Hello!

Levy Lozada

- Police Chief Inspector
- 09189448682
- levylozada@gmail.com

EnCE Certified EnCase Examiner Guidance Software

cellebrite delivering mobile expertise CCLO Cellebrite Certified Logical Operator

cellebrite delivering mobile expertise CCPA Cellebrite Certified Physical Analyst

Oxygen Forensic Certified

Microsoft CERTIFIED Professional

Microsoft CERTIFIED Systems Administrator

CompTIA Security+ CERTIFIED

Introduction to Digital Forensic

What you will learn:

- Identification and seizure of electronic evidence
- Digital forensic principles and tools
- Techniques for searching and identifying evidence on digital media pertinent to a case

Participants Introduction

- Please Provide:
  - Name
  - Position
  - Experience in digital forensic
  - Course expectation

Course Schedule

Day 1	Modules
	- **Course introduction** - **Identification and seizure of electronic evidence**
	- **Imaging: Forensic acquisition of digital evidence** - **Forensic Tools Overview**
	- **Hash analysis** - **Signature analysis**

Course Schedule

Day 2	Modules
	- **Search techniques** - **Windows artifacts**
	- **Internet artifacts** - **Email artifacts**
	- **Logical Data storage** - **Analysis of Volatile Data**
	- **Reporting**

*The **more I learn**, the more I learn that **I need to learn more**.*

- unknown

Albert Einstein — 'The more I learn, the more I realize how much I don't know.'

Aristotle — 'The more you know, the more you know you don't know.'

Socrates —'The more I learn, the more I learn how little I know.

Thanks!

Any questions?

Understanding Digital Forensic

Digital Evidence

What is Digital Forensic?

Digital Forensic

- The scientific examination and analysis of data held on or retrieved from computer storage media or network and its presentation in a manner legally acceptable to a Court

What is Digital Evidence?

Digital Evidence

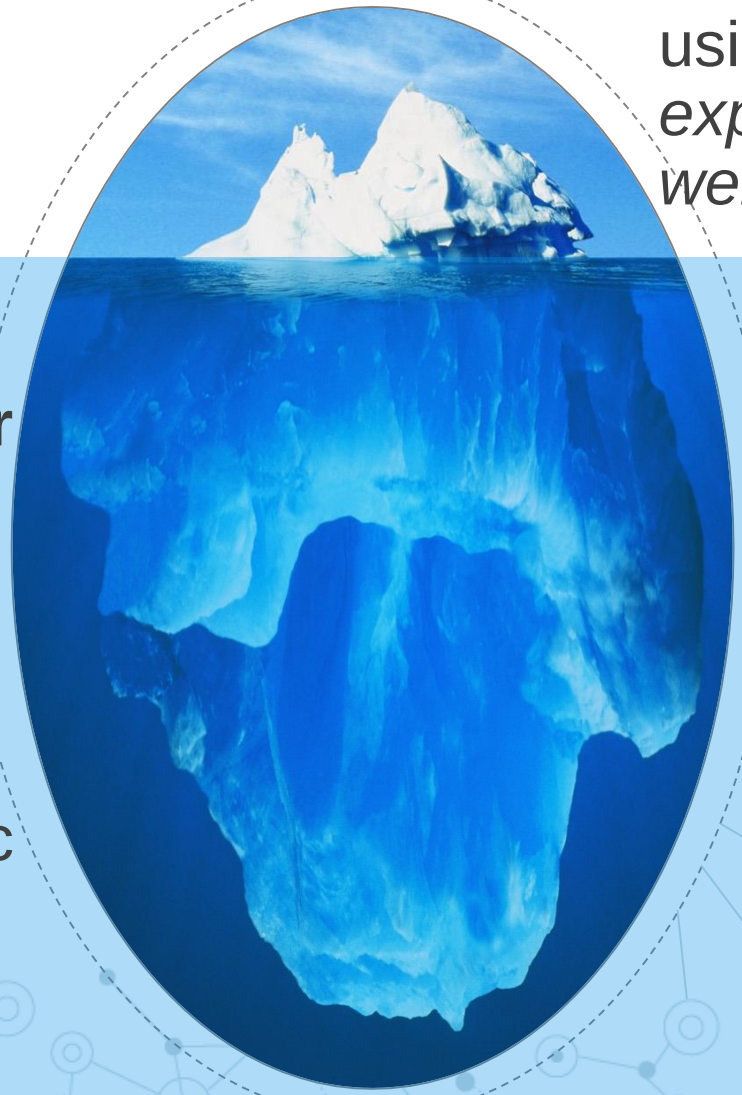
- Refers to digital information that may be used as evidence in a case
- Any information being subject to human intervention or not, that can be extracted from a computer system
- Must be in human-readable format or capable of being interpreted by a person with expertise in the subject

Digital Forensic Examples

- Recovering evidence from deliberately formatted hard drive
- Recovering thousands of deleted emails and chat messages
- Recovering internet artifacts and file's metadata
- Performing computer related crime investigation

Why Digital Forensic

Data as seen by **common users** using *windows explorer, cmd shell, web browser*



Data as seen by **forensic investigator** using *sophisticated forensic tools*.

These data may include *deleted, hidden, encrypted*, etc

Why Digital Forensic?

Any person can gather information from a computer

“ **BUT** “

The Forensic element means it has to be gathered in a manner which makes it reliable to a Court or other body and the information has to become

“ **EVIDENCE** ”

Not a law, but…

Non-compliance will often make evidence inadmissible

http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf

ACPO Digital Evidence Principles

Principle 1 – Primary Rule…

- No action taken by the law enforcement agencies or their agents should change the data held on a computer or other media which may subsequently be relied upon in Court.
- Where possible computer data must be '**imaged**' and that version be examined.

Principle 2

- In exceptional circumstances it may be necessary to access the original data held on a target computer.
- However it is imperative that the person doing so is competent and can account for their actions.

Principle 3

- An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine these processes and achieve the same result.

Principle 4

- The person in charge of the case has overall responsibility for ensuring that a computer has been correctly examined in accordance with the law and these principles.

Digital Forensic Process

Identification → Acquisition/ Imaging → Analysis → Reporting → Court Presentation

MD5 = ABC123 MD5 = ABC123

Reports

Evidence
LEFs
Exports

Thanks!

Any questions?

Overview: Identification and Seizure of Electronic Evidence

Objective

- By the end of this module, participants will demonstrate the ability to properly seize electronic evidence.

Responder's Role

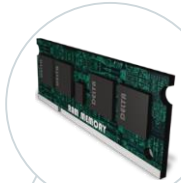
- Identify all potential electronic evidence at a crime scene

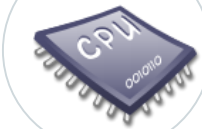
- Seize the evidence in a manner that supports the investigation and prosecution

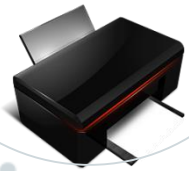
Identification of Electronic Evidence

- Electronic evidence evolves with advances in technology and market demand
- Training and awareness by the first responder are critical for identifying evidence

Computer Hardware







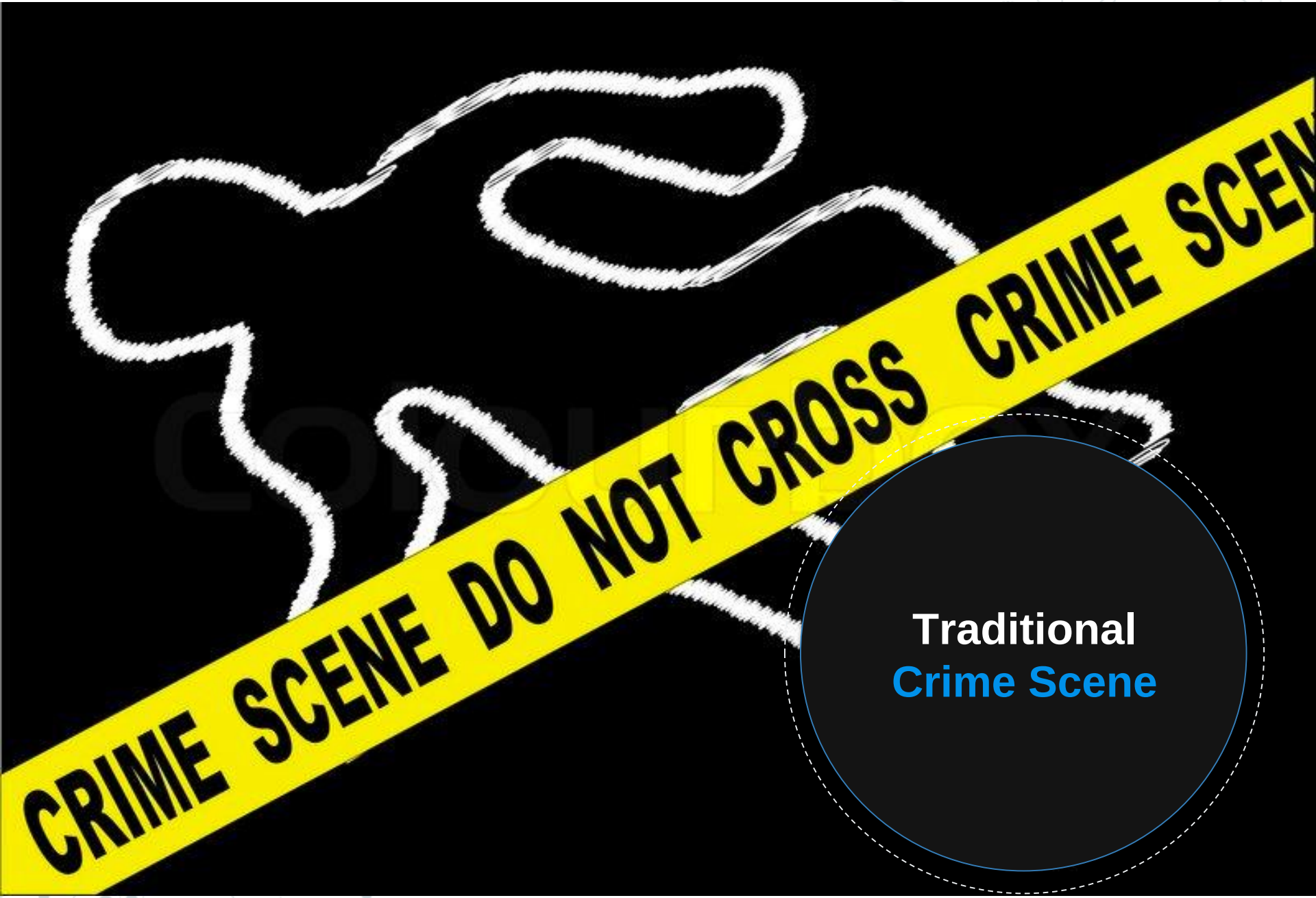
Computer Software

Where Is the Evidence?

- Digital Evidence
  - Non-volatile data
  - Volatile data

Computer Crime Scene

Preservation and Documentation

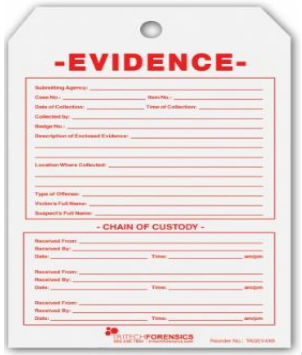

CRIME SCENE DO NOT CROSS CRIME SCEN
Traditional
Crime Scene


CRIME SCENE DO NOT CROSS
CRIME SCENE DO N
Crime Scene Training
Compose
Dashboard
Blogs
Don Perryen
Account
Upgrade
Help
Sign Out
View blog
By: Don Perryen
Rarely does a day go by that we don't come across the preface "Cyber." We hear it in conversation, on TV and radio. We see it in print. Regardless of the source, we mostly tend to think of the term as having some relation to computers and the Internet.
Cyberspace is recognized in my Word spell-checker, but cyberstudy is not. And to further cloud the issue, cyber is often used a single word, i.e. cyber crime, cyber intelligence. As time passes, what we once used as two words are now often merged into one. "Website" is now recognized as a single word in the Associated Press (AP) Style Manual (the guidebook for journalists).
Categories
Arson Investigation
Blood at Crime Scenes
CasTips
Crime Scene Investigation
Crime Scene to Courtroom
Share This Post
Facebook
DELL
Computer
Crime Scene

Documentation

- The first responder must document all steps taken on the scene

- Documentation:
  - Continues through the investigation
  - Does not stop until case completion



Windows Task Manager

File Options View Help

Processes | Performance | App History | Startup | Users | Details | Services

Process	Status	1% CPU	37% Memory	0% Disk	0% Network
Applications (4)					
Internet Explorer		0%	125.8 MB	0 MB/s	0 Mbps
Microsoft Word (32 bit)		0.3%	71.6 MB	0 MB/s	0 Mbps
Paint		0%	14.6 MB	0 MB/s	0 Mbps
Windows Task Manager		1.2%	13.3 MB	0 MB/s	0 Mbps
Background processes (10)					
Fast User Switching Utility Service		0%	0.5 MB	0 MB/s	0 Mbps
Media Catalog Object (32 bit)		0%		MB/s	0 Mbps
Microsoft Windows Search Indexer					0 Mbps
Print driver host for applications					Mbps
SMSvcHost.exe					
SMSvcHost.exe					
SMSvcHost.exe					
Spooler SubSystem App					
Windows processes (28)					
Client Server Runtime Process					
Client Server Runtime Process					Mbps
Desktop Window Manager					0 Mbps

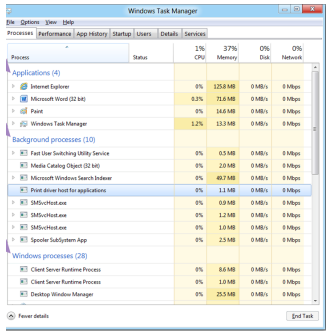
Fewer details

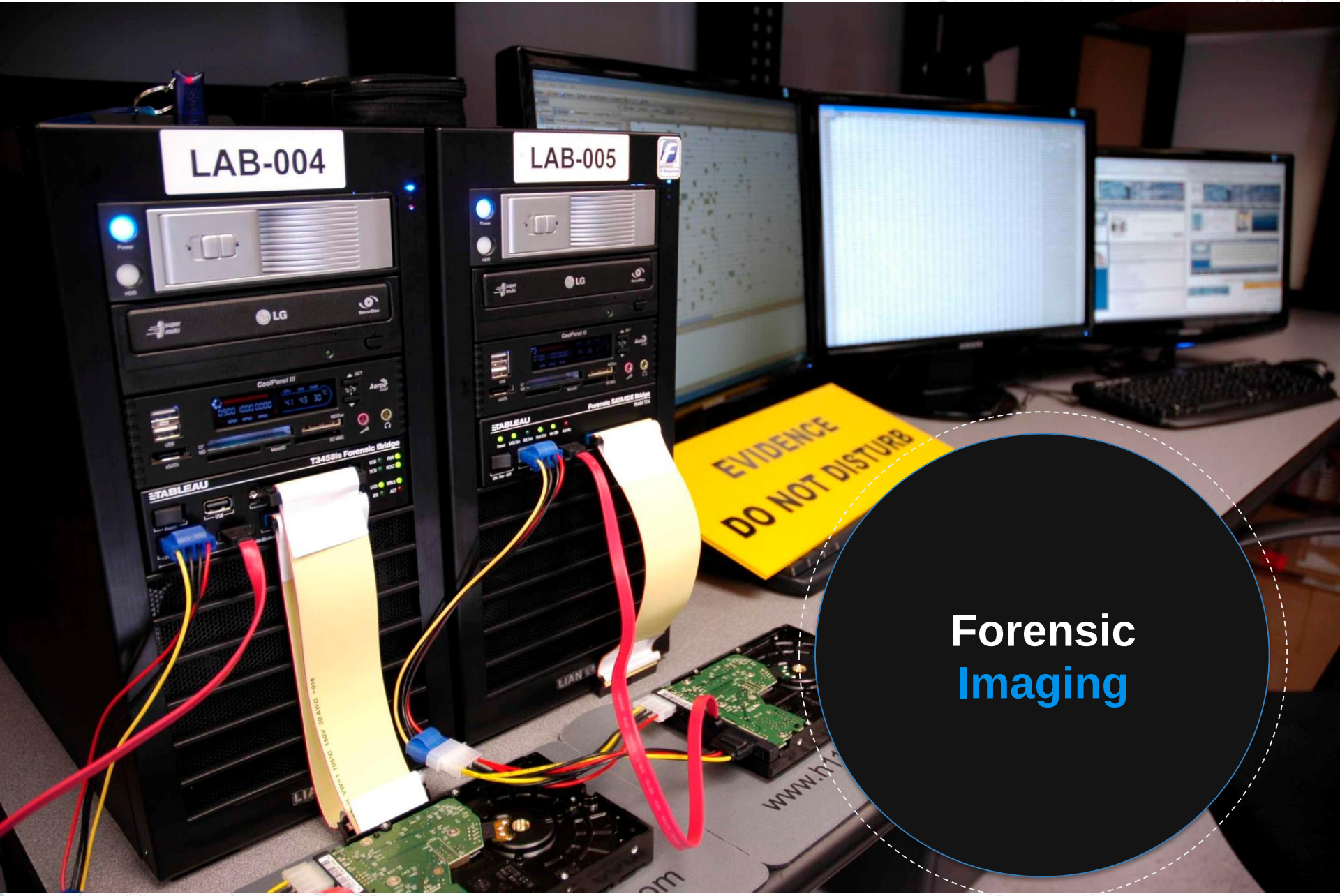
End Task

Collection of
Volatile Data

Collect Volatile Data

- Resides in temporary storage media and is lost when power is removed
- Could contain evidence of actions occurring on the system at the exact time of seizure
- Must be collected quickly at the crime scene using validated tools and proper procedures




LAB-004
LAB-005
EVIDENCE
DO NOT DISTURB
Forensic
Imaging

Forensic Imaging

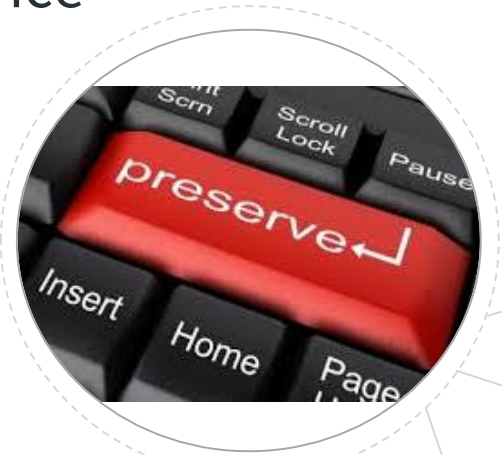
- Non-volatile data resides in persistent storage media
- The first responder must understand legal and technical boundaries
  - Can you legally obtain a forensic copy of source media?
  - Does obtaining a forensic image make sense?
  - If so…which kind? Logical or physical?
  - Do you have the tools to properly obtain the image?

Process Physical Evidence

- Execute “bag and tag” procedures to transport seized items
  - Computer hardware
  - Collected software
    - Volatile data
    - Triage data
    - Forensic Images collected on-scene

Troubleshooting

- The first responder must:
  - Have problem solving skills and patience
  - Consider:
    - How to collect physical/digital evidence
    - The benefit of using a specific tool or technique
    - How to avoid contaminating evidence



Summary

- The proper collection of physical/digital evidence is one of the most important aspects of the digital forensics process

- If this collection is not done correctly, critical evidence can be lost

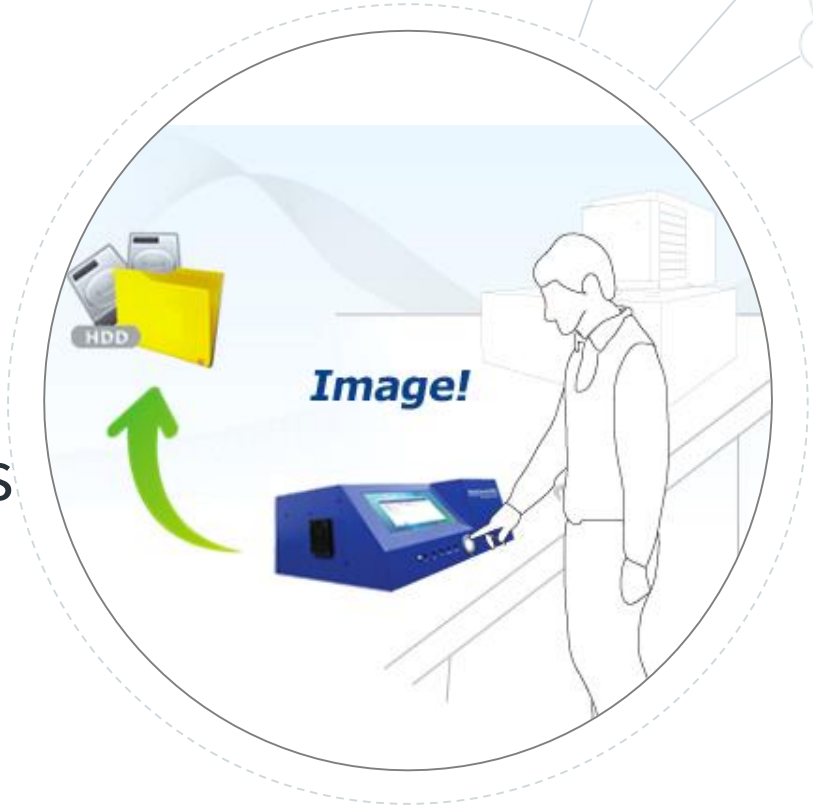
Thanks!

Any questions?

Imaging: Forensic Acquisition of Digital Evidence

Objective

- By the end of this module, participants will be able to create a forensically sound image of digital media consistent with industry best practices

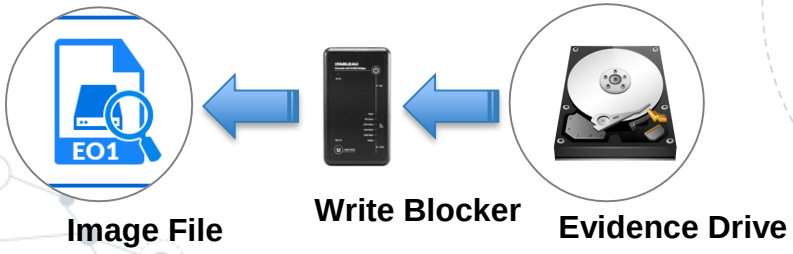


Digital Forensic Process

- Imaging is the second phase and requires forensically-sound procedures and validated tools

Digital Forensic Image Acquisition

- Forensic image is:
  - A verifiable duplicate of all the contents of a storage media or selected files in a form of encapsulated file.
  - Acquired by trained digital forensic examiner using validated hardware and software tools



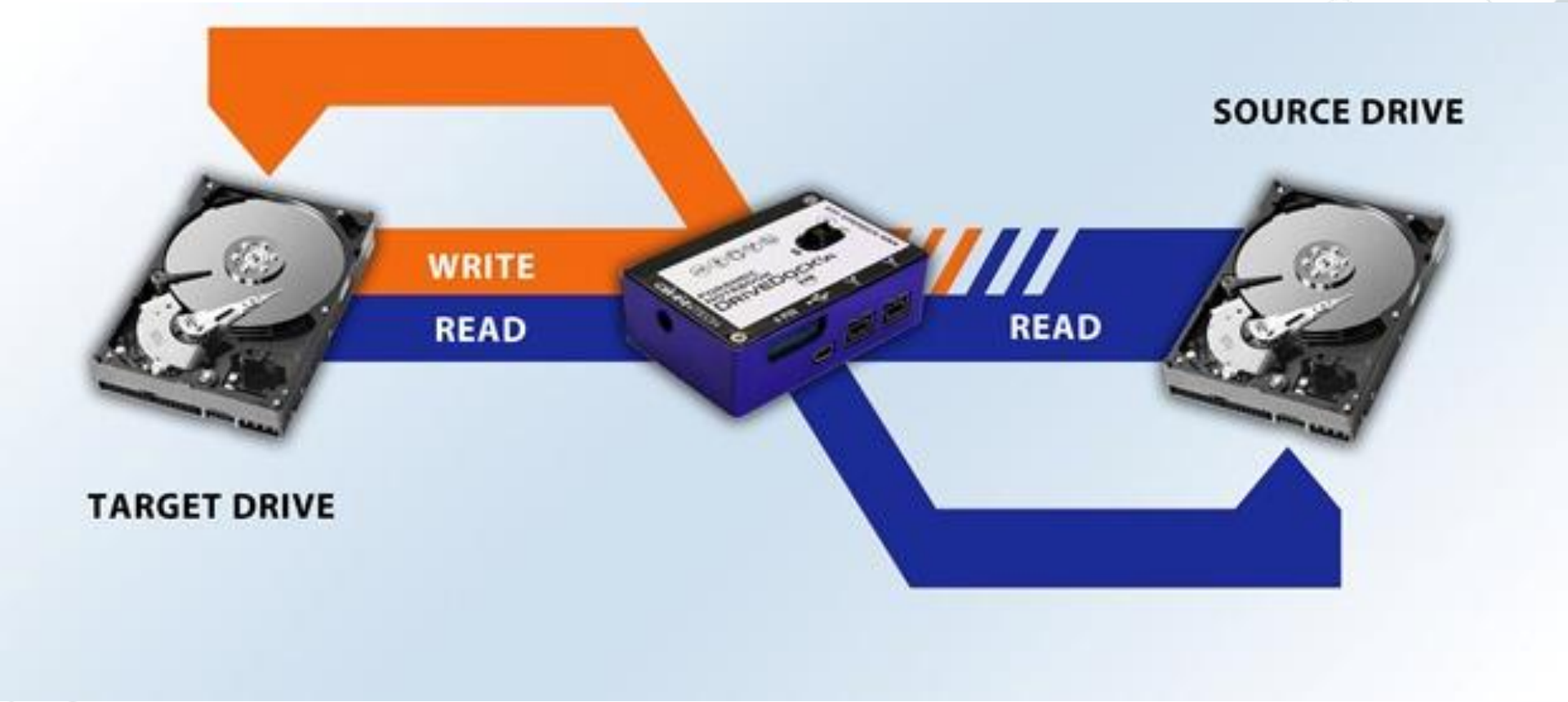
Hardware-based Imaging Tools

- Write blocker (physical bridge)
- Stand-alone imaging device (multifunction tool with dedicated forensic capabilities)

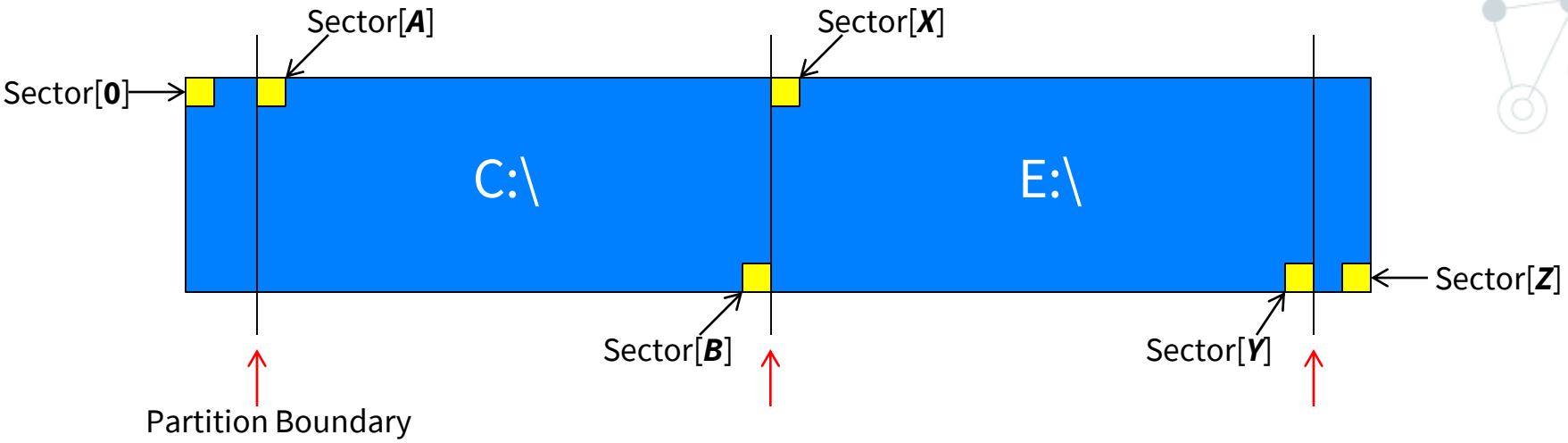
Software-based Imaging Tools

- Write-blocker: Specialized application
- Forensic Imager: Multi-function tools that assist with hard drive preparation and duplication, forensic imaging, and verification

Imaging Tools Concept



Imaging a Hard Disk Drive



You can also split your content

Sector [0] → Sector [Z]

Physical image:

A forensic copy of every addressable sector from source media

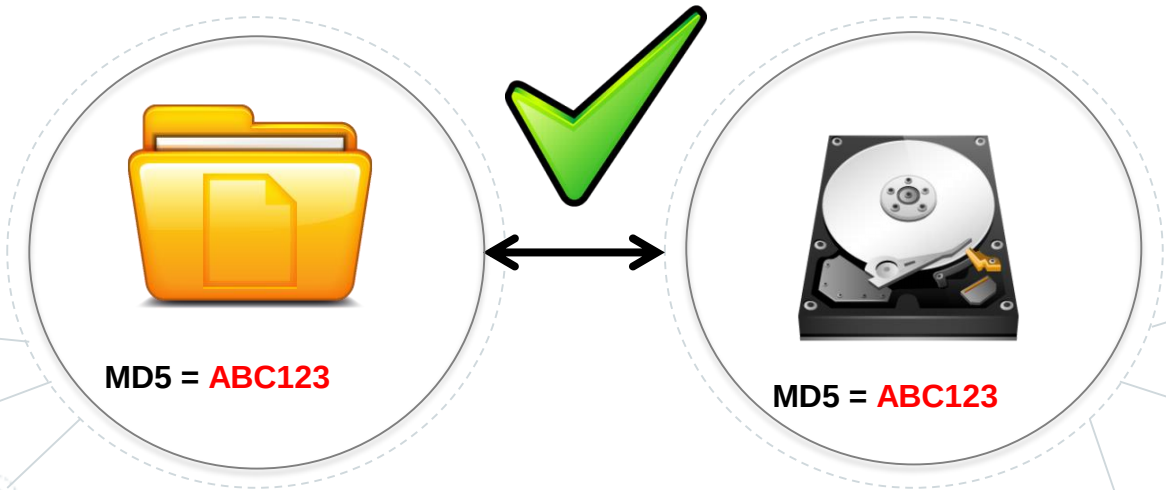
Sector [A] → Sector [B]

Logical image:

A forensic copy of every addressable sector between two partition boundaries

Verification of Forensic Image

- Hash:
  - Is a mathematical algorithm
  - Produces a unique digital fingerprint
  - Verifies that binary content of an acquired forensic image is exactly the same as the source media



Preparation of Destination Storage Media

- Verify size requirements of original evidence
- Select storage media that meets or exceeds capacity of source
- Sterilize destination media
- Format storage media

Summary

- Forensic Imaging of digital evidence is one of the important phase of digital forensic process to preserve and ensure the integrity of the evidence
- Digital forensic examiner must follow established forensic procedures when acquiring digital evidence from source media

Thanks!

Any questions?

Overview: Digital Forensic Tools

Objective

- By the end of this module, participants will be able to use basic features of a forensic tool to examine digital evidence

Software: Digital Forensic Tool

- Enables searches within image files
- Streamlines investigations
- Includes:
  - **EnCase** by Guidance Software
  - **Forensic Toolkit (FTK)** by Access Data
  - **Autopsy** Open Source

EnCase Forensic

ACCESSDATA FTK FORENSIC TOOLKIT

EnCase

Guidance Software

Introduction to EnCase

- Digital data acquisition tool that enables:
  - Email and file system analysis
  - Remote imaging and investigations
  - Advanced searches
  - Remote previewing
  - Malicious code discovery

- Step Action, you will work individually to:
  - Install and configure EnCase
  - Examine evidence files
  - Sort files
  - Create bookmarks
  - Generate report

Forensic Tool Kit (FTK)

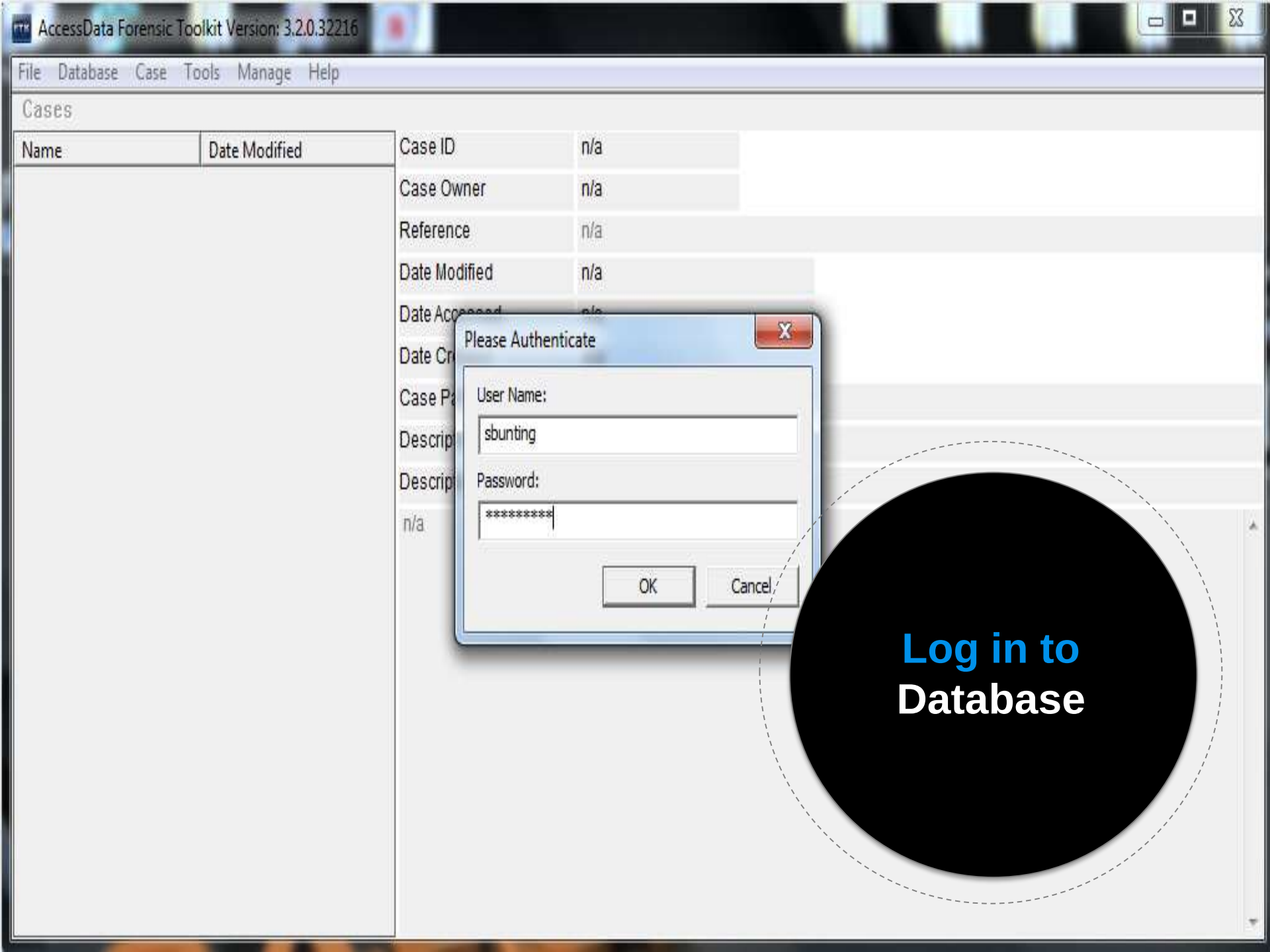
Access Data

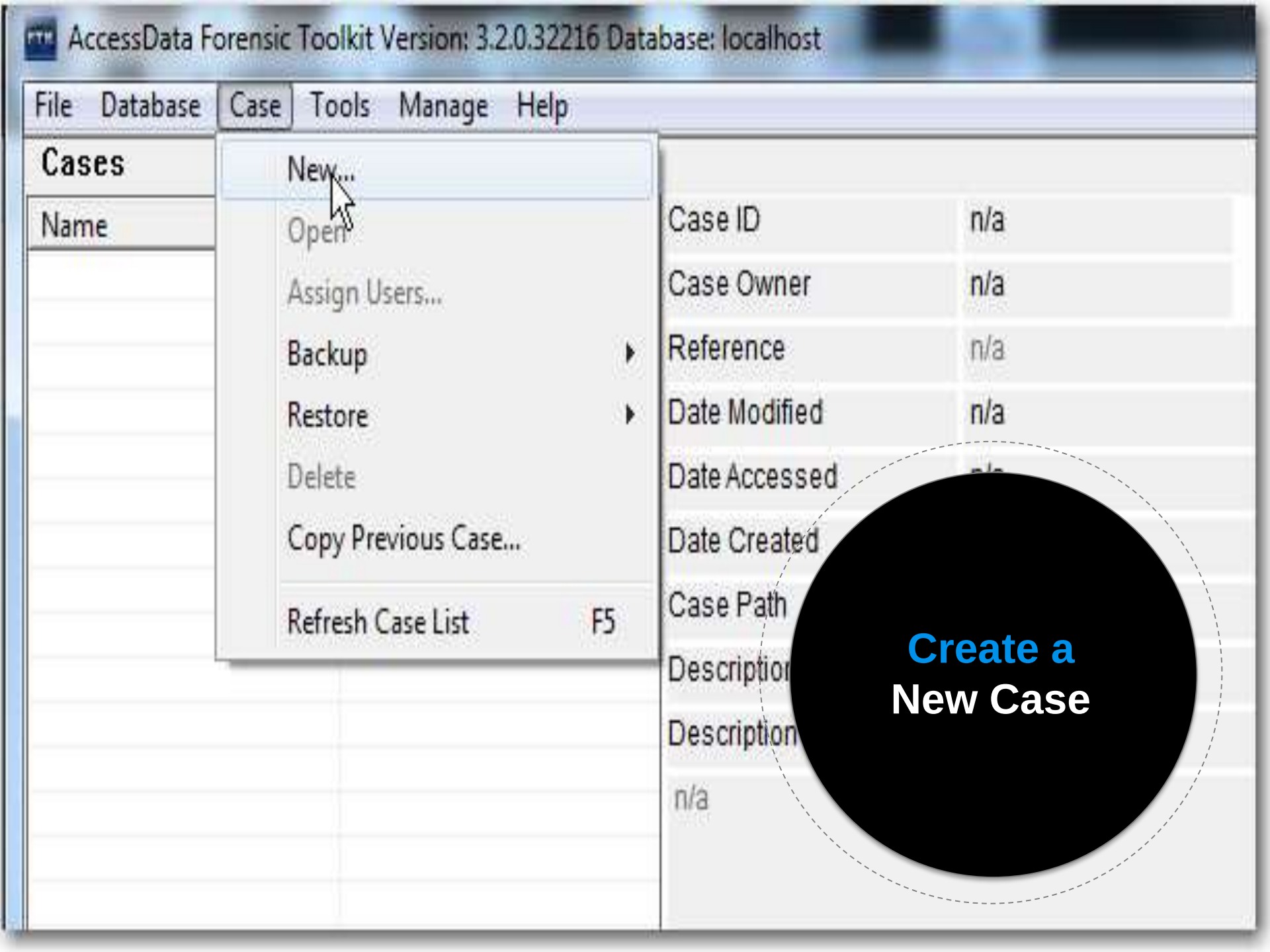
Introduction to FTK

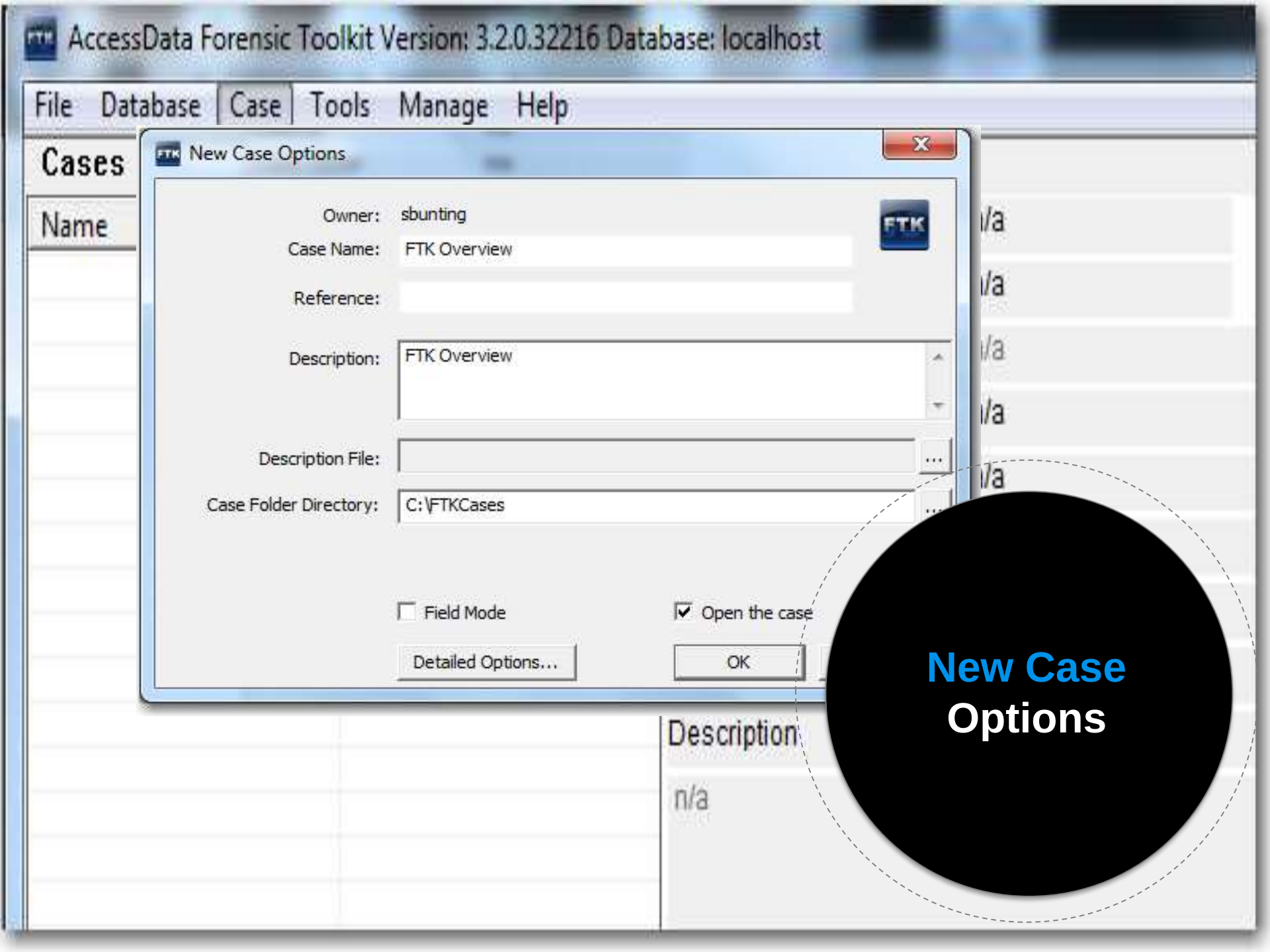
- Digital data acquisition tool that:
  - Is similar to EnCase in overall features
  - Uses a different approach to data storage and terminology

