CYBER502x
Computer Forensics

Week 7: Windows Forensics Analysis

Forensics involves

- Discover and Collect
- Preserve
- Analyze
- Present / Report

Analysis

- General steps:
  - Start an analysis by looking at the partition table on the suspect drive
  - Retrieve deleted files
  - Create and examine MAC times
  - Use data carving technologies to recover hidden data
  - Keyword search for terms related to your case
  - Check for emails, pictures, Internet data
  - Glean evidence from registry, recycle bin, shortcuts, event logs, etc.

MAC TIMES

- Windows records the date and time of a file’s
  - Creation (**C**reated)
  - Last modification (**M**odification)
  - The date that a file was last accessed (**A**ccessed)
  - The MFT entry last modified (changed) time (**E**)

Registry

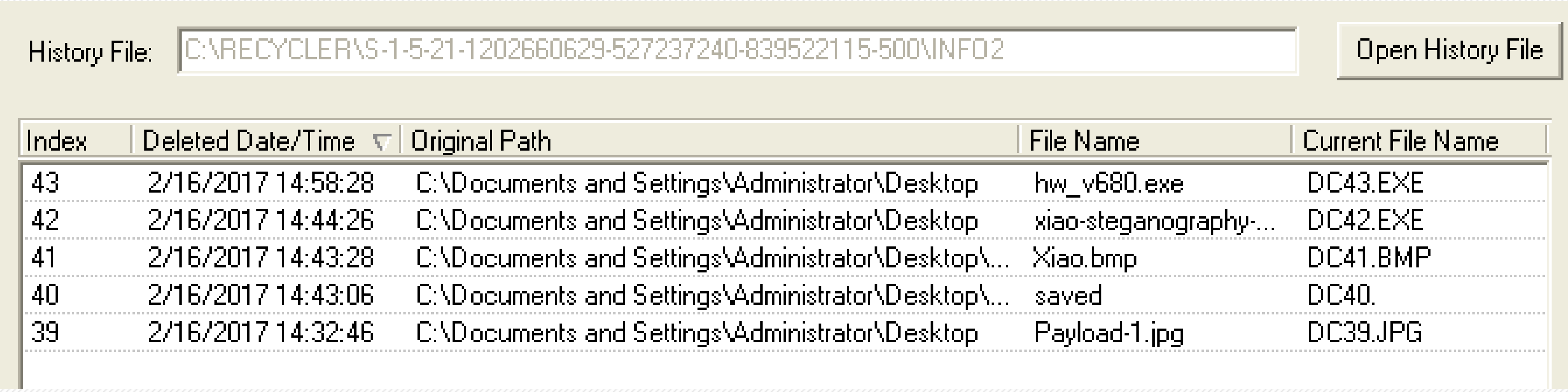
- Covered in Unit 6

Recycle Bin

- The Recycle Bin is a hidden system folder named
  - Recycled in Windows 95 and 98
  - Recycler in WinNT/2K
- NTFS
  - Subfolder is created with user's SID
  - Users can only access the file associated with their own SID
- FAT
  - Do not track who deleted the files

INFO2 record

- INFO2 record contains
  - Deletion date, time
  - File’s original name and path
  - Index number --(0 assigns to the first file)
  - a new name in D
    [original drive letter of file][index no].[original extension]
- Note: Files deleted by the operating system or by pressing *Shift* + *Delete* will not have INFO2 records.



History File: C:\RECYCLER\S-1-5-21-1202660629-527237240-839522115-500\INFO2

Index	Deleted Date/Time	Original Path	File Name	Current File Name
43	2/16/2017 14:58:28	C:\Documents and Settings\Administrator\Desktop	hw_v680.exe	DC43.EXE
42	2/16/2017 14:44:26	C:\Documents and Settings\Administrator\Desktop	xiao-steganography-...	DC42.EXE
41	2/16/2017 14:43:28	C:\Documents and Settings\Administrator\Desktop\...	Xiao.bmp	DC41.BMP
40	2/16/2017 14:43:06	C:\Documents and Settings\Administrator\Desktop\...	saved	DC40.
39	2/16/2017 14:32:46	C:\Documents and Settings\Administrator\Desktop	Payload-1.jpg	DC39.JPG

Windows Vista (and later) Recycle Bin

- It is named *C:\$Recycle.Bin*
- INFO2 is not used
- Each deleted file has a pair of files in
- *C:\$Recycle.Bin\<USER_SID>*
  - the deleted file: *$Rxxx.original_ext*
  - the correspondent index file: *$Ixxx. original_ext*
    - Contains the original path and timestamps.

