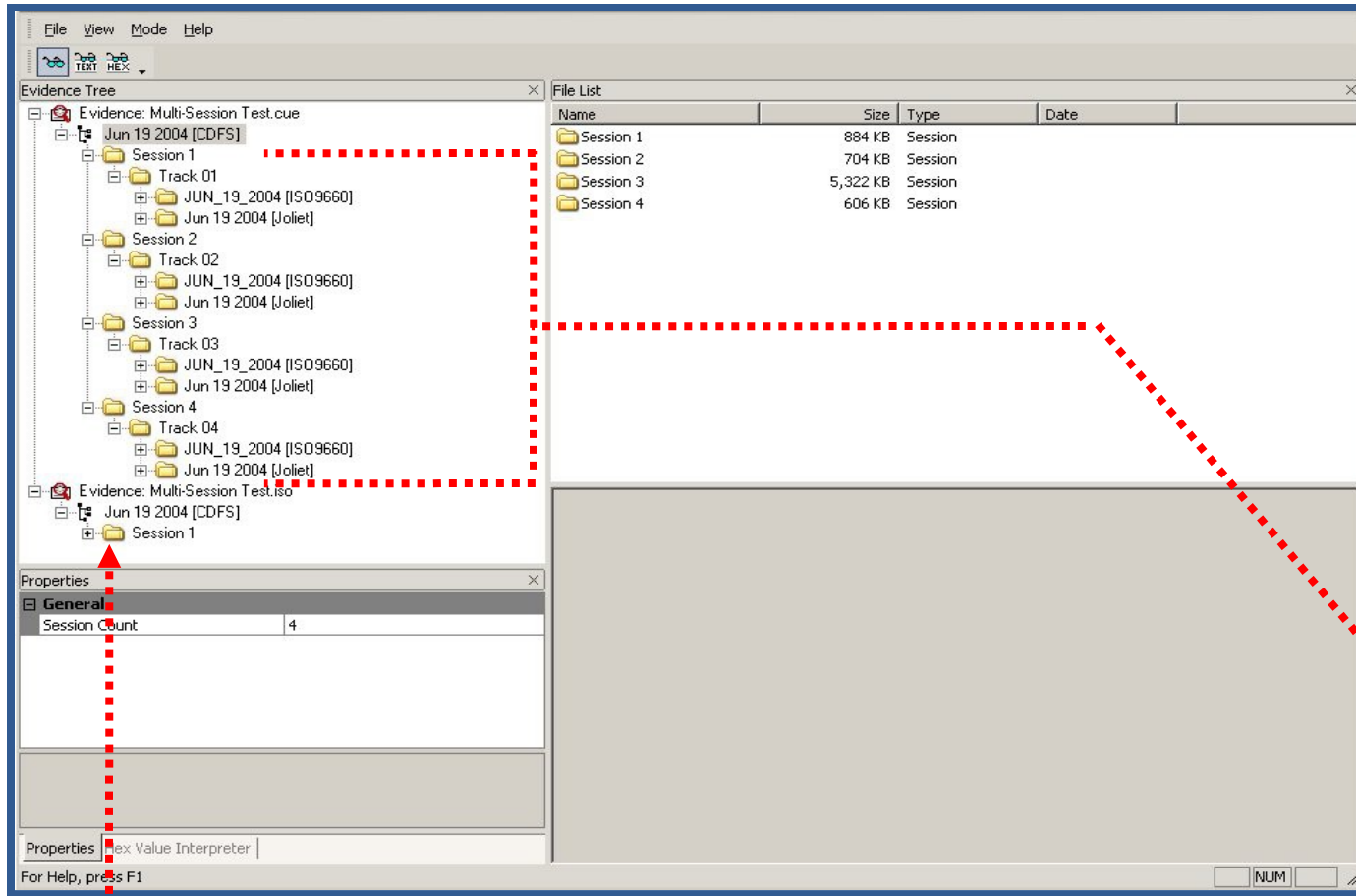
# Verification

**Encase / DD ??**



**Verified based on image format**

# CD / DVD Images



**.CUE files**  
**.ISO files**



**Use the .CUE file to map sessions**