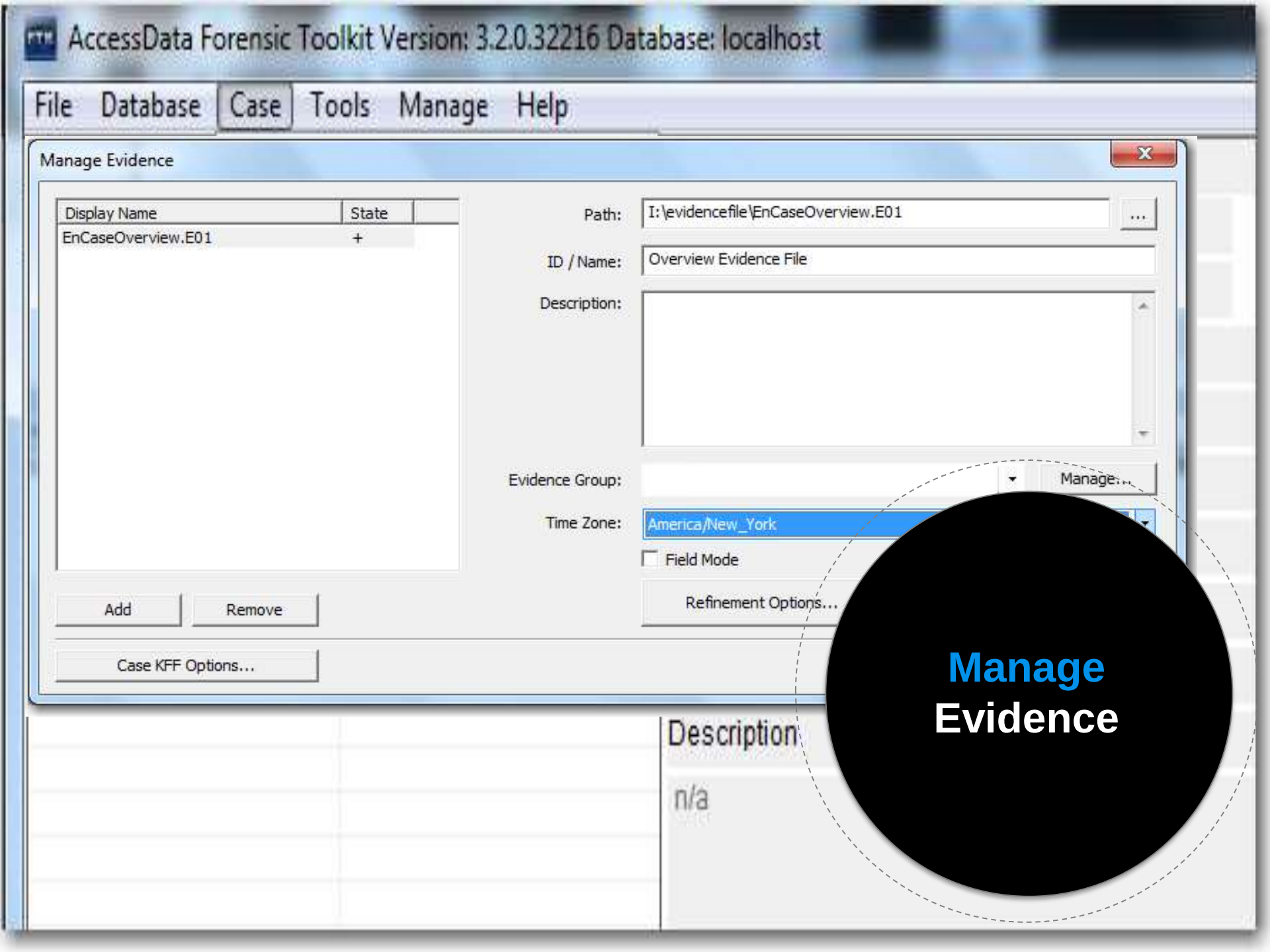
Introduction to FTK

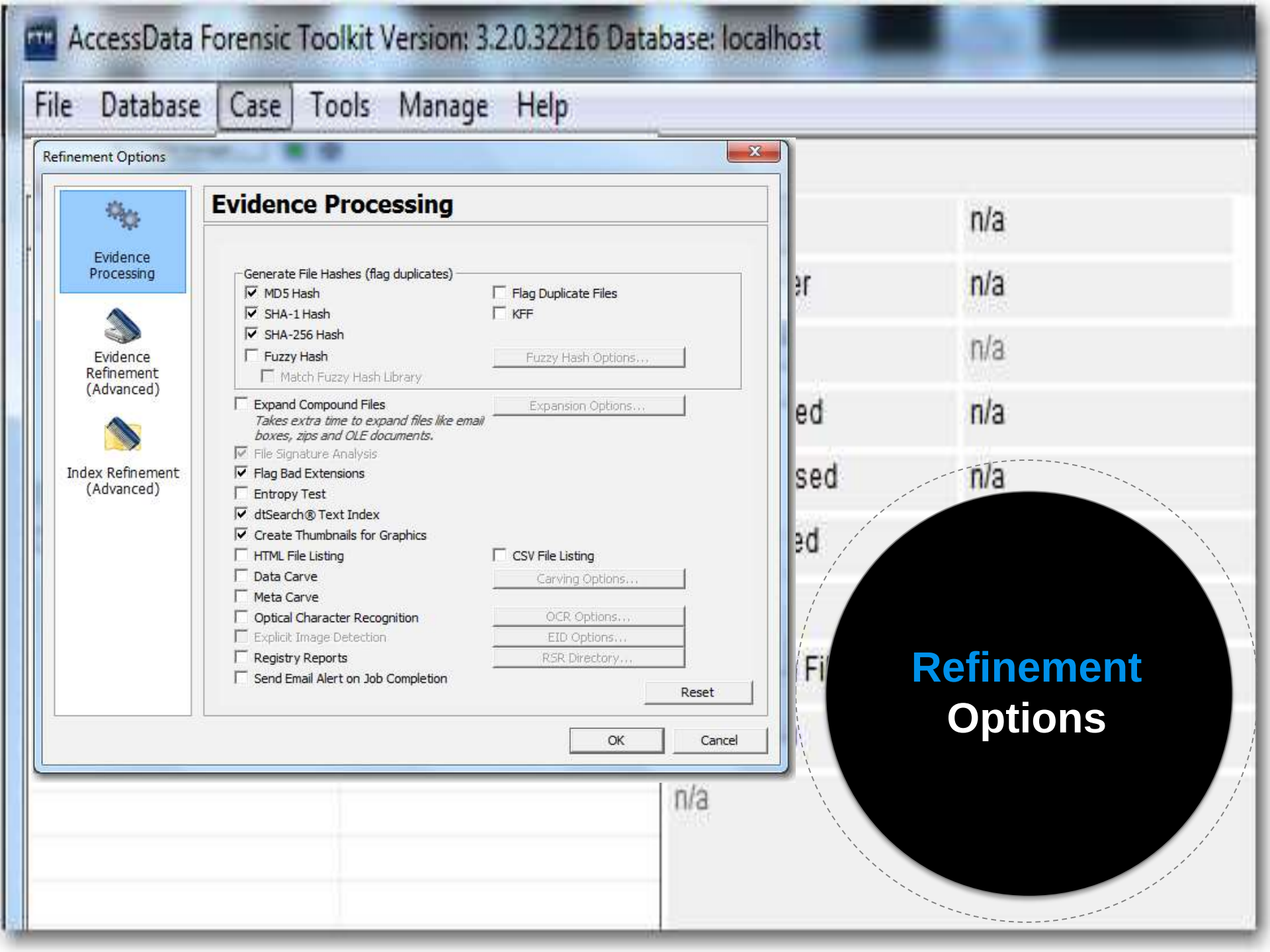
- The facilitators will demonstrate how to
  - Log in to the database
  - Create a new case
  - Manage evidence
  - Refine results
  - Generate a report

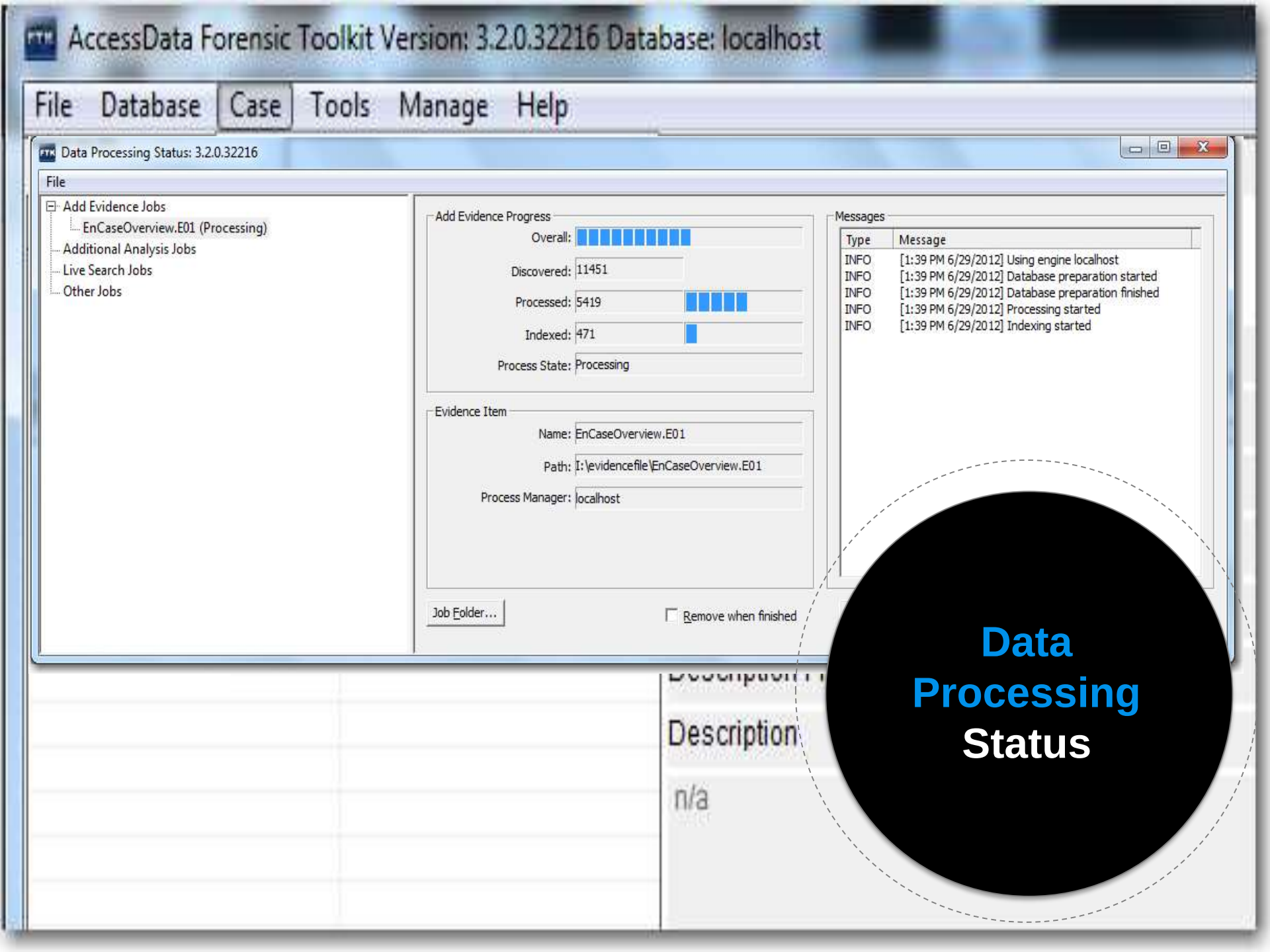

AccessData Forensic Toolkit Version: 3.2.0.32216
File Database Case Tools Manage Help
Cases
Name
Date Modified
Case ID
n/a
Case Owner
n/a
Reference
n/a
Date Modified
n/a
Please Authenticate
User Name:
sbunting
Password:
OK
Cancel
Log in to
Database

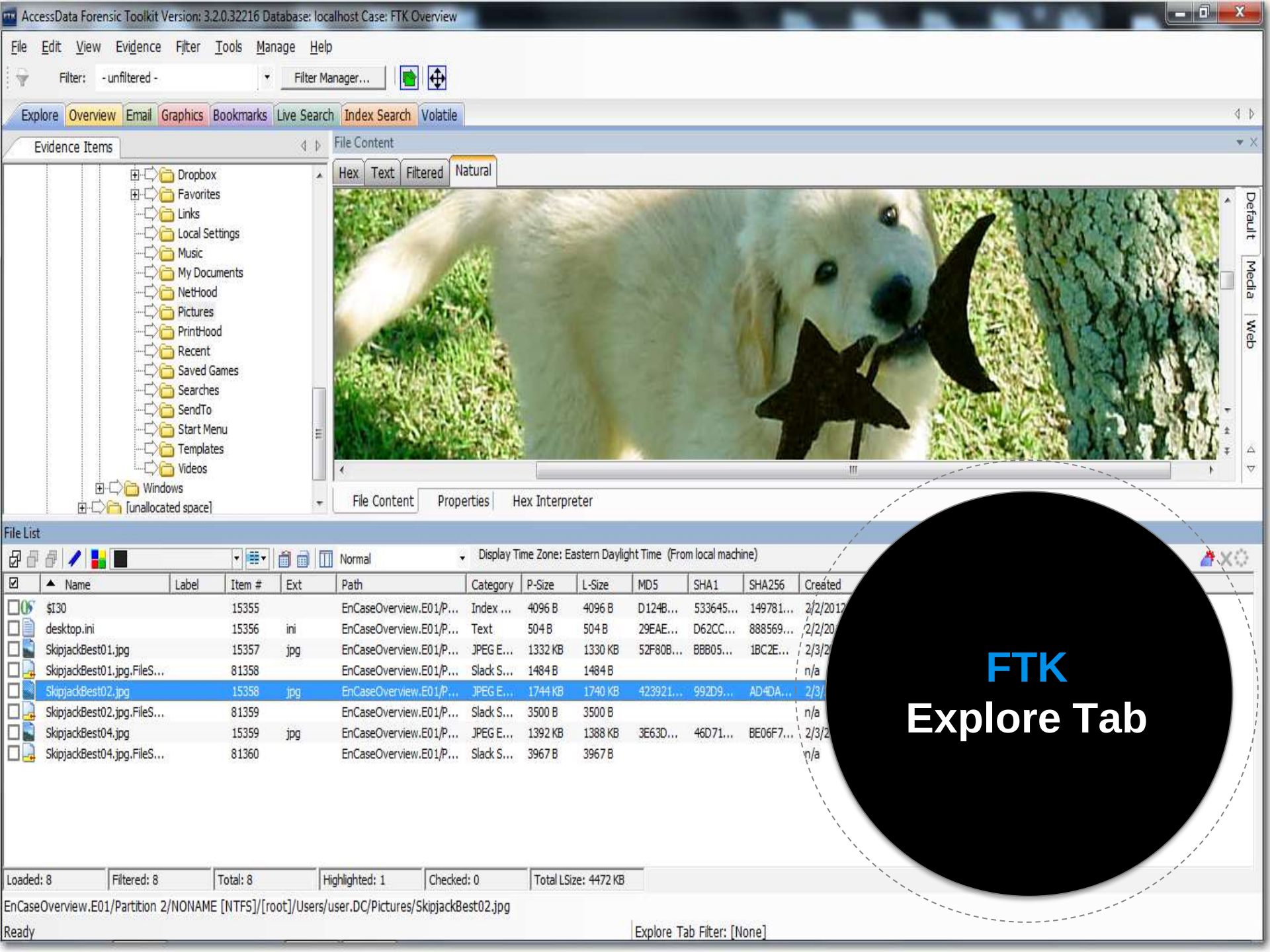

AccessData Forensic Toolkit Version: 3.2.0.32216 Database: localhost
File
Database
Case
Tools
Manage
Help
Cases
Name
New...
Open
Assign Users...
Backup
Restore
Delete
Copy Previous Case...
Refresh Case List
F5
Case ID
n/a
Case Owner
n/a
Reference
n/a
Date Modified
n/a
Date Accessed
Date Created
Case Path
Description
Description
n/a
Create a
New Case

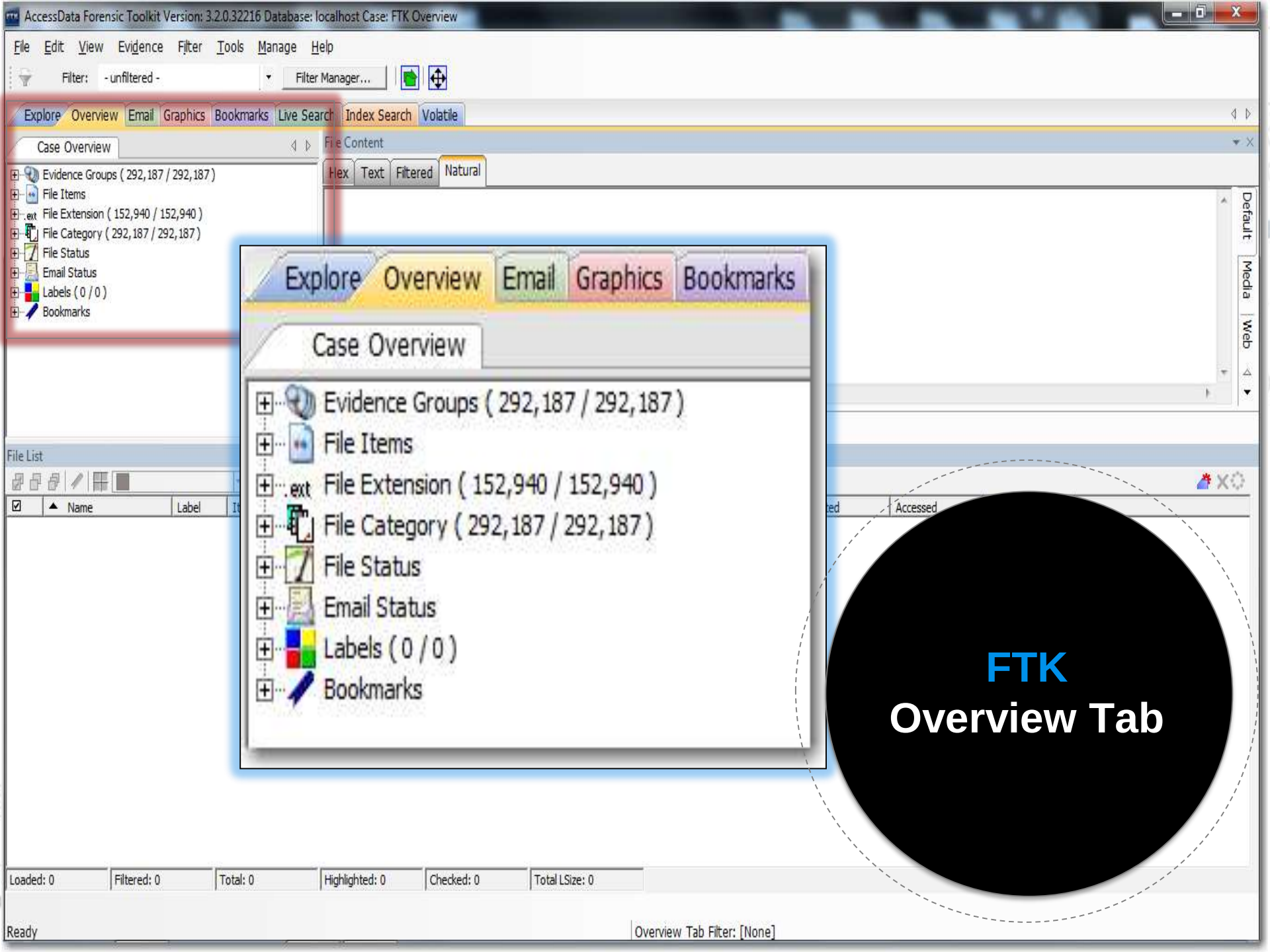

AccessData Forensic Toolkit Version: 3.2.0.32216 Database: localhost
File
Database
Case
Tools
Manage
Help
Cases
Name
New Case Options
Owner:
sbunting
Case Name:
FTK Overview
Reference:
Description:
FTK Overview
Description File:
Case Folder Directory:
C:\FTKCases
Field Mode
Open the case
Detailed Options...
OK
Description
n/a
New Case
Options

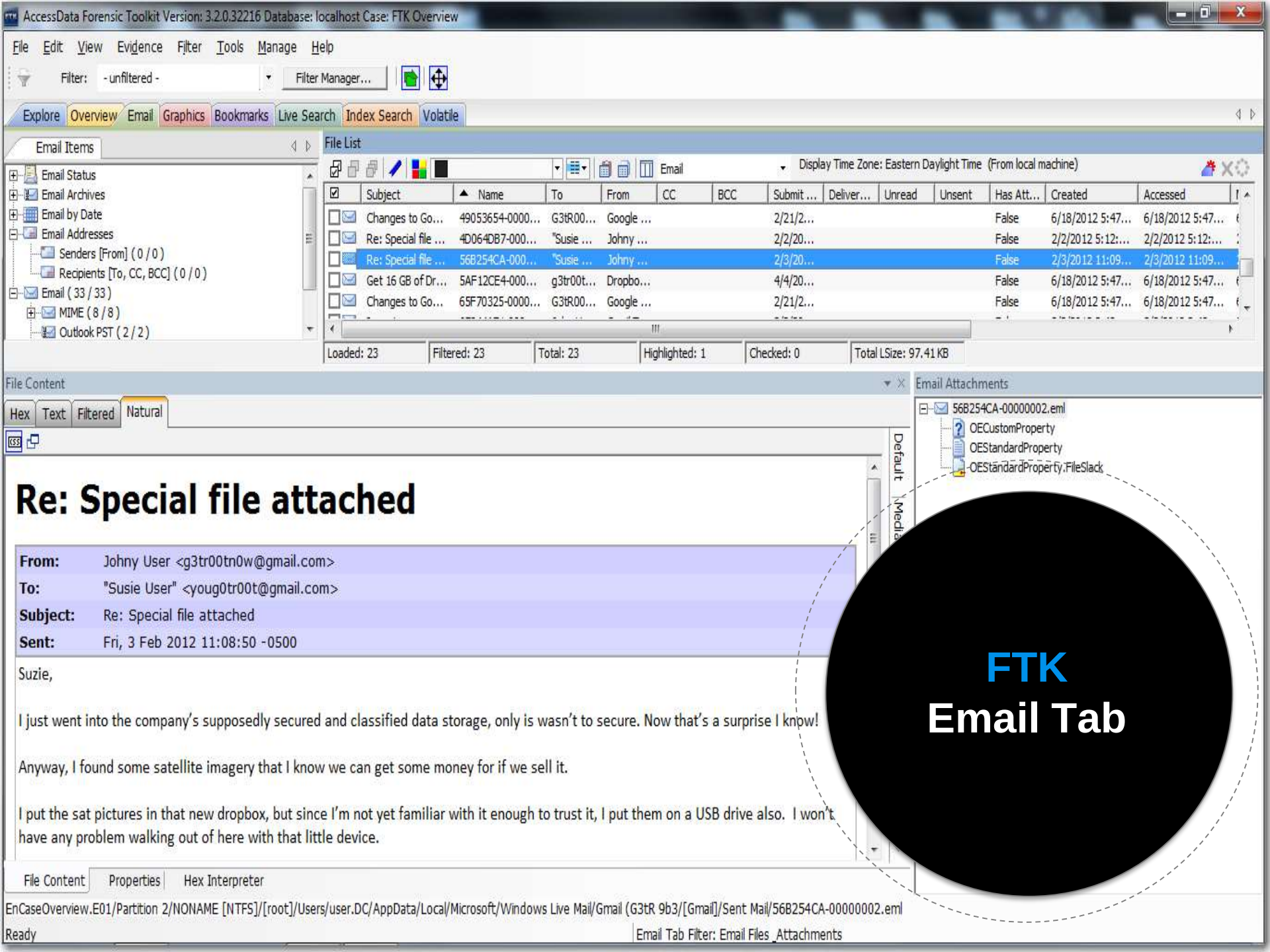

AccessData Forensic Toolkit Version: 3.2.0.32216 Database: localhost
File
Database
Case
Tools
Manage
Help
Manage Evidence
Display Name
State
EnCaseOverview.E01
+
Path:
I:\evidencefile\EnCaseOverview.E01
...
ID / Name:
Overview Evidence File
Description:
Evidence Group:
Manage...
Time Zone:
America/New_York
Field Mode
Add
Remove
Refinement Options...
Case KFF Options...
Description
n/a
Manage
Evidence

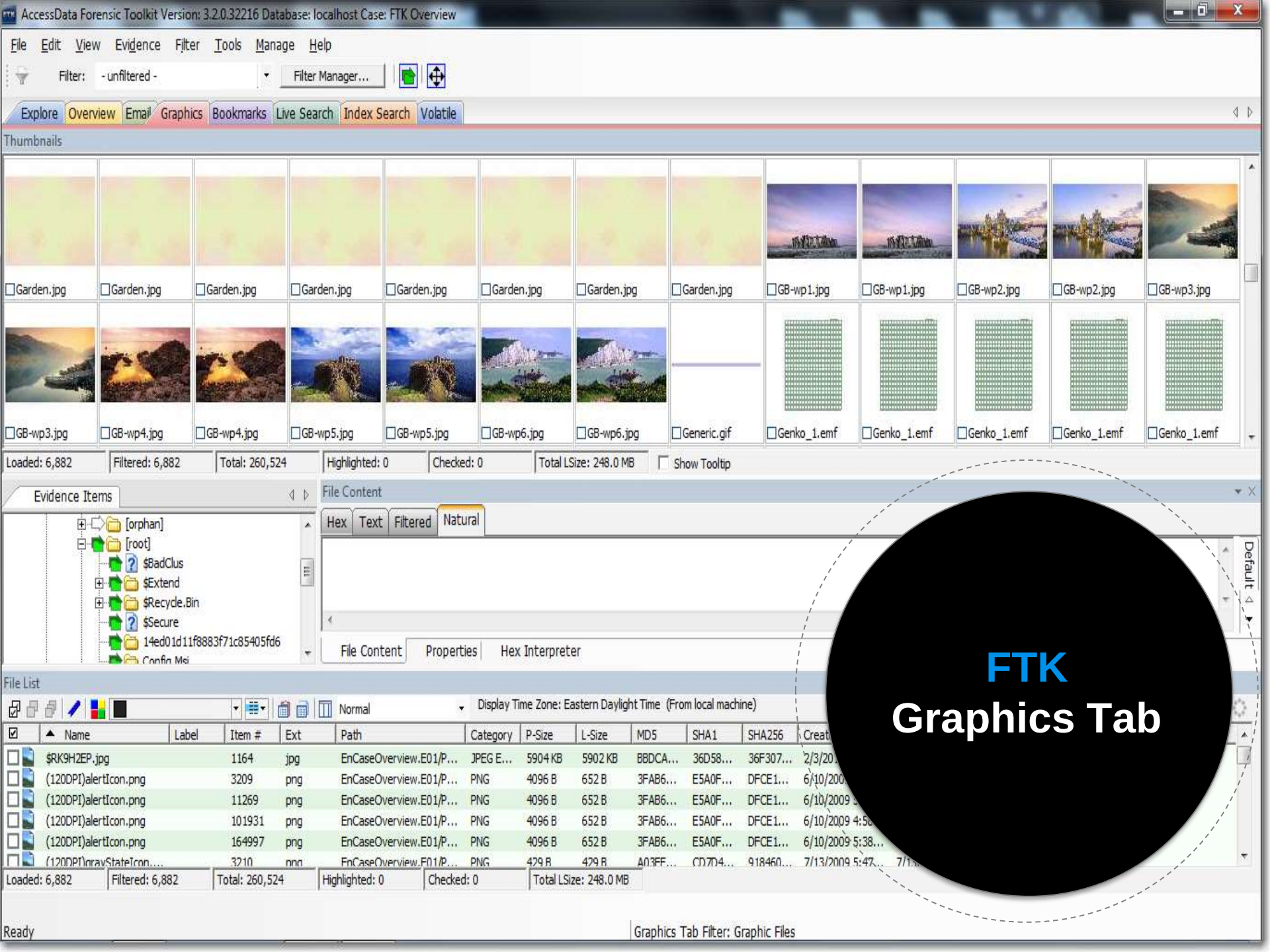

AccessData Forensic Toolkit Version: 3.2.0.32216 Database: localhost
File
Database
Case
Tools
Manage
Help
Refinement Options
Evidence Processing
Evidence Refinement (Advanced)
Index Refinement (Advanced)
Evidence Processing
Generate File Hashes (flag duplicates)
MD5 Hash
SHA-1 Hash
SHA-256 Hash
Fuzzy Hash
Match Fuzzy Hash Library
Flag Duplicate Files
KFF
Fuzzy Hash Options...
Expand Compound Files
Takes extra time to expand files like email boxes, zips and OLE documents.
Expansion Options...
File Signature Analysis
Flag Bad Extensions
Entropy Test
dtSearch® Text Index
Create Thumbnails for Graphics
HTML File Listing
Data Carve
Meta Carve
Optical Character Recognition
Explicit Image Detection
Registry Reports
Send Email Alert on Job Completion
CSV File Listing
Carving Options...
OCR Options...
EID Options...
RSR Directory...
Reset
OK
Cancel
n/a
Refinement
Options

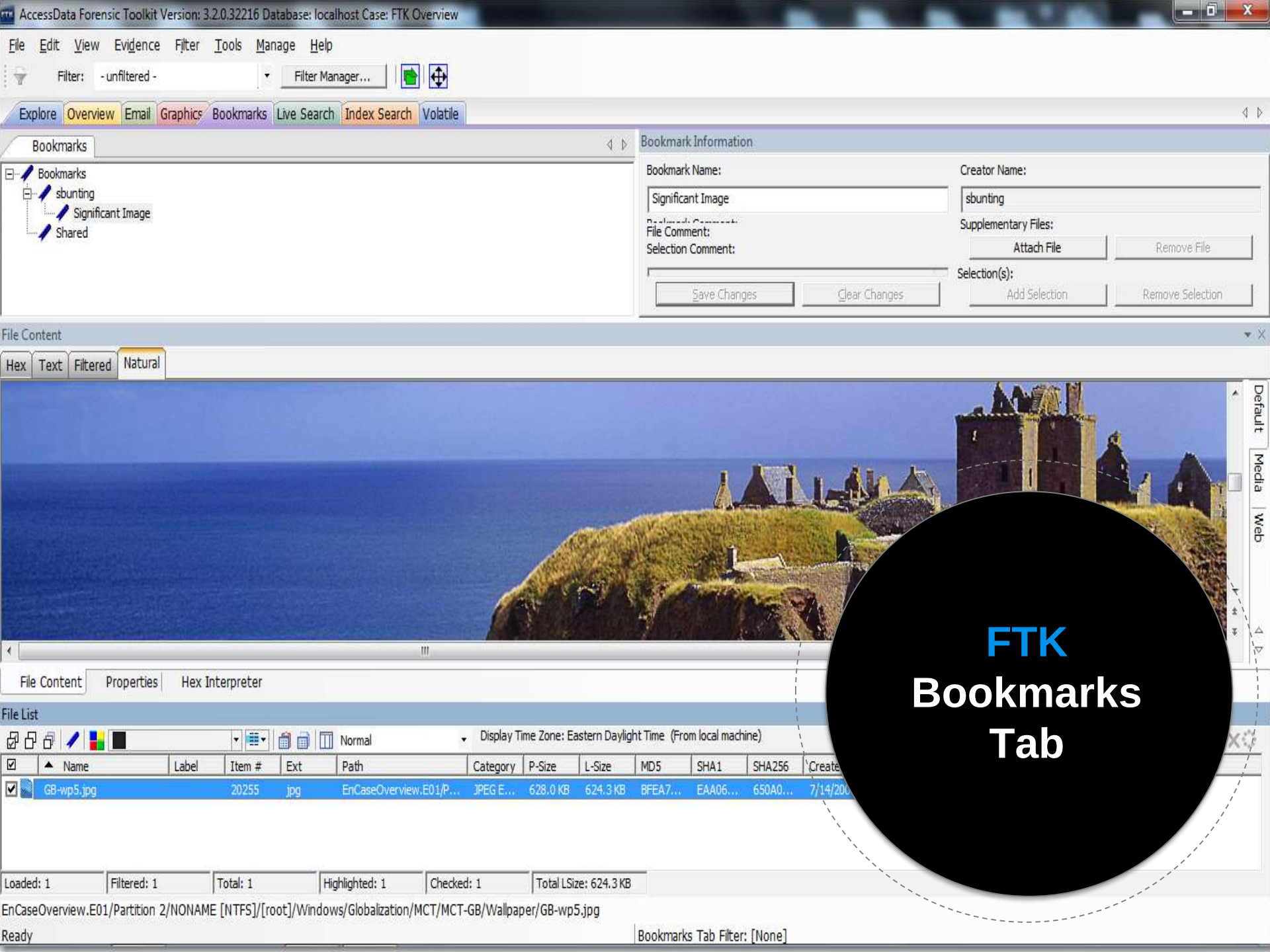

AccessData Forensic Toolkit Version: 3.2.0.32216 Database: localhost
File Database Case Tools Manage Help
Data Processing Status: 3.2.0.32216
File
Add Evidence Jobs
EnCaseOverview.E01 (Processing)
Additional Analysis Jobs
Live Search Jobs
Other Jobs
Add Evidence Progress
Overall:
Discovered: 11451
Processed: 5419
Indexed: 471
Process State: Processing
Evidence Item
Name: EnCaseOverview.E01
Path: I:\evidencefile\EnCaseOverview.E01
Process Manager: localhost
Messages
Type Message
INFO [1:39 PM 6/29/2012] Using engine localhost
INFO [1:39 PM 6/29/2012] Database preparation started
INFO [1:39 PM 6/29/2012] Database preparation finished
INFO [1:39 PM 6/29/2012] Processing started
INFO [1:39 PM 6/29/2012] Indexing started
Job Folder...
Remove when finished
Description
n/a
Data Processing Status