The file structure for $I

- 544 bytes in total
- Bytes 0-7: $I File header – always set to 01followed by seven sets of 00.
- Bytes 8-15: Original file size in hex
- Bytes 16-23: Deleted date/time stamp. A free tool called Decode can be used to interpret the exact date/time
- Bytes 24-543: Original file path/name

Read INFO2 file

- Rifiuti, a free McAfee tool
- Runs on Windows (through Cygwin), Mac OS X, Linux, and *BSD platforms
  - Rifiuti INFO2
  - rifiuti –t delimiter INFO2

Read $I file

- Use EnCase or FTK export the $I files
- Use *$I file parser* from Flashback Data to parse $I files

When the Recycle Bin is emptied,

- *Unfortunately…*
  - INFO2 file is resized back to 20 (header) bytes
  - $I files are deleted
  - the Recycle Bin icon changes to display an empty waste bucket
- *But…*
  - The INFO2 records and $I files may still be intact in unallocated or slack space

How can INFO2 and $I files help for investigations?

- They can effectively confirm or refute users’ explanations
- They indicate that users intentionally deleted files or folders.
  - They tell us that we may have missed a critical piece of media (a partition or a USB).

How does EnCase recover deleted INFO2 records or $I?

- Go through the unallocated clusters and file slack to recover all Recycle Bin records

- Before EnCase 7
  - Run the info Record Finder EnScript
- EnCase 7 and after
  - EnCase Evidence Processor > Modules > Windows Artifact Parser

FTK uses regular expressions

- The regular expression for INFO2 entries
  - *[\x02-\x19]\x00{3}.{6}\xc3\x01.{4}[c-z]\x00\:\x00\\*
  - All the drive letters C-Z followed by three bytes of zero
  - Followed by six bytes of any hour, date, and time;
  - Followed by two bytes of a specific year.
  - Continue with four bytes of any physical file size,
  - Followed by a drive letter range (C-Z:\) followed by any path.

Shortcut files

- Exist in
    - Recent Documents
    - Start Menu
    - SendTo
    - Windows Desktop
- With extension of .lnk

Shortcut files

- Contain
  - Serial number of the volume where the target was stored
  - The fully qualified paths of the files that they refer to
  - The MAC times for the LNK file
  - The MAC times of the target file
  - Target attributes such hidden, system, encryption, compressed, etc.
- Help to identify
  - The files that may no longer exist on the device they’re examining

LNK file parser

- EnCase
  - Before Version 7: uses the EnScript, link file parser
  - EnCase 7: EnCase Evidence Processor > Modules > Windows Artifact Parser (Link Files)
- FTK
  - Classifies link files in the Other Known Type container
- Other free lnk file analyzer and parser

Thumbnails

- Used by Windows since Windows 95
- A Hidden system file that contains
  - a copy of each graphics file in a folder
- Locations
  - Windows XP and earlier: Thumbs.db alongside pictures
  - Windows Vista, Windows 7, 8, 8.1 and Windows 10: use centralized cache
    - at *%userprofile%\AppData\Local\Microsoft\Windows\Explorer*
    - includes a number of thumbcache_xxx.db (numbered by size).

How can thumbnails help us?

- The user may delete files from the folder, but the copies of those files still in the thumbnails file.
- Thumbnails show the files existed on the volume, and modification dates of those file, even though the files did not exist at the time of the examination.

