AccessData®

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



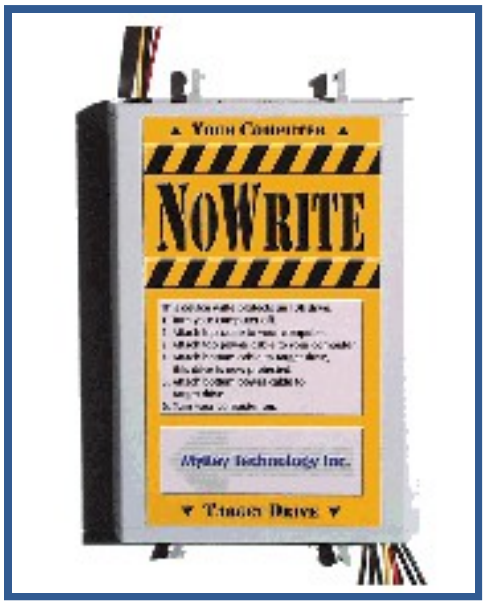
Alternative Media

- 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

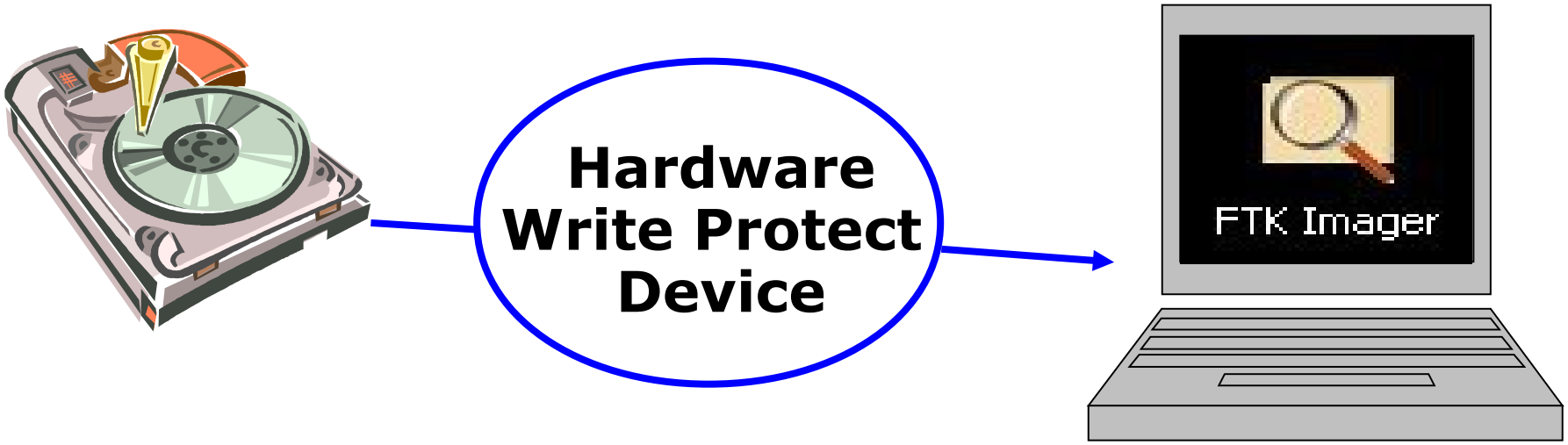
Bygga forensisk boot media

- 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-stämplar
  - 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 Enviroment) eller BartPE (Bart’s Preinstalled Enviroment) 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



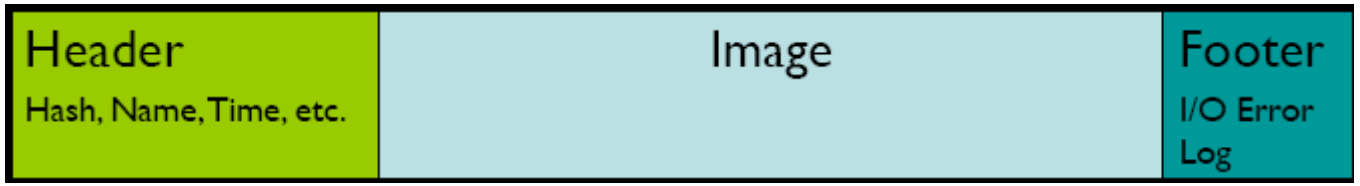
- DOS - diskcopy
  - a:\>diskcopy [drive1] [drive2] /V
- Linux – dd (disk dumper?), forensiska varianter finns
  - http://en.wikipedia.org/wiki/Dd_(Unix)
  - dd if=/dev/floppy of=/evidence/floppyImage.dat
  - Parametrar: bs=4096 conv=noerror count=1

Mjukvaru insamlingsverktyg och deras native image filformat

- FTK Imager – www.accessdata.com raw dd,.e01
- Expert Witness Format (EWF), Encase – www.guidancesoftware.com, .e01
- Raw dd (Linux/Unix dd)
- Drivespy - www.digitalintelligence.com, .img
- SMART – www.linux-forensics.com och www.asrdata.com, .s01
- Winimage – www.winimage.com, ett antal format
- Symantec Ghost (med forensiska switchar), .gho
- ICS - http://www.ics-iq.com
- SafeBack – www.forensics-intl.com
- SnapBack - www.snapback.com
- Advanced Forensic Format (AFF) - www.afflib.org
- Technology Pathways Prodiscover - 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

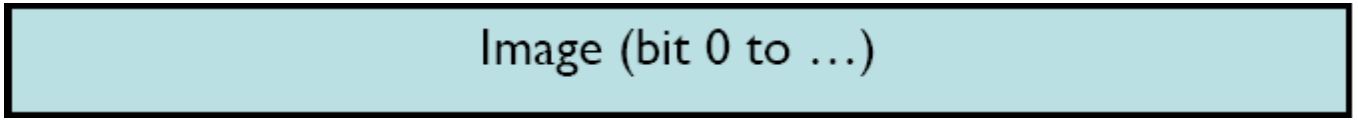
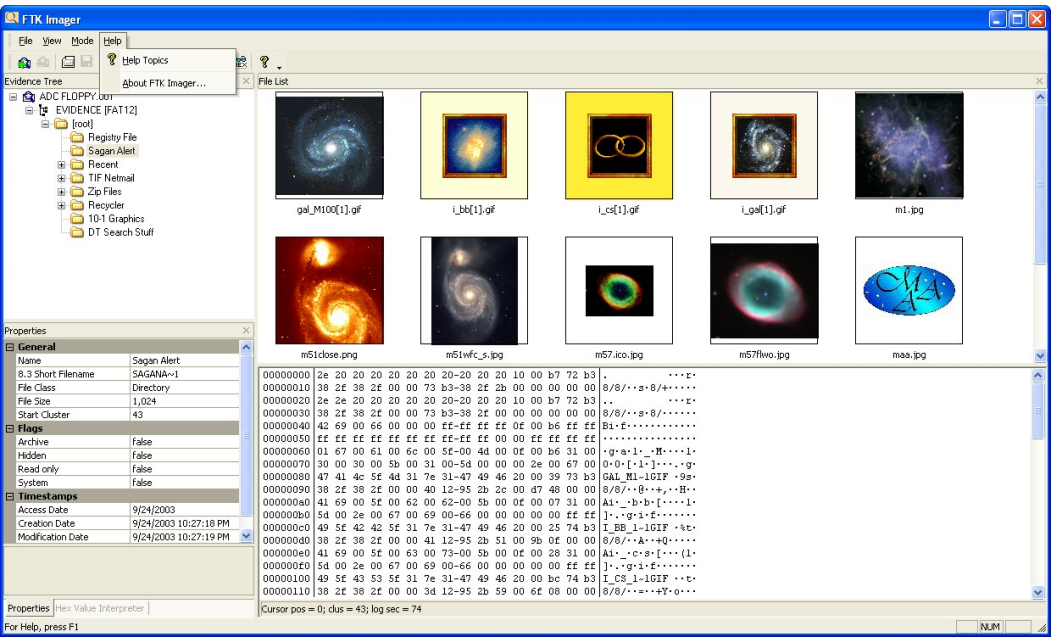