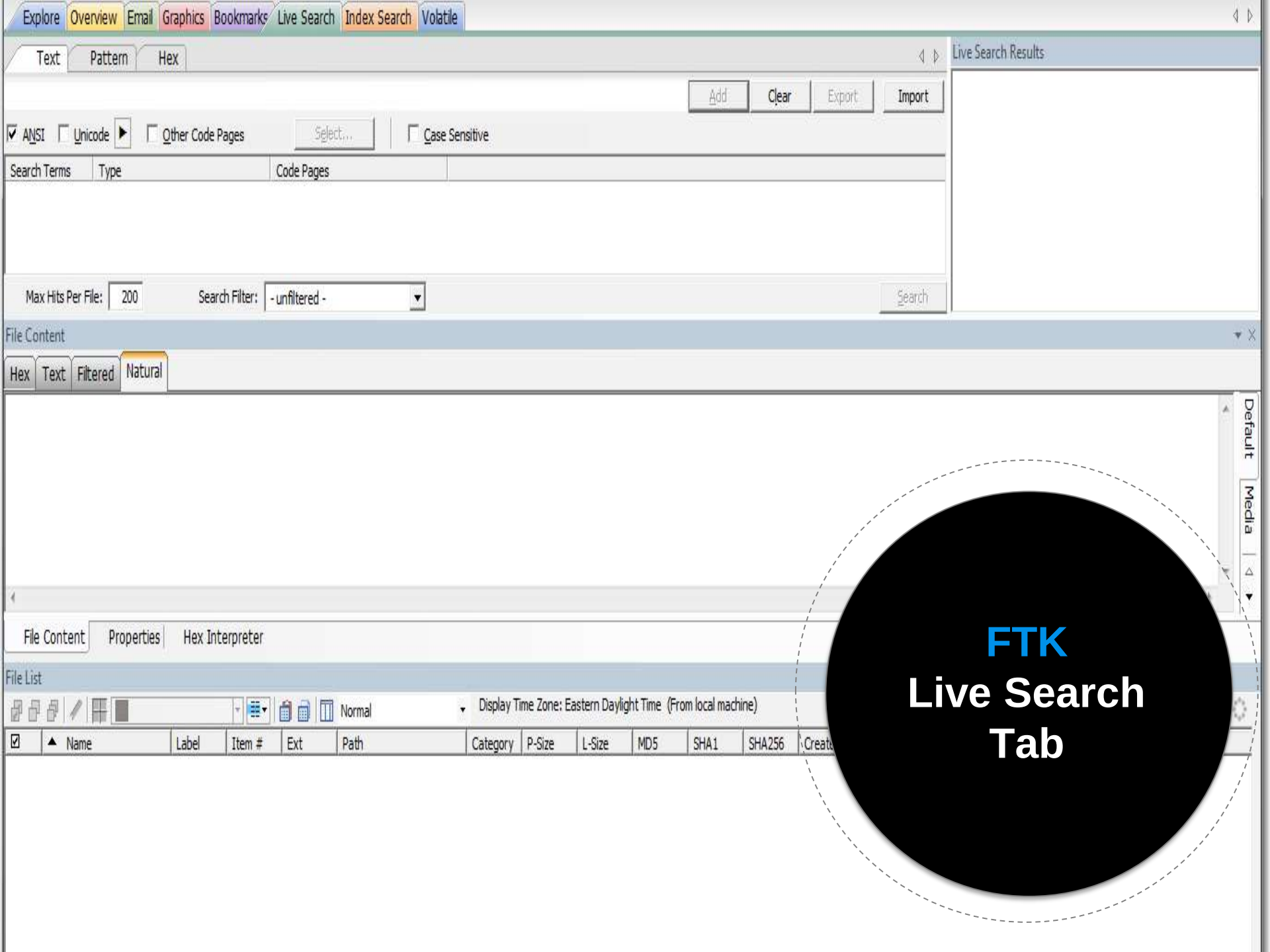

AccessData Forensic Toolkit Version: 3.2.0.32216 Database: localhost Case: FTK Overview
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered - Filter Manager...
Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile
Evidence Items
Dropbox
Favorites
Links
Local Settings
Music
My Documents
NetHood
Pictures
PrintHood
Recent
Saved Games
Searches
SendTo
Start Menu
Templates
Videos
Windows
[unallocated space]
File Content
Hex Text Filtered Natural
Default Media Web
File Content Properties Hex Interpreter
File List
Normal
Display Time Zone: Eastern Daylight Time (From local machine)
Name Label Item # Ext Path Category P-Size L-Size MD5 SHA1 SHA256 Created
$I30 15355 EnCaseOverview.E01/P... Index ... 4096 B 4096 B D124B... 533645... 149781... 2/2/2012
desktop.ini 15356 ini EnCaseOverview.E01/P... Text 504 B 504 B 29EAE... D62CC... 888569... 2/2/20
SkipjackBest01.jpg 15357 jpg EnCaseOverview.E01/P... JPEG E... 1332 KB 1330 KB 52F80B... BBB05... 1BC2E... 2/3/2
SkipjackBest01.jpg.FileS... 81358 EnCaseOverview.E01/P... Slack S... 1484 B 1484 B n/a
SkipjackBest02.jpg 15358 jpg EnCaseOverview.E01/P... JPEG E... 1744 KB 1740 KB 423921... 992D9... AD4DA... 2/3/
SkipjackBest02.jpg.FileS... 81359 EnCaseOverview.E01/P... Slack S... 3500 B 3500 B n/a
SkipjackBest04.jpg 15359 jpg EnCaseOverview.E01/P... JPEG E... 1392 KB 1388 KB 3E63D... 46D71... BE06F7... 2/3/2
SkipjackBest04.jpg.FileS... 81360 EnCaseOverview.E01/P... Slack S... 3967 B 3967 B n/a
Loaded: 8 Filtered: 8 Total: 8 Highlighted: 1 Checked: 0 Total LSize: 4472 KB
EnCaseOverview.E01/Partition 2/NONAME [NTFS]/[root]/Users/user.DC/Pictures/SkipjackBest02.jpg
Ready
Explore Tab Filter: [None]
FTK
Explore Tab

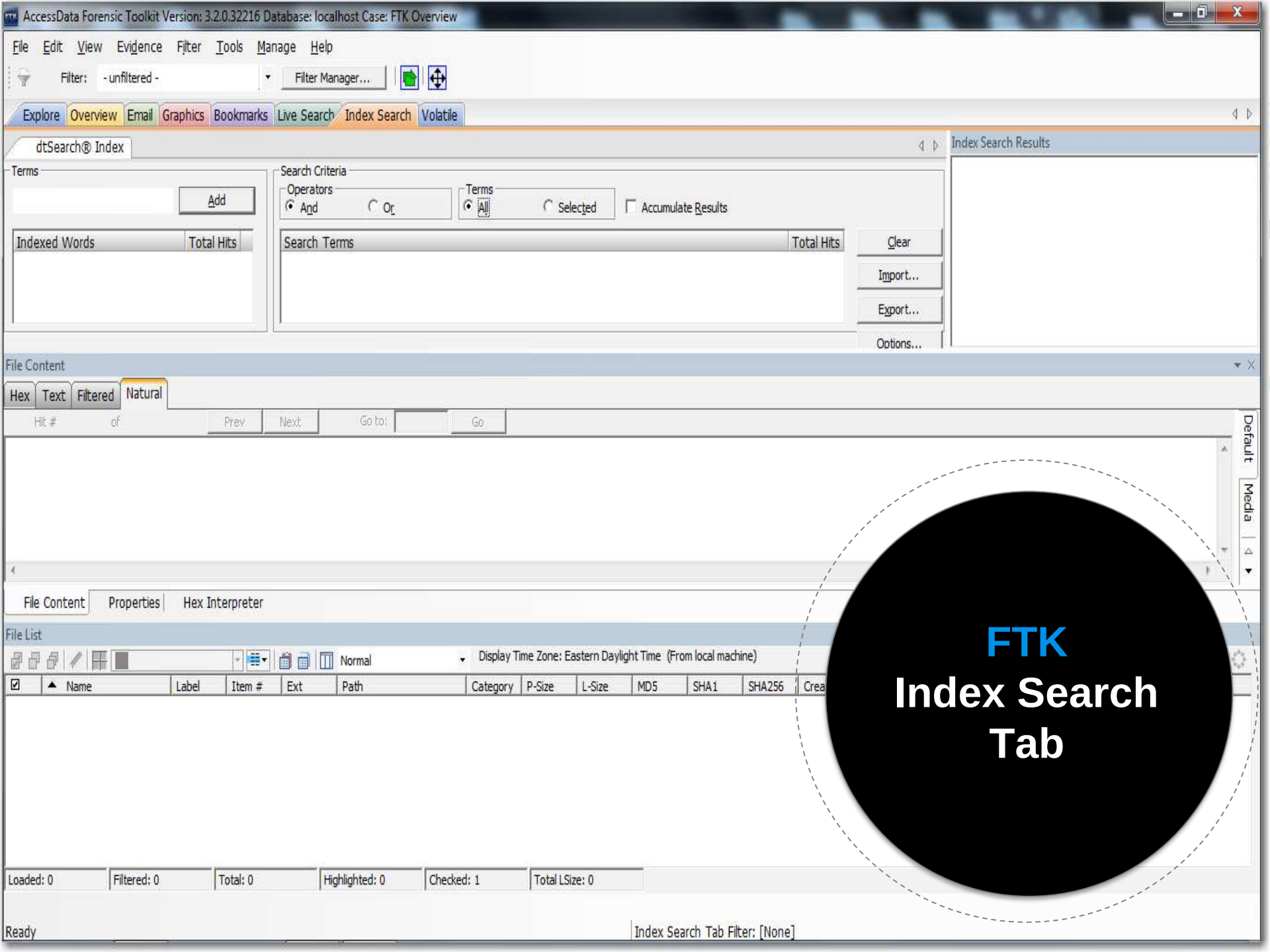

AccessData Forensic Toolkit Version: 3.2.0.32216 Database: localhost Case: FTK Overview
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered - Filter Manager...
Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile
Case Overview
Evidence Groups (292,187 / 292,187)
File Items
File Extension (152,940 / 152,940)
File Category (292,187 / 292,187)
File Status
Email Status
Labels (0 / 0)
Bookmarks
File Content
Hex Text Filtered Natural
Default Media Web
File List
Name Label
Accessed
Loaded: 0 Filtered: 0 Total: 0 Highlighted: 0 Checked: 0 Total LSize: 0
Ready
Overview Tab Filter: [None]
FTK
Overview Tab

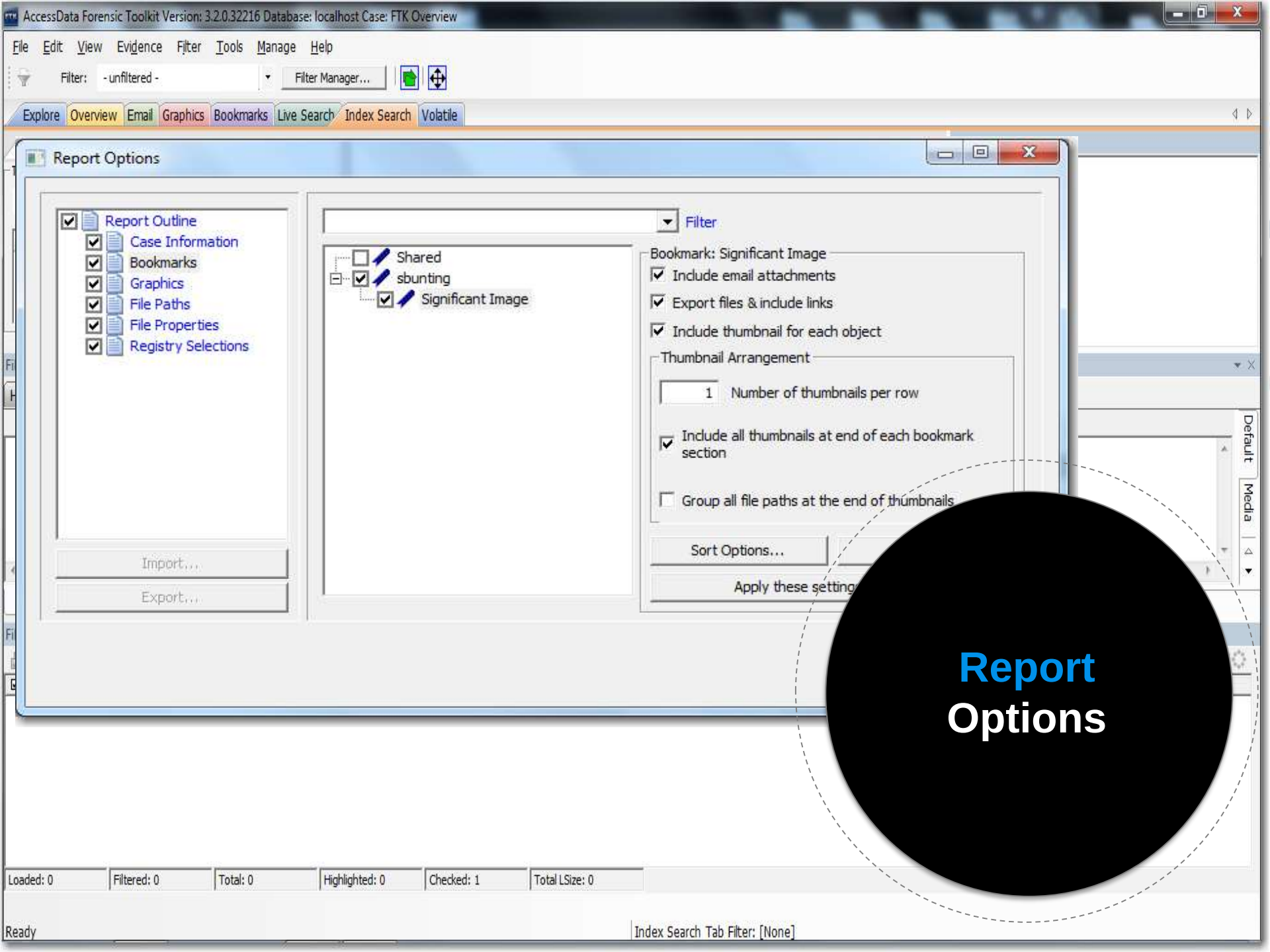

AccessData Forensic Toolkit Version: 3.2.0.32216 Database: localhost Case: FTK Overview
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered - Filter Manager...
Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile
Email Items
Email Status
Email Archives
Email by Date
Email Addresses
Senders [From] (0 / 0)
Recipients [To, CC, BCC] (0 / 0)
Email (33 / 33)
MIME (8 / 8)
Outlook PST (2 / 2)
File List
Email
Display Time Zone: Eastern Daylight Time (From local machine)
Subject Name To From CC BCC Submit ... Deliver... Unread Unsent Has Att... Created Accessed
Changes to Go... 49053654-0000... G3tR00... Google ... 2/21/2... False 6/18/2012 5:47... 6/18/2012 5:47...
Re: Special file ... 4D064DB7-000... "Susie ... Johny ... 2/2/20... False 2/2/2012 5:12:... 2/2/2012 5:12:...
Re: Special file ... 56B254CA-000... "Susie ... Johny ... 2/3/20... False 2/3/2012 11:09... 2/3/2012 11:09...
Get 16 GB of Dr... 5AF12CE4-000... g3tr00t... Dropbo... 4/4/20... False 6/18/2012 5:47... 6/18/2012 5:47...
Changes to Go... 65F70325-0000... G3tR00... Google ... 2/21/2... False 6/18/2012 5:47... 6/18/2012 5:47...
Loaded: 23 Filtered: 23 Total: 23 Highlighted: 1 Checked: 0 Total LSize: 97.41 KB
File Content
Hex Text Filtered Natural
Default
Media
Re: Special file attached
From: Johny User <g3tr00tn0w@gmail.com>
To: "Susie User" <youg0tr00t@gmail.com>
Subject: Re: Special file attached
Sent: Fri, 3 Feb 2012 11:08:50 -0500
Suzie,
I just went into the company's supposedly secured and classified data storage, only is wasn't to secure. Now that's a surprise I know!
Anyway, I found some satellite imagery that I know we can get some money for if we sell it.
I put the sat pictures in that new dropbox, but since I'm not yet familiar with it enough to trust it, I put them on a USB drive also. I won't have any problem walking out of here with that little device.
Email Attachments
56B254CA-00000002.eml
OECustomProperty
OEStandardProperty
OEStandardProperty.FileSlack
File Content Properties Hex Interpreter
EnCaseOverview.E01/Partition 2/NONAME [NTFS]/[root]/Users/user.DC/AppData/Local/Microsoft/Windows Live Mail/Gmail (G3tR 9b3/[Gmail]/Sent Mail/56B254CA-00000002.eml
Ready
Email Tab Filter: Email Files _Attachments
FTK
Email Tab


AccessData Forensic Toolkit Version: 3.2.0.32216 Database: localhost Case: FTK Overview
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered - Filter Manager...
Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile
Thumbnails
Garden.jpg
GB-wp1.jpg
GB-wp2.jpg
GB-wp3.jpg
GB-wp4.jpg
GB-wp5.jpg
GB-wp6.jpg
Generic.gif
Genko_1.emf
Loaded: 6,882 Filtered: 6,882 Total: 260,524 Highlighted: 0 Checked: 0 Total LSize: 248.0 MB Show Tooltip
Evidence Items
[orphan]
[root]
$BadClus
$Extend
$Recycle.Bin
$Secure
14ed01d11f8883f71c85405fd6
File Content
Hex Text Filtered Natural
File Content Properties Hex Interpreter
Default
File List
Normal
Display Time Zone: Eastern Daylight Time (From local machine)
Name Label Item # Ext Path Category P-Size L-Size MD5 SHA1 SHA256
$RK9H2EP.jpg 1164 jpg EnCaseOverview.E01/P... JPEG E... 5904 KB 5902 KB BBDCA... 36D58... 36F307...
(120DPI)alertIcon.png 3209 png EnCaseOverview.E01/P... PNG 4096 B 652 B 3FAB6... E5A0F... DFCE1...
(120DPI)alertIcon.png 11269 png EnCaseOverview.E01/P... PNG 4096 B 652 B 3FAB6... E5A0F... DFCE1...
(120DPI)alertIcon.png 101931 png EnCaseOverview.E01/P... PNG 4096 B 652 B 3FAB6... E5A0F... DFCE1...
(120DPI)alertIcon.png 164997 png EnCaseOverview.E01/P... PNG 4096 B 652 B 3FAB6... E5A0F... DFCE1...
Loaded: 6,882 Filtered: 6,882 Total: 260,524 Highlighted: 0 Checked: 0 Total LSize: 248.0 MB
Ready
Graphics Tab Filter: Graphic Files
FTK
Graphics Tab


AccessData Forensic Toolkit Version: 3.2.0.32216 Database: localhost Case: FTK Overview
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered - Filter Manager...
Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile
Bookmarks
Bookmarks
sbunting
Significant Image
Shared
Bookmark Information
Bookmark Name:
Significant Image
Creator Name:
sbunting
File Comment:
Selection Comment:
Supplementary Files:
Attach File
Remove File
Selection(s):
Save Changes
Clear Changes
Add Selection
Remove Selection
File Content
Hex Text Filtered Natural
Default
Media
Web
File Content Properties Hex Interpreter
File List
Normal
Display Time Zone: Eastern Daylight Time (From local machine)
Name Label Item # Ext Path Category P-Size L-Size MD5 SHA1 SHA256 Create
GB-wp5.jpg 20255 jpg EnCaseOverview.E01/P... JPEG E... 628.0 KB 624.3 KB BFEA7... EAA06... 650A0... 7/14/200
Loaded: 1 Filtered: 1 Total: 1 Highlighted: 1 Checked: 1 Total LSize: 624.3 KB
EnCaseOverview.E01/Partition 2/NONAME [NTFS]/[root]/Windows/Globalization/MCT/MCT-GB/Wallpaper/GB-wp5.jpg
Ready
Bookmarks Tab Filter: [None]
FTK
Bookmarks
Tab


Explore
Overview
Email
Graphics
Bookmarks
Live Search
Index Search
Volatile
Text
Pattern
Hex
Live Search Results
Add
Clear
Export
Import
ANSI
Unicode
Other Code Pages
Select...
Case Sensitive
Search Terms
Type
Code Pages
Max Hits Per File:
200
Search Filter:
- unfiltered -
Search
File Content
Hex
Text
Filtered
Natural
Default
Media
File Content
Properties
Hex Interpreter
File List
Normal
Display Time Zone: Eastern Daylight Time (From local machine)
Name
Label
Item #
Ext
Path
Category
P-Size
L-Size
MD5
SHA1
SHA256
FTK
Live Search
Tab


AccessData Forensic Toolkit Version: 3.2.0.32216 Database: localhost Case: FTK Overview
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered - Filter Manager...
Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile
dtSearch® Index
Terms
Add
Indexed Words Total Hits
Search Criteria
Operators And Or
Terms All Selected
Accumulate Results
Search Terms Total Hits
Clear
Import...
Export...
Options...
Index Search Results
File Content
Hex Text Filtered Natural
Hit # of Prev Next Go to: Go
Default
Media
File Content Properties Hex Interpreter
File List
Normal
Display Time Zone: Eastern Daylight Time (From local machine)
Name Label Item # Ext Path Category P-Size L-Size MD5 SHA1 SHA256
Loaded: 0 Filtered: 0 Total: 0 Highlighted: 0 Checked: 1 Total LSize: 0
Ready
Index Search Tab Filter: [None]
FTK
Index Search
Tab


AccessData Forensic Toolkit Version: 3.2.0.32216 Database: localhost Case: FTK Overview
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered - Filter Manager...
Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile
Report Options
Report Outline
Case Information
Bookmarks
Graphics
File Paths
File Properties
Registry Selections
Import...
Export...
Filter
Shared
sbunting
Significant Image
Bookmark: Significant Image
Include email attachments
Export files & include links
Include thumbnail for each object
Thumbnail Arrangement
1 Number of thumbnails per row
Include all thumbnails at end of each bookmark section
Group all file paths at the end of thumbnails
Sort Options...
Apply these setting
Report
Options
Loaded: 0
Filtered: 0
Total: 0
Highlighted: 0
Checked: 1
Total LSize: 0
Ready
Index Search Tab Filter: [None]

FTK Report - Mozilla Firefox

File Edit View History Bookmarks Tools Help

FTK Report

file:///C:/Users/sbunting/Desktop/New folder/Index.html

FTK CASE REPORT

- Case Summary
  - Case Information
  - File Overview
  - Evidence List
- Bookmarks
  - sbunting
    - Significant Image
      - Thumbnails
- Graphics
  - Page 1
- File Paths
- File Properties
- Selected Registry Types

Bookmark: Significant Image

Comments:

Creator: sbunting

File Count: 1

Files

File Comments:

Thumbnail	1
Name	GB-wp5.jpg
Physical Size	643072 B
Logical Size	639243 B
Created Date	7/14/2009 3:26:29 AM (2009-07-14 07:26:29 UTC)
Modified Date	7/14/2009 3:26:29 AM (2009-07-14 07:26:29 UTC)
Accessed Date	7/14/2009 3:26:29 AM (2009-07-14 07:26:29 UTC)
Path	EnCaseOverview.E01/Partition 2/NONAME [NTFS]/[root]/Windows/Globa
Exported as	files\GB-wp5.jpg

The Report

Autopsy

Open Source

Introduction to Autopsy

- Digital data acquisition tool that:
  - Is also similar to EnCase in overall features
  - Email and file system analysis
  - Advanced searches
  - File type identification
  - Data carving

Introduction to Autopsy

- Step Action, you will work individually to:
  - Install Autopsy
  - Create new case
  - Examine evidence files
  - Sort files
  - Create bookmarks
  - Generate reports

What forensic tool features would most benefit my investigations?

Summary

- You should now be familiar with using forensic tools to:
  - Create a case
  - Add and verify evidence
  - Adjust time zone offsets
  - Process, navigate through, and bookmark evidence
  - Create reports from your findings

Thanks!

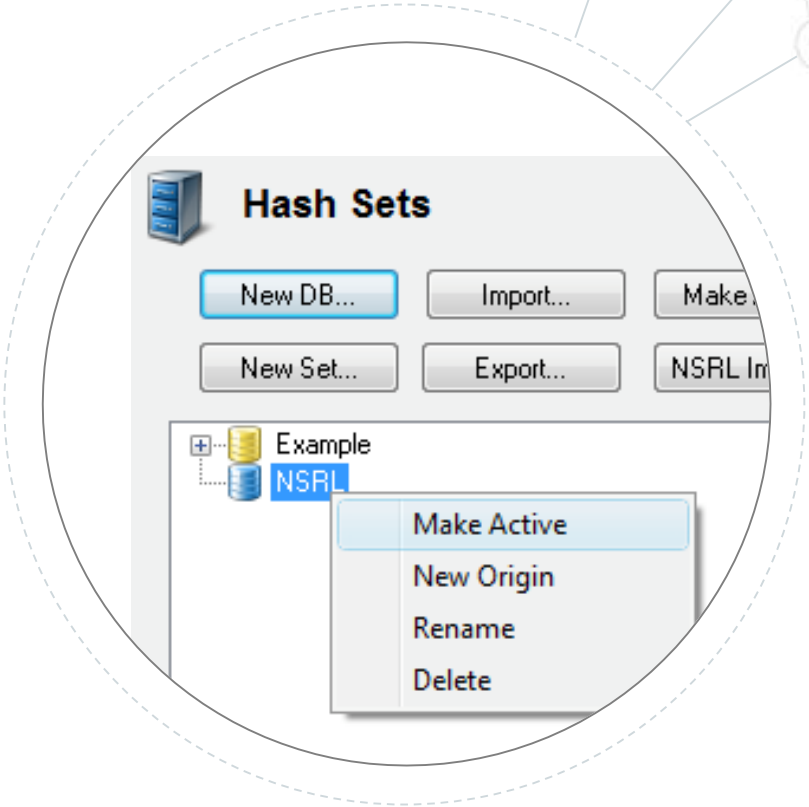
Any questions?

You can find me at:
@username
user@mail.me

Hash Analysis

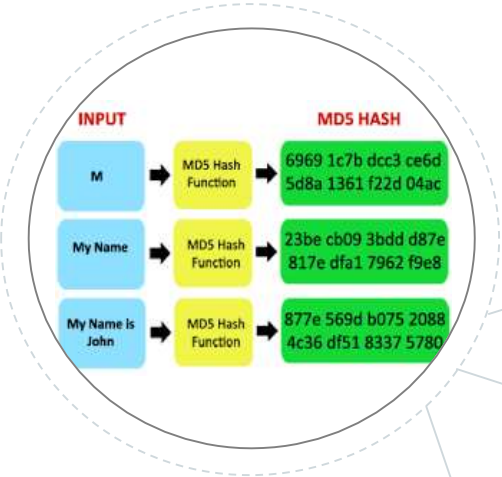
Objective

- By the end of the module, participants will be able to use a hash set to identify known trusted and malicious files



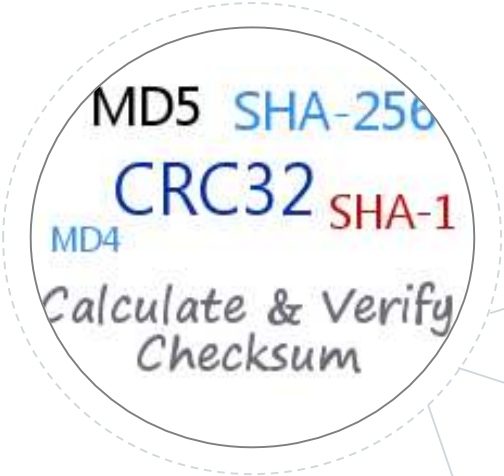
Hash Definition

- Hashes:
  - Calculations or algorithms that result in unique value for each file or stream of data to which the calculation is applied



Hash Algorithm

- The two key forensics hash algorithms are:
  - **Message Digest 5** (128-bit value)
  - **Secure Hash Algorithm 1** (160-bit value)
- Two files with the same hash value are statistically likely to contain the same data



Hash Uses

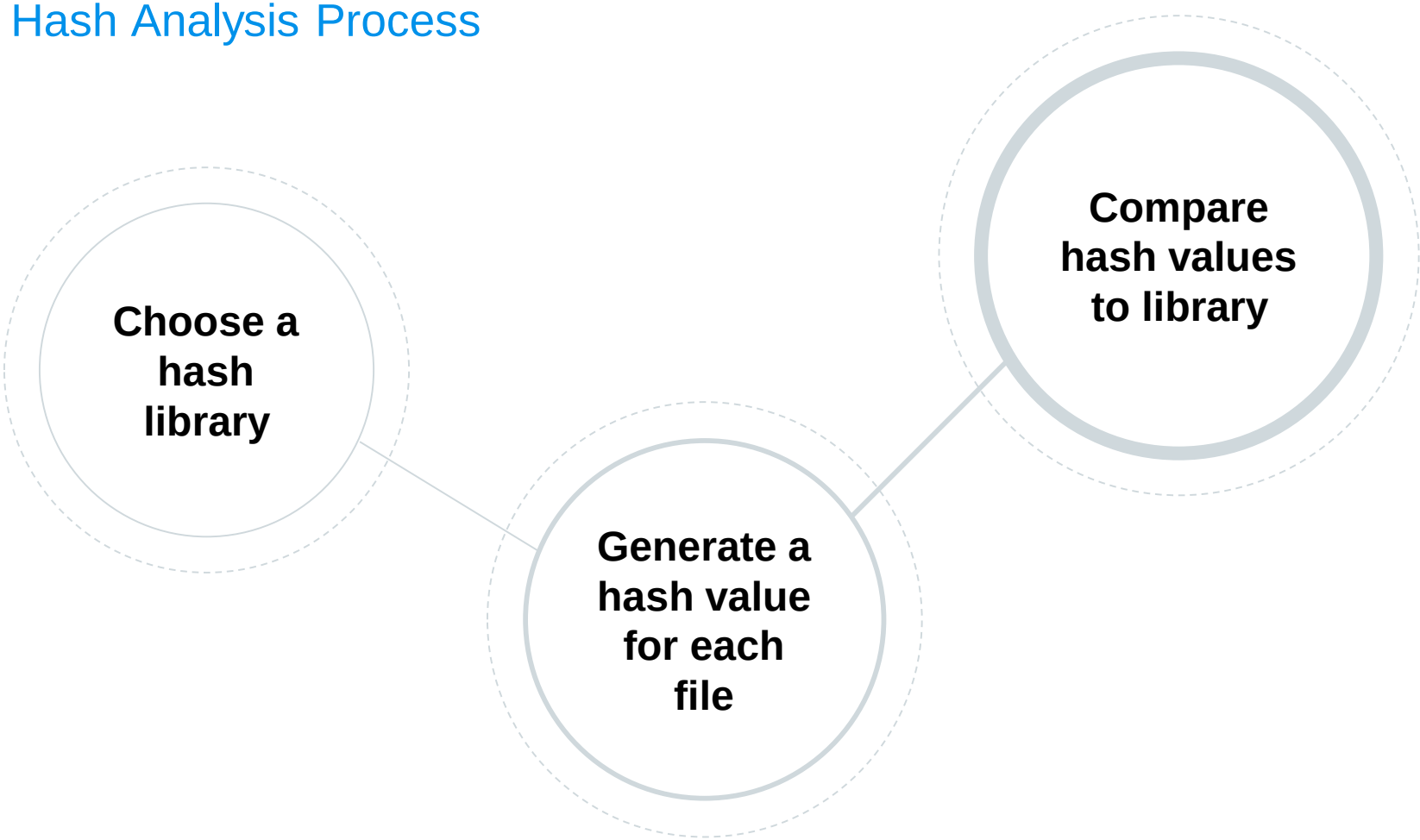
Use	Process
Verify evidence file acquisitions	Compare acquisition and verification hash values
Identify known good files	Compare file hashes to libraries of known files
Identify known bad files	Compare file hashes to tables of known hashes

Hash Sets and Hash Libraries

- **Hash Set:** A collection of hash values with similar traits

- **Hash Library:** A collection of hash sets

Hash Analysis Process



Sources of Hash Sets

- Forensic software vendors
- U.S. National Institutes of Standards and Technology/National Software Reference Library
- Specialized collections
- Collections created by examiners/agencies

Known vs Unknown Files

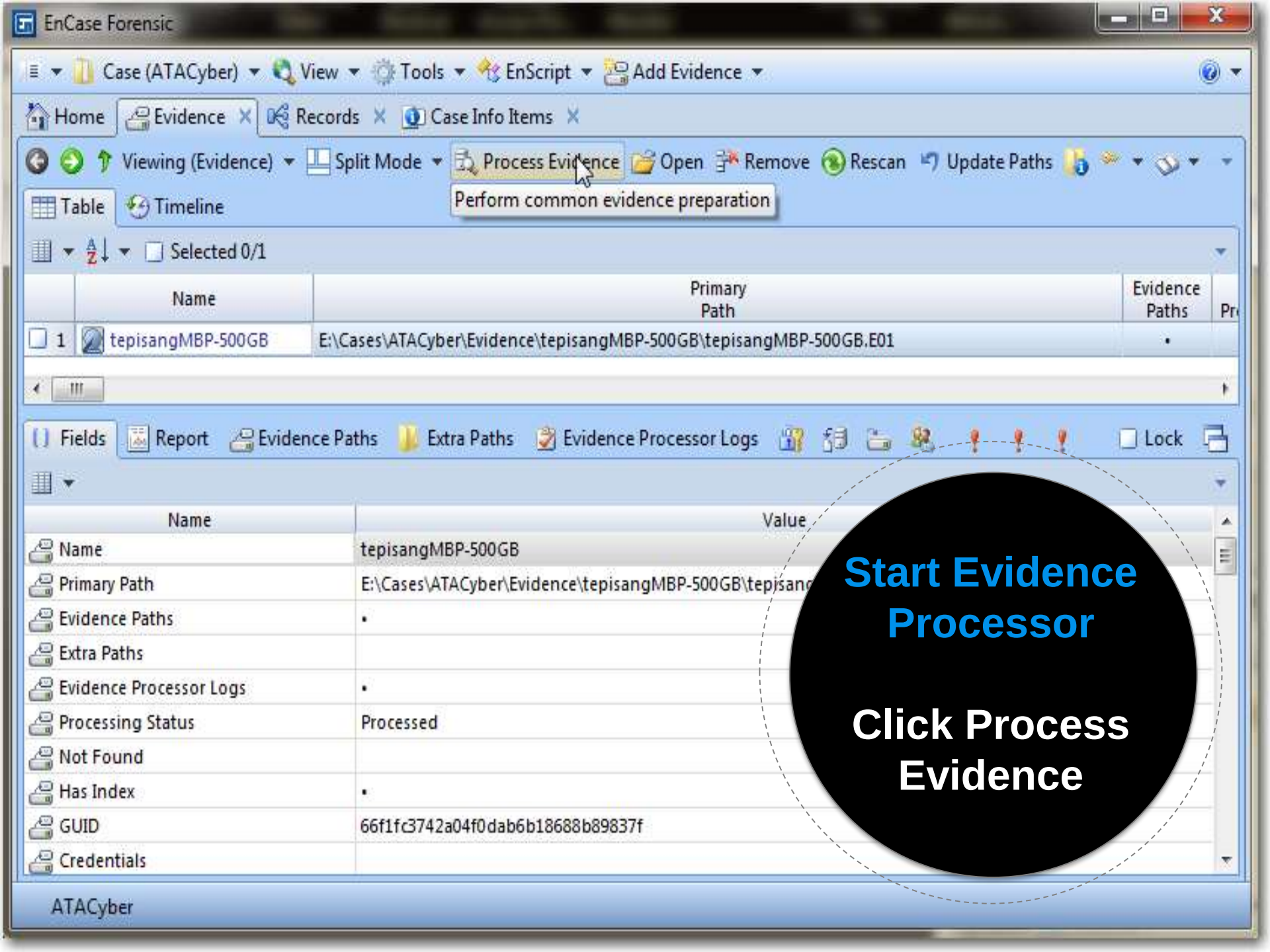
- Known files can be good or bad
- Most files will be unknown
- A forensic examiner must be capable of creating hash sets for local use