Extract and view thumbnails file

- EnCase views that file as a compound file
- FTK classifies the files in the Archives container

Web browsing activities: IE

- Internet Explorer stores user browsing history
  - URLs that a user visited, cookies and pages downloaded, and the time of access
  - Before IE 10, stored in *…\index.dat* (location varies based on OS)
  - Since IE10, stored in a central database located at *C:\user\username\AppData\Local\Microsoft\Windows\WebCache\WebcacheV01.dat*
- Examine an index.dat file
  - IEHistory.exe for Windows
  - Pasco) ("browse" in Latin) supports Windows (through Cygwin), Mac OS X, Linux, and *BSD platforms
    - *pasco index.dat > webHistroy*
    - *pasco –t delimiter index.dat > webHistroy*

Websites cache: Firefox

- Firefox - http://davidkoepi.wordpress.com/2010/11/27/firefoxforensics/
  - file downloaded by the user in downloads.sqlite
    - It stores Filename, Size, type, download from, file save location, application to open file and download start and end time
  - Cookies in cookies.sqlite
  - Forms in formhistory.sqlite
  - Bookmarks and internet history in places.sqlite

- Read a SQLite file
  - Open source SQLite Browser
  - SQLite Manager – Firefox Addons

Websites cache: Safari

- Apple’s Safari and iPhone
  - Stored in plist files: History.plist, Bookmarks.plist, TopSites.plist and Downloads.plist.
  - On a Mac OS X, the Safari Internet History is located under the folder: */Users/%USERNAME%/Library/Safari*.
  - Mari DeGrazia wrote plist parsers http://az4n6.blogspot.com/p/downloads.html
- Safari Cookies
  - Stored in *~/Library/Cookies/Cookies.binarycookies*
  - Cookies.binarycookies reader: *http://www.securitylearn.net/2012/10/27/cookies-binarycookies-reader/*

Track Websites in EnCase and FTK

- EnCase: Run the Internet History in EnScript
  - Find Internet Artifacts via Process Evidence
- FTK: Through File Extension in FTK
  - Check HTML and HTM files
- Tracks Eraser Pro or Ccleaner: delete browser history

Print

- Printing involves a spooling process
- The local print provider
    - writes the file’s contents to a spool file (.SPL) and creates a separate graphics file (EMF) for each page
    - Tracks username, filename, and data type in a shadow file (SHD)
    - Spooling protects a print job by saving it on disk

Print

- For each print job, two files are created
  - .SHD (shadow file) contains information about the print job
    - the owner
    - the printer
    - the name of the file printed
    - The fully qualified path
    - the printing method (RAW or EMF)
  - .SPL contains file contents with .EMF pictures

After the print job completes

- .SHD, and .SPL files are deleted.
- They may still exist in unallocated space or Windows memory/page file.
- Data carving techniques can be used to carve out the .EMF graphics from .SPL files

Jumplists

- Provide the user with quick access to documents and tasks that have frequently or recently used
- List up to10 most recently accessed files or frequently assessed destination per application
- Contain information
  - full file name and path
  - computer name and MAC address
  - last access date and time
  - application used to open the file

Two type of jumplists

- Automatic jumplists (*.automaticDestinations-ms) *%appdata%\microsoft\windows\recent\automaticdestinations\** (OS genterated)
- Custom jumplists (*.customDestinations)
  - *C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations*
- Jumplists Interpretation
  - Each jumplist embeds or includes LNK files formation
  - LNK files are stored in an order from the oldest one to the most recent one

Jumplists references and parsing

- Windows Jump List Parser (jmp) by TZWorks: https://tzworks.net/prototype_page.php?proto_id=20
- Jumplister by Mark Woan: http://www.woanware.co.uk/forensics/jumplister.html

Why jumplists are important?

- Jumplists contain files even if they have been deleted

Other Advanced Windows Artifacts (not required)

- https://digital-forensics.sans.org/media/poster-windows-forensics-2016.pdf
- If you are interested, check the appendix slides.
  - Shadow Copies
  - Windows Prefetch
  - Control Panel (.cpl)
  - ShellBag

Event Log files

- Event logs for the system
  - SECEVENT.EVT
  - SYSEVENT.EVT
  - APPEVENT.EVT
- These files are written with a binary format
- Use Event Viewer to read the log files.
- EnScript: Windows Event Log parser

.EVT files

- SECEVENT.EVT
  - Stores security-related events, including failed login attempts and attempts to access files without proper permissions.
- SYSEVENT.EVT
  - Stores events associated with the system’s functioning, including the failure of a driver or the inability of a service to start.
- APPEVENT.EVT
  - Stores events associated with applications, such as databases, Web servers, User applications.