Table 2. Summary of features supported by various file formats.

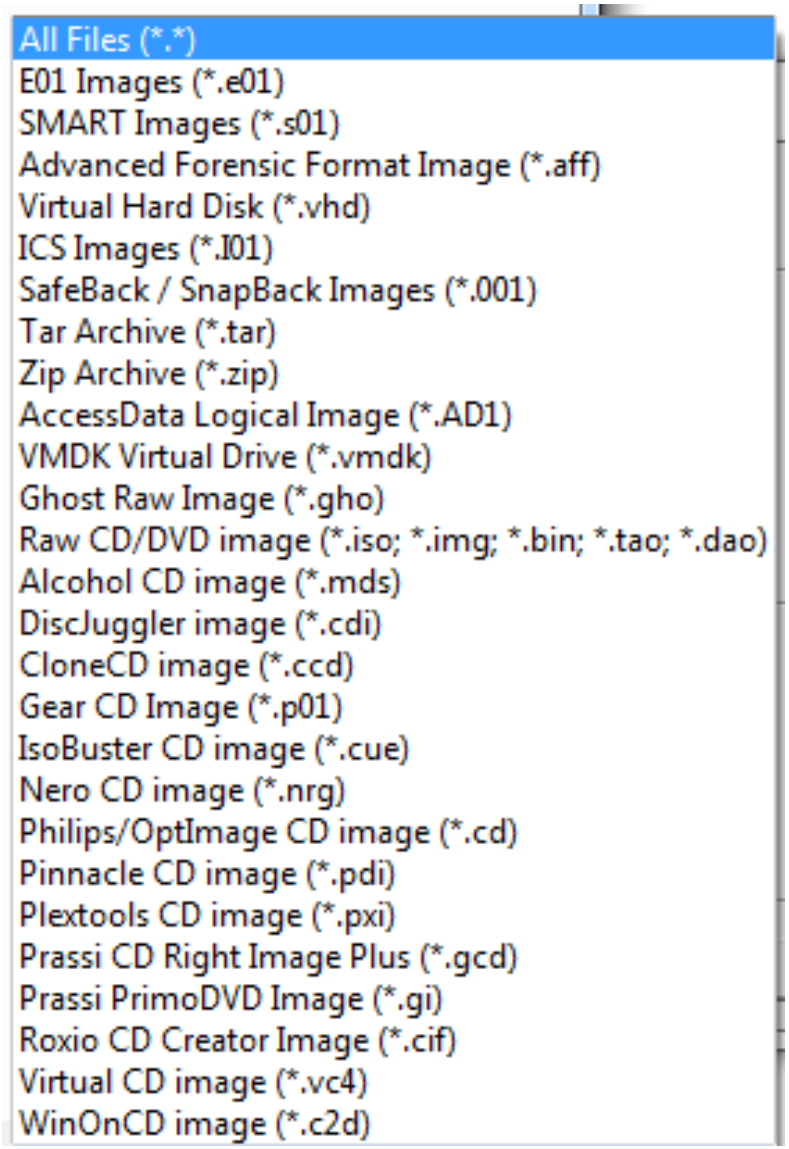
	Extensible	Non-Proprietary	Compressed & Seekable
AFF	•	•	•
EnCase			•
ILook	?		•
ProDiscover		•	•
PyFlag		•	•
RAID		•	
SafeBack	?		?
SDi32		•	
SMART		•	

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)

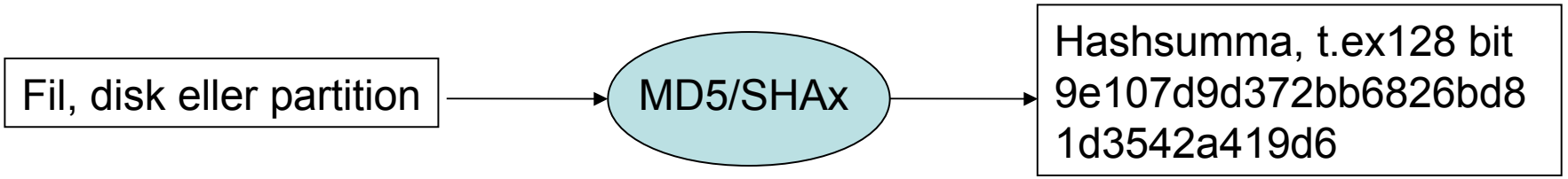
- Kom ihåg! Det viktiga är att kunna göra en exakt spegelkopia av ALLT!
  - Filer
  - Rå (meta) data – MFT (Master File Table), FAT, MBR osv.
  - Raderade filer
  - Ej allokerad diskyta och slack space

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 envägsfuktion (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”

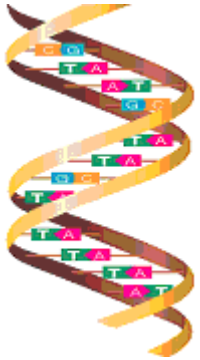
KFF är ett databasverktyg som jämför kända filers hash-värden mot ditt cases filer

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!