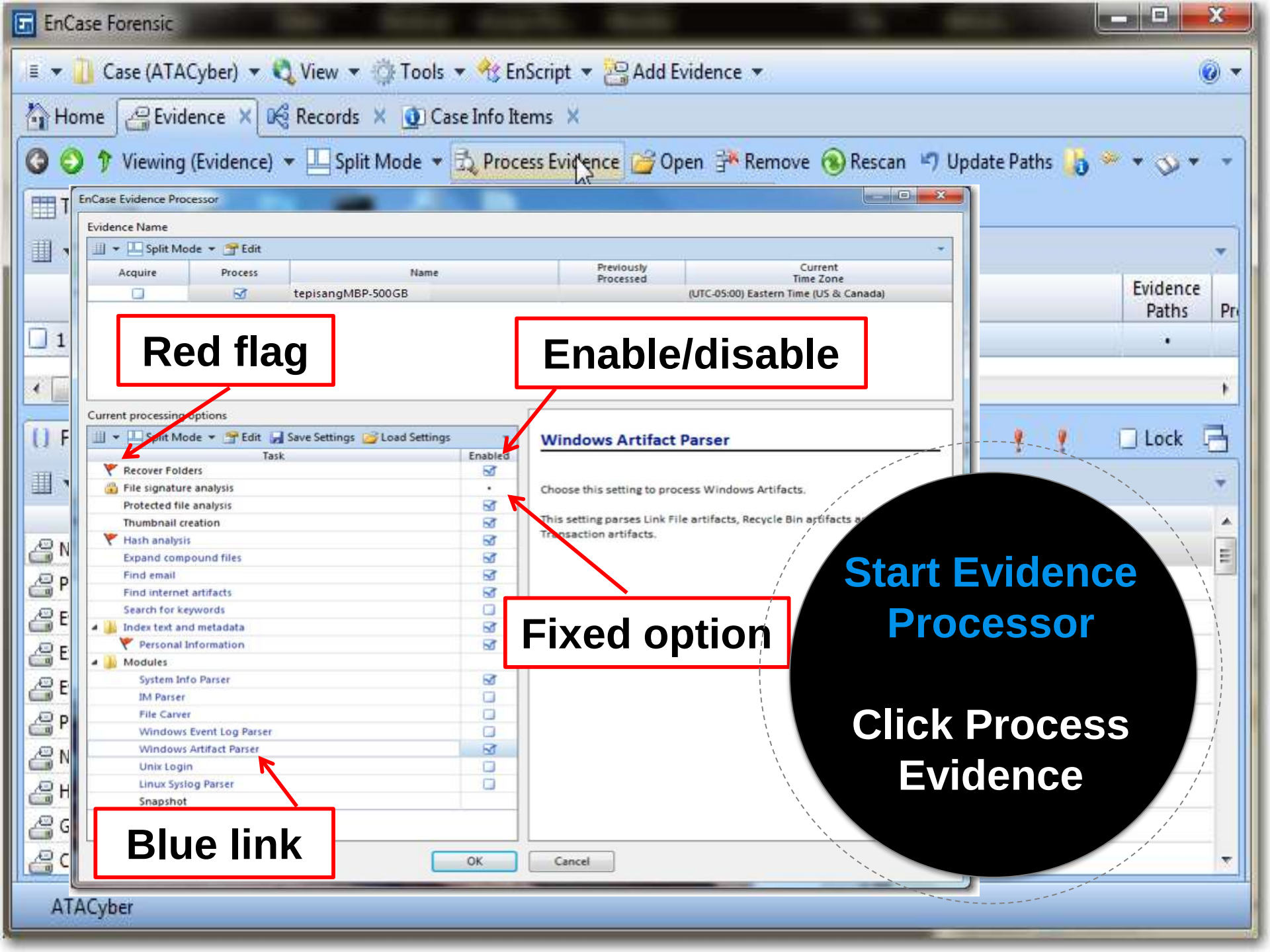
EnCase

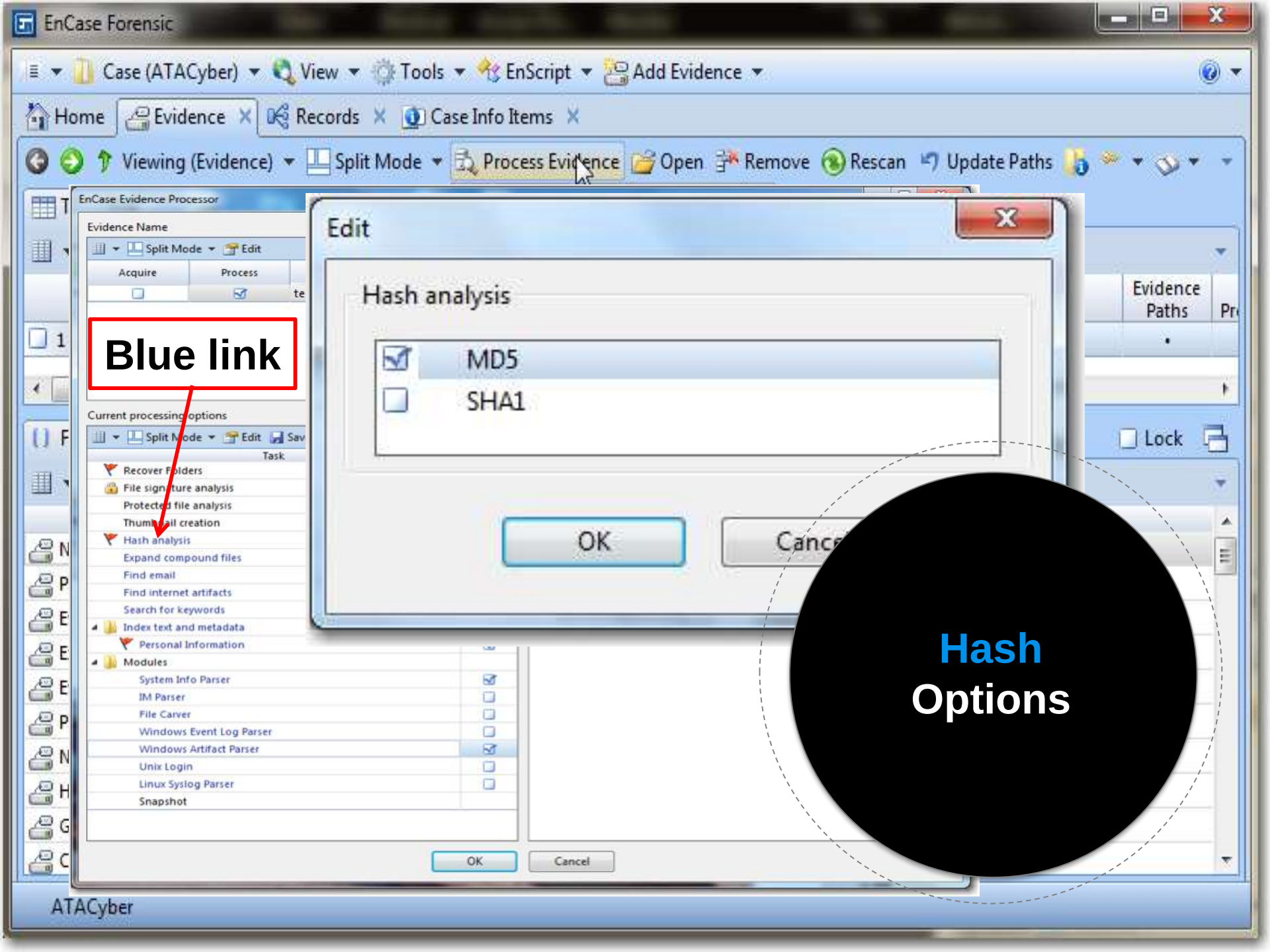
Evidence Processor

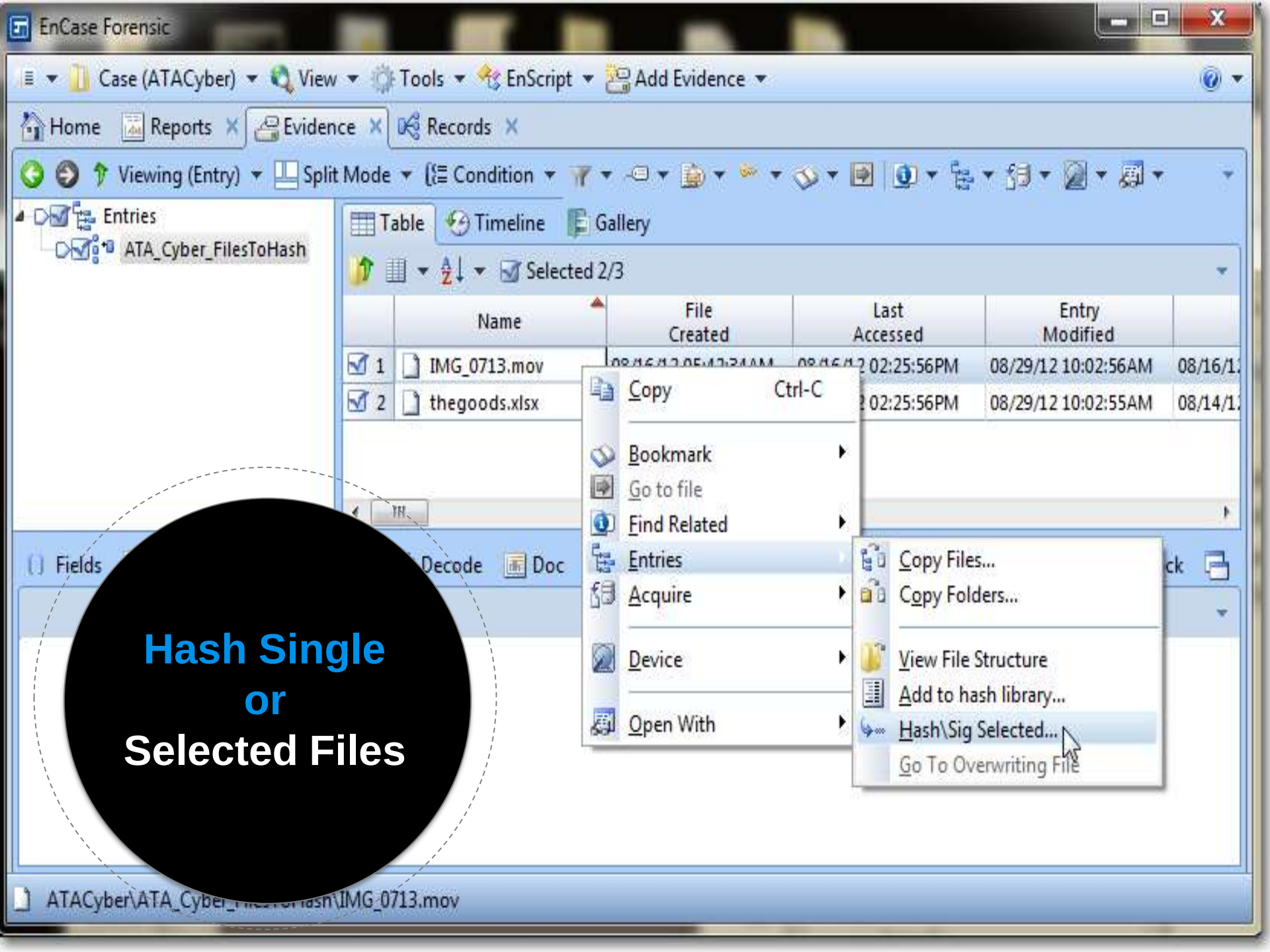
EnCase Evidence Processor

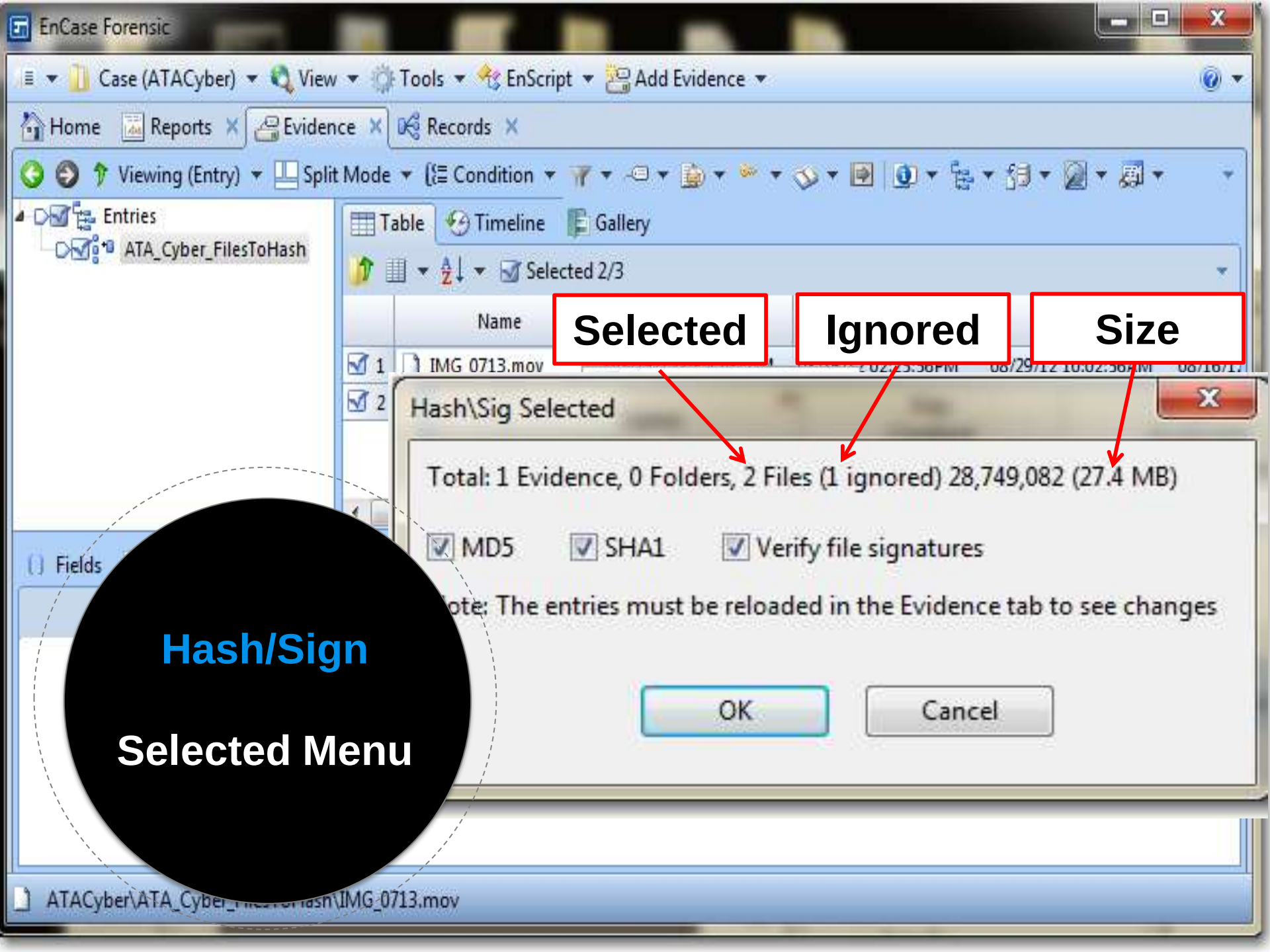
- Hashing occurs during evidence processing with EnCase 7
- EnCase Evidence Processor (EEP) provides hash analysis for files in the selected evidence items

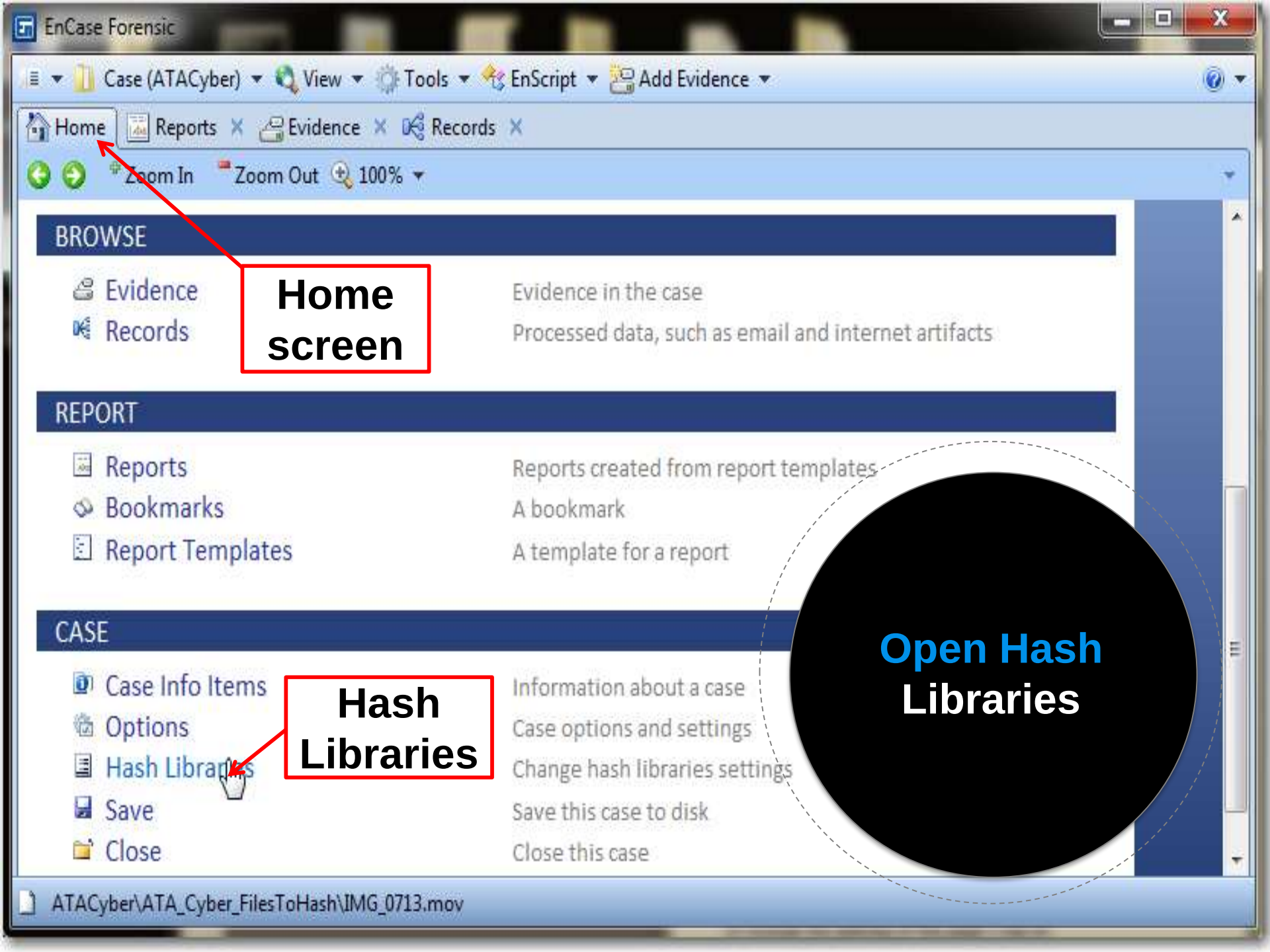

EnCase Forensic
Case (ATACyber)
View
Tools
EnScript
Add Evidence
Home
Evidence
Records
Case Info Items
Viewing (Evidence)
Split Mode
Process Evidence
Open
Remove
Rescan
Update Paths
Perform common evidence preparation
Table
Timeline
Selected 0/1
Name
Primary Path
Evidence Paths
1
tepisangMBP-500GB
E:\Cases\ATACyber\Evidence\tepisangMBP-500GB\tepisangMBP-500GB.E01
Fields
Report
Evidence Paths
Extra Paths
Evidence Processor Logs
Lock
Name
Value
Name
tepisangMBP-500GB
Primary Path
E:\Cases\ATACyber\Evidence\tepisangMBP-500GB\tepisanc
Evidence Paths
Extra Paths
Evidence Processor Logs
Processing Status
Processed
Not Found
Has Index
GUID
66f1fc3742a04f0dab6b18688b89837f
Credentials
ATACyber
Start Evidence Processor
Click Process Evidence

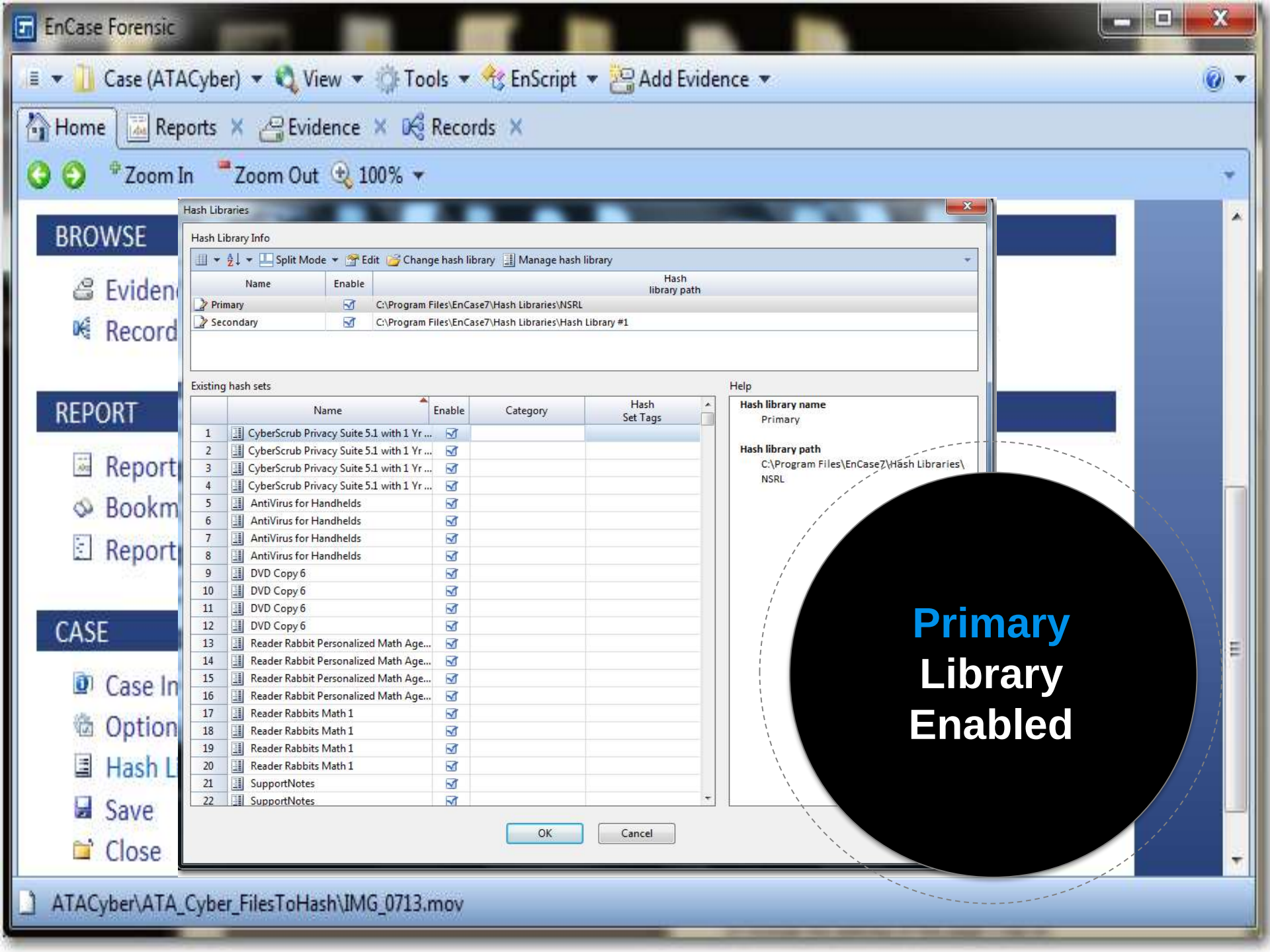

EnCase Forensic
Case (ATACyber)
View
Tools
EnScript
Add Evidence
Home
Evidence
Records
Case Info Items
Viewing (Evidence)
Split Mode
Process Evidence
Open
Remove
Rescan
Update Paths
EnCase Evidence Processor
Evidence Name
Split Mode
Edit
Acquire
Process
Name
Previously Processed
Current Time Zone
tepisangMBP-500GB
(UTC-05:00) Eastern Time (US & Canada)
Red flag
Enable/disable
Current processing options
Split Mode
Edit
Save Settings
Load Settings
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
Personal Information
Modules
System Info Parser
IM Parser
File Carver
Windows Event Log Parser
Windows Artifact Parser
Unix Login
Linux Syslog Parser
Snapshot
Windows Artifact Parser
Choose this setting to process Windows Artifacts.
This setting parses Link File artifacts, Recycle Bin artifacts
Transaction artifacts.
Fixed option
Blue link
OK
Cancel
Start Evidence Processor
Click Process Evidence
Evidence Paths
Lock
ATACyber

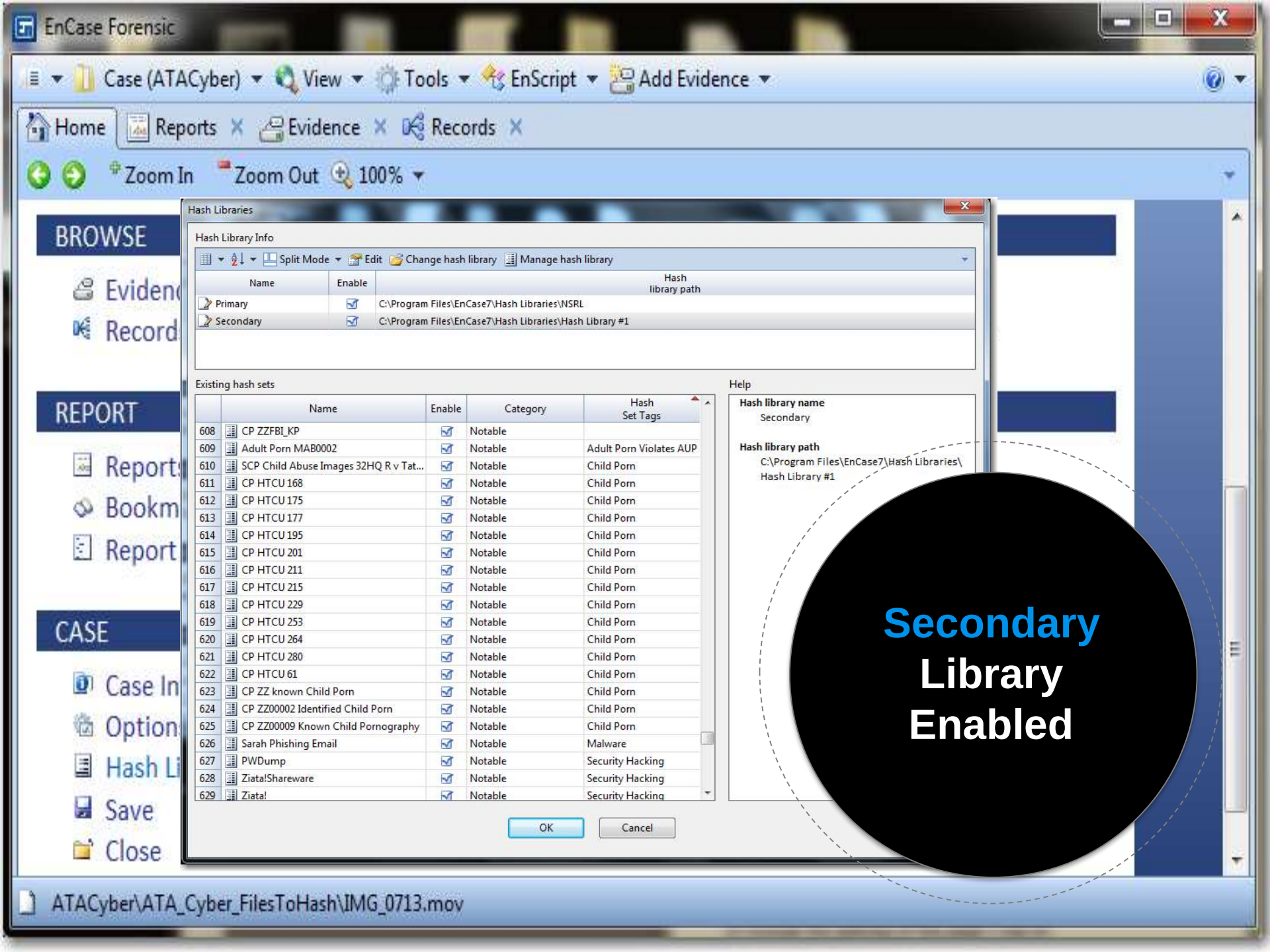

EnCase Forensic
Case (ATACyber)
View
Tools
EnScript
Add Evidence
Home
Evidence
Records
Case Info Items
Viewing (Evidence)
Split Mode
Process Evidence
Open
Remove
Rescan
Update Paths
EnCase Evidence Processor
Evidence Name
Split Mode
Edit
Acquire
Process
Blue link
Current processing options
Split Mode
Edit
Task
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
Personal Information
Modules
System Info Parser
IM Parser
File Carver
Windows Event Log Parser
Windows Artifact Parser
Unix Login
Linux Syslog Parser
Snapshot
OK
Cancel
Edit
Hash analysis
MD5
SHA1
OK
Cancel
Evidence Paths
Lock
Hash
Options
ATACyber

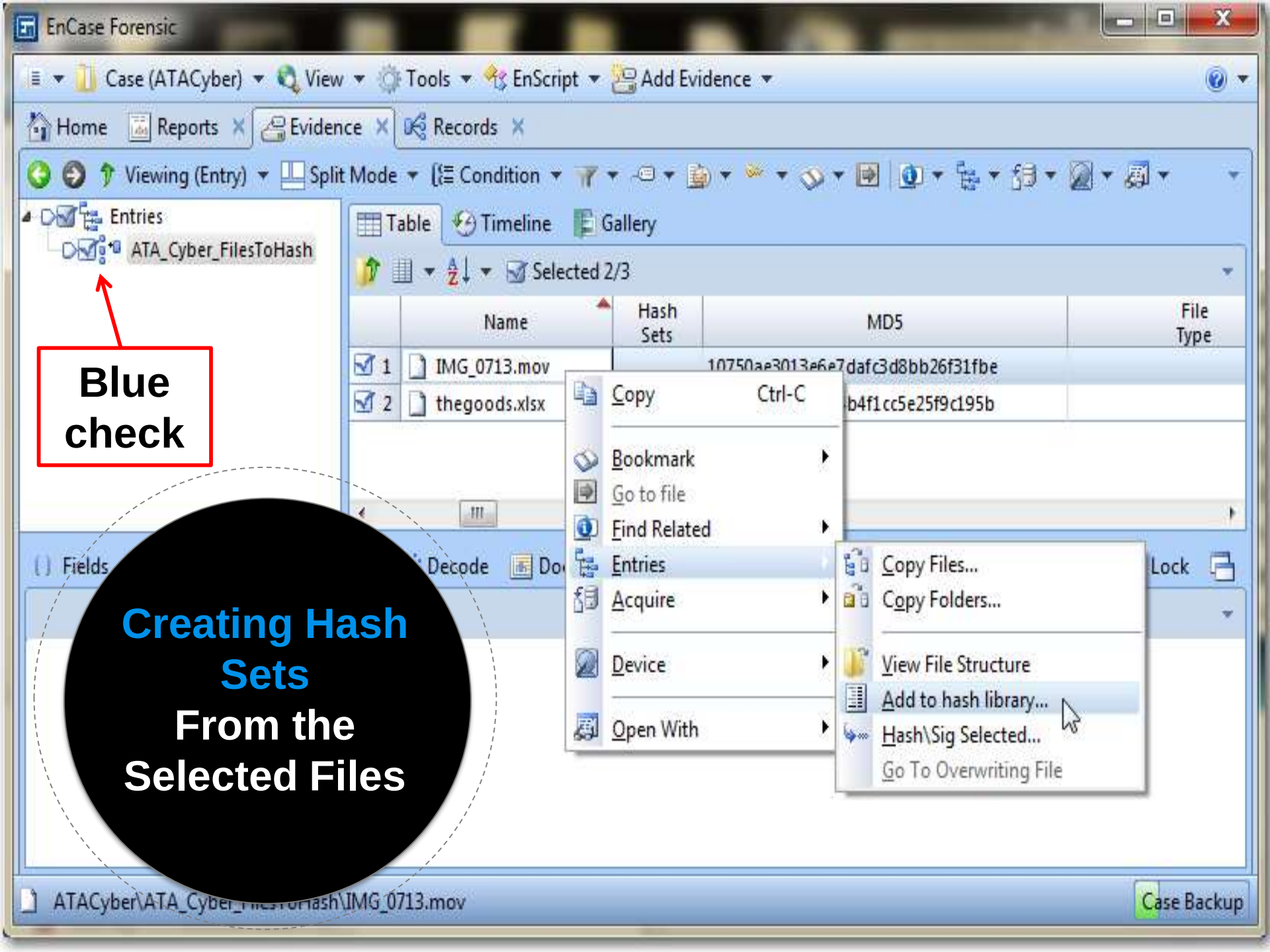

EnCase Forensic
Case (ATACyber)
View
Tools
EnScript
Add Evidence
Home
Reports
Evidence
Records
Viewing (Entry)
Split Mode
Condition
Entries
ATA_Cyber_FilesToHash
Table
Timeline
Gallery
Selected 2/3
Name
File Created
Last Accessed
Entry Modified
1
IMG_0713.mov
02:25:56PM
08/29/12 10:02:56AM
2
thegoods.xlsx
02:25:56PM
08/29/12 10:02:55AM
Copy Ctrl-C
Bookmark
Go to file
Find Related
Entries
Acquire
Device
Open With
Copy Files...
Copy Folders...
View File Structure
Add to hash library...
Hash\Sig Selected...
Go To Overwriting File
Fields
Decode
Doc
Hash Single
or
Selected Files
ATACyber\ATA_Cyber_FilesToHash\IMG_0713.mov

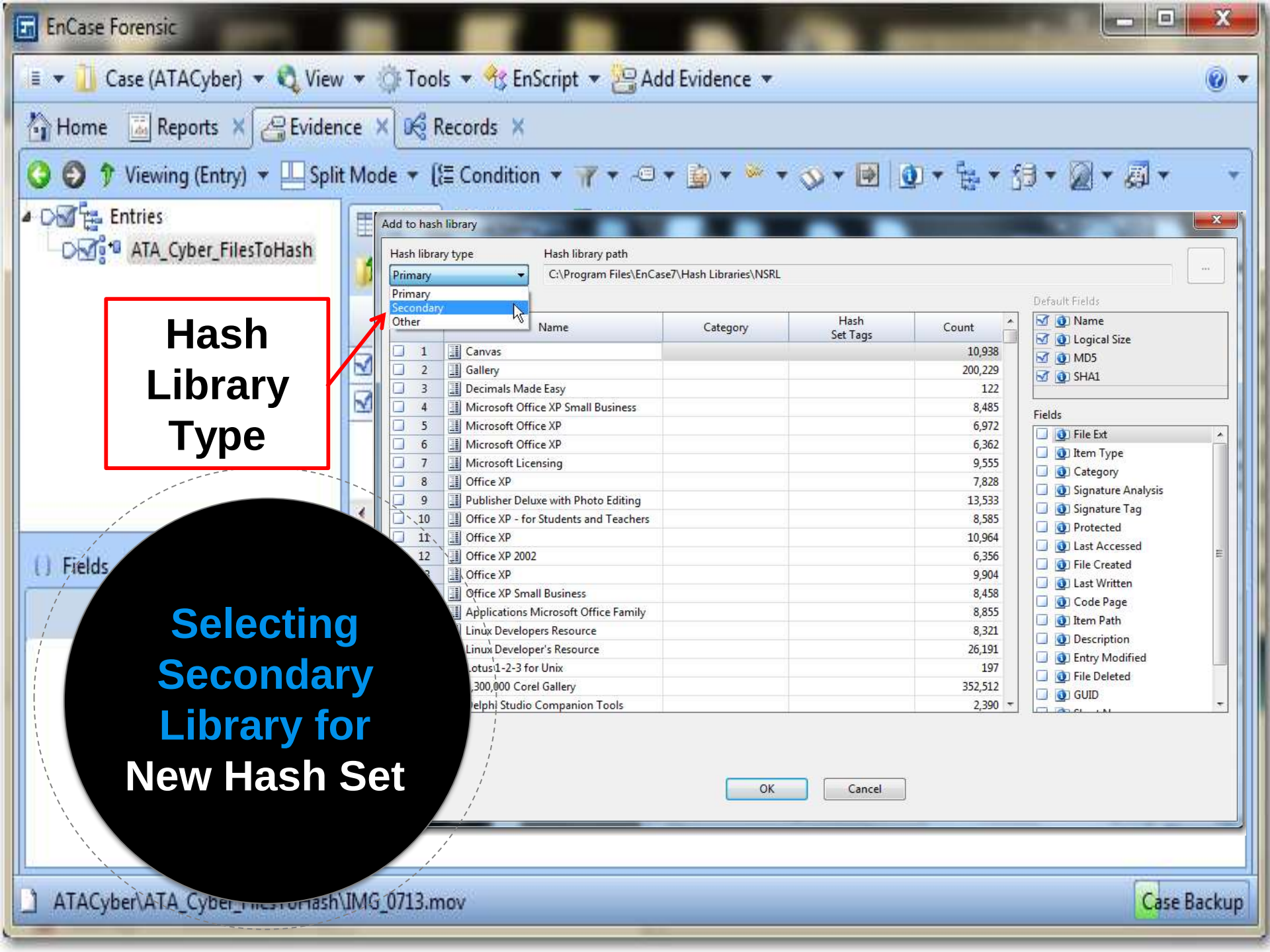

EnCase Forensic
Case (ATACyber)
View
Tools
EnScript
Add Evidence
Home
Reports
Evidence
Records
Viewing (Entry)
Split Mode
Condition
Entries
ATA_Cyber_FilesToHash
Table
Timeline
Gallery
Selected 2/3
Name
Selected
Ignored
Size
1
IMG_0713.mov
2
Hash\Sig Selected
Total: 1 Evidence, 0 Folders, 2 Files (1 ignored) 28,749,082 (27.4 MB)
MD5
SHA1
Verify file signatures
ote: The entries must be reloaded in the Evidence tab to see changes
OK
Cancel
Fields
Hash/Sign
Selected Menu
ATACyber\ATA_Cyber_FilesToHash\IMG_0713.mov

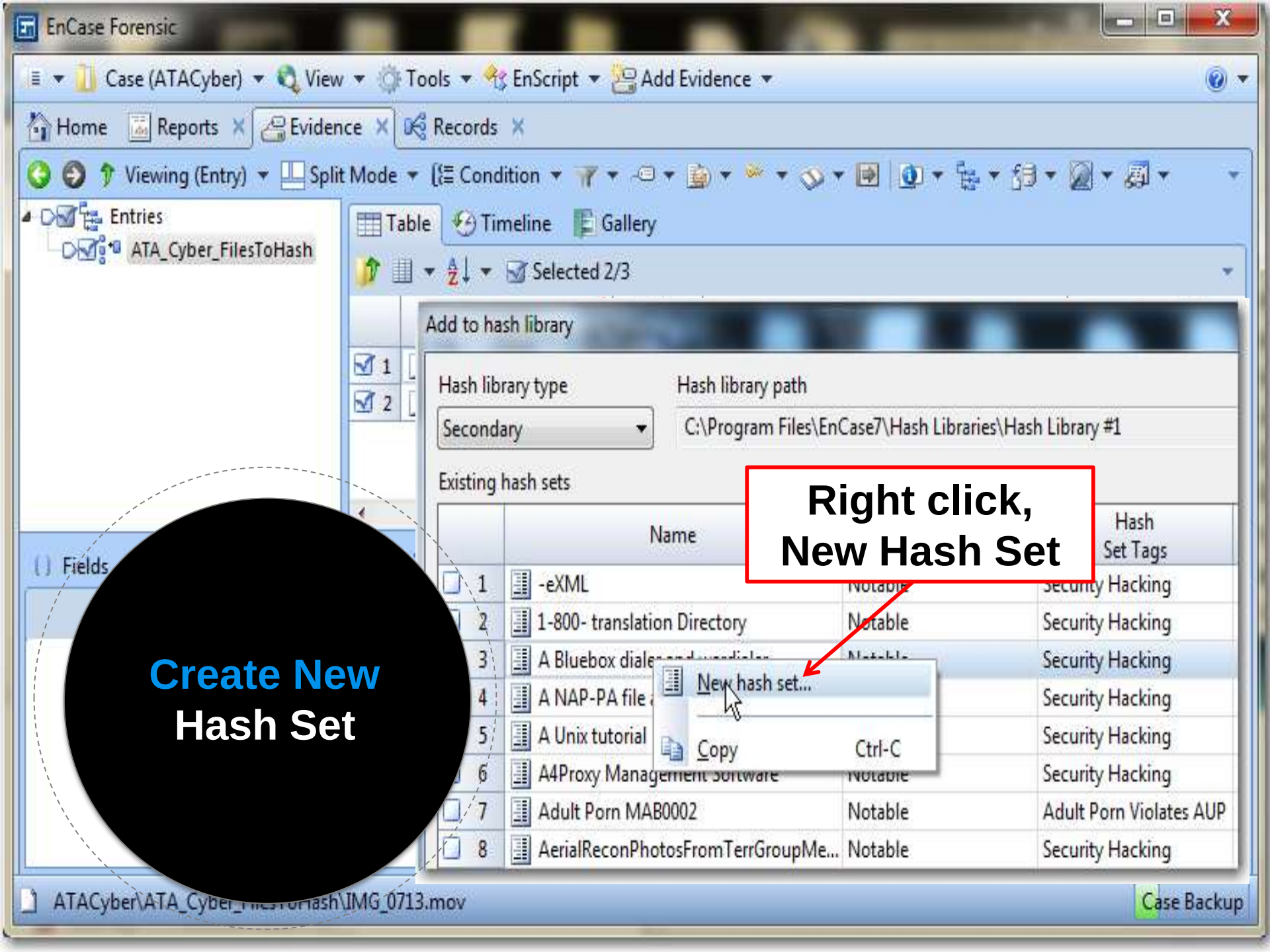

EnCase Forensic
Case (ATACyber)
View
Tools
EnScript
Add Evidence
Home
Reports
Evidence
Records
Zoom In
Zoom Out
100%
BROWSE
Evidence
Evidence in the case
Records
Processed data, such as email and internet artifacts
Home screen
REPORT
Reports
Reports created from report templates
Bookmarks
A bookmark
Report Templates
A template for a report
CASE
Case Info Items
Information about a case
Options
Case options and settings
Hash Libraries
Change hash libraries settings
Save
Save this case to disk
Close
Close this case
Hash Libraries
Open Hash Libraries
ATACyber\ATA_Cyber_FilesToHash\IMG_0713.mov