Windows Event Log for User Logon/Logoff

- Records successful or failed logon/logoff events under the Secevent.evt
  - Event ID: 4624– Successful Logon
  - Event ID: 4625– Failed Logon
  - Event ID: 4634– Successful Logoff
  - Event ID: 540– Successful Network Logon
- https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx

Logon Type Values

2	Logon via console
3	Network Logon
5	Windows Service Logon
7	Credentials used to unlock screen
8	Network logon sending credentials (clear text)
9	Different credentials used than logged on user
10	Remote interactive logon (RDP)
11	Cached credentials used to logon

Be aware…

- Attacker may altering event logs.
- At a minimum to alter SecEvent.evt

Forensic analysis tools

- Sleuthkit/Autopsy
- EnCase
- FTK
- OSForensics
  - http://www.osforensics.com/download.html
  - 30 days trial
- ProDiscover
- Forensic Explorer

EnCase and FTK

- Both are commercial software.
- EnCase Forensic
    - Latest version: EnCase Forensic 8
- FTK
    - Latest version: FTK 6
    - demo version FTK 1.8x for small images less than 5000 files – it is no longer supported by AccessData

Analysis procedure

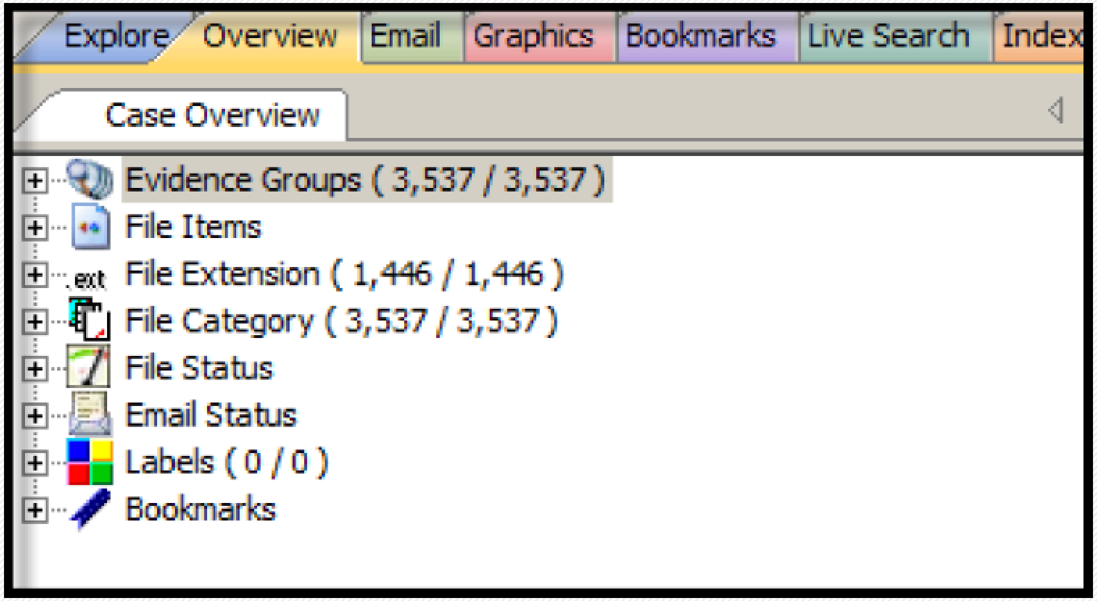
- Create a case
- Add evidence to a case
- Perform thorough analysis
- Obtain finding and supporting data
- Generate report

Forensic analysis tools in Common

- Features include
    - Deleted files recovery including data carving
    - MAC times analysis
    - Index search and live search
    - Signature analysis
    - Email analysis
    - Hash analysis
    - Graphics view
    - Internet and website analysis
    - Registry analysis, recycle bin, shortcuts, and other Windows artifacts analysis