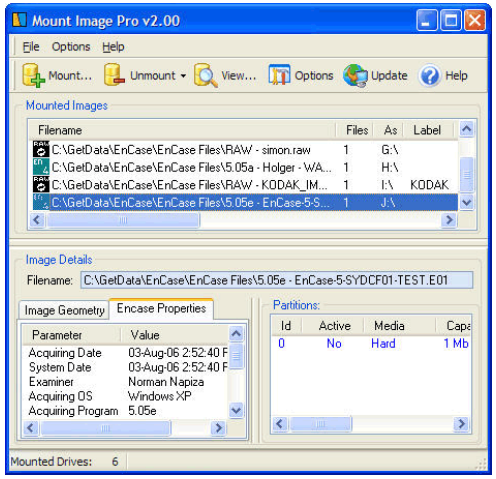
Mer om Image – återställningsverktyg

- 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

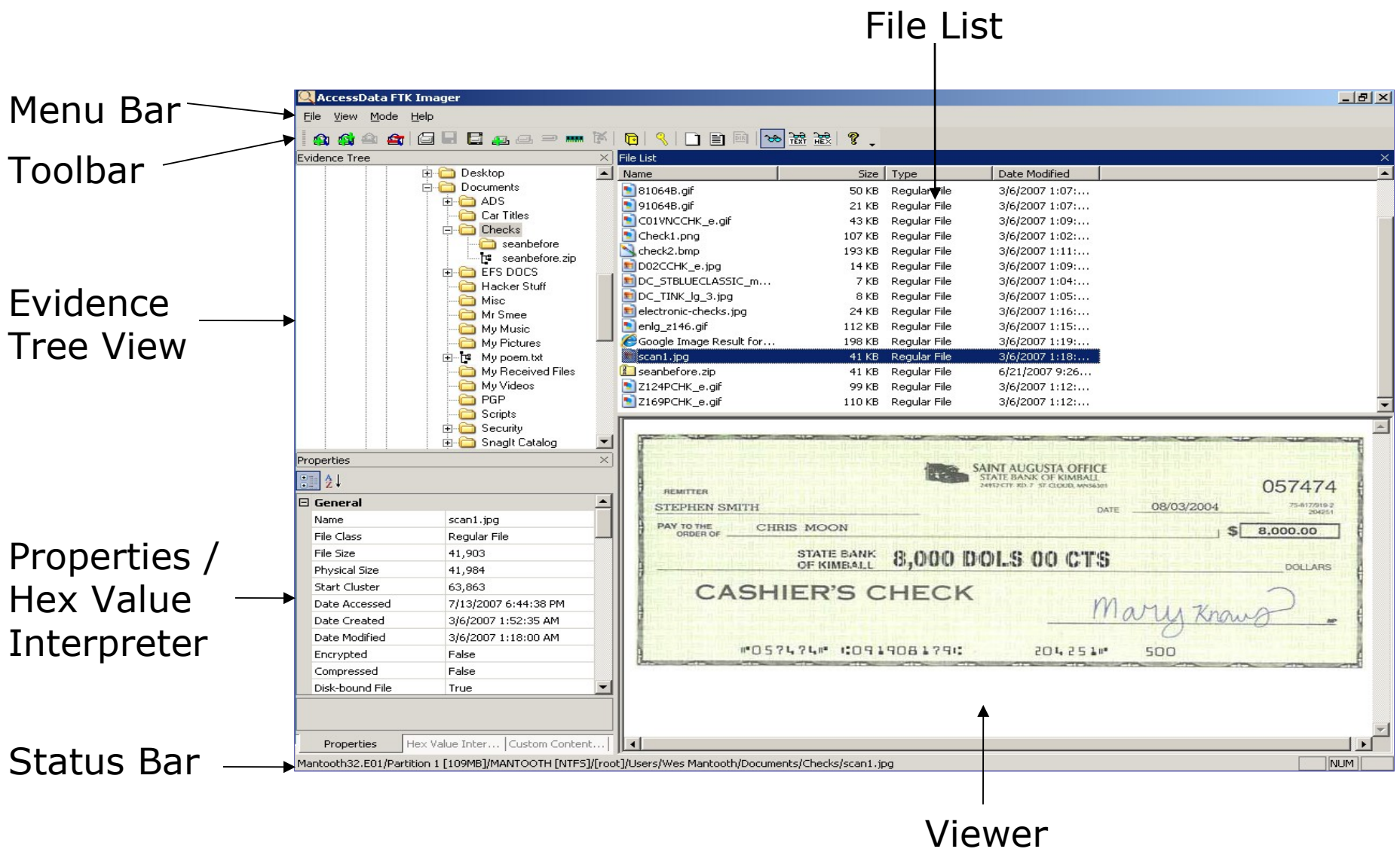
- Diskar som drabbats av fysiska fel
  - Byt kabel, kontrollerkort (drivelektronik), kortplats, dator, BIOS inställning, drivrutin etc.
  - ”klick döden”, ”bad sectors” på fel ställen, ej bootbara etc. kan ofta det mesta räddas ifrån
    - Disken måste kunna hittas av BIOS
    - Bootsektorn måste vara 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 erros & continue, padda med ’0’
    - Kan också skrivas direkt till ny disk
- Disktillverkares utility
  - PowerMax, Drive Fitnetss Tool, SeaTools etc.