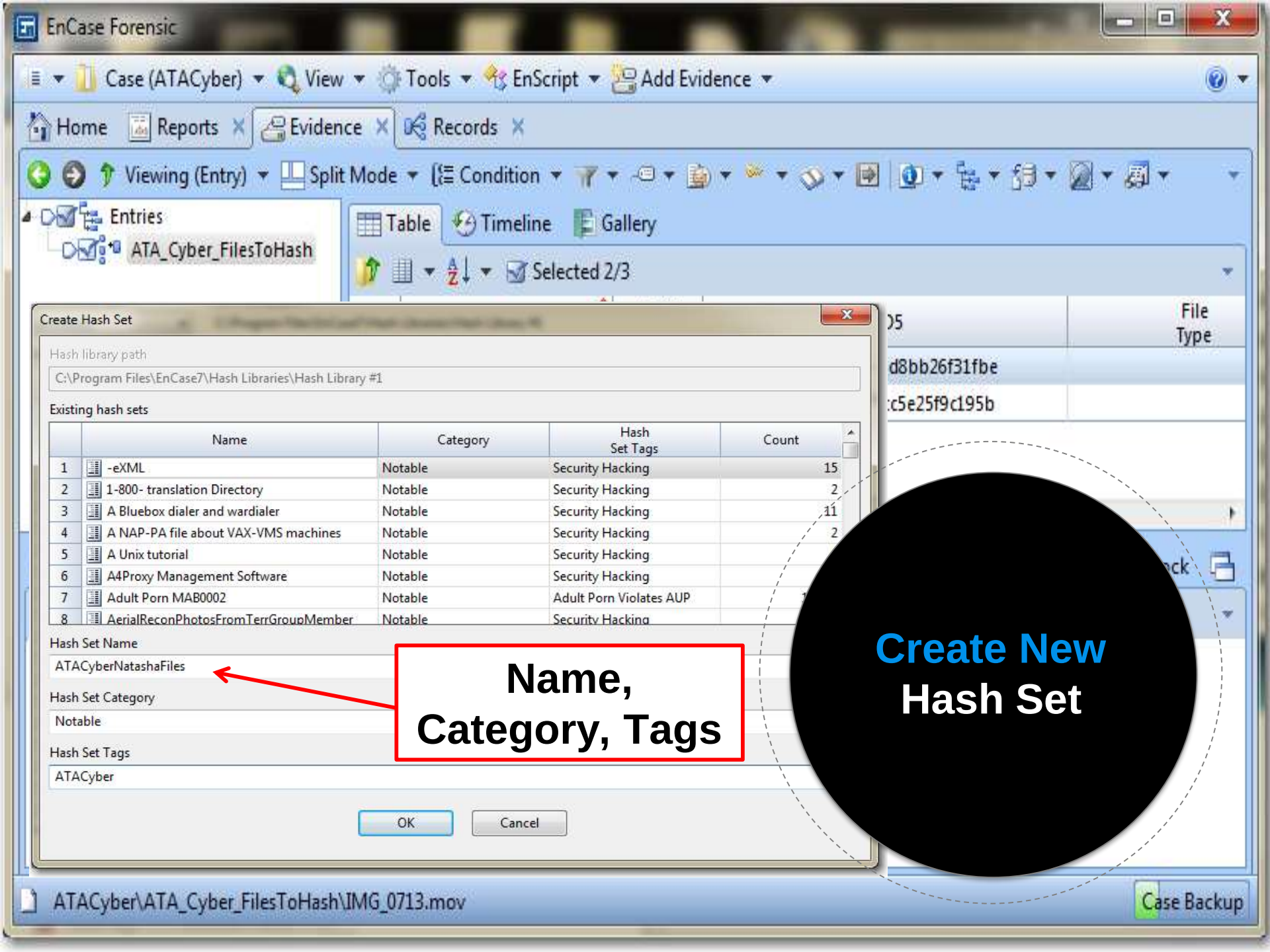

EnCase Forensic
Case (ATACyber)
View
Tools
EnScript
Add Evidence
Home
Reports
Evidence
Records
Zoom In
Zoom Out
100%
BROWSE
REPORT
CASE
Hash Libraries
Hash Library Info
Split Mode
Edit
Change hash library
Manage hash library
Name
Enable
Hash library path
Primary
C:\Program Files\EnCase7\Hash Libraries\NSRL
Secondary
C:\Program Files\EnCase7\Hash Libraries\Hash Library #1
Existing hash sets
Name
Enable
Category
Hash Set Tags
CyberScrub Privacy Suite 5.1 with 1 Yr ...
AntiVirus for Handhelds
DVD Copy 6
Reader Rabbit Personalized Math Age...
Reader Rabbits Math 1
SupportNotes
Help
Hash library name
Primary
Hash library path
C:\Program Files\EnCase7\Hash Libraries\
NSRL
OK
Cancel
Primary
Library
Enabled
ATACyber\ATA_Cyber_FilesToHash\IMG_0713.mov

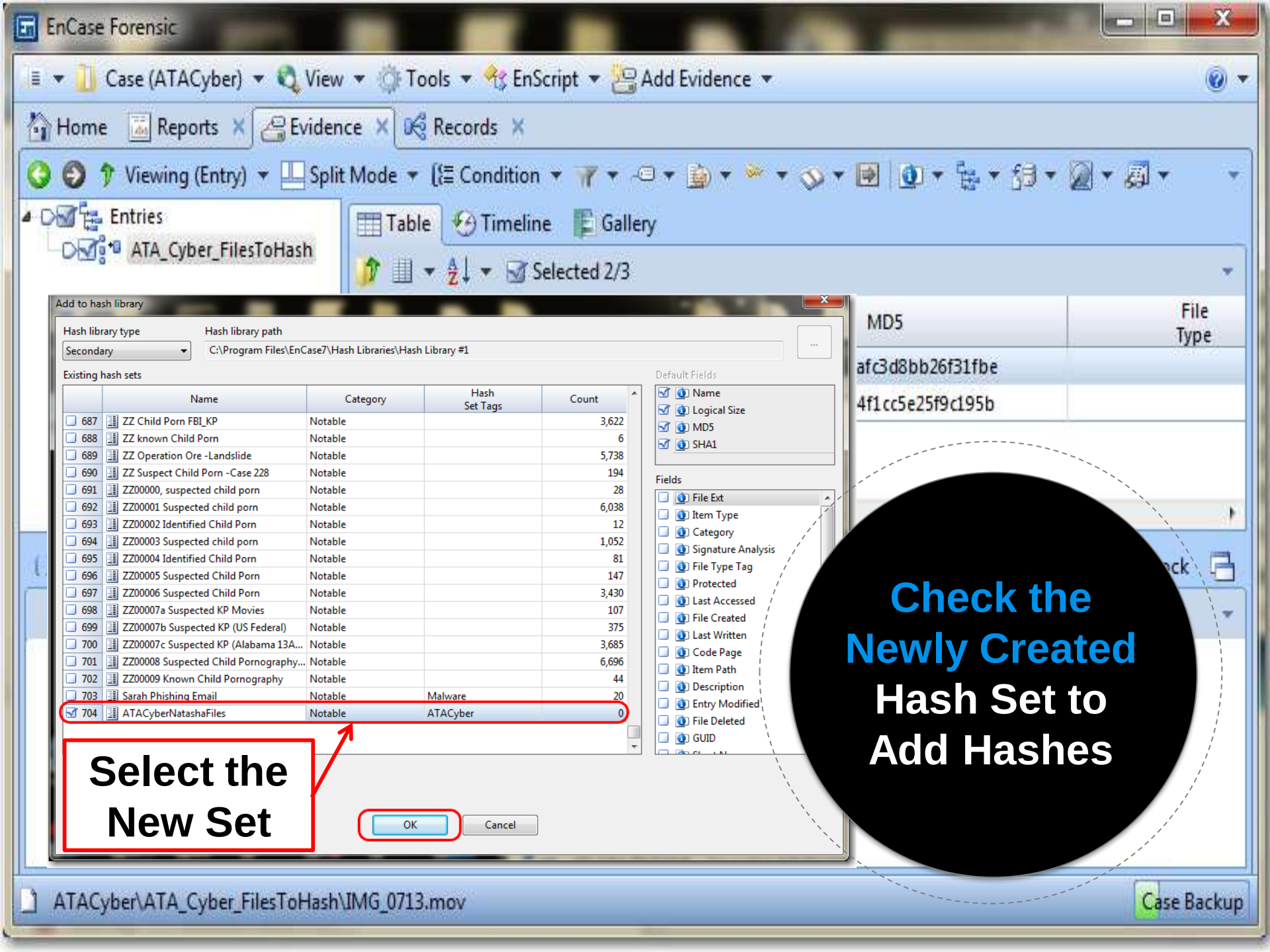

EnCase Forensic
Case (ATACyber)
View
Tools
EnScript
Add Evidence
Home
Reports
Evidence
Records
Zoom In
Zoom Out
100%
BROWSE
REPORT
CASE
Hash Libraries
Hash Library Info
Split Mode
Edit
Change hash library
Manage hash library
Name
Enable
Hash library path
Primary
C:\Program Files\EnCase7\Hash Libraries\NSRL
Secondary
C:\Program Files\EnCase7\Hash Libraries\Hash Library #1
Existing hash sets
Name
Enable
Category
Hash Set Tags
608 CP ZZFBI_KP Notable
609 Adult Porn MAB0002 Notable Adult Porn Violates AUP
610 SCP Child Abuse Images 32HQ R v Tat... Notable Child Porn
611 CP HTCU 168 Notable Child Porn
612 CP HTCU 175 Notable Child Porn
613 CP HTCU 177 Notable Child Porn
614 CP HTCU 195 Notable Child Porn
615 CP HTCU 201 Notable Child Porn
616 CP HTCU 211 Notable Child Porn
617 CP HTCU 215 Notable Child Porn
618 CP HTCU 229 Notable Child Porn
619 CP HTCU 253 Notable Child Porn
620 CP HTCU 264 Notable Child Porn
621 CP HTCU 280 Notable Child Porn
622 CP HTCU 61 Notable Child Porn
623 CP ZZ known Child Porn Notable Child Porn
624 CP ZZ00002 Identified Child Porn Notable Child Porn
625 CP ZZ00009 Known Child Pornography Notable Child Porn
626 Sarah Phishing Email Notable Malware
627 PWDump Notable Security Hacking
628 Ziata!Shareware Notable Security Hacking
629 Ziata! Notable Security Hacking
Help
Hash library name
Secondary
Hash library path
C:\Program Files\EnCase7\Hash Libraries\
Hash Library #1
OK
Cancel
Secondary
Library
Enabled
ATACyber\ATA_Cyber_FilesToHash\IMG_0713.mov

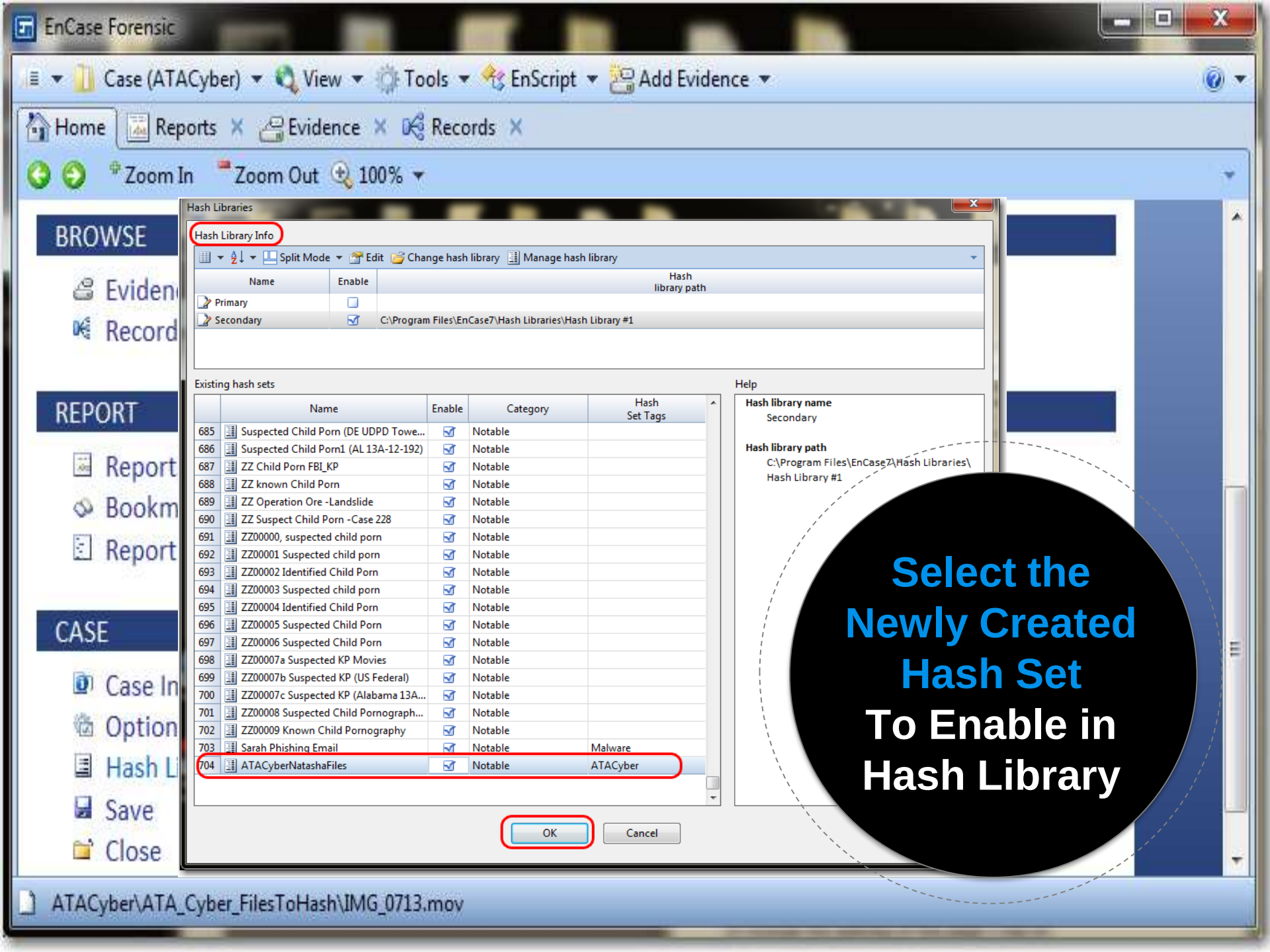

EnCase Forensic
Case (ATACyber)
View
Tools
EnScript
Add Evidence
Home
Reports
Evidence
Records
Viewing (Entry)
Split Mode
Condition
Entries
ATA_Cyber_FilesToHash
Blue check
Table
Timeline
Gallery
Selected 2/3
Name
Hash Sets
MD5
File Type
1
IMG_0713.mov
2
thegoods.xlsx
Copy
Ctrl-C
Bookmark
Go to file
Find Related
Entries
Acquire
Device
Open With
Copy Files...
Copy Folders...
View File Structure
Add to hash library...
Hash\Sig Selected...
Go To Overwriting File
Fields
Decode
Lock
Creating Hash Sets From the Selected Files
ATACyber\ATA_Cyber_FilesToHash\IMG_0713.mov
Case Backup

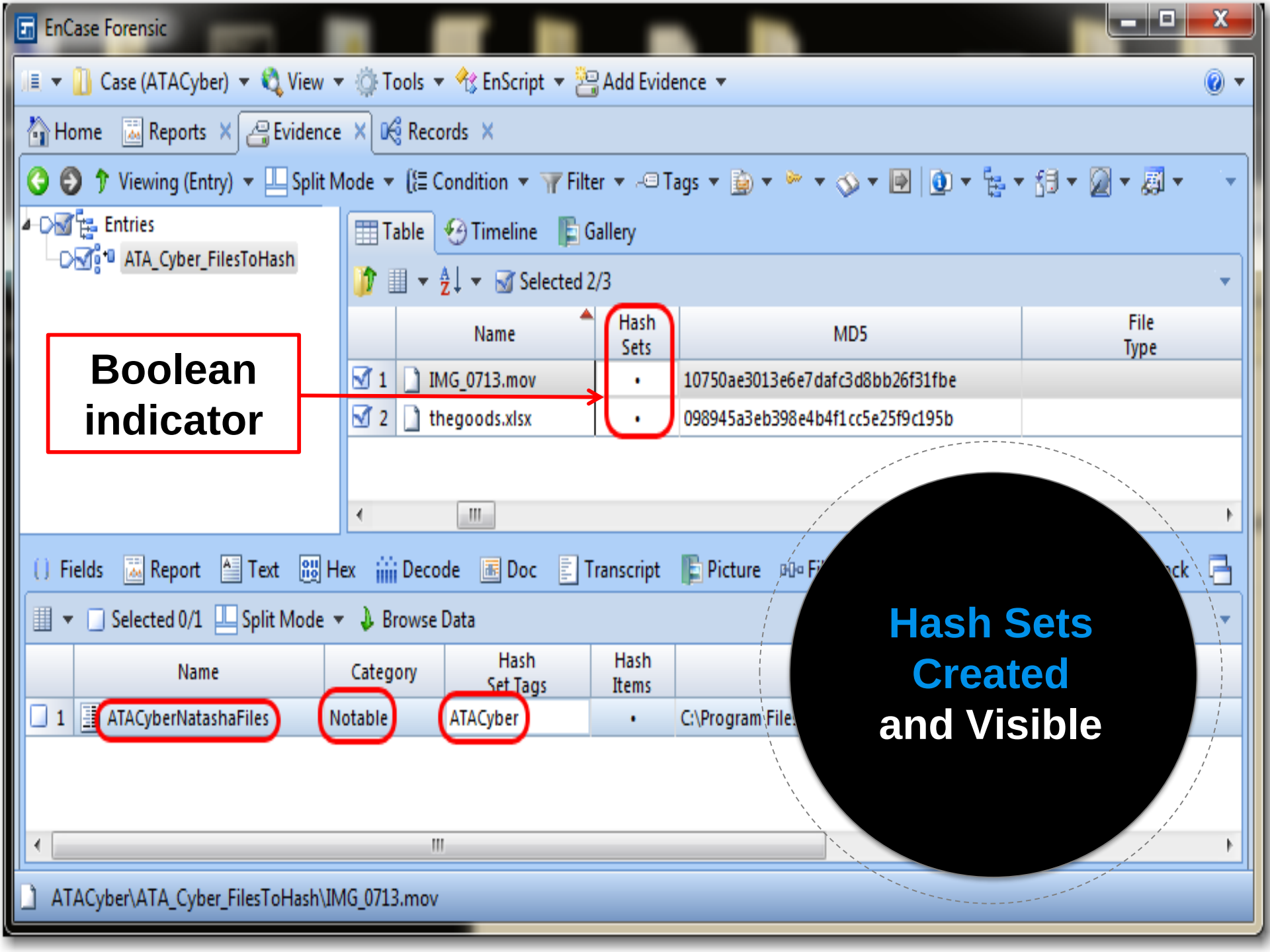

EnCase Forensic
Case (ATACyber)
View
Tools
EnScript
Add Evidence
Home
Reports
Evidence
Records
Viewing (Entry)
Split Mode
Condition
Entries
ATA_Cyber_FilesToHash
Hash Library Type
Add to hash library
Hash library type
Primary
Secondary
Other
Hash library path
C:\Program Files\EnCase7\Hash Libraries\NSRL
Name
Category
Hash Set Tags
Count
1 Canvas 10,938
2 Gallery 200,229
3 Decimals Made Easy 122
4 Microsoft Office XP Small Business 8,485
5 Microsoft Office XP 6,972
6 Microsoft Office XP 6,362
7 Microsoft Licensing 9,555
8 Office XP 7,828
9 Publisher Deluxe with Photo Editing 13,533
10 Office XP - for Students and Teachers 8,585
11 Office XP 10,964
12 Office XP 2002 6,356
Office XP 9,904
Office XP Small Business 8,458
Applications Microsoft Office Family 8,855
Linux Developers Resource 8,321
Linux Developer's Resource 26,191
Lotus 1-2-3 for Unix 197
300,000 Corel Gallery 352,512
Delphi Studio Companion Tools 2,390
Default Fields
Name
Logical Size
MD5
SHA1
Fields
File Ext
Item Type
Category
Signature Analysis
Signature Tag
Protected
Last Accessed
File Created
Last Written
Code Page
Item Path
Description
Entry Modified
File Deleted
GUID
OK
Cancel
Fields
Selecting Secondary Library for New Hash Set
ATACyber\ATA_Cyber_FilesToHash\IMG_0713.mov
Case Backup


EnCase Forensic
Case (ATACyber)
View
Tools
EnScript
Add Evidence
Home
Reports
Evidence
Records
Viewing (Entry)
Split Mode
Condition
Entries
ATA_Cyber_FilesToHash
Table
Timeline
Gallery
Selected 2/3
Add to hash library
Hash library type
Secondary
Hash library path
C:\Program Files\EnCase7\Hash Libraries\Hash Library #1
Existing hash sets
Name
Hash Set Tags
1 -eXML
2 1-800- translation Directory Notable Security Hacking
3 A Bluebox dial Security Hacking
4 A NAP-PA file Security Hacking
5 A Unix tutorial Security Hacking
6 A4Proxy Management Software Security Hacking
7 Adult Porn MAB0002 Notable Adult Porn Violates AUP
8 AerialReconPhotosFromTerrGroupMe... Notable Security Hacking
New hash set...
Copy Ctrl-C
Right click, New Hash Set
Create New Hash Set
Fields
ATACyber\ATA_Cyber_FilesToHash\IMG_0713.mov
Case Backup


EnCase Forensic
Case (ATACyber)
View
Tools
EnScript
Add Evidence
Home
Reports
Evidence
Records
Viewing (Entry)
Split Mode
Condition
Entries
ATA_Cyber_FilesToHash
Table
Timeline
Gallery
Selected 2/3
Create Hash Set
Hash library path
C:\Program Files\EnCase7\Hash Libraries\Hash Library #1
Existing hash sets
Name
Category
Hash Set Tags
Count
1 -eXML Notable Security Hacking 15
2 1-800- translation Directory Notable Security Hacking 2
3 A Bluebox dialer and wardialer Notable Security Hacking 11
4 A NAP-PA file about VAX-VMS machines Notable Security Hacking 2
5 A Unix tutorial Notable Security Hacking
6 A4Proxy Management Software Notable Security Hacking
7 Adult Porn MAB0002 Notable Adult Porn Violates AUP
8 AerialReconPhotosFromTerrGroupMember Notable Security Hacking
Hash Set Name
ATACyberNatashaFiles
Hash Set Category
Notable
Hash Set Tags
ATACyber
OK
Cancel
Name, Category, Tags
Create New Hash Set
File Type
d8bb26f31fbe
c5e25f9c195b
ATACyber\ATA_Cyber_FilesToHash\IMG_0713.mov
Case Backup

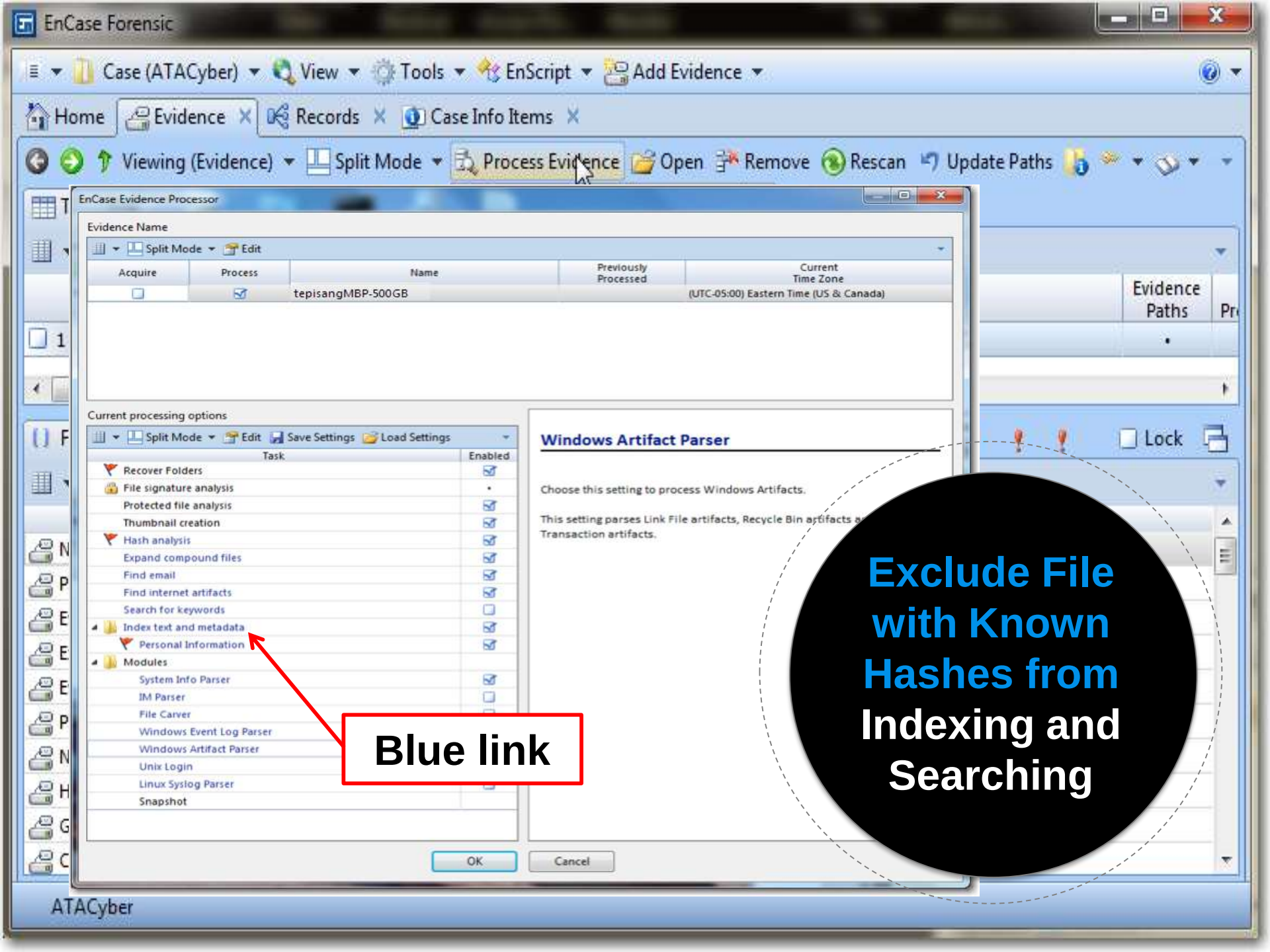

EnCase Forensic
Case (ATACyber)
View
Tools
EnScript
Add Evidence
Home
Reports
Evidence
Records
Viewing (Entry)
Split Mode
Condition
Entries
ATA_Cyber_FilesToHash
Table
Timeline
Gallery
Selected 2/3
Add to hash library
Hash library type
Secondary
Hash library path
C:\Program Files\EnCase7\Hash Libraries\Hash Library #1
Existing hash sets
Name
Category
Hash Set Tags
Count
687 ZZ Child Porn FBI_KP Notable 3,622
688 ZZ known Child Porn Notable 6
689 ZZ Operation Ore -Landslide Notable 5,738
690 ZZ Suspect Child Porn -Case 228 Notable 194
691 ZZ00000, suspected child porn Notable 28
692 ZZ00001 Suspected child porn Notable 6,038
693 ZZ00002 Identified Child Porn Notable 12
694 ZZ00003 Suspected child porn Notable 1,052
695 ZZ00004 Identified Child Porn Notable 81
696 ZZ00005 Suspected Child Porn Notable 147
697 ZZ00006 Suspected Child Porn Notable 3,430
698 ZZ00007a Suspected KP Movies Notable 107
699 ZZ00007b Suspected KP (US Federal) Notable 375
700 ZZ00007c Suspected KP (Alabama 13A... Notable 3,685
701 ZZ00008 Suspected Child Pornography... Notable 6,696
702 ZZ00009 Known Child Pornography Notable 44
703 Sarah Phishing Email Notable Malware 20
704 ATACyberNatashaFiles Notable ATACyber 0
Default Fields
Name
Logical Size
MD5
SHA1
Fields
File Ext
Item Type
Category
Signature Analysis
File Type Tag
Protected
Last Accessed
File Created
Last Written
Code Page
Item Path
Description
Entry Modified
File Deleted
GUID
OK
Cancel
MD5
File Type
afc3d8bb26f31fbe
4f1cc5e25f9c195b
Select the New Set
Check the Newly Created Hash Set to Add Hashes
ATACyber\ATA_Cyber_FilesToHash\IMG_0713.mov
Case Backup

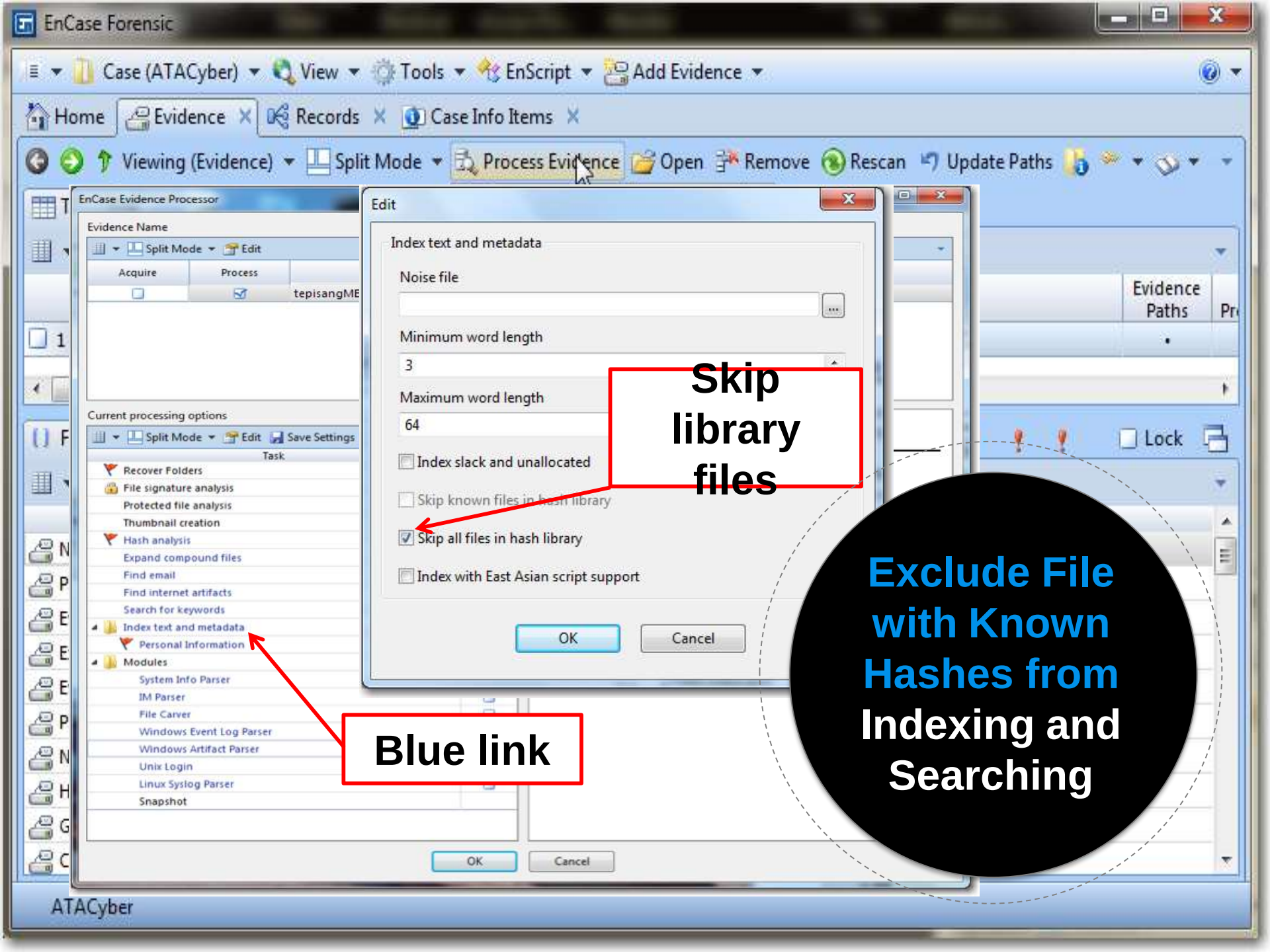

EnCase Forensic
Case (ATACyber)
View
Tools
EnScript
Add Evidence
Home
Reports
Evidence
Records
Zoom In
Zoom Out
100%
BROWSE
REPORT
CASE
Hash Libraries
Hash Library Info
Split Mode
Edit
Change hash library
Manage hash library
Name
Enable
Hash library path
Primary
Secondary
C:\Program Files\EnCase7\Hash Libraries\Hash Library #1
Existing hash sets
Name
Enable
Category
Hash Set Tags
685 Suspected Child Porn (DE UDPD Towe... Notable
686 Suspected Child Porn1 (AL 13A-12-192) Notable
687 ZZ Child Porn FBI_KP Notable
688 ZZ known Child Porn Notable
689 ZZ Operation Ore -Landslide Notable
690 ZZ Suspect Child Porn -Case 228 Notable
691 ZZ00000, suspected child porn Notable
692 ZZ00001 Suspected child porn Notable
693 ZZ00002 Identified Child Porn Notable
694 ZZ00003 Suspected child porn Notable
695 ZZ00004 Identified Child Porn Notable
696 ZZ00005 Suspected Child Porn Notable
697 ZZ00006 Suspected Child Porn Notable
698 ZZ00007a Suspected KP Movies Notable
699 ZZ00007b Suspected KP (US Federal) Notable
700 ZZ00007c Suspected KP (Alabama 13A... Notable
701 ZZ00008 Suspected Child Pornograph... Notable
702 ZZ00009 Known Child Pornography Notable
703 Sarah Phishing Email Notable Malware
704 ATACyberNatashaFiles Notable ATACyber
Help
Hash library name
Secondary
Hash library path
C:\Program Files\EnCase7\Hash Libraries\
Hash Library #1
OK
Cancel
Select the Newly Created Hash Set To Enable in Hash Library
ATACyber\ATA_Cyber_FilesToHash\IMG_0713.mov

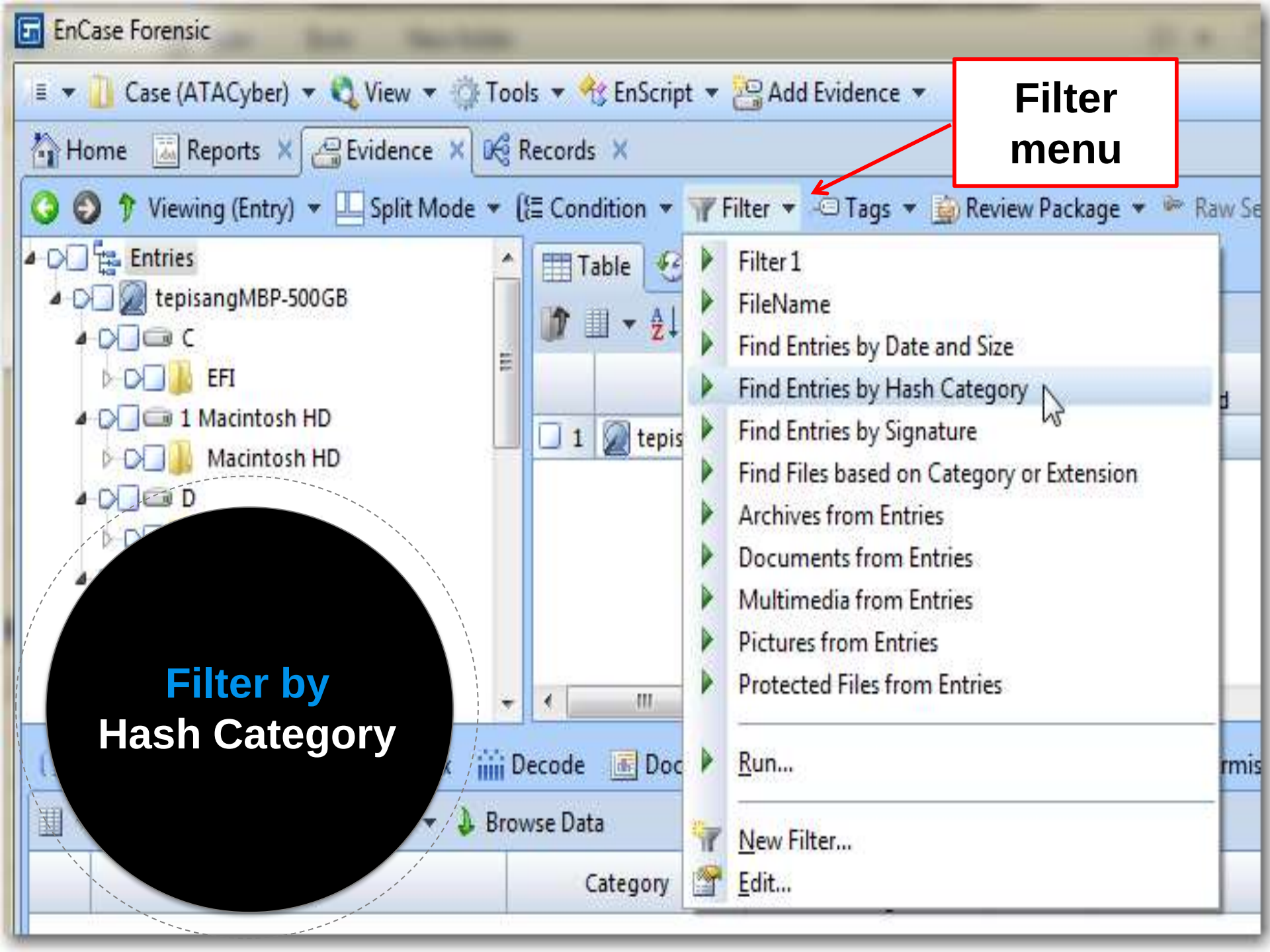

EnCase Forensic
Case (ATACyber)
View
Tools
EnScript
Add Evidence
Home
Reports
Evidence
Records
Viewing (Entry)
Split Mode
Condition
Filter
Tags
Entries
ATA_Cyber_FilesToHash
Table
Timeline
Gallery
Selected 2/3
Name
Hash Sets
MD5
File Type
1
IMG_0713.mov
10750ae3013e6e7dafc3d8bb26f31fbe
2
thegoods.xlsx
098945a3eb398e4b4f1cc5e25f9c195b
Boolean indicator
Fields
Report
Text
Hex
Decode
Doc
Transcript
Picture
Selected 0/1
Split Mode
Browse Data
Name
Category
Hash Set Tags
Hash Items
1
ATACyberNatashaFiles
Notable
ATACyber
C:\Program Files
Hash Sets Created and Visible
ATACyber\ATA_Cyber_FilesToHash\IMG_0713.mov

Using Hash Sets

- Exclude files with known hashes from indexing and searching to save time
- Locate files within hash categories using filters or conditions

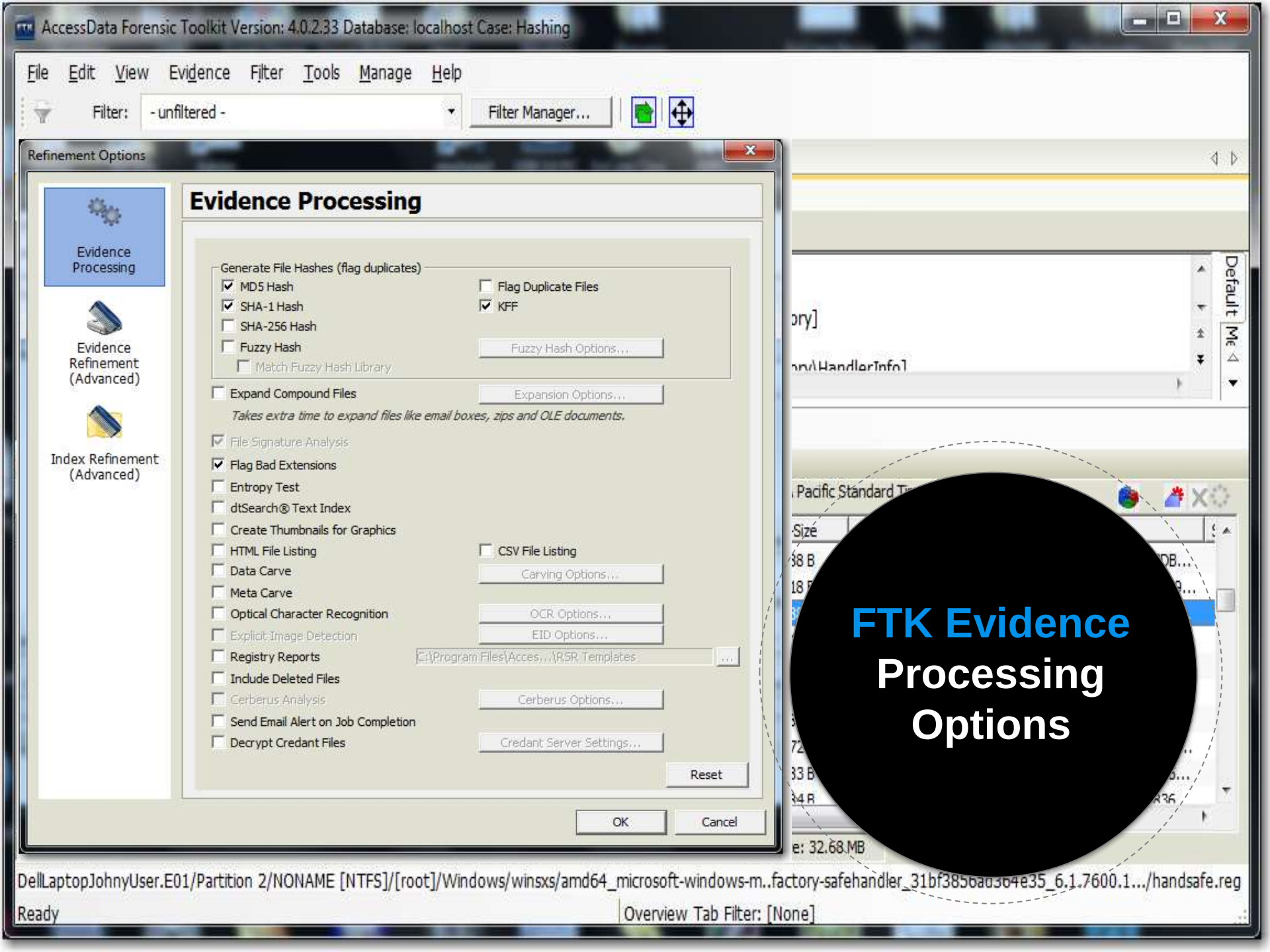

EnCase Forensic
Case (ATACyber)
View
Tools
EnScript
Add Evidence
Home
Evidence
Records
Case Info Items
Viewing (Evidence)
Split Mode
Process Evidence
Open
Remove
Rescan
Update Paths
EnCase Evidence Processor
Evidence Name
Split Mode
Edit
Acquire
Process
Name
Previously Processed
Current Time Zone
tepisangMBP-500GB
(UTC-05:00) Eastern Time (US & Canada)
Evidence Paths
Current processing options
Split Mode
Edit
Save Settings
Load Settings
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
Personal Information
Modules
System Info Parser
IM Parser
File Carver
Windows Event Log Parser
Windows Artifact Parser
Unix Login
Linux Syslog Parser
Snapshot
Windows Artifact Parser
Choose this setting to process Windows Artifacts.
This setting parses Link File artifacts, Recycle Bin artifacts
Transaction artifacts.
OK
Cancel
Lock
ATACyber
Blue link
Exclude File with Known Hashes from Indexing and Searching