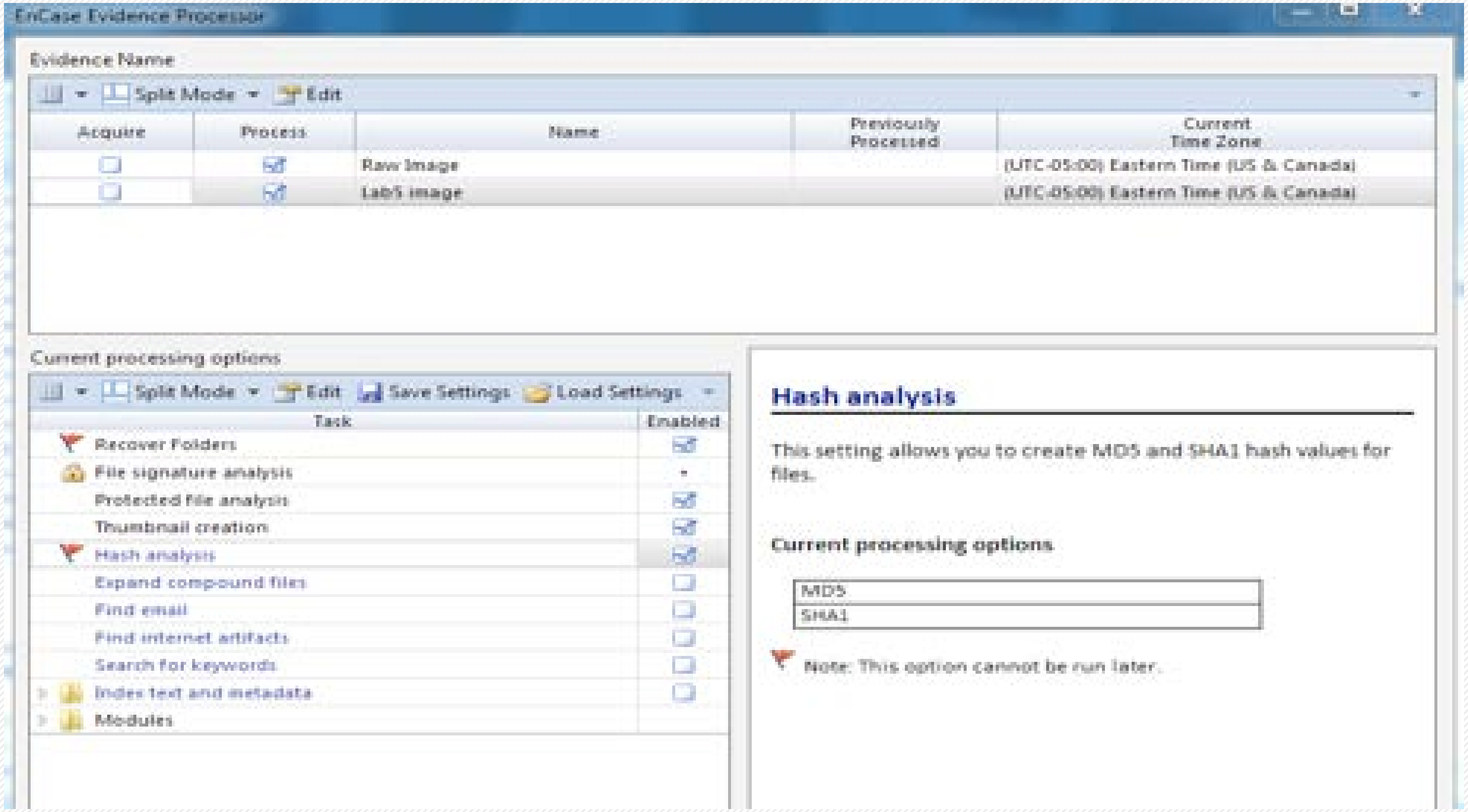
FTK
Create a case – Process options

- Evidence Preprocessing Options
  - MD5 Hash and SHA1 Hash
  - File Signature Analysis
  - Entropy Test (to test if the file is compressed or encrypted)
  - Data Carving
  - Flag bad extensions
  - index



Evidence Groups (3,537 / 3,537)
File Items
File Extension (1,446 / 1,446)
File Category (3,537 / 3,537)
File Status
Email Status
Labels (0 / 0)
Bookmarks

EnCase Evidence Processor



Evidence Name

Acquire	Process	Name	Previously Processed	Current Time Zone
☐	☑	Raw Image		(UTC-05:00) Eastern Time (US & Canada)
☐	☑	Lab5 image		(UTC-05:00) Eastern Time (US & Canada)

Current processing options

Task	Enabled
Recover Folders	☑
File signature analysis	•
Protected file analysis	☑
Thumbnail creation	☑
Hash analysis	☑
Expand compound files	☐
Find email	☐
Find internet artifacts	☐
Search for keywords	☐
Index text and metadata	☐
Modules	