Mer om Image – montera image

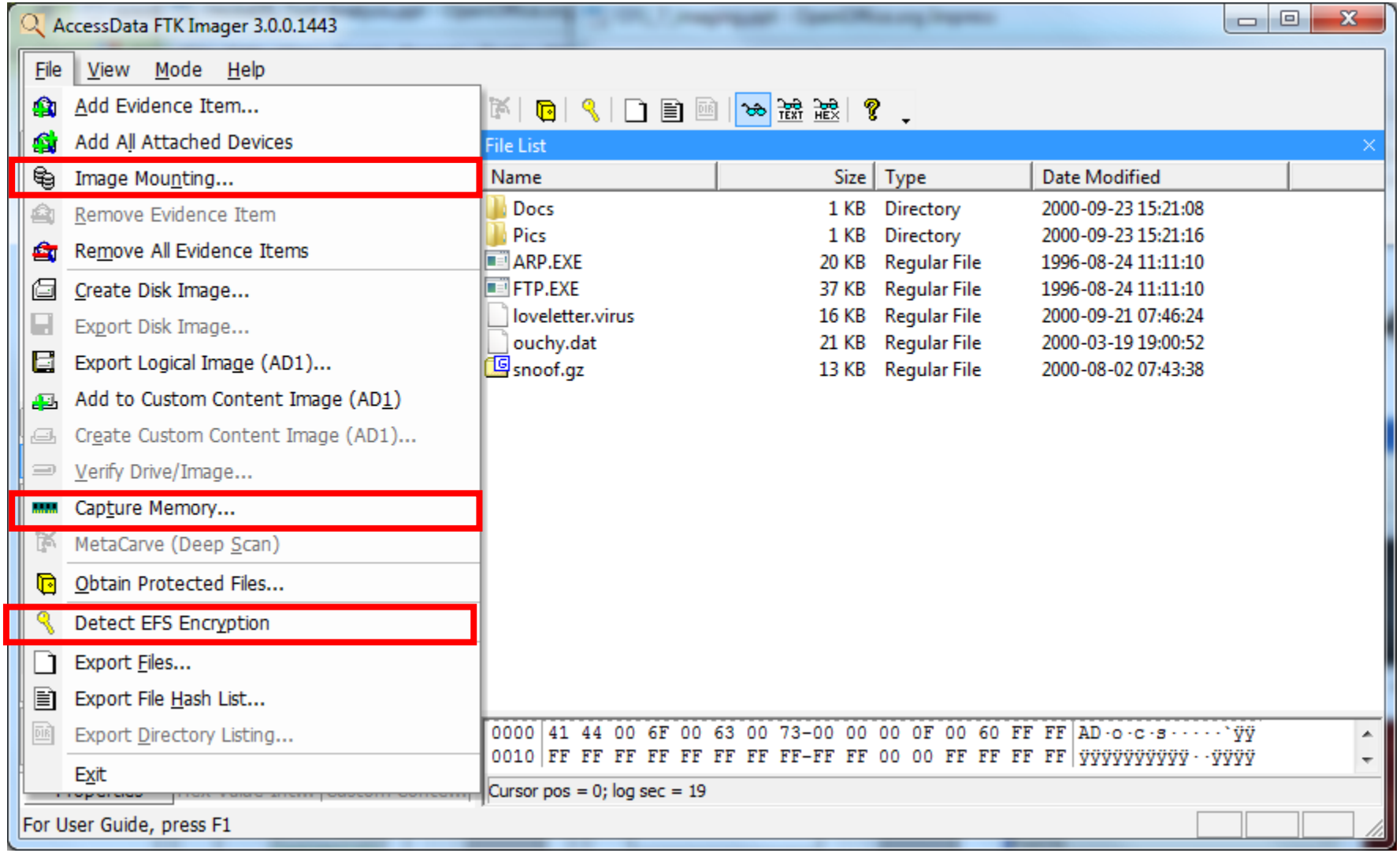


- Linux - montera dd on loopback device
  - http://wiki.edseek.com/guide:mount_loopback
- Mount EWF (E01) on Linux (FUSE)
  - http://stephenventer.blogspot.com/2009/02/mount-ewf-e01-on-linux.html
- Windows
  - Paraben P2 eXplorer - http://www.paraben.com/programs/p2x.html
  - Mount Image Pro - www.mountimage.com (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 Coversion -> VMware
    - LiveView - 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.