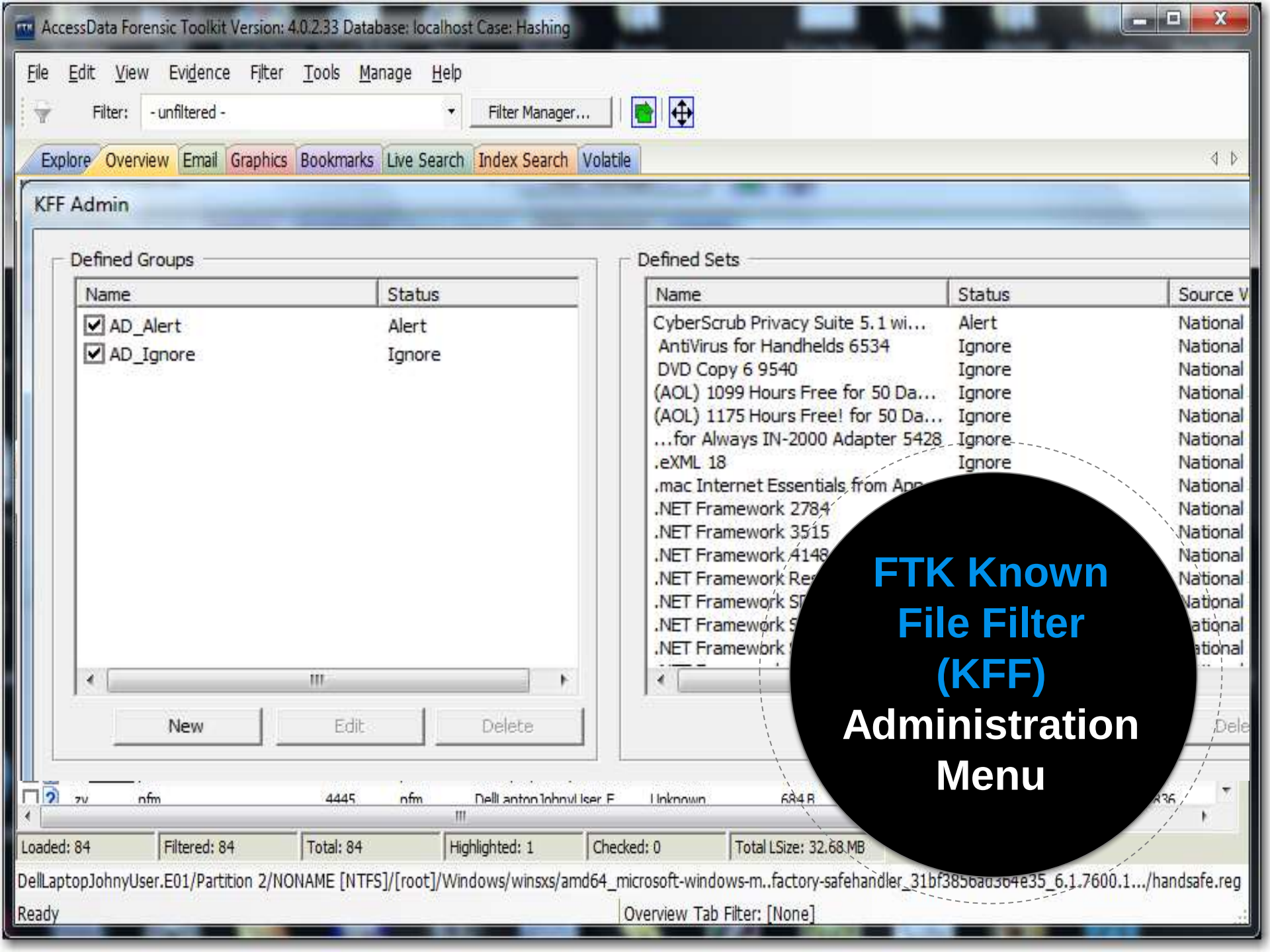

EnCase Forensic
Case (ATACyber)
View
Tools
EnScript
Add Evidence
Home
Evidence
Records
Case Info Items
Viewing (Evidence)
Split Mode
Process Evidence
Open
Remove
Rescan
Update Paths
EnCase Evidence Processor
Evidence Name
Split Mode
Edit
Acquire
Process
Current processing options
Split Mode
Edit
Save Settings
Task
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
Personal Information
Modules
System Info Parser
IM Parser
File Carver
Windows Event Log Parser
Windows Artifact Parser
Unix Login
Linux Syslog Parser
Snapshot
OK
Cancel
Edit
Index text and metadata
Noise file
Minimum word length
3
Maximum word length
64
Index slack and unallocated
Skip known files in hash library
Skip all files in hash library
Index with East Asian script support
OK
Cancel
Skip library files
Blue link
Exclude File with Known Hashes from Indexing and Searching
Evidence Paths
Lock
ATACyber

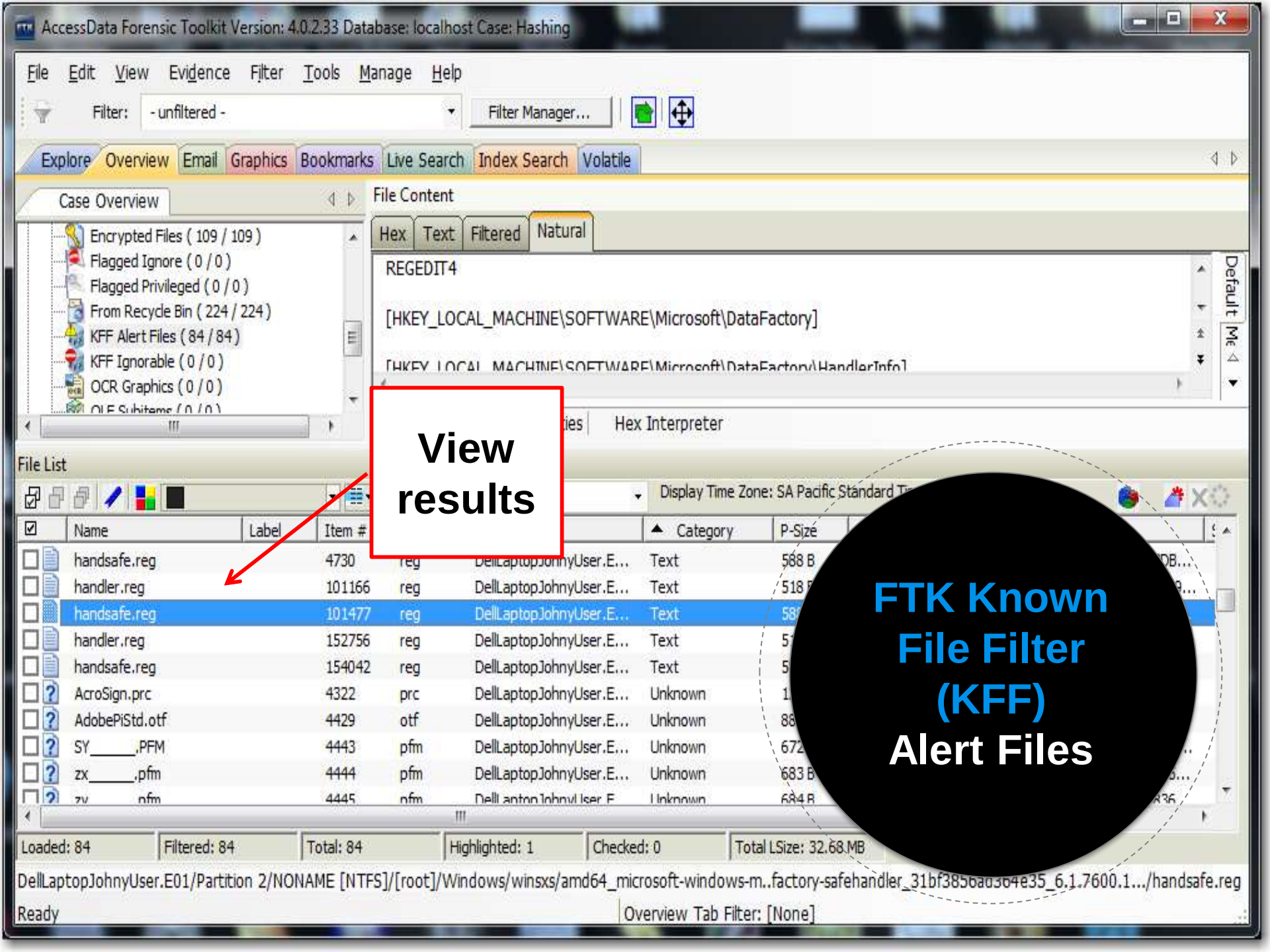

EnCase Forensic
Case (ATACyber)
View
Tools
EnScript
Add Evidence
Home
Reports
Evidence
Records
Viewing (Entry)
Split Mode
Condition
Filter
Tags
Review Package
Entries
tepisangMBP-500GB
C
EFI
1 Macintosh HD
Macintosh HD
D
Table
Filter 1
FileName
Find Entries by Date and Size
Find Entries by Hash Category
Find Entries by Signature
Find Files based on Category or Extension
Archives from Entries
Documents from Entries
Multimedia from Entries
Pictures from Entries
Protected Files from Entries
Run...
New Filter...
Edit...
Decode
Browse Data
Category
Filter menu
Filter by
Hash Category

FTK Hash Analysis Features

- FTK uses the term Known File Filter (KFF)
- Hashing occurs during pre-processing
- Results can be seen using KFF filter feature


AccessData Forensic Toolkit Version: 4.0.2.33 Database: localhost Case: Hashing
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Refinement Options
Evidence Processing
Evidence Refinement (Advanced)
Index Refinement (Advanced)
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
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
HTML File Listing
CSV File Listing
Data Carve
Carving Options...
Meta Carve
Optical Character Recognition
OCR Options...
Explicit Image Detection
EID Options...
Registry Reports
Include Deleted Files
Cerberus Analysis
Cerberus Options...
Send Email Alert on Job Completion
Decrypt Credant Files
Credant Server Settings...
Reset
OK
Cancel
FTK Evidence Processing Options
DellLaptopJohnyUser.E01/Partition 2/NONAME [NTFS]/[root]/Windows/winsxs/amd64_microsoft-windows-m..factory-safehandler_31bf3856ad364e35_6.1.7600.1.../handsafe.reg
Ready
Overview Tab Filter: [None]


AccessData Forensic Toolkit Version: 4.0.2.33 Database: localhost Case: Hashing
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile
KFF Admin
Defined Groups
Name Status
AD_Alert Alert
AD_Ignore Ignore
New Edit Delete
Defined Sets
Name Status Source V
CyberScrub Privacy Suite 5.1 wi... Alert National
AntiVirus for Handhelds 6534 Ignore National
DVD Copy 6 9540 Ignore National
(AOL) 1099 Hours Free for 50 Da... Ignore National
(AOL) 1175 Hours Free! for 50 Da... Ignore National
...for Always IN-2000 Adapter 5428 Ignore National
.eXML 18 Ignore National
.mac Internet Essentials from App National
.NET Framework 2784 National
.NET Framework 3515 National
.NET Framework 4148 National
.NET Framework Re National
.NET Framework SD National
.NET Framework S ational
.NET Framework ational
FTK Known File Filter (KFF) Administration Menu
Loaded: 84 Filtered: 84 Total: 84 Highlighted: 1 Checked: 0 Total LSize: 32.68 MB
DellLaptopJohnyUser.E01/Partition 2/NONAME [NTFS]/[root]/Windows/winsxs/amd64_microsoft-windows-m..factory-safehandler_31bf3856ad364e35_6.1.7600.1.../handsafe.reg
Ready
Overview Tab Filter: [None]


AccessData Forensic Toolkit Version: 4.0.2.33 Database: localhost Case: Hashing
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile
Case Overview
Encrypted Files (109 / 109)
Flagged Ignore (0 / 0)
Flagged Privileged (0 / 0)
From Recycle Bin (224 / 224)
KFF Alert Files (84 / 84)
KFF Ignorable (0 / 0)
OCR Graphics (0 / 0)
File Content
Hex Text Filtered Natural
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DataFactory]
Hex Interpreter
View results
File List
Display Time Zone: SA Pacific Standard Ti
Name Label Item # Category P-Size
handsafe.reg 4730 reg DellLaptopJohnyUser.E... Text 588 B
handler.reg 101166 reg DellLaptopJohnyUser.E... Text 518 B
handsafe.reg 101477 reg DellLaptopJohnyUser.E... Text
handler.reg 152756 reg DellLaptopJohnyUser.E... Text
handsafe.reg 154042 reg DellLaptopJohnyUser.E... Text
AcroSign.prc 4322 prc DellLaptopJohnyUser.E... Unknown
AdobePiStd.otf 4429 otf DellLaptopJohnyUser.E... Unknown
SY_____.PFM 4443 pfm DellLaptopJohnyUser.E... Unknown
zx_____.pfm 4444 pfm DellLaptopJohnyUser.E... Unknown 683 B
Loaded: 84 Filtered: 84 Total: 84 Highlighted: 1 Checked: 0 Total LSize: 32.68 MB
DellLaptopJohnyUser.E01/Partition 2/NONAME [NTFS]/[root]/Windows/winsxs/amd64_microsoft-windows-m..factory-safehandler_31bf3856ad364e35_6.1.7600.1.../handsafe.reg
Ready
Overview Tab Filter: [None]
FTK Known File Filter (KFF) Alert Files

Summary

- You should now be familiar with:
  - Identifying available sources of hash sets
  - Creating hash sets
  - Identifying known files using hash sets

Thanks!

Any questions?

File Signature Analysis

Objective

- By the end of this module, participants will be able to search digital evidence for changes in file extensions

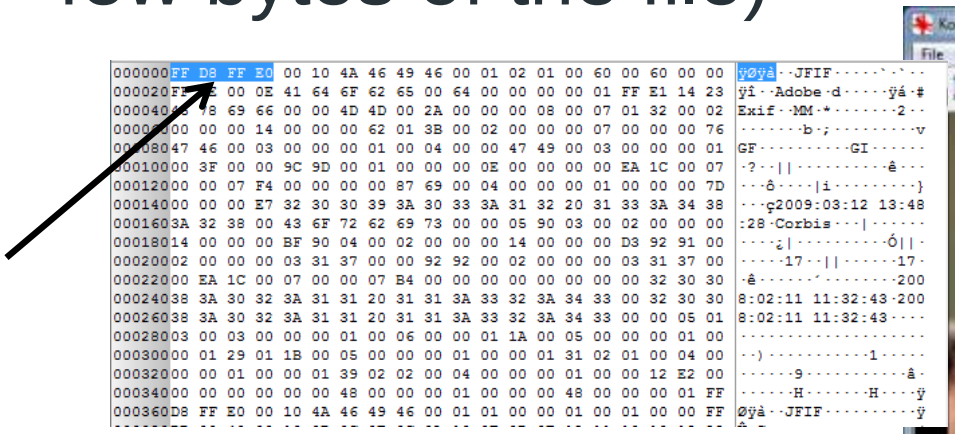
File Types Overview

- Files are accessed by applications and identified by their *type* (header and extension)

- The Windows environment binds a file to an application using its *extension*

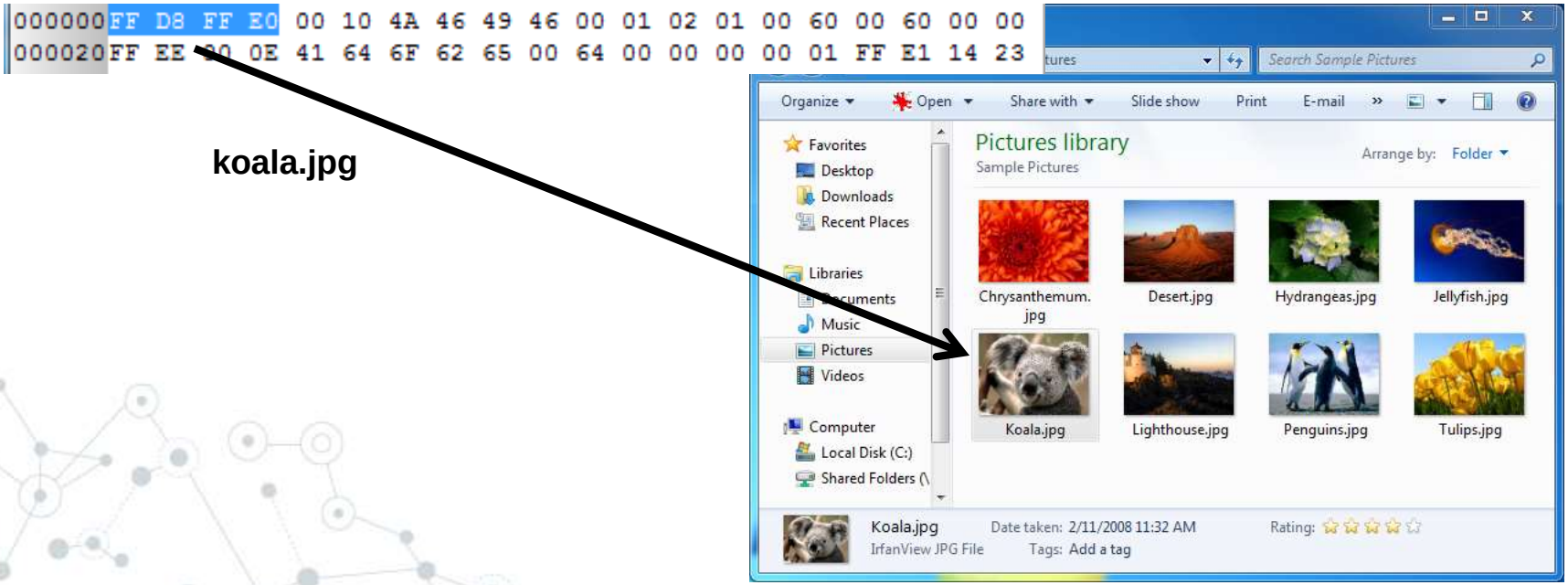
File Header

- Digital signature that applications use to uniquely identify files of a specific type
- Typically located in the *header* (or first few bytes of the file)



File Extension

- Part of the filename that is also typically used to identify the file's type
  - The file header and extension should match
  - Example: koala.jpg → JPEG picture file



Investigative Consideration

- Windows relies on the extension—NOT the header
- Data can be hidden by changing the filename and extension
  - Example: koala.jpg → win32sys.dll
  - Binary content of koala.jpg remains the same
  - Windows will now treat the file as a dynamically linked library

Investigative Software

Digital forensics software:

- Analyzes file headers to correctly identify data

  win32sys.dll ←→ JPG Header = MISMATCH!!

- Installs with a default set of common file signatures

- Allows examiners to create customized signature searches

Summary

- File signature analysis:
  - Is a critical component of digital forensics
  - Quickly identifies files that might have been intentionally hidden
  - Can decrease the data set for analysis

Thanks!

Any questions?

Search Techniques

Objective

- By the end of this module, participants will be able to perform keyword searches

American Standard Code for Information Interchange (ASCII)

- **A character-encoding scheme originally based on U.S. English**
- **Uses 8 bits per characters**
- **Is limited to 256 character codes**

ASCII Table Overview

- **The ASCII table consists of the codes for:**
  - **Characters (Codes 0-127)**
  - **Decimal values (Codes 128-255)**
- **It contains characters found in the Latin alphabet and other characters**

ASCII Table

REGULAR ASCII CHART (character codes 0 – 127)

000d	00h		(nul)	016d	10h	►	(dle)	032d	20h	␣	048d	30h	0	064d	40h	@	080d	50h	P	096d	60h	`	112d	70h	p
001d	01h	☺	(soh)	017d	11h	◄	(dc1)	033d	21h	!	049d	31h	1	065d	41h	A	081d	51h	Q	097d	61h	a	113d	71h	q
002d	02h	●	(stx)	018d	12h	↕	(dc2)	034d	22h	"	050d	32h	2	066d	42h	B	082d	52h	R	098d	62h	b	114d	72h	r
003d	03h	♥	(etx)	019d	13h	‼	(dc3)	035d	23h	#	051d	33h	3	067d	43h	C	083d	53h	S	099d	63h	c	115d	73h	s
004d	04h	♦	(eot)	020d	14h	¶	(dc4)	036d	24h	$	052d	34h	4	068d	44h	D	084d	54h	T	100d	64h	d	116d	74h	t
005d	05h	♣	(enq)	021d	15h	§	(nak)	037d	25h	%	053d	35h	5	069d	45h	E	085d	55h	U	101d	65h	e	117d	75h	u
006d	06h	♠	(ack)	022d	16h	▬	(syn)	038d	26h	&	054d	36h	6	070d	46h	F	086d	56h	V	102d	66h	f	118d	76h	v
007d	07h	•	(bel)	023d	17h	↨	(etb)	039d	27h	'	055d	37h	7	071d	47h	G	087d	57h	W	103d	67h	g	119d	77h	w
008d	08h	◘	(bs)	024d	18h	↑	(can)	040d	28h	(	056d	38h	8	072d	48h	H	088d	58h	X	104d	68h	h	120d	78h	x
009d	09h		(tab)	025d	19h	↓	(em)	041d	29h	)	057d	39h	9	073d	49h	I	089d	59h	Y	105d	69h	i	121d	79h	y
010d	0Ah	◙	(lf)	026d	1Ah	→	(eof)	042d	2Ah	*	058d	3Ah	:	074d	4Ah	J	090d	5Ah	Z	106d	6Ah	j	122d	7Ah	z
011d	0Bh	♂	(vt)	027d	1Bh	←	(esc)	043d	2Bh	+	059d	3Bh	;	075d	4Bh	K	091d	5Bh	[	107d	6Bh	k	123d	7Bh	{
012d	0Ch		(np)	028d	1Ch	∟	(fs)	044d	2Ch	,	060d	3Ch	<	076d	4Ch	L	092d	5Ch	\	108d	6Ch	l	124d	7Ch	|
013d	0Dh	♪	(cr)	029d	1Dh	↔	(gs)	045d	2Dh	-	061d	3Dh	=	077d	4Dh	M	093d	5Dh	]	109d	6Dh	m	125d	7Dh	}
014d	0Eh	♫	(so)	030d	1Eh	▲	(rs)	046d	2Eh	.	062d	3Eh	>	078d	4Eh	N	094d	5Eh	^	110d	6Eh	n	126d	7Eh	~
015d	0Fh	☼	(si)	031d	1Fh	▼	(us)	047d	2Fh	/	063d	3Fh	?	079d	4Fh	O	095d	5Fh	_	111d	6Fh	o	127d	7Fh	⌂

EXTENDED ASCII CHART (character codes 128 – 255) LATIN1/CP1252

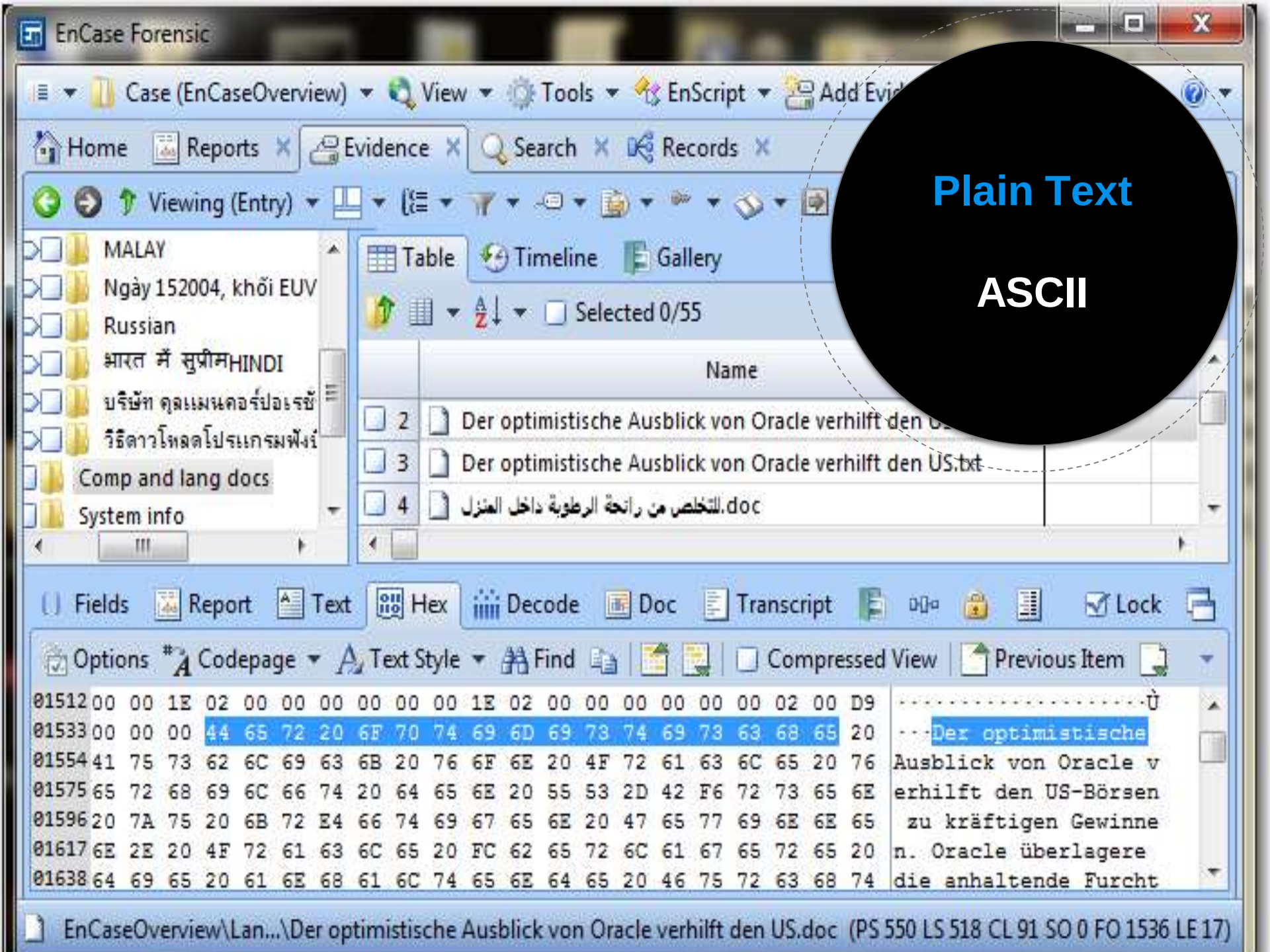
128d	80h	€	144d	90h		160d	A0h		176d	B0h	°	192d	C0h	À	208d	D0h	Ð	224d	E0h	à	240d	F0h	ð
129d	81h		145d	91h	‘	161d	A1h	¡	177d	B1h	±	193d	C1h	Á	209d	D1h	Ñ	225d	E1h	á	241d	F1h	ñ
130d	82h	‚	146d	92h	’	162d	A2h	¢	178d	B2h	²	194d	C2h	Â	210d	D2h	Ò	226d	E2h	â	242d	F2h	ò
131d	83h	ƒ	147d	93h	“	163d	A3h	£	179d	B3h	³	195d	C3h	Ã	211d	D3h	Ó	227d	E3h	ã	243d	F3h	ó
132d	84h	„	148d	94h	”	164d	A4h	¤	180d	B4h	´	196d	C4h	Ä	212d	D4h	Ô	228d	E4h	ä	244d	F4h	ô
133d	85h	…	149d	95h	•	165d	A5h	¥	181d	B5h	µ	197d	C5h	Å	213d	D5h	Õ	229d	E5h	å	245d	F5h	õ
134d	86h	†	150d	96h	–	166d	A6h	¦	182d	B6h	¶	198d	C6h	Æ	214d	D6h	Ö	230d	E6h	æ	246d	F6h	ö
135d	87h	‡	151d	97h	—	167d	A7h	§	183d	B7h	·	199d	C7h	Ç	215d	D7h	×	231d	E7h	ç	247d	F7h	÷
136d	88h	ˆ	152d	98h	˜	168d	A8h	¨	184d	B8h	¸	200d	C8h	È	216d	D8h	Ø	232d	E8h	è	248d	F8h	ø
137d	89h	‰	153d	99h	™	169d	A9h	©	185d	B9h	¹	201d	C9h	É	217d	D9h	Ù	233d	E9h	é	249d	F9h	ù
138d	8Ah	Š	154d	9Ah	š	170d	AAh	ª	186d	BAh	º	202d	CAh	Ê	218d	DAh	Ú	234d	EAh	ê	250d	FAh	ú
139d	8Bh	‹	155d	9Bh	›	171d	ABh	«	187d	BBh	»	203d	CBh	Ë	219d	DBh	Û	235d	EBh	ë	251d	FBh	û
140d	8Ch	Œ	156d	9Ch	œ	172d	ACh	¬	188d	BCh	¼	204d	CCh	Ì	220d	DCh	Ü	236d	ECh	ì	252d	FCh	ü
141d	8Dh		157d	9Dh		173d	ADh		189d	BDh	½	205d	CDh	Í	221d	DDh	Ý	237d	EDh	í	253d	FDh	ý
142d	8Eh	Ž	158d	9Eh	ž	174d	AEh	®	190d	BEh	¾	206d	CEh	Î	222d	DEh	Þ	238d	EEh	î	254d	FEh	þ
143d	8Fh		159d	9Fh	Ÿ	175d	AFh	¯	191d	BFh	¿	207d	CFh	Ï	223d	DFh	ß	239d	EFh	ï	255d	FFh	ÿ

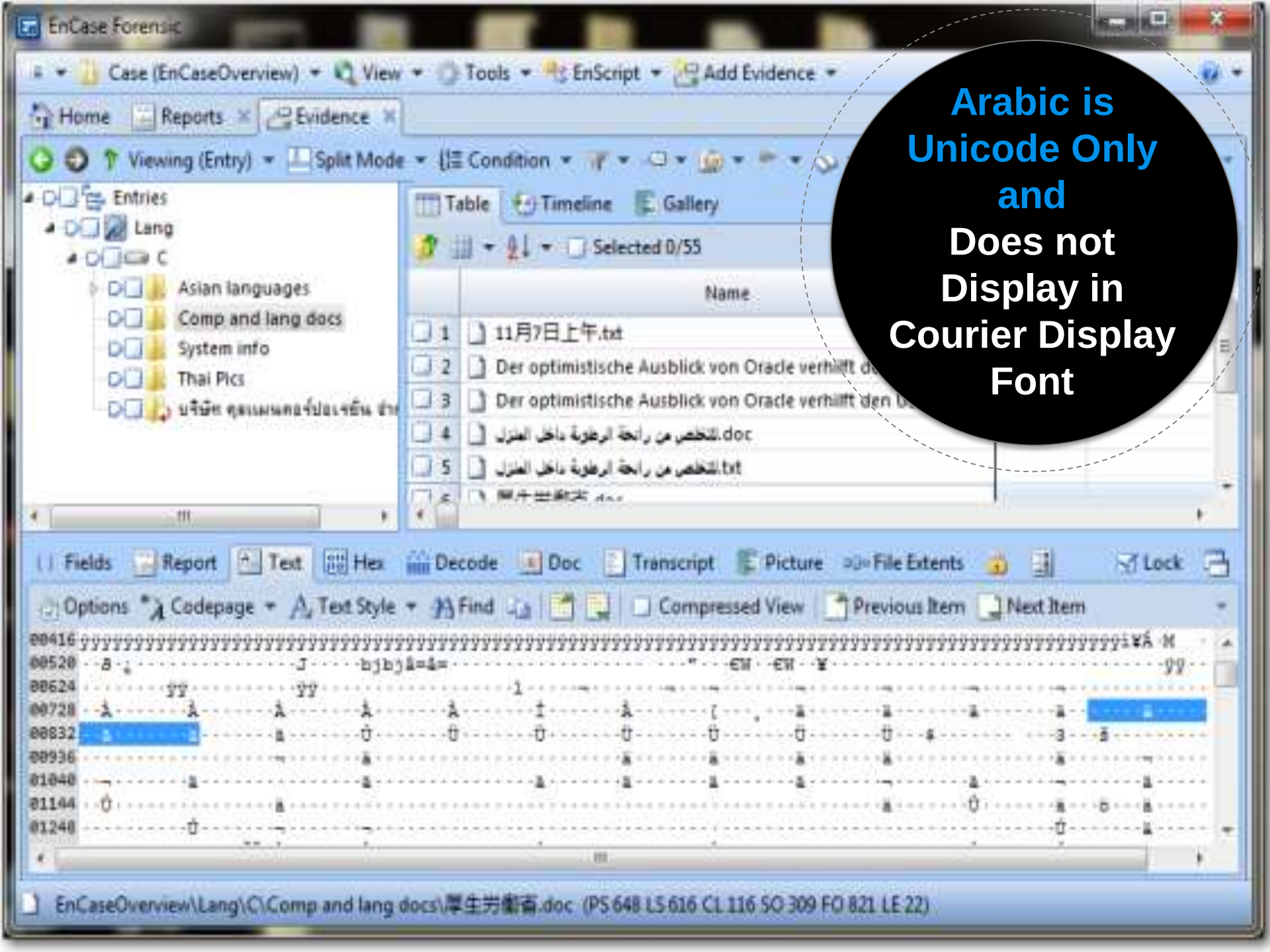
Unicode

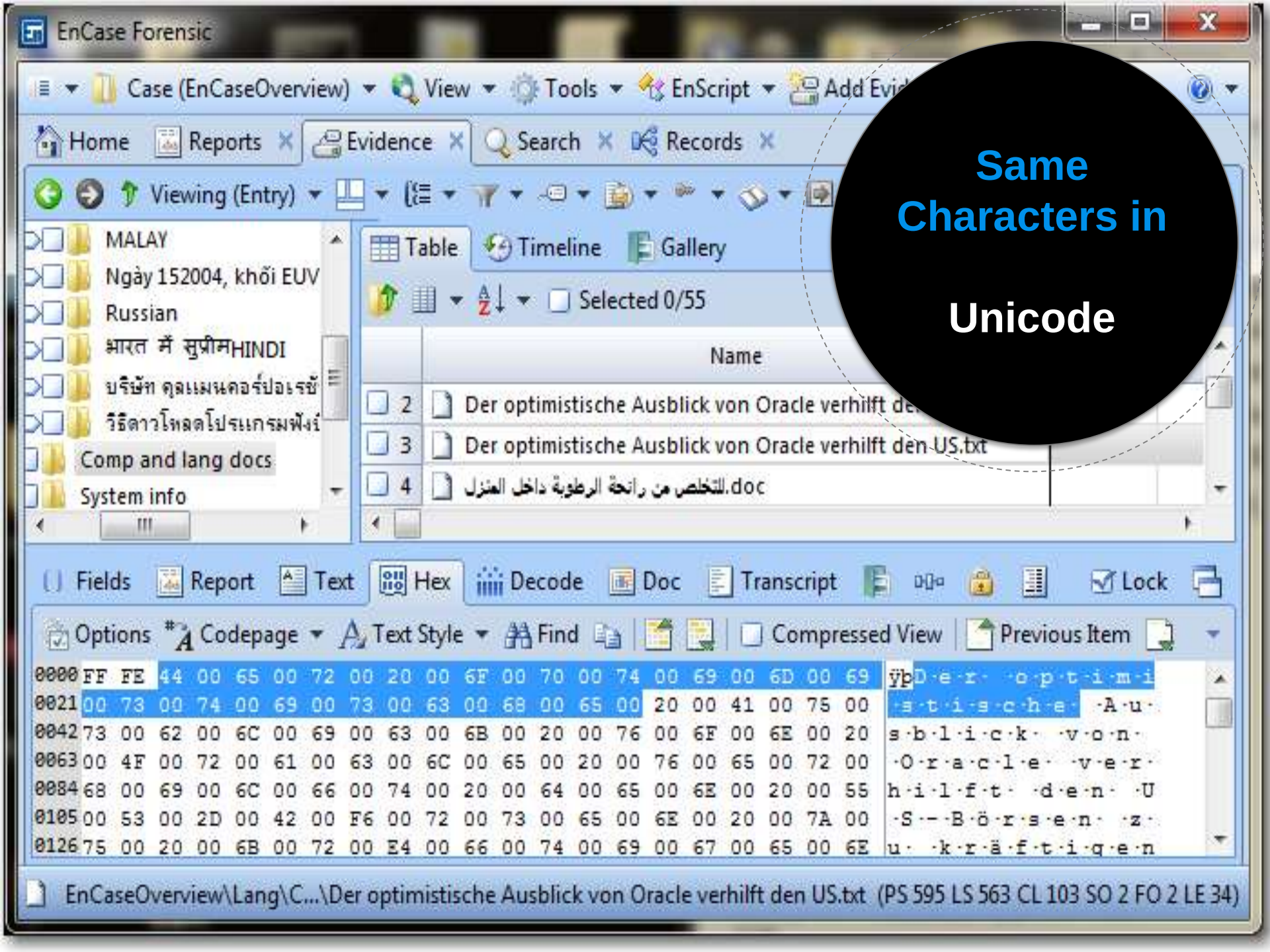
- **Initially, telegraph and computers used only English/Latin characters**
- **When other languages were required, ASCII character codes were insufficient**

Unicode

- **Uses a unique two-byte number for every character**
- **Can define more than 65,000 characters, allowing the computer to display any world language**