Hash analysis

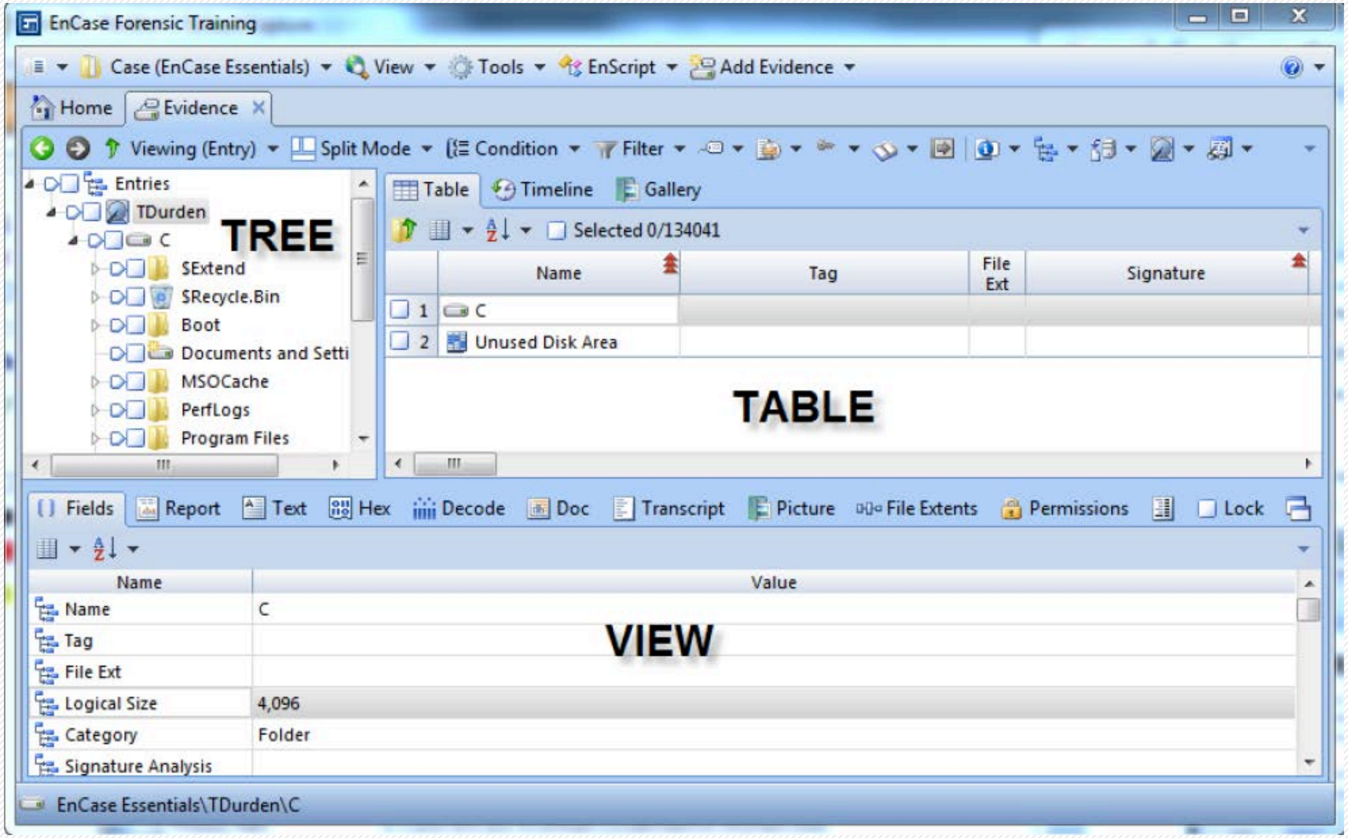
This setting allows you to create MD5 and SHA1 hash values for files.

Current processing options

MD5
SHA1

Note: This option cannot be run later.