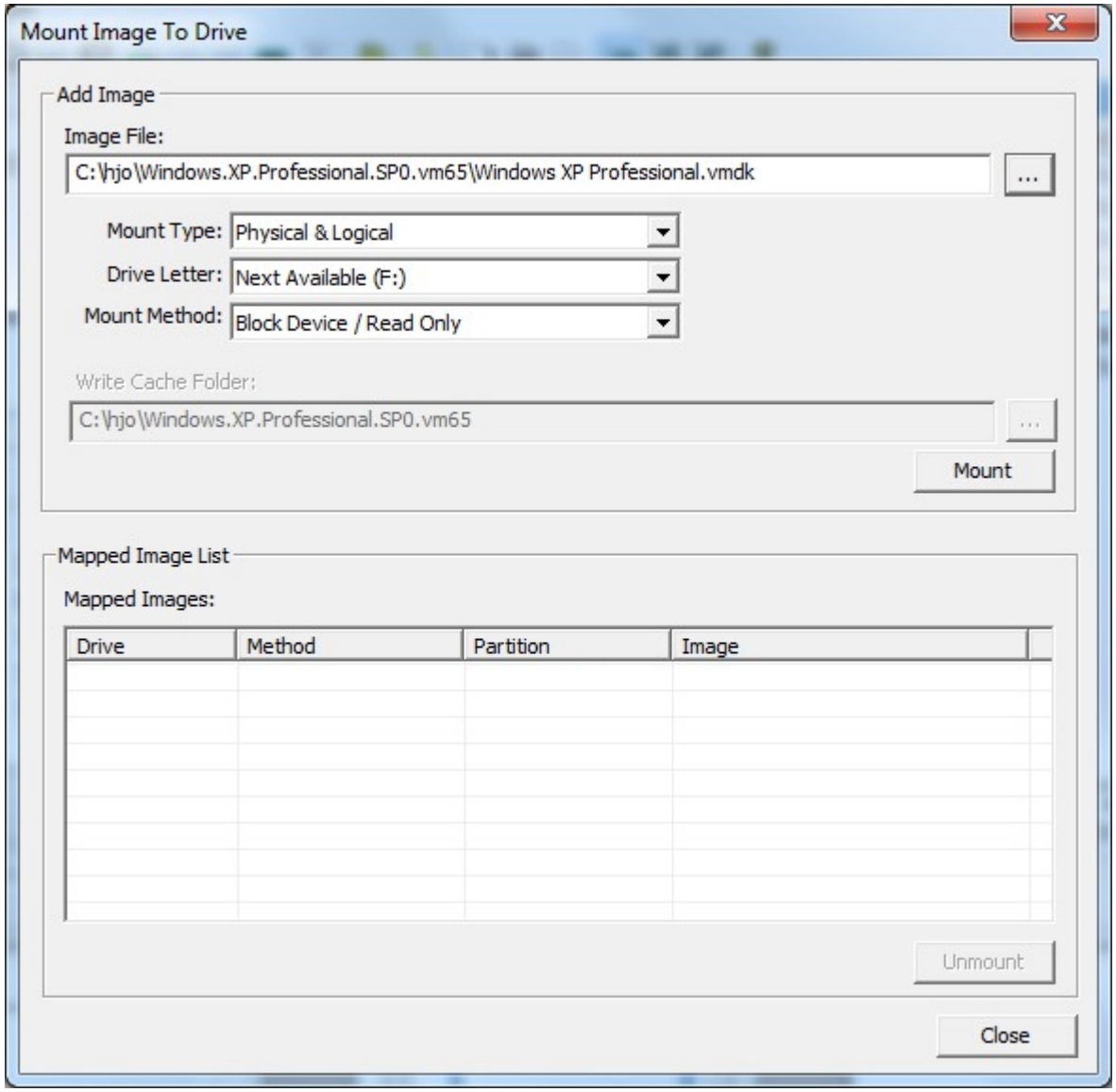
FTK Imager Interface

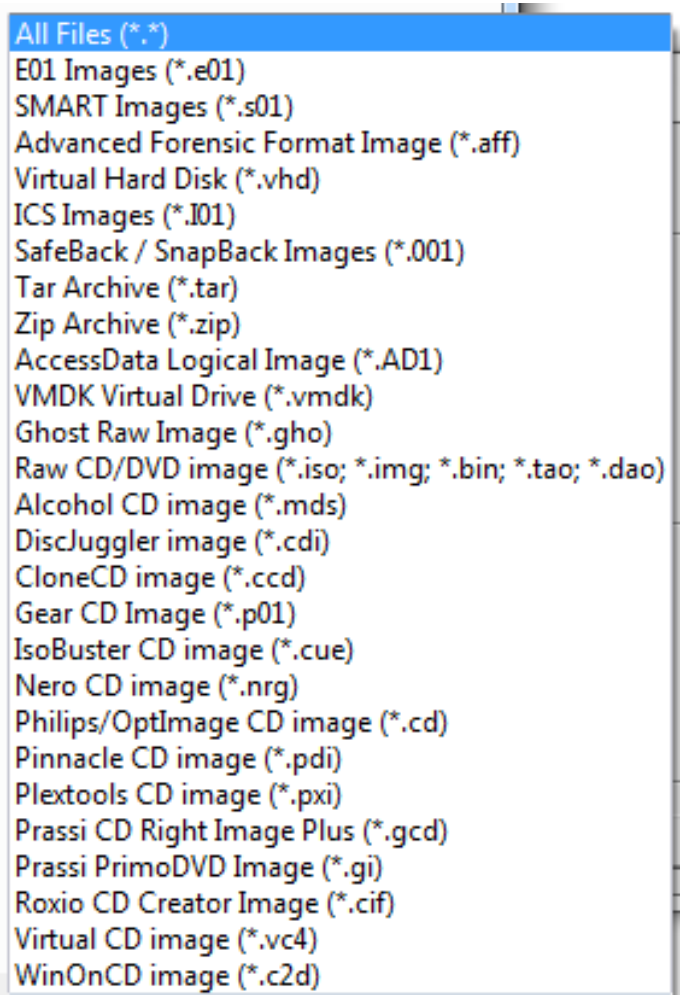


News in FTK Imager 3.x

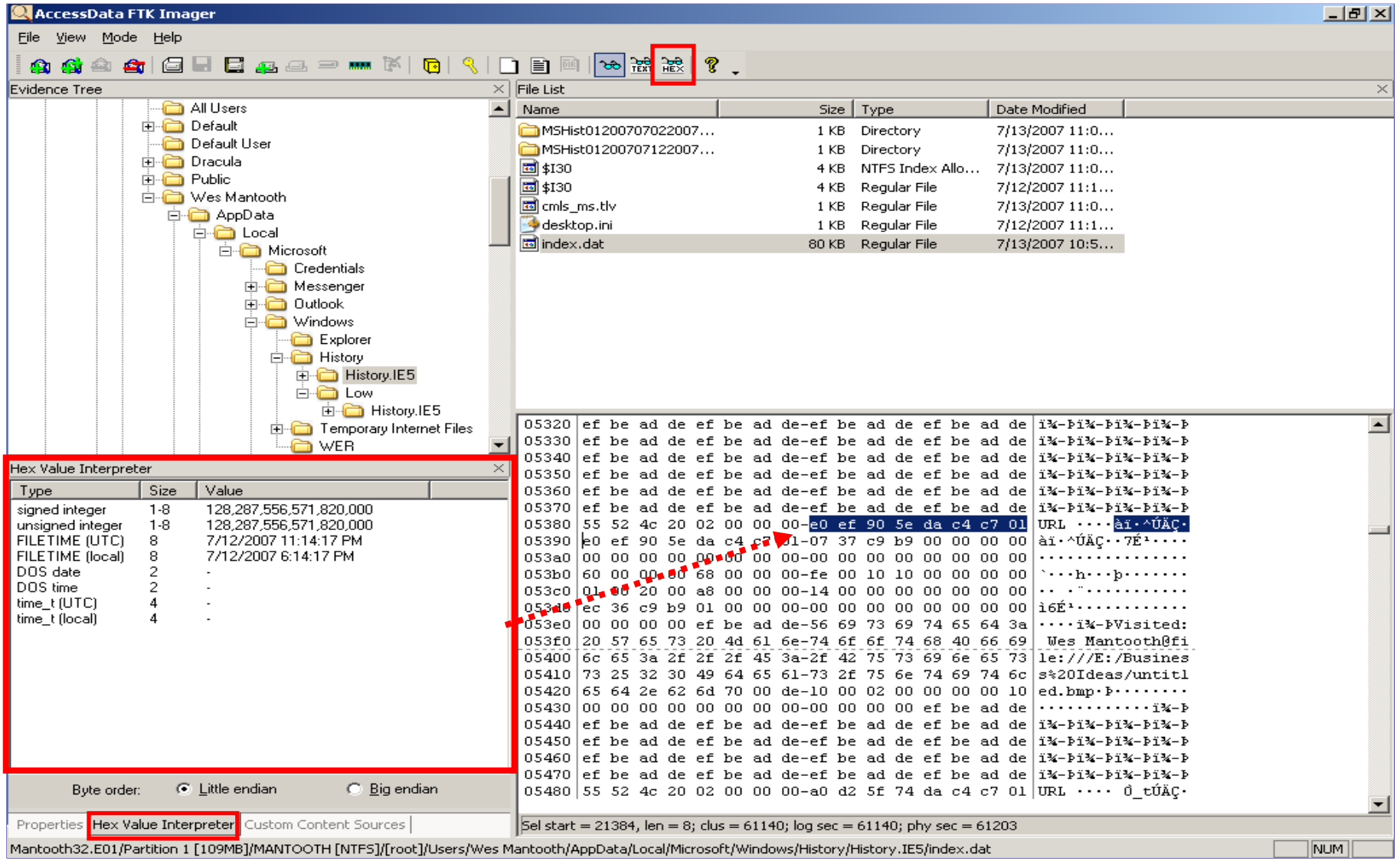


News in FTK Imager 3.x