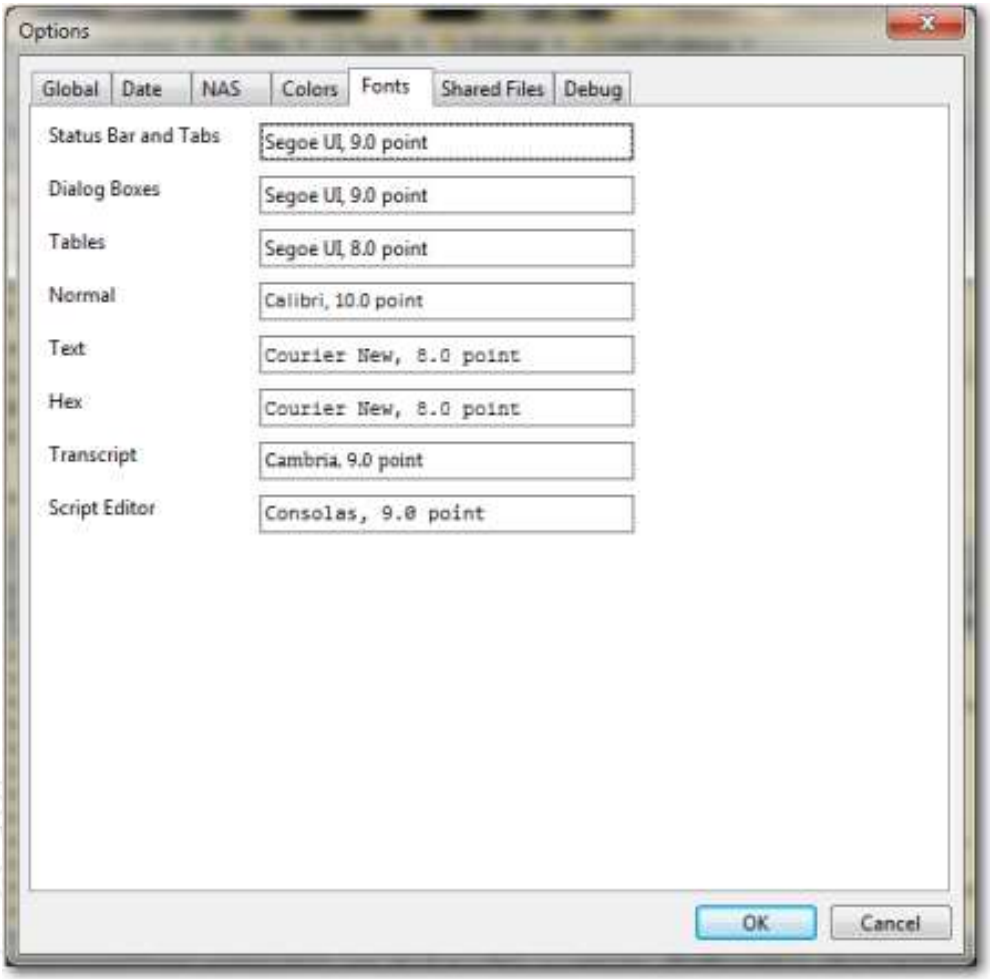

EnCase Forensic
Case (EnCaseOverview)
View
Tools
EnScript
Home
Reports
Evidence
Search
Records
Viewing (Entry)
MALAY
Ngày 152004, khối EUV
Russian
भारत में सुप्रीमHINDI
บริษัท คุลแมนคอร์ปอเรชั
วิธีดาวโหลดโปรแกรมฟังเ
Comp and lang docs
System info
Table
Timeline
Gallery
Selected 0/55
Name
2 Der optimistische Ausblick von Oracle verhilft den
3 Der optimistische Ausblick von Oracle verhilft den US.txt
4 للتخلص من رائحة الرطوبة داخل المنزل.doc
Fields
Report
Text
Hex
Decode
Doc
Transcript
Lock
Options
Codepage
Text Style
Find
Compressed View
Previous Item
01512 00 00 1E 02 00 00 00 00 00 00 1E 02 00 00 00 00 00 00 02 00 D9
01533 00 00 00 44 65 72 20 6F 70 74 69 6D 69 73 74 69 73 63 68 65 20
01554 41 75 73 62 6C 69 63 6B 20 76 6F 6E 20 4F 72 61 63 6C 65 20 76
01575 65 72 68 69 6C 66 74 20 64 65 6E 20 55 53 2D 42 F6 72 73 65 6E
01596 20 7A 75 20 6B 72 E4 66 74 69 67 65 6E 20 47 65 77 69 6E 6E 65
01617 6E 2E 20 4F 72 61 63 6C 65 20 FC 62 65 72 6C 61 67 65 72 65 20
01638 64 69 65 20 61 6E 68 61 6C 74 65 6E 64 65 20 46 75 72 63 68 74
Plain Text
ASCII
EnCaseOverview\Lan...\Der optimistische Ausblick von Oracle verhilft den US.doc (PS 550 LS 518 CL 91 SO 0 FO 1536 LE 17)


EnCase Forensic
Case (EnCaseOverview)
View
Tools
EnScript
Add Evidence
Home
Reports
Evidence
Viewing (Entry)
Split Mode
Condition
Entries
Lang
C
Asian languages
Comp and lang docs
System info
Thai Pics
Table
Timeline
Gallery
Selected 0/55
Name
1 11月7日上午.txt
2 Der optimistische Ausblick von Oracle verhilft
3 Der optimistische Ausblick von Oracle verhilft den
4 .doc
5 .txt
Fields
Report
Text
Hex
Decode
Doc
Transcript
Picture
File Extents
Lock
Options
Codepage
Text Style
Find
Compressed View
Previous Item
Next Item
EnCaseOverview\Lang\C\Comp and lang docs\.doc (PS 648 LS 616 CL 116 SO 309 FO 821 LE 22)
Arabic is Unicode Only and Does not Display in Courier Display Font


EnCase Forensic
Case (EnCaseOverview)
View
Tools
EnScript
Home
Reports
Evidence
Search
Records
Viewing (Entry)
MALAY
Ngày 152004, khối EUV
Russian
भारत में सुप्रीमHINDI
บริษัท คุลแมนคอร์ปอเรชั
วิธีดาวโหลดโปรแกรมฟังเ
Comp and lang docs
System info
Table
Timeline
Gallery
Selected 0/55
Name
2 Der optimistische Ausblick von Oracle verhilft de
3 Der optimistische Ausblick von Oracle verhilft den US.txt
4 للتخلص من رائحة الرطوبة داخل المنزل.doc
Fields
Report
Text
Hex
Decode
Doc
Transcript
Lock
Options
Codepage
Text Style
Find
Compressed View
Previous Item
0000 FF FE 44 00 65 00 72 00 20 00 6F 00 70 00 74 00 69 00 6D 00 69
0021 00 73 00 74 00 69 00 73 00 63 00 68 00 65 00 20 00 41 00 75 00
0042 73 00 62 00 6C 00 69 00 63 00 6B 00 20 00 76 00 6F 00 6E 00 20
0063 00 4F 00 72 00 61 00 63 00 6C 00 65 00 20 00 76 00 65 00 72 00
0084 68 00 69 00 6C 00 66 00 74 00 20 00 64 00 65 00 6E 00 20 00 55
0105 00 53 00 2D 00 42 00 F6 00 72 00 73 00 65 00 6E 00 20 00 7A 00
0126 75 00 20 00 6B 00 72 00 E4 00 66 00 74 00 69 00 67 00 65 00 6E
EnCaseOverview\Lang\C...\Der optimistische Ausblick von Oracle verhilft den US.txt (PS 595 LS 563 CL 103 SO 2 FO 2 LE 34)
Same
Characters in
Unicode

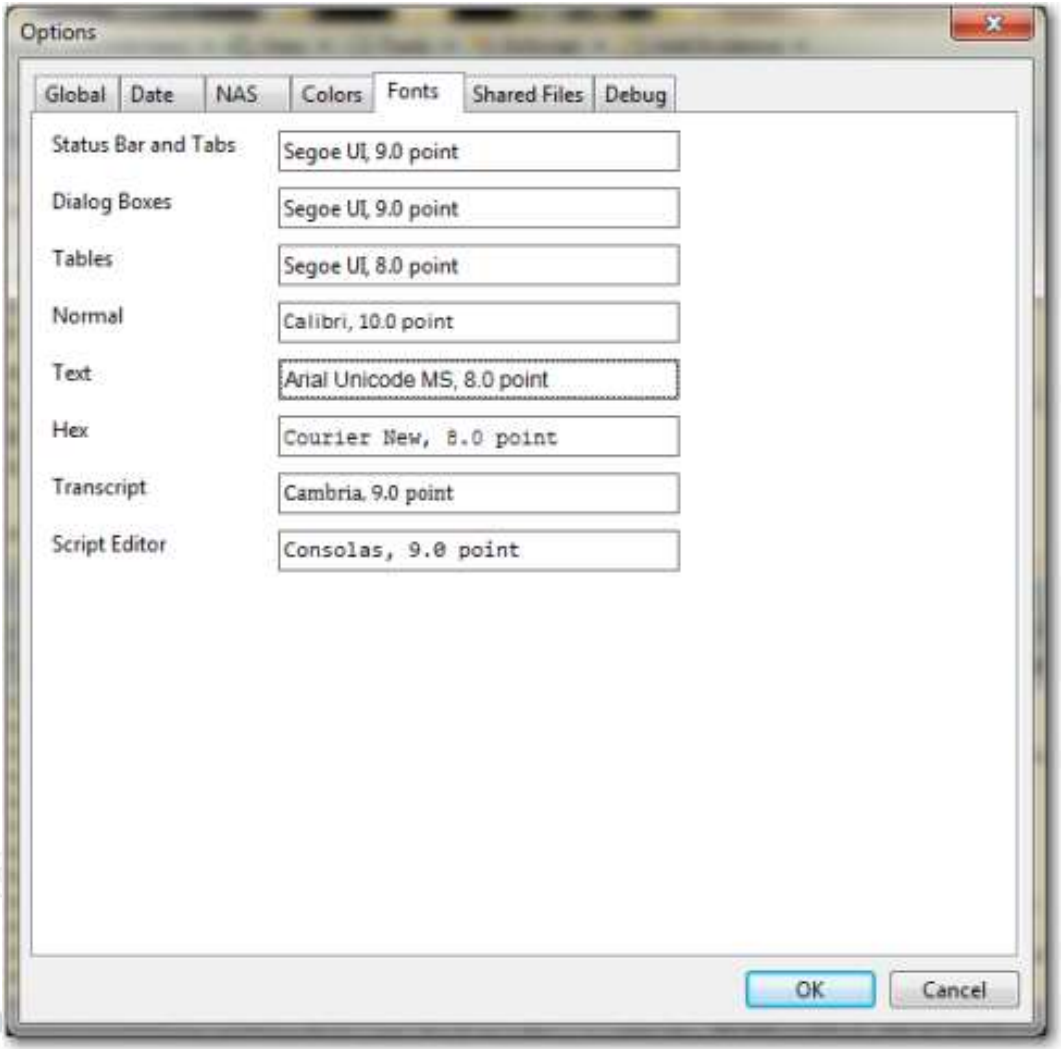
Modifying the Display Font

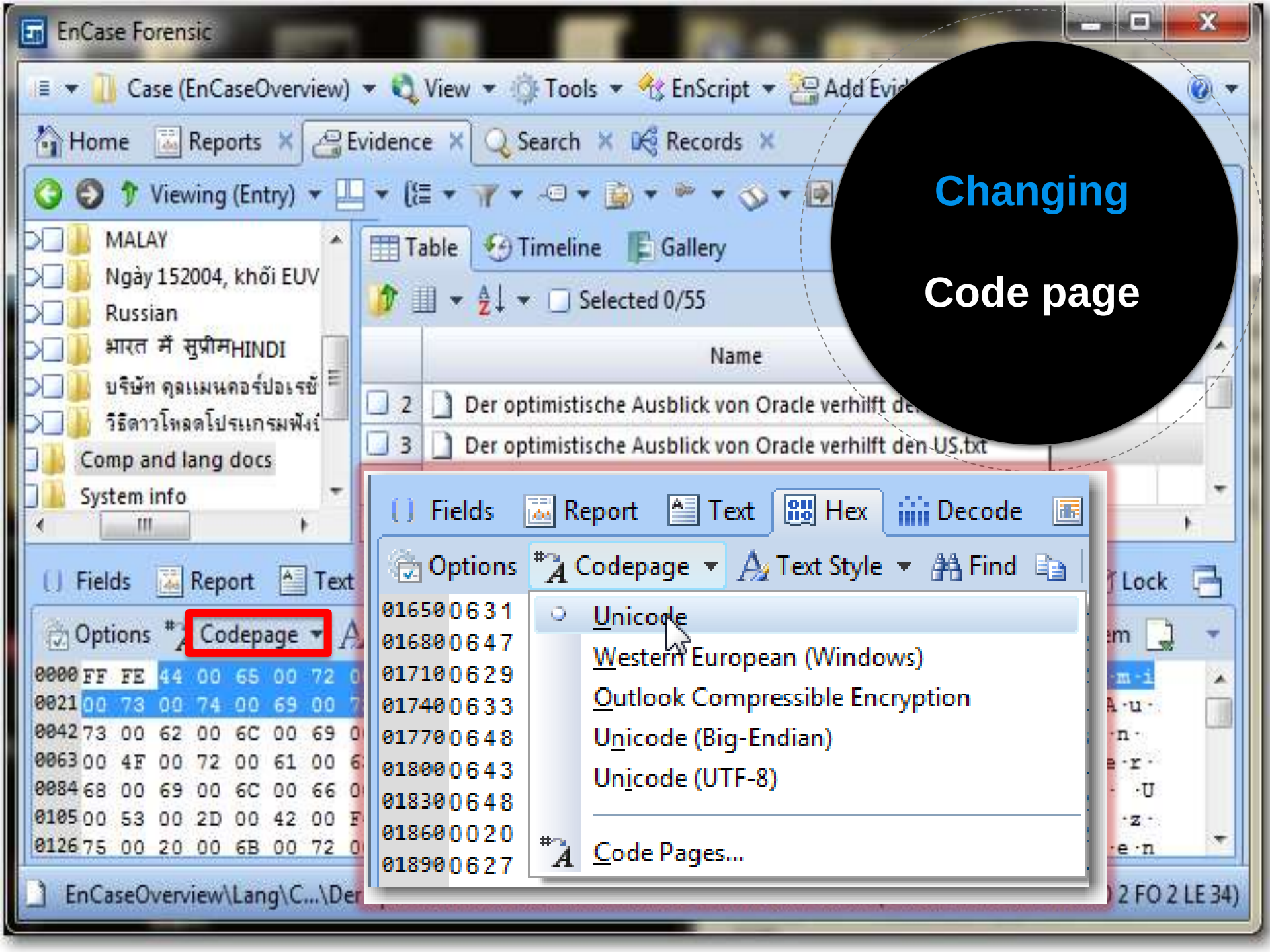
- **To display Unicode fonts, go to: Tools > Options > Fonts**



Changing the Font

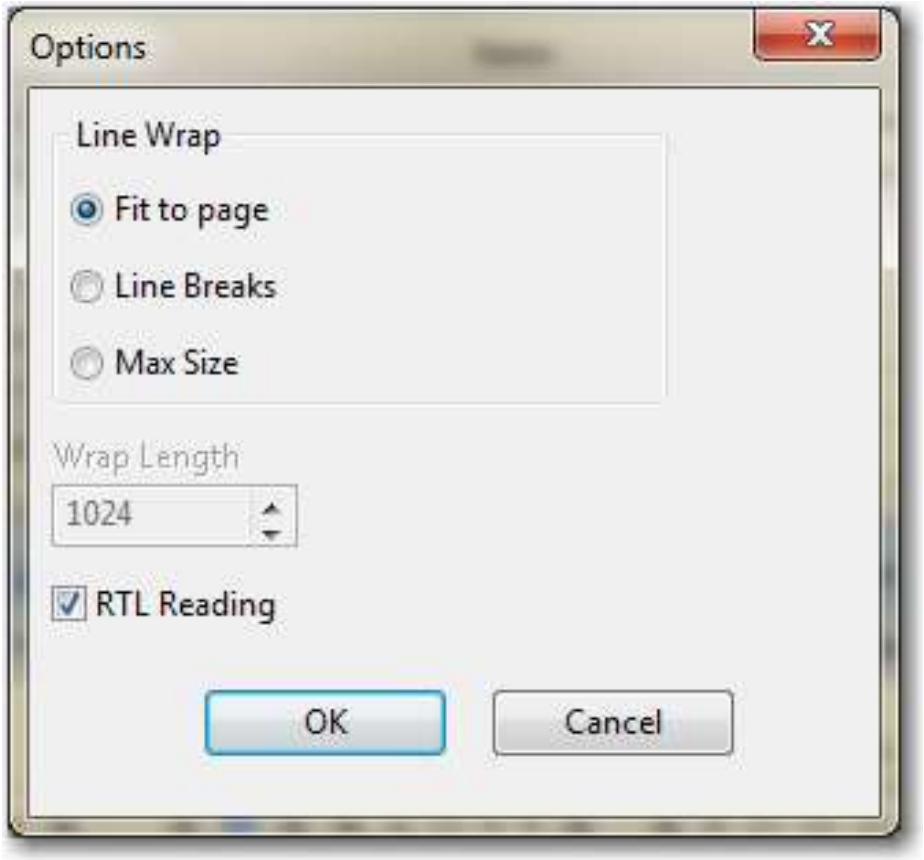
- **Select Arial Unicode MS Font**

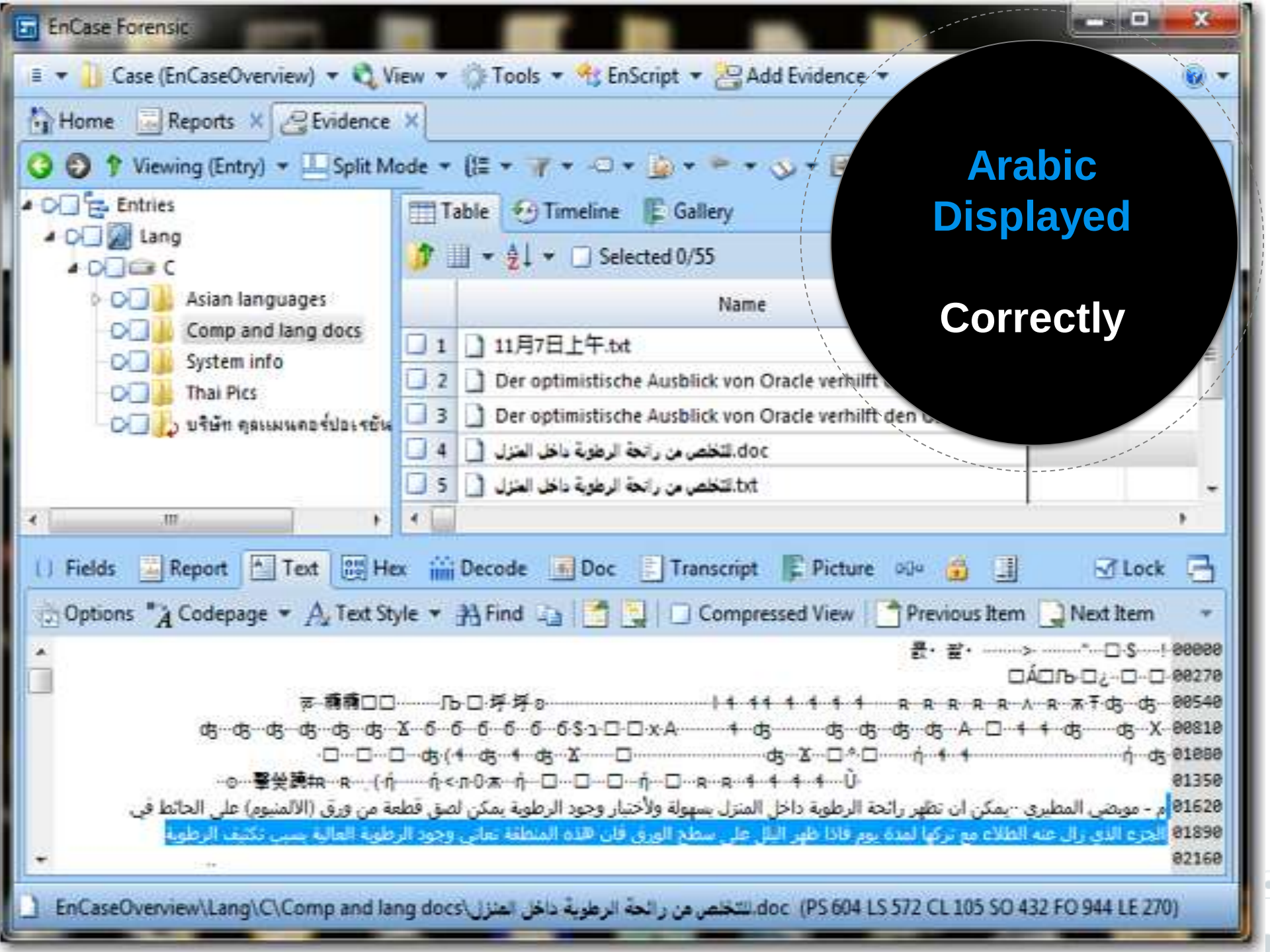



EnCase Forensic
Case (EnCaseOverview)
View
Tools
EnScript
Home
Reports
Evidence
Search
Records
Viewing (Entry)
MALAY
Ngày 152004, khối EUV
Russian
भारत में सुप्रीमHINDI
Comp and lang docs
System info
Table
Timeline
Gallery
Selected 0/55
Name
2 Der optimistische Ausblick von Oracle verhilft de
3 Der optimistische Ausblick von Oracle verhilft den US.txt
Changing
Code page
Fields
Report
Text
Hex
Decode
Options
Codepage
Text Style
Find
Lock
Unicode
Western European (Windows)
Outlook Compressible Encryption
Unicode (Big-Endian)
Unicode (UTF-8)
Code Pages...
EnCaseOverview\Lang\C...\Der

Changing Reading Direction

- **On Options Menu, Check RTL Reading**



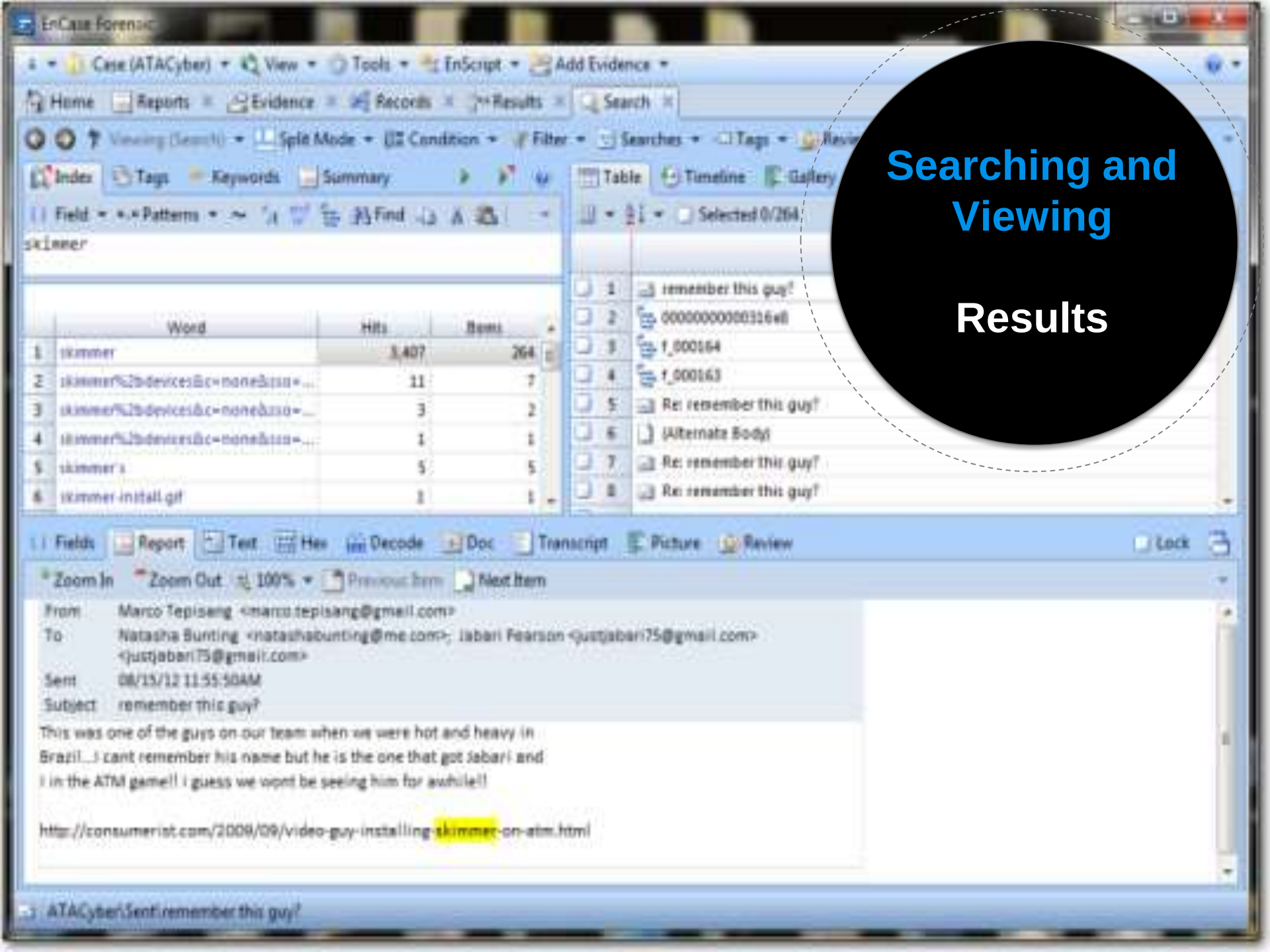

EnCase Forensic
Case (EnCaseOverview)
View
Tools
EnScript
Add Evidence
Home
Reports
Evidence
Viewing (Entry)
Split Mode
Entries
Lang
C
Asian languages
Comp and lang docs
System info
Thai Pics
Table
Timeline
Gallery
Selected 0/55
Name
1 11月7日上午.txt
2 Der optimistische Ausblick von Oracle verhilft
3 Der optimistische Ausblick von Oracle verhilft den
4 للتخلص من رائحة الرطوبة داخل المنزل.doc
5 للتخلص من رائحة الرطوبة داخل المنزل.txt
Fields
Report
Text
Hex
Decode
Doc
Transcript
Picture
Lock
Options
Codepage
Text Style
Find
Compressed View
Previous Item
Next Item
Arabic Displayed
Correctly
EnCaseOverview\Lang\C\Comp and lang docs\للتخلص من رائحة الرطوبة داخل المنزل.doc (PS 604 LS 572 CL 105 SO 432 FO 944 LE 270)

EnCase

Search Techniques

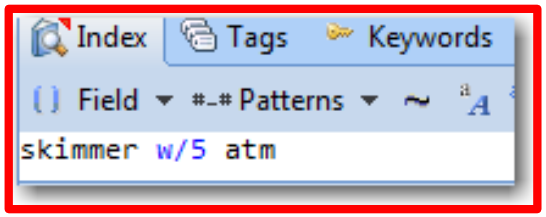
Conducting an Index Search

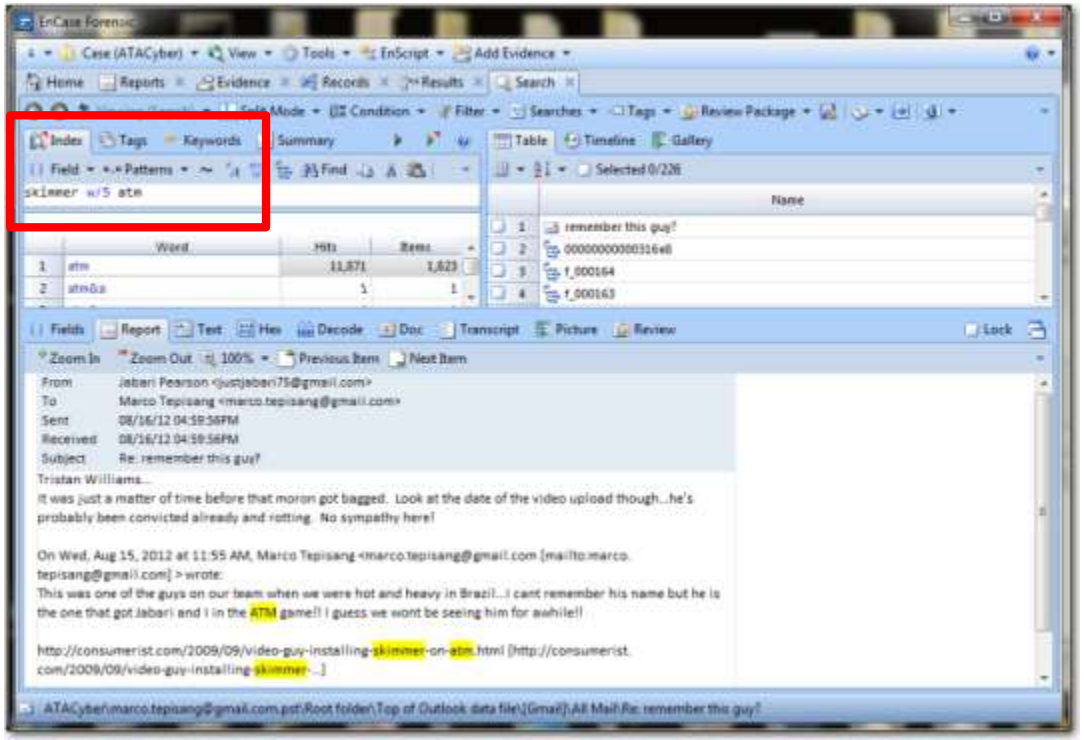
- **To create the index:**
  - **Run the EnCase Evidence Processor**
  - **Enable the *Index text and metadata* feature**
  - **Index personal information (optional)**

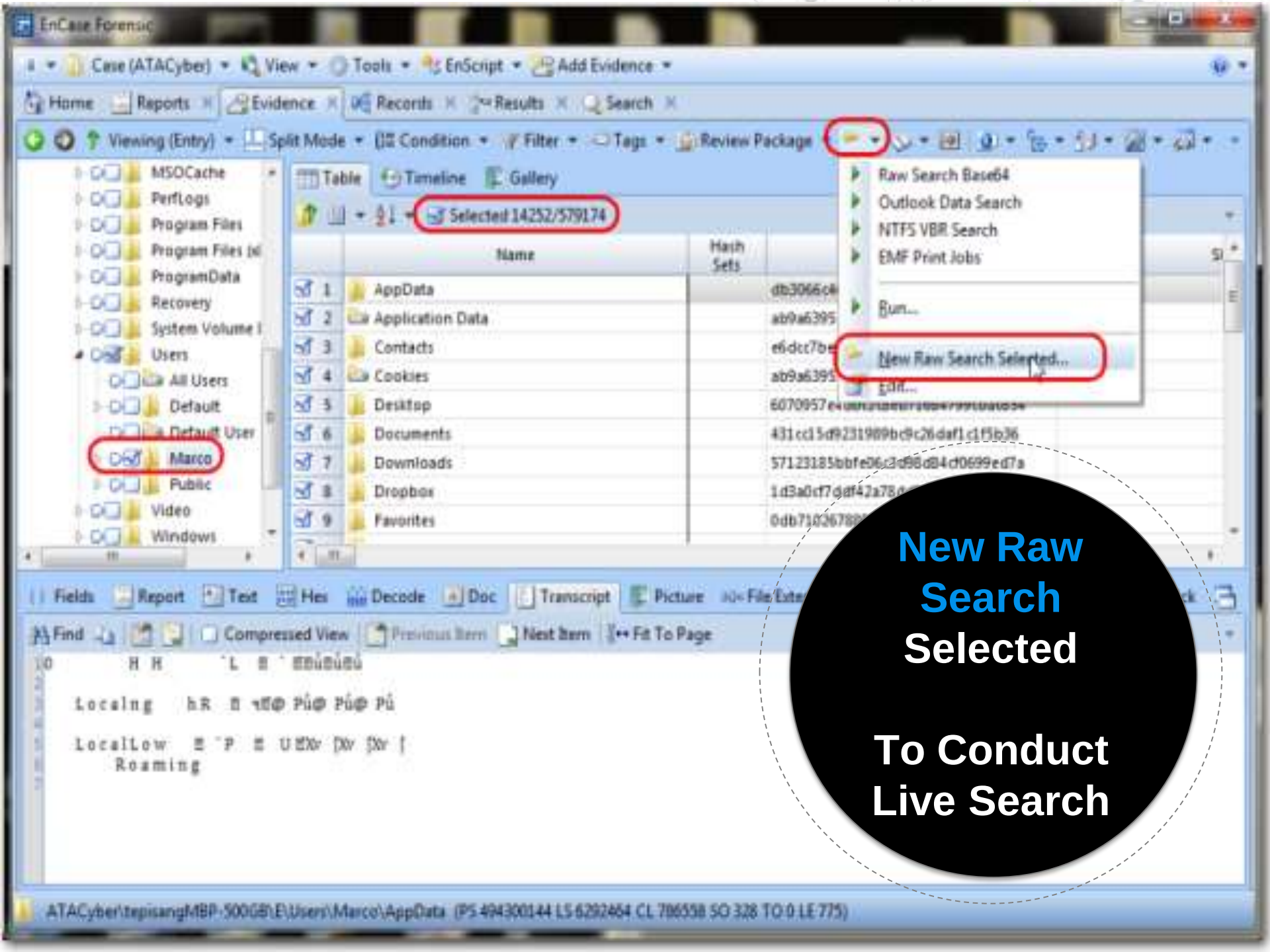

Searching and Viewing
Results

Proximity Searches

- **Keyword1 w/35 Keyword2 or keywords in quotes**
- **Boolean logic**
- **Stemming and fuzzy searches**
- **Pattern searches**

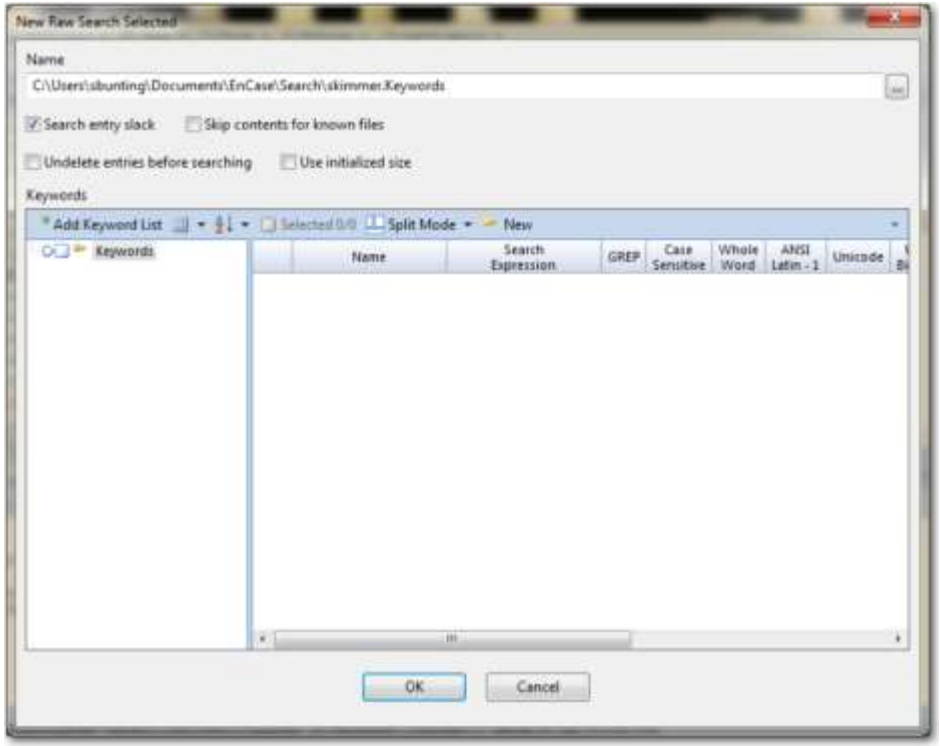





New Raw Search Selected
To Conduct Live Search

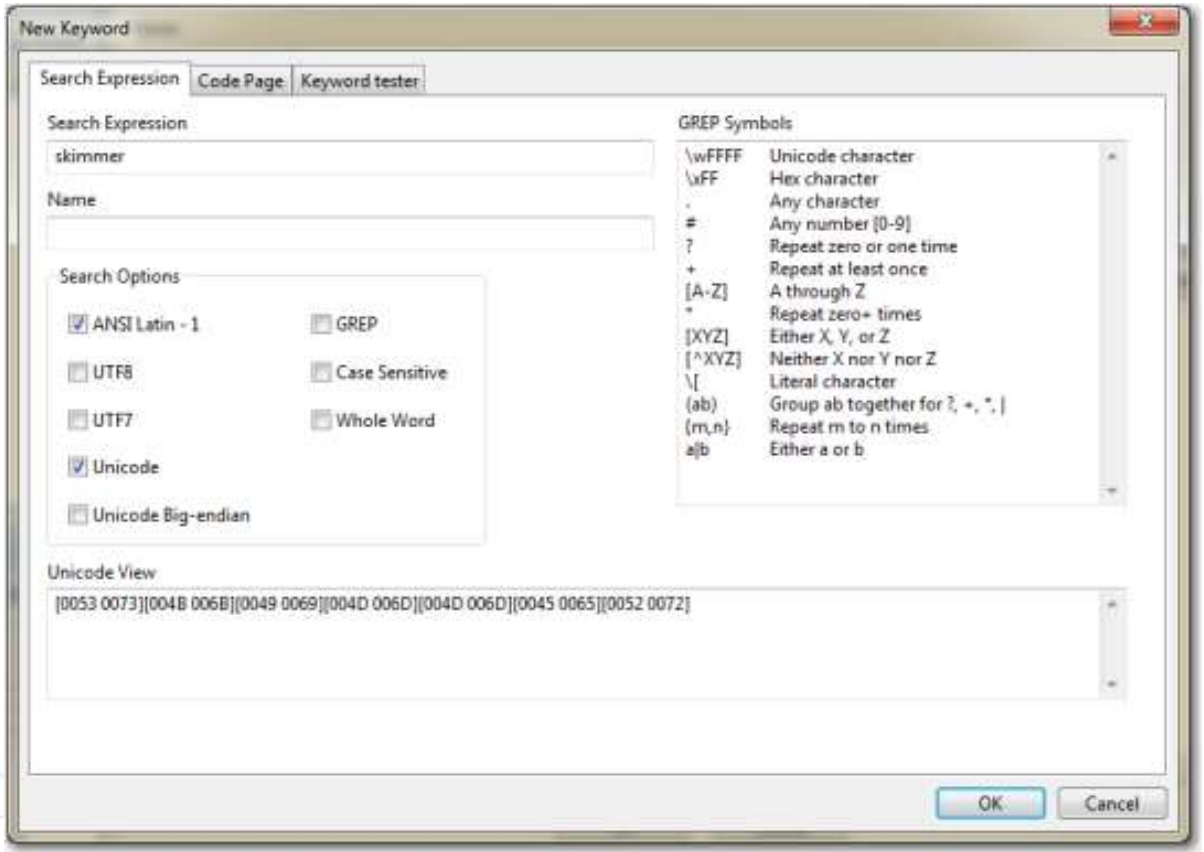
Creating a New Keyword

- **On the New Raw Search Selected Menu:**
  - **Name the search**
  - **Select the path for storage**
  - **Click *New* in the keywords toolbar**