EnCase Forensic’s tree-table-view

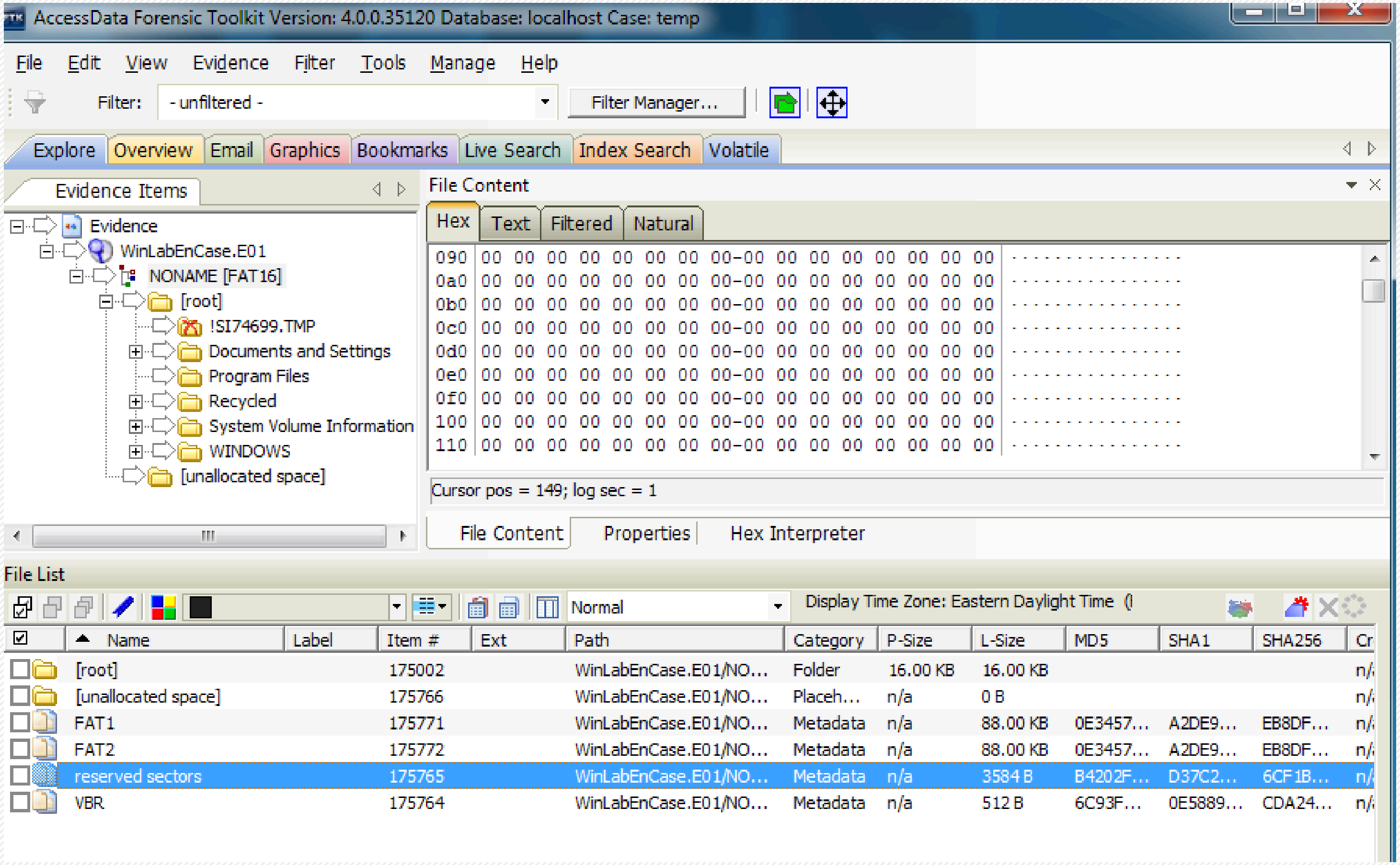


		Name	Tag	File Ext	Signature
□	1	C			
□	2	Unused Disk Area			

Name	Value
Name	C
Tag	
File Ext	
Logical Size	4,096
Category	Folder
Signature Analysis	

Image copied from *EnCase Forensics V7 User Guide*

FTK’s Explore view



```
Evidence
  WinLabEnCase.E01
    NONAME [FAT16]
      [root]
        !SI74699.TMP
        Documents and Settings
        Program Files
        Recycled
        System Volume Information
        WINDOWS
      [unallocated space]
```

```
090  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
0a0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
0b0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
0c0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
0d0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
0e0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
0f0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
100  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
110  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
```