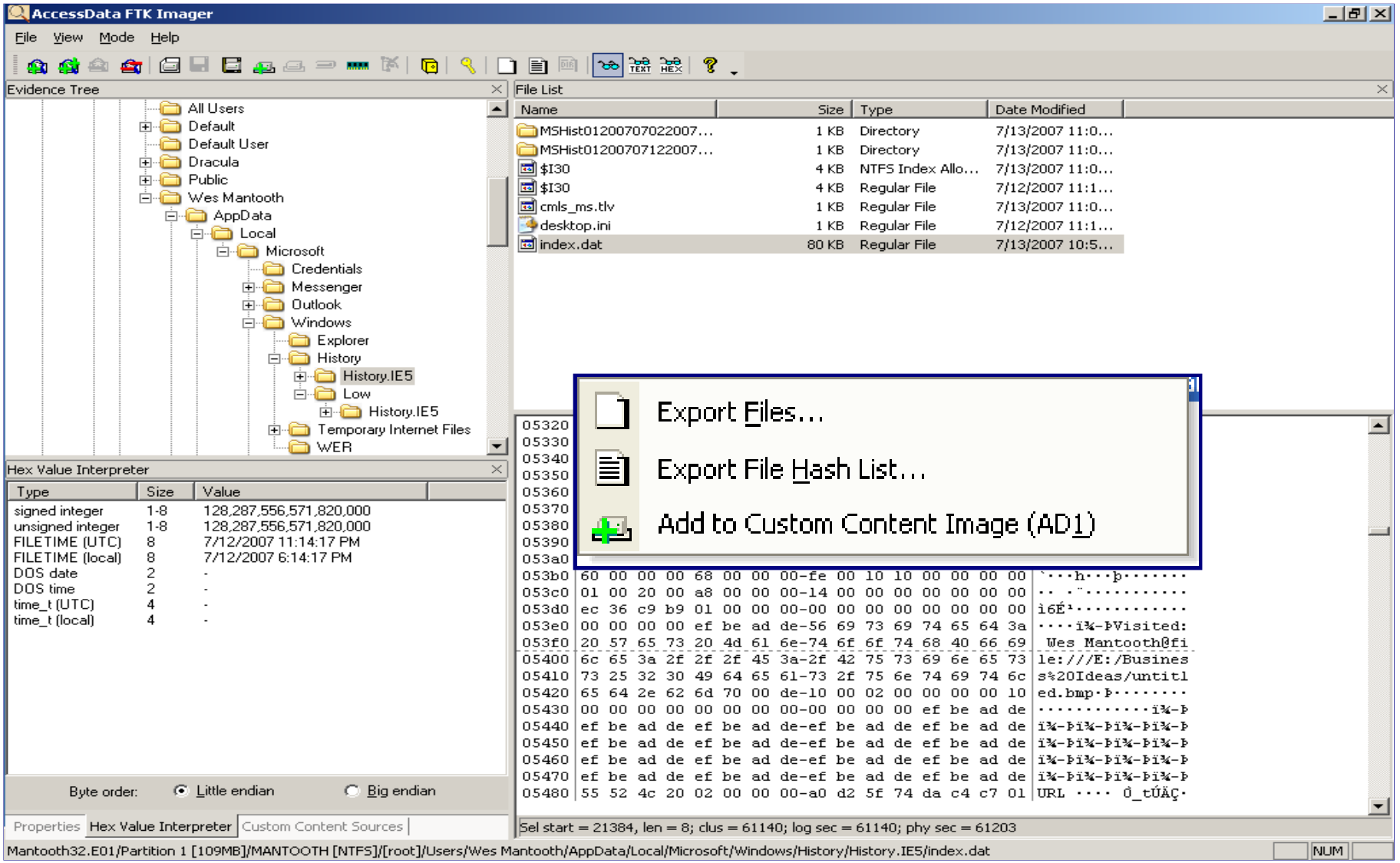




Interpreters



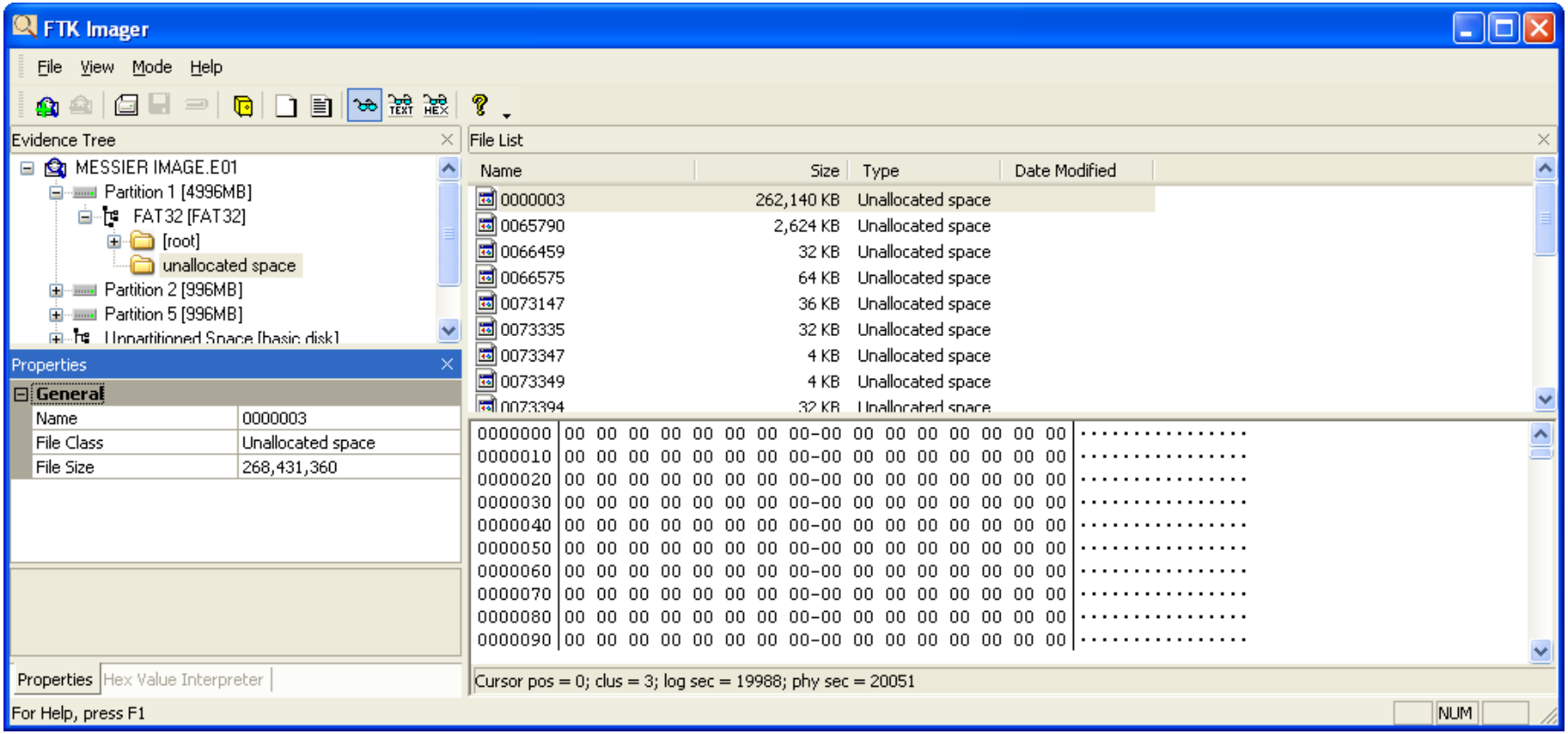
Right Click Menu Options



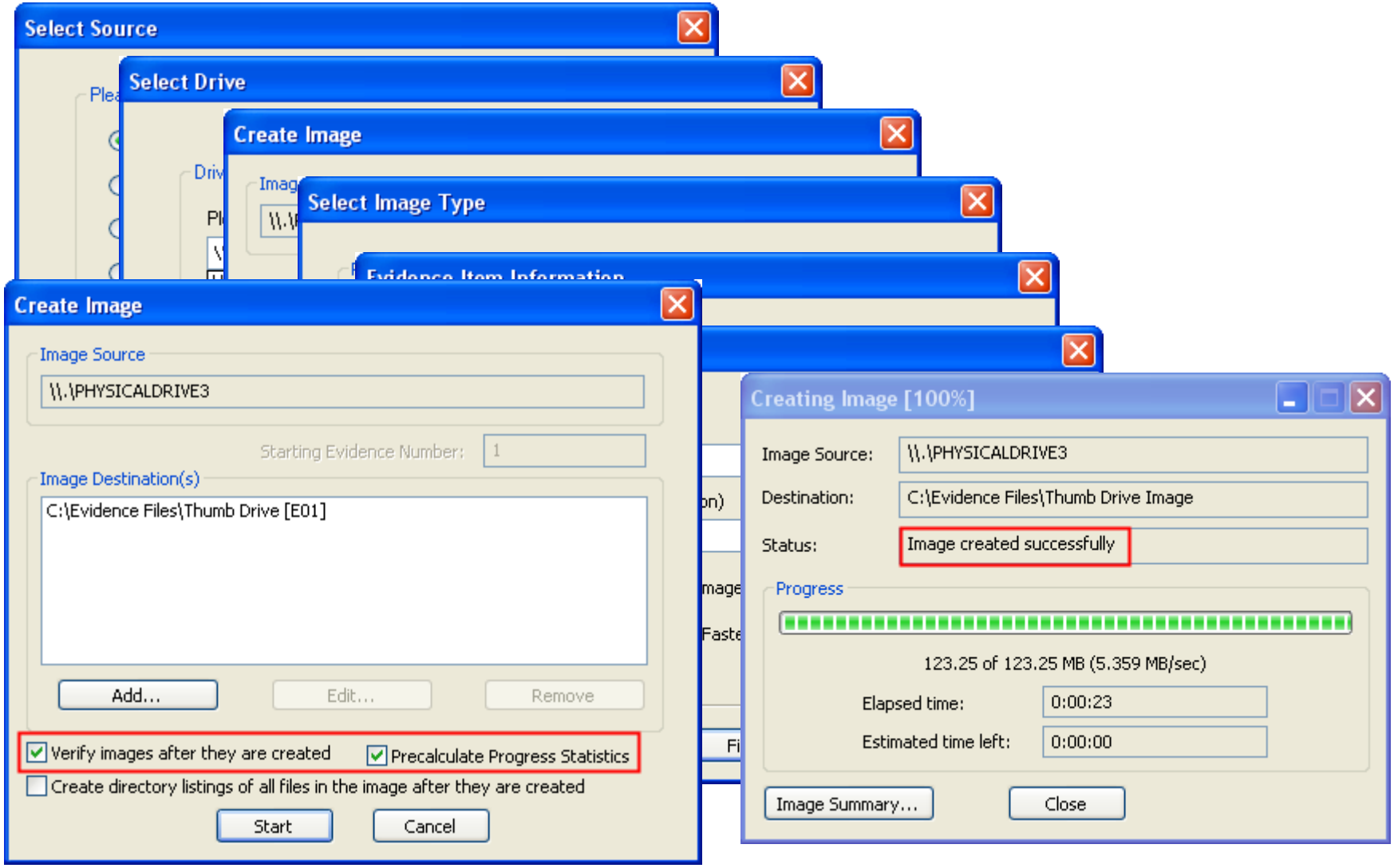
Drive Freespace

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

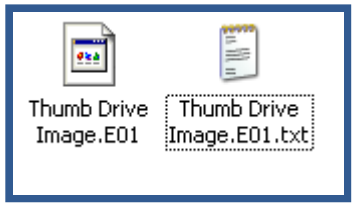
Nedan kan vi se en 262140 KB klump som börjar på kluster 3 och en annan 2624 KB klump som börjar på kluster 65790 osv.



Acquisition



Acquisition

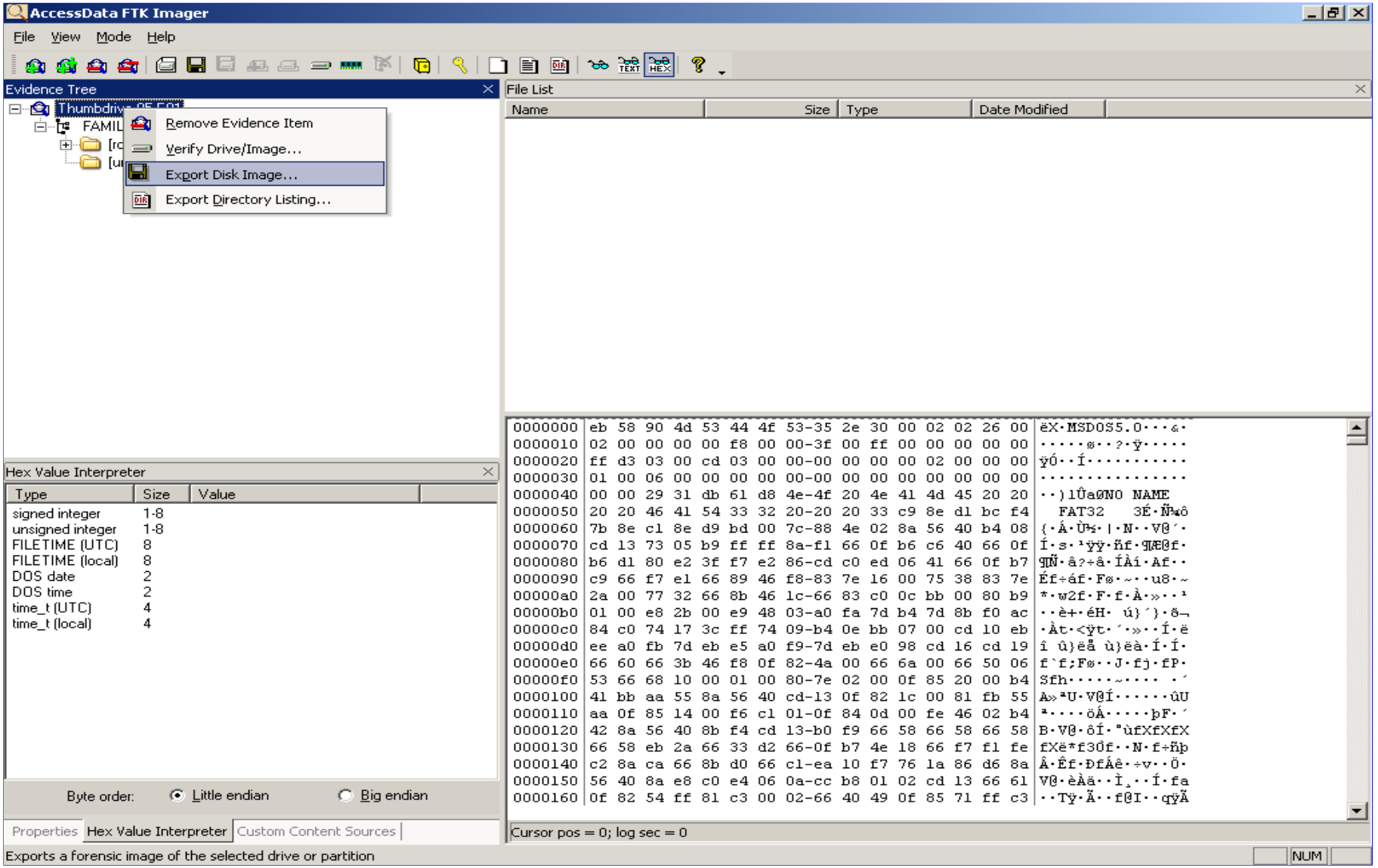


Thumb Drive Image.E01.txt - Notepad

File Edit Format View Help

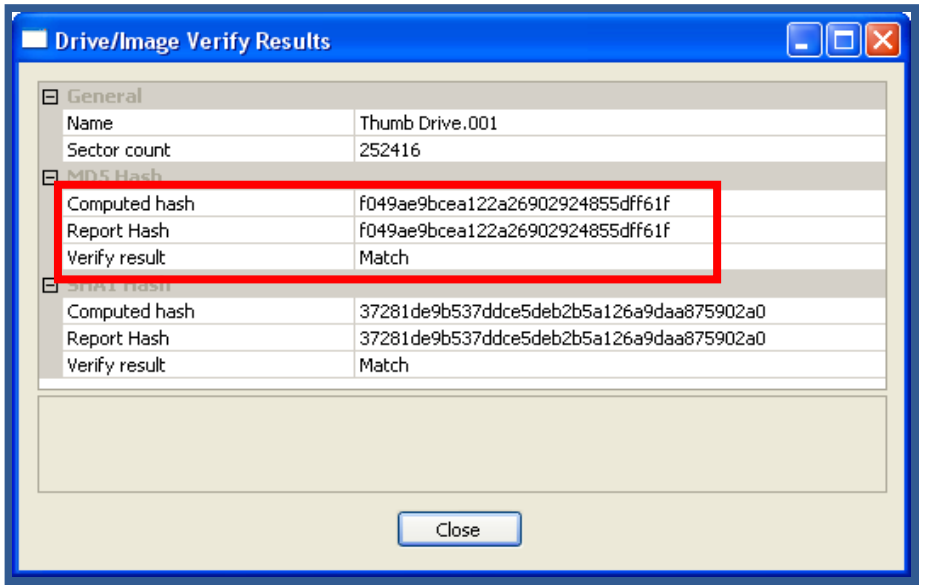
```
Created By AccessData® FTK® Imager 2.5.3.14 071018

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
```

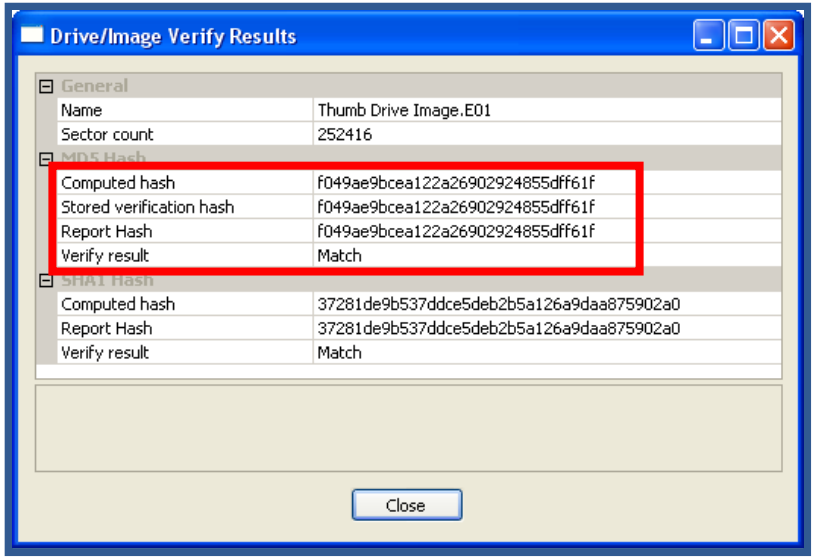
Conversion – Image and Image



Verification

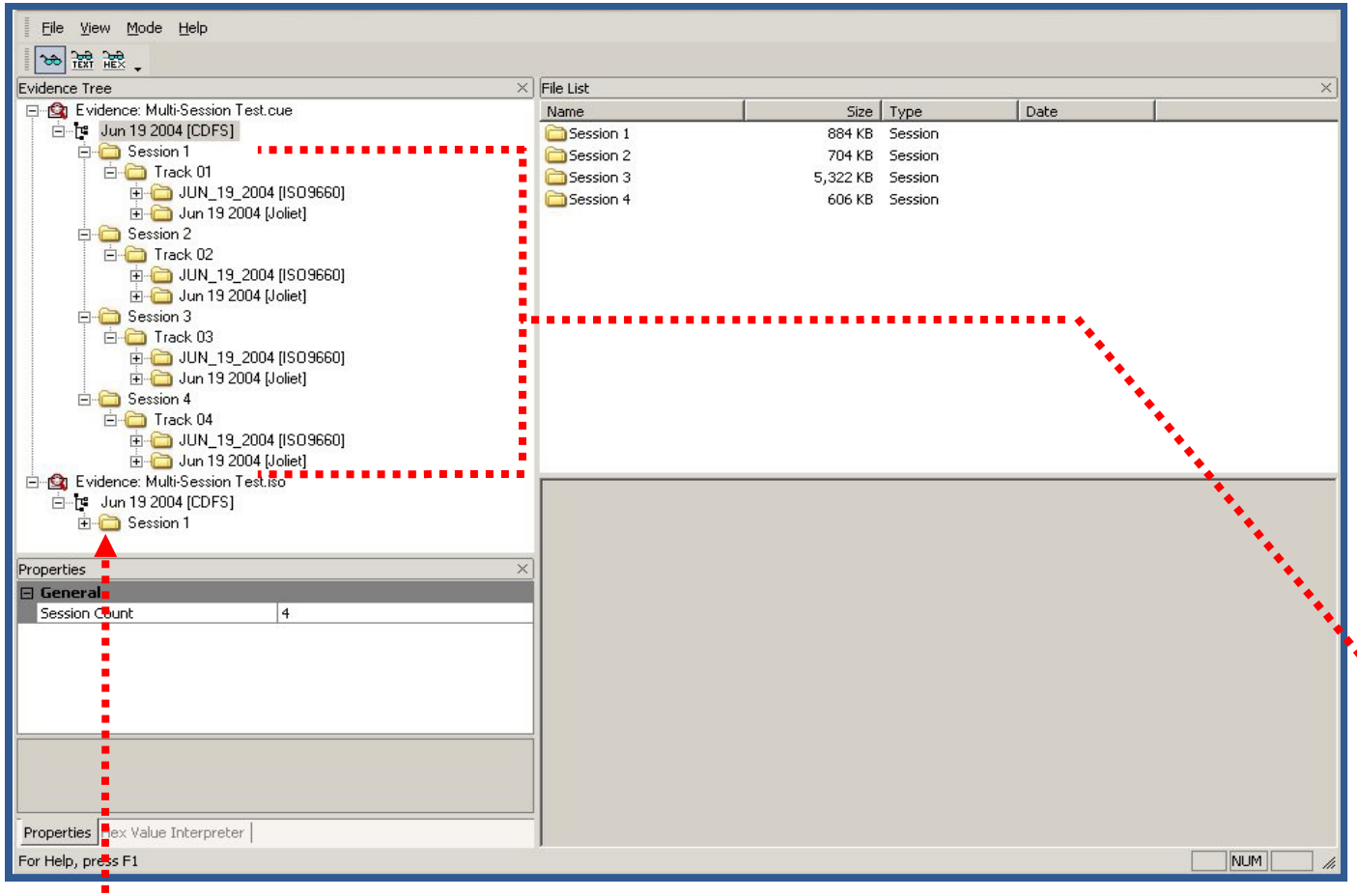
Encase / DD ??





Verified based on image format

CD / DVD Images



.CUE files

.ISO files

Use the .CUE file to map sessions