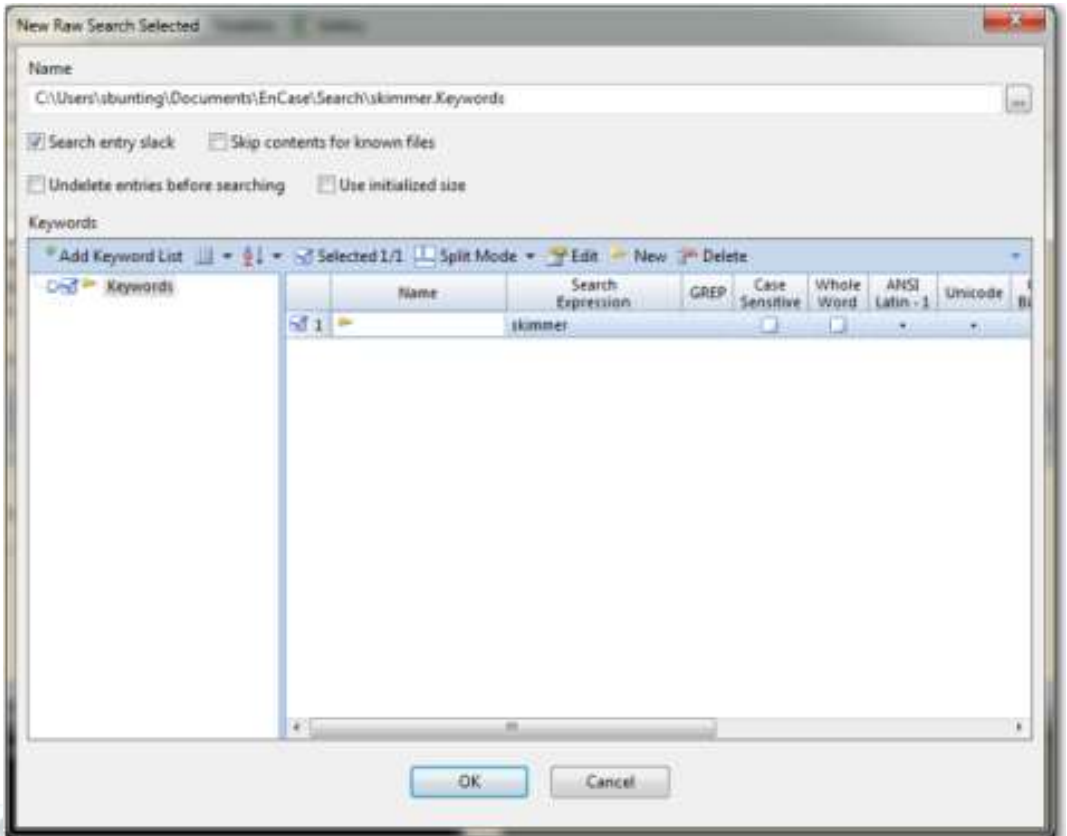
Keyword Search Expression

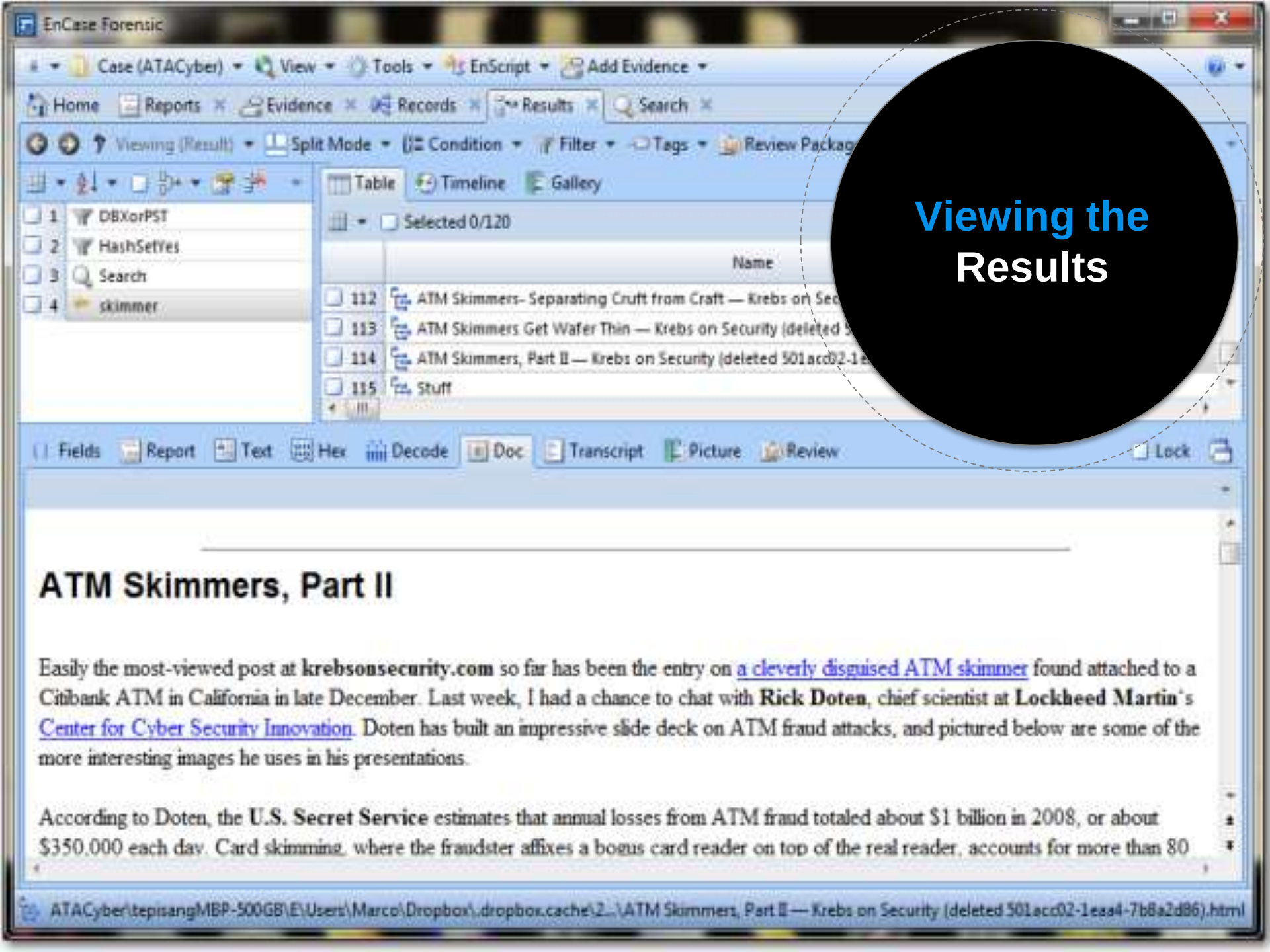
- **On the New Keyword Menu:**
  - **Type the keyword under Search Expression**
  - **Select the Unicode search option**



Running the Search

- Verify the file name, path, and search options
- Click OK to start the search
- Monitor the progress bar





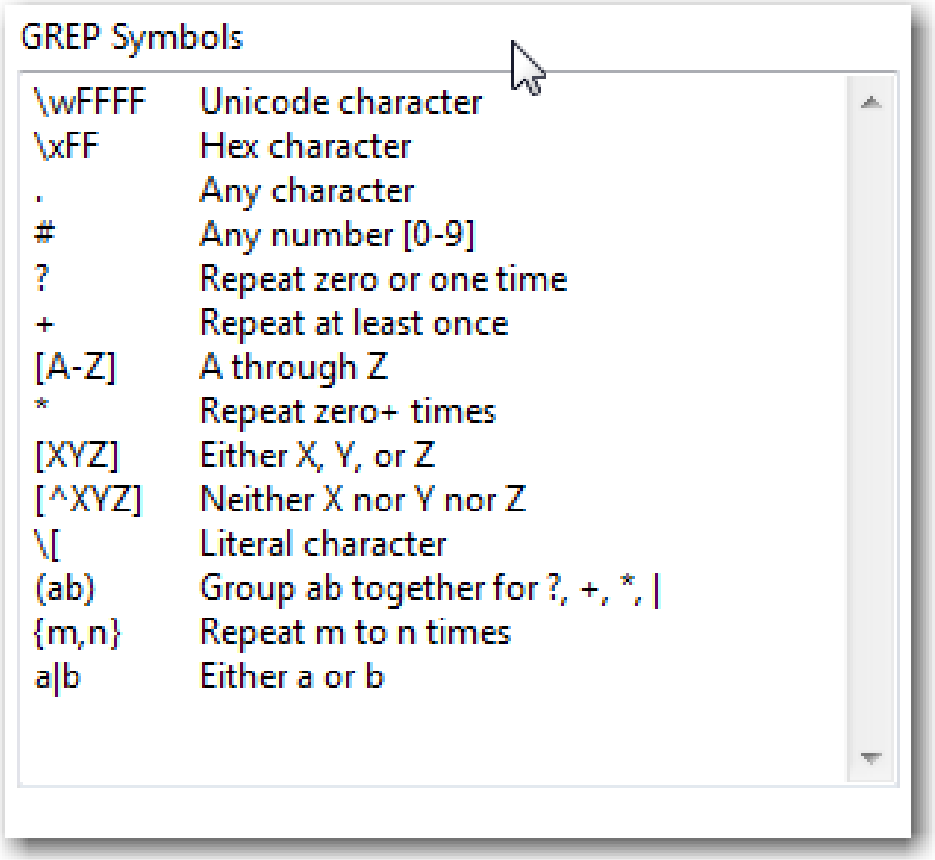
Viewing the Results

GREP Search

- **Global Regular Expression Parser (GREP):**
  - **Searches for plain text with regular expressions**
  - **Matches strings of text against characters, words, numbers, patterns, wildcards, etc.**

GREP Symbols

- **From the New Keyword Menu, select GREP symbols to combine with text and numbers**

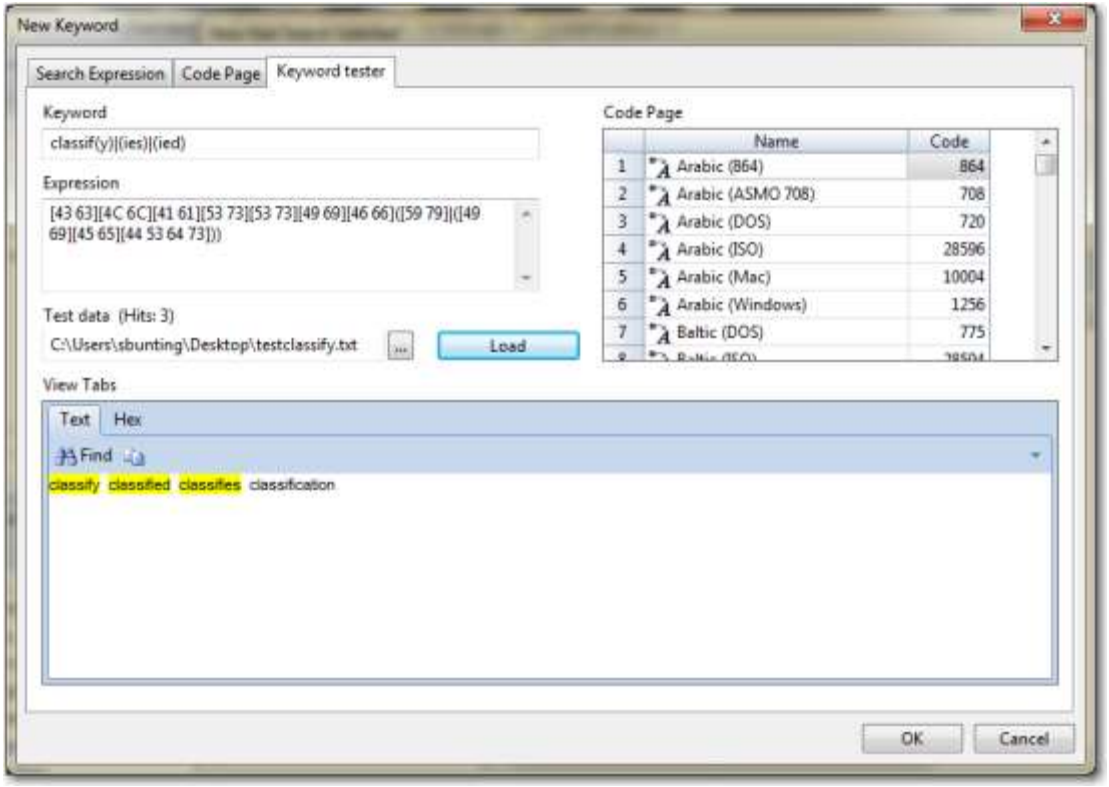


GREP Examples

GREP Search	Results
re[ae]d	Will find read or reed
reads?	Will find read or reads
classif(y)|(ied)|(ies)	Will find classify or classified or classifies

Using the Keyword Tester

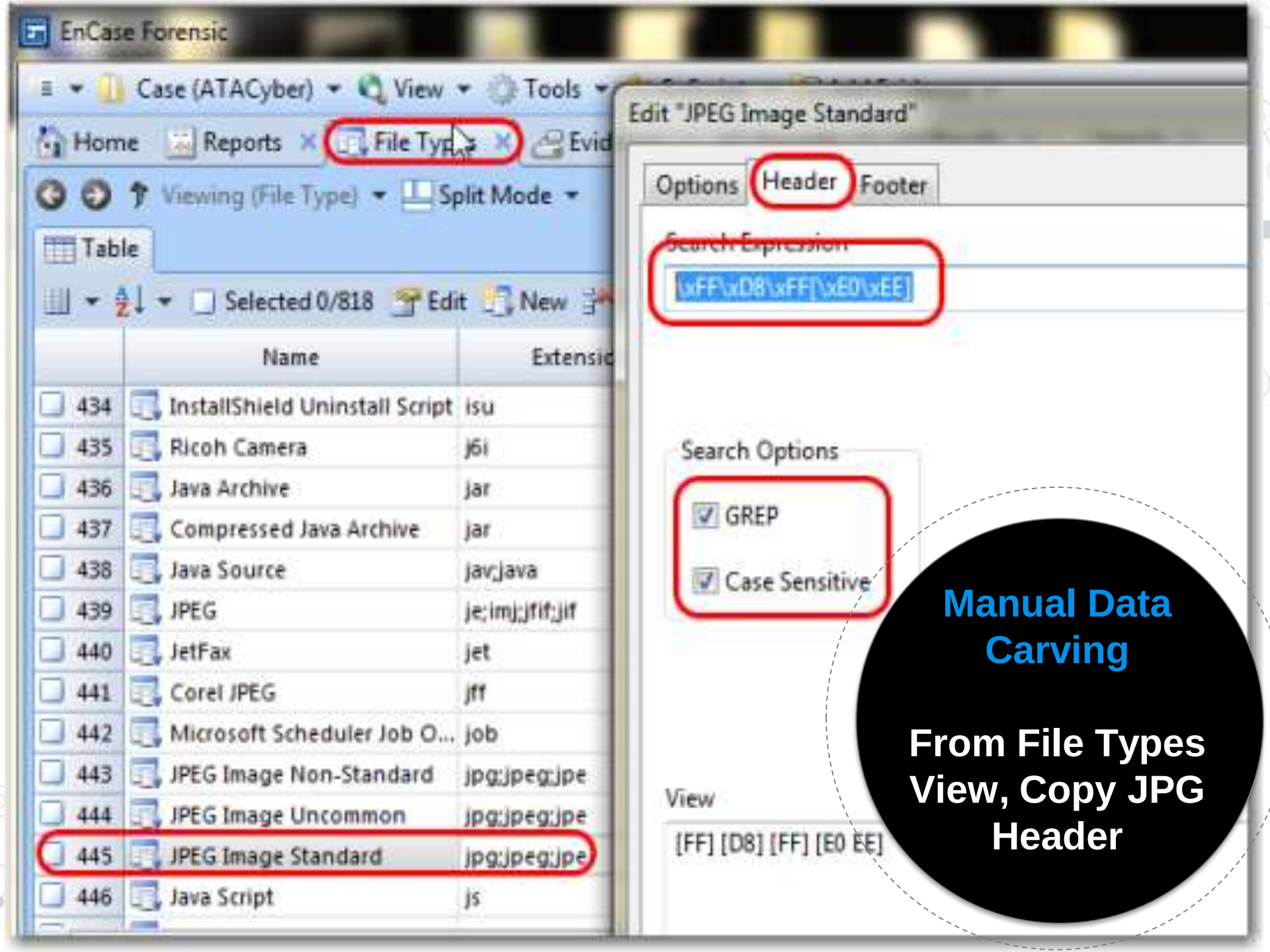
- On the New Keyword menu, go to the keyword tester tab
- Test the GREP search on a list you created

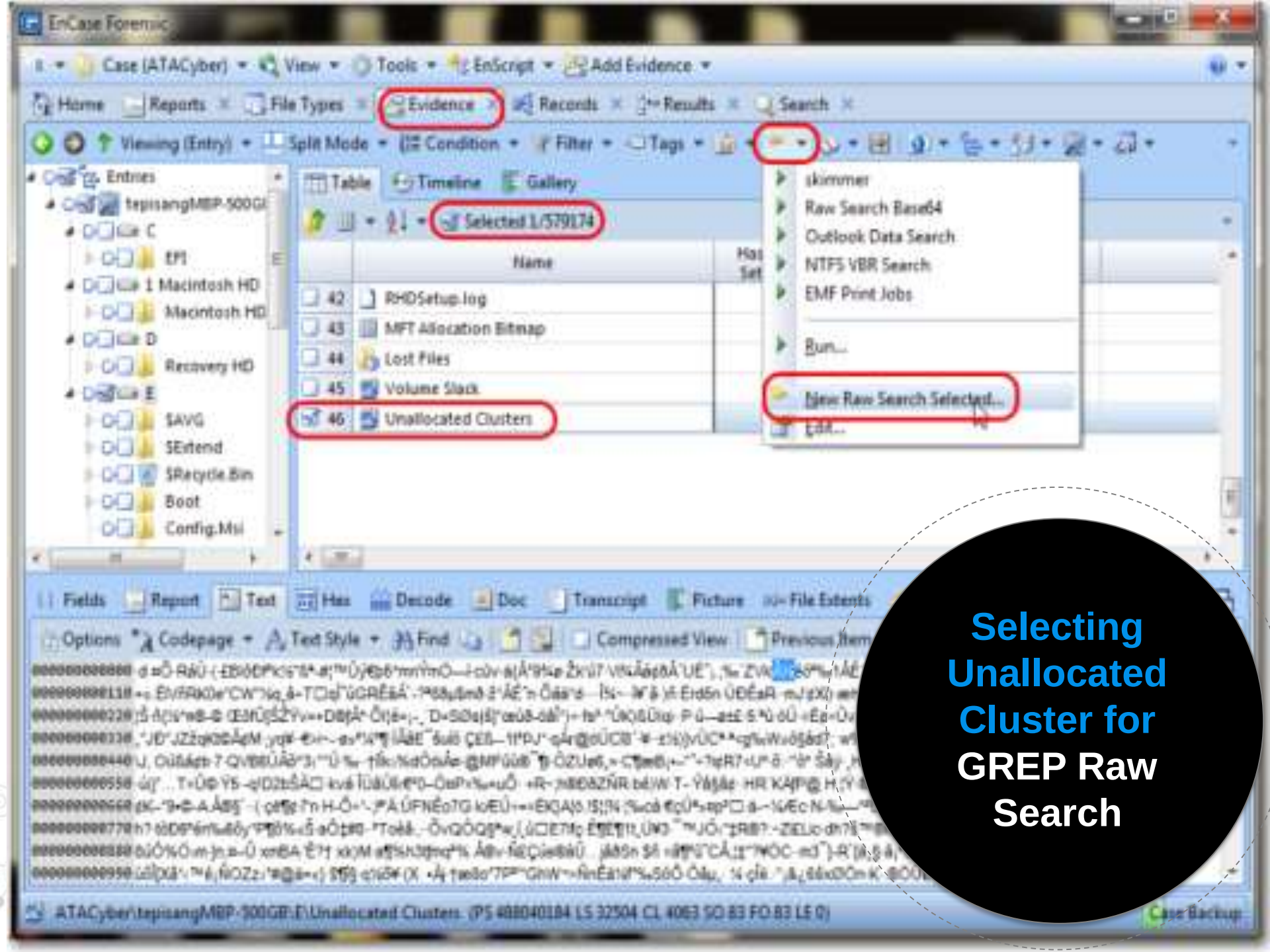


Data Carving

- **Locates files, primarily in unallocated spaces, based on file signature (header)**

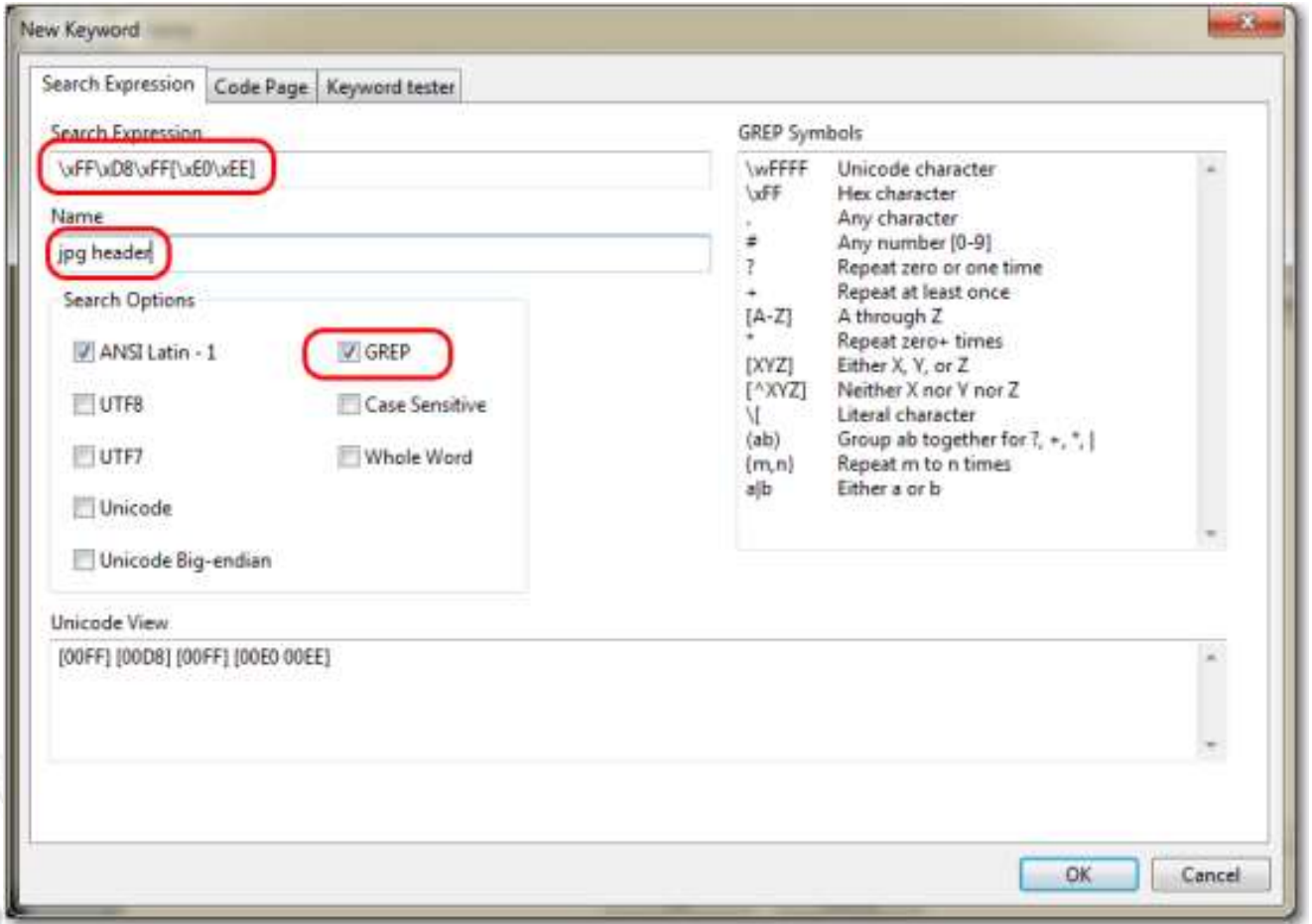
- **Can be:**
  - **Used against RAM dumps, swap files, and hibernation files**
  - **Performed manually or automated**


EnCase Forensic
Case (ATACyber)
View
Tools
Home
Reports
File Types
Viewing (File Type)
Split Mode
Table
Selected 0/818
Edit
New
Name
Extensic
434 InstallShield Uninstall Script isu
435 Ricoh Camera j6i
436 Java Archive jar
437 Compressed Java Archive jar
438 Java Source jav;java
439 JPEG je;jmj;jfif;jif
440 JetFax jet
441 Corel JPEG jff
442 Microsoft Scheduler Job O... job
443 JPEG Image Non-Standard jpg;jpeg;jpe
444 JPEG Image Uncommon jpg;jpeg;jpe
445 JPEG Image Standard jpg;jpeg;jpe
446 Java Script js
Edit "JPEG Image Standard"
Options
Header
Footer
Search Expression
\xFF\xD8\xFF[\xE0\xEE]
Search Options
GREP
Case Sensitive
View
[FF] [D8] [FF] [E0 EE]
Manual Data Carving
From File Types View, Copy JPG Header


Selecting Unallocated Cluster for GREP Raw Search

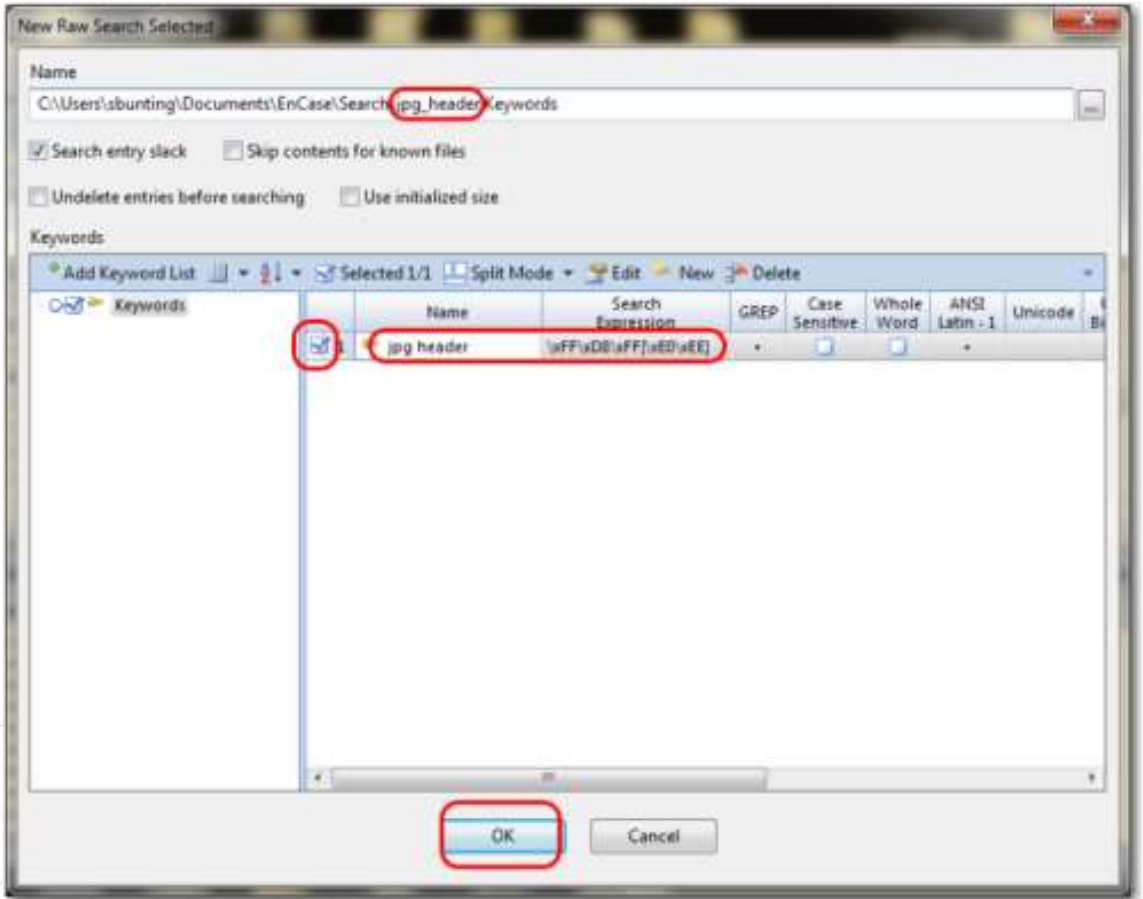
Creating the GREP Keyword

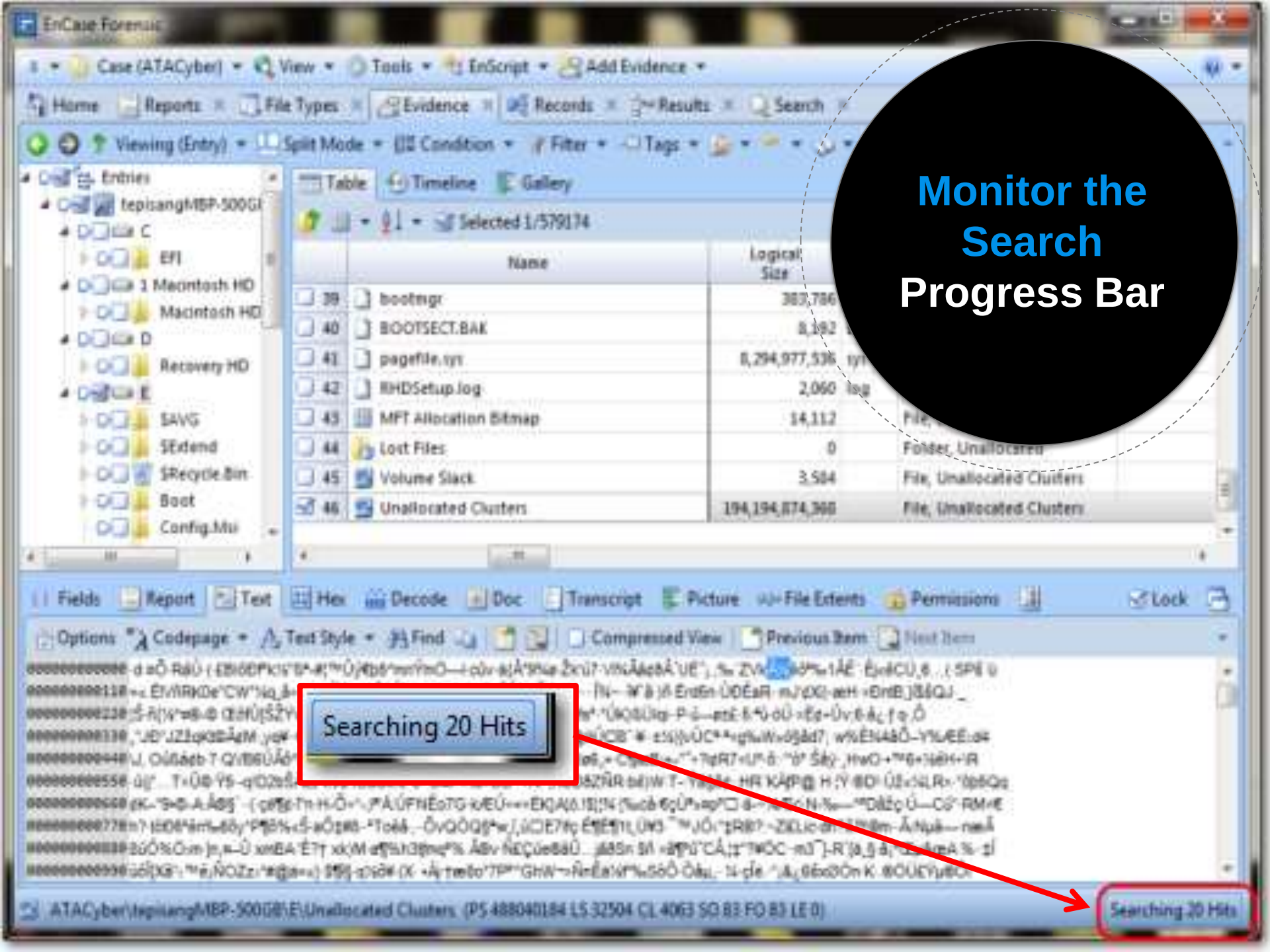
- **From the New Keyword Menu, paste the JPG header**

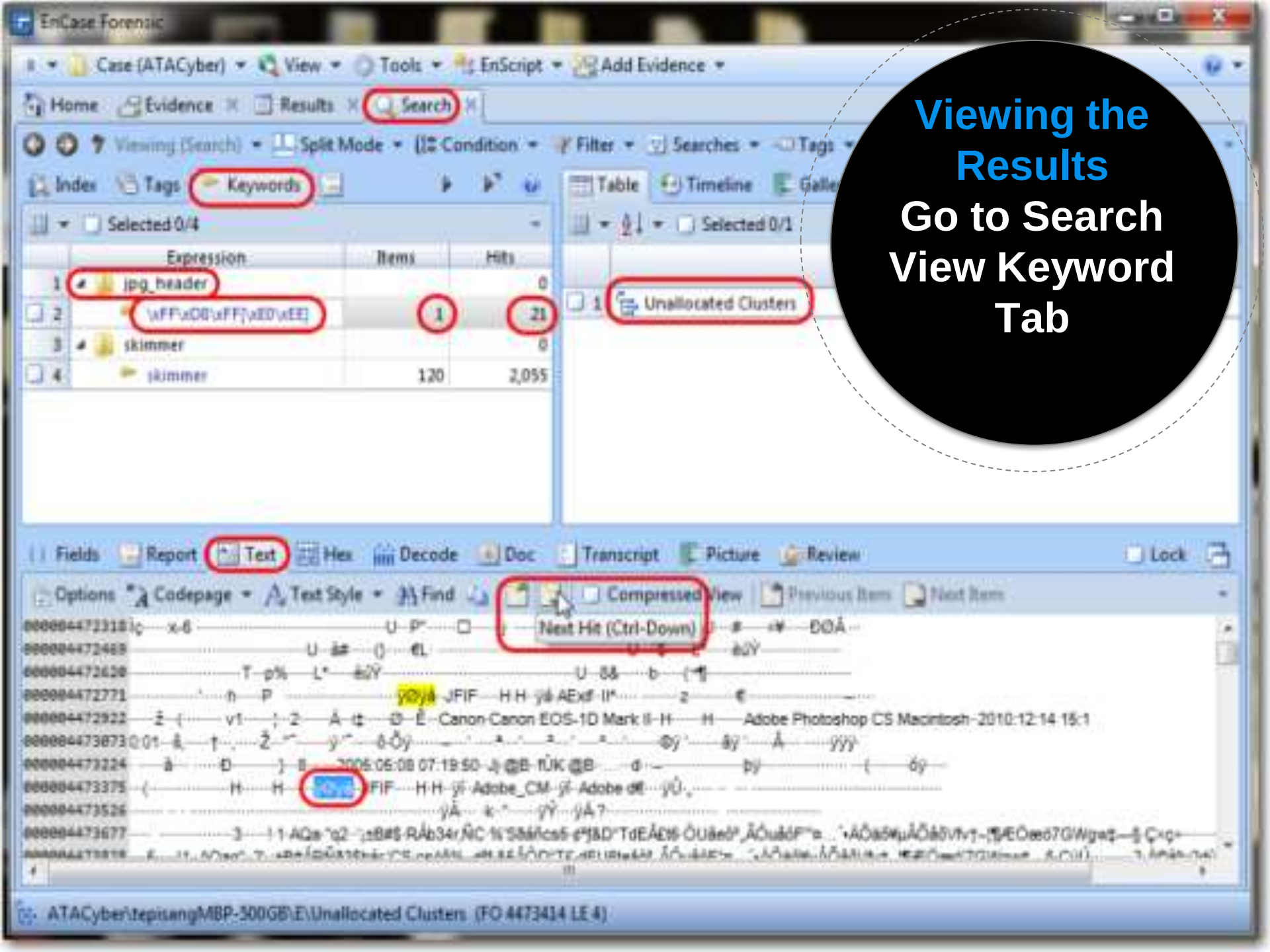


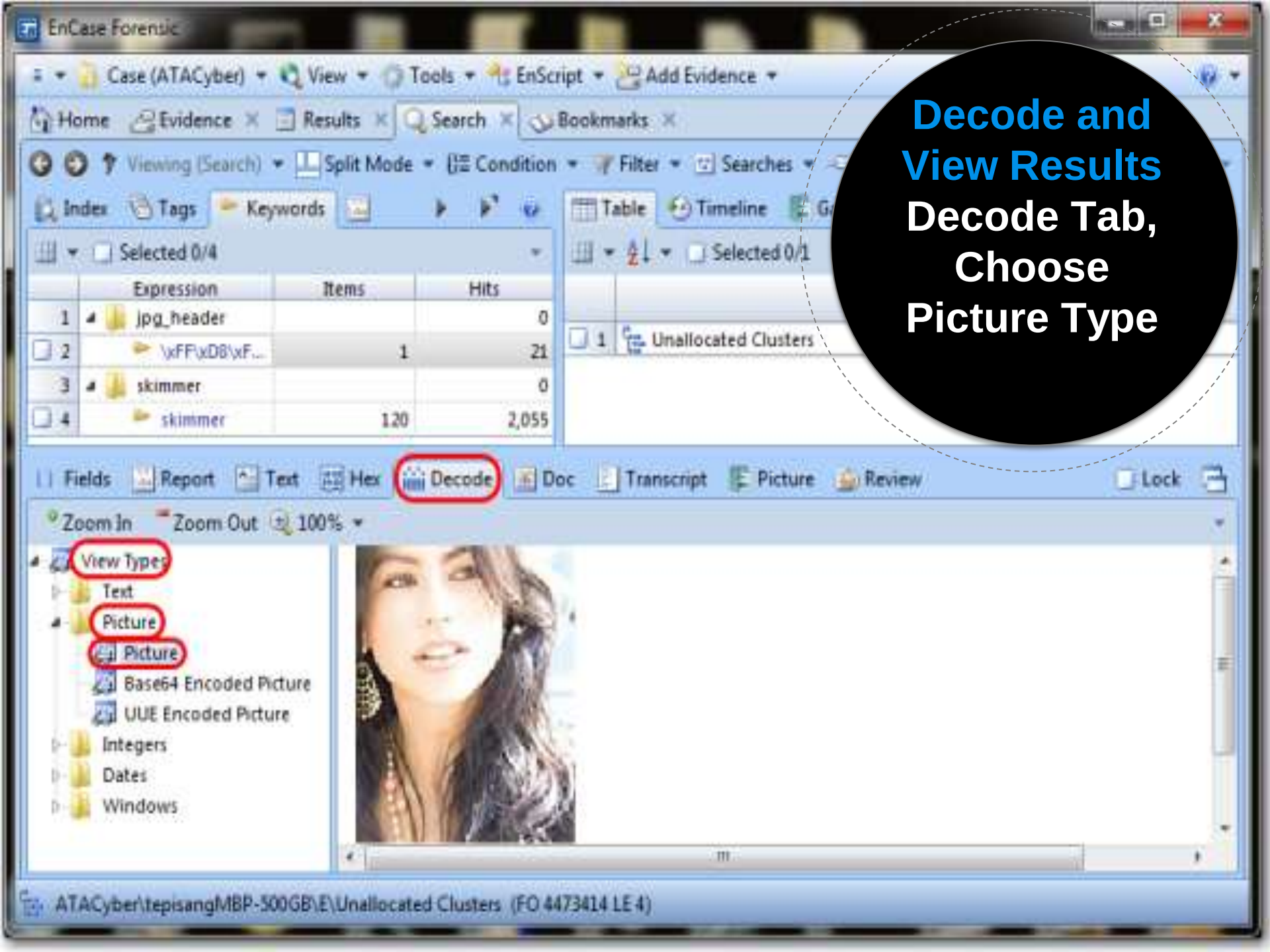
Running the Search

- **On the New Raw Search Selected menu, name the search file and path, then click OK**




Monitor the Search Progress Bar
Searching 20 Hits
Searching 20 Hits