Cursor pos = 149; log sec = 1

☑	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Cr
□	[root]		175002		WinLabEnCase.E01/NO...	Folder	16.00 KB	16.00 KB				n/
□	[unallocated space]		175766		WinLabEnCase.E01/NO...	Placeh...	n/a	0 B				n/
□	FAT1		175771		WinLabEnCase.E01/NO...	Metadata	n/a	88.00 KB	0E3457...	A2DE9...	EB8DF...	n/
□	FAT2		175772		WinLabEnCase.E01/NO...	Metadata	n/a	88.00 KB	0E3457...	A2DE9...	EB8DF...	n/
□	reserved sectors		175765		WinLabEnCase.E01/NO...	Metadata	n/a	3584 B	B4202F...	D37C2...	6CF1B...	n/
□	VBR		175764		WinLabEnCase.E01/NO...	Metadata	n/a	512 B	6C93F...	0E5889...	CDA24...	n/

Graphic View or Gallery View

- A quick and easy way to view images that were stored on the subject media
  - Images purposely stored
  - Images inadvertently downloaded from the web
  - Displays files based on their file extension
    - How about renamed files?
    - Do the signature analysis first

Keywords search

- Index search:
  data is indexed prior to searching
- Raw/live search:
  searches based on non-indexed, raw data using regular expression

Bookmark

- Organize your analysis of a case in a group of selected items
- Help to write reports

- How to create a bookmark
  - Right-click and select *Create Bookmark*

Generate a report

- File > Report Wizard
- Includes
  - Case Information
  - Bookmarks
  - Flagged Graphics
  - File Management
  - Supplementary Files
  - Location
  - Custom graphic for the report

Additional slides for Windows artifacts

(not required)

Shadow Copies

- Snapshots of files on a NTFS formatted volume.
- The Microsoft Volume Shadow Copy Service, vss
  - monitors all changes made to a VSS enabled volume
  - only backs up a block if it is about to be modified

Examine volume shadow copy

- Windows built-in
  - List shadow copies
    - Vssadmin list shadows
      - Shadow Copy Volume: *\\?\xxxxx\Device\HarddiskVolumeShadowCopy3*
  - Mount the volume
    - *mklink /d c:\shadow 1 \\?\xxxxx\Device\HarddiskVolumeShadowCopy3\*
- Volume Shadow Scanner
  - *IEF 6.3 - https://www.magnetforensics.com/computer-forensics/volume-shadow-copy-forensics/*

Windows Prefetch

- Purpose: speed up the Windows operating system and application startup
- Caching files that are needed by an app to RAM as the app is launched
- Located in *C:\Windows\Prefetch*, called
    - *AppName-eightCharacterHashOfTheAppLocation.pf*

Information in .pf

- The metadata includes the app name, app location, associated timestamps (file created, last accessed, and file modified), and the number of times the file was executed.
- A ten-second snapshot of files that are associated with the executed file (legible)

Control Panel (.cpl)

- Changes Windows system features
- an applet file, xxx.cpl, in Windows\System folder
- To run it, ex: control.exe timedate.cpl
- Investigate Control Panel, to find out:
  - Firewall changes by unauthorized software (firewall.cpl)
  - User account additions/modifications (nusrmgr.cpl)
  - Turning off System Restore/Volume Shadow Copies(sysdm.cpl)
  - System time changes (timedate.cpl)
  - ...

Evidence of cpl execution

- http://forensicmethods.com/control-panel-forensics#more-1968
- Prefetch
  - Through RunDLL32.exe and DLLHost prefetch files
- Windows Registry Userassist (before Windows 7)
  - *NTUSER.DAT\Software\Microsoft\Windows\Current\Version\Explorer\UserAssist*
  - Track frequency of program execution, per user
- Jumplists (Windows 7 and later)
  - *%user profile%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\7e4dca80246863e3.automaticDestinations-ms*
  - control panel application identifier, 7e4dca80246863e3

ShellBag

- Microsoft Windows store user preferences for GUI folder in Windows Explorer in Shellbag subkeys in *ntuser.dat* and *usrclass.dat*
- Contain registry keys that indicates which folders the user accessed
- The timestamps may demonstrate when the user accessed them.
- https://digital-forensics.sans.org/blog/2011/07/05/shellbags/
- Windows ShellBag Parser (sbag)
  - https://tzworks.net/prototype_page.php?proto_id=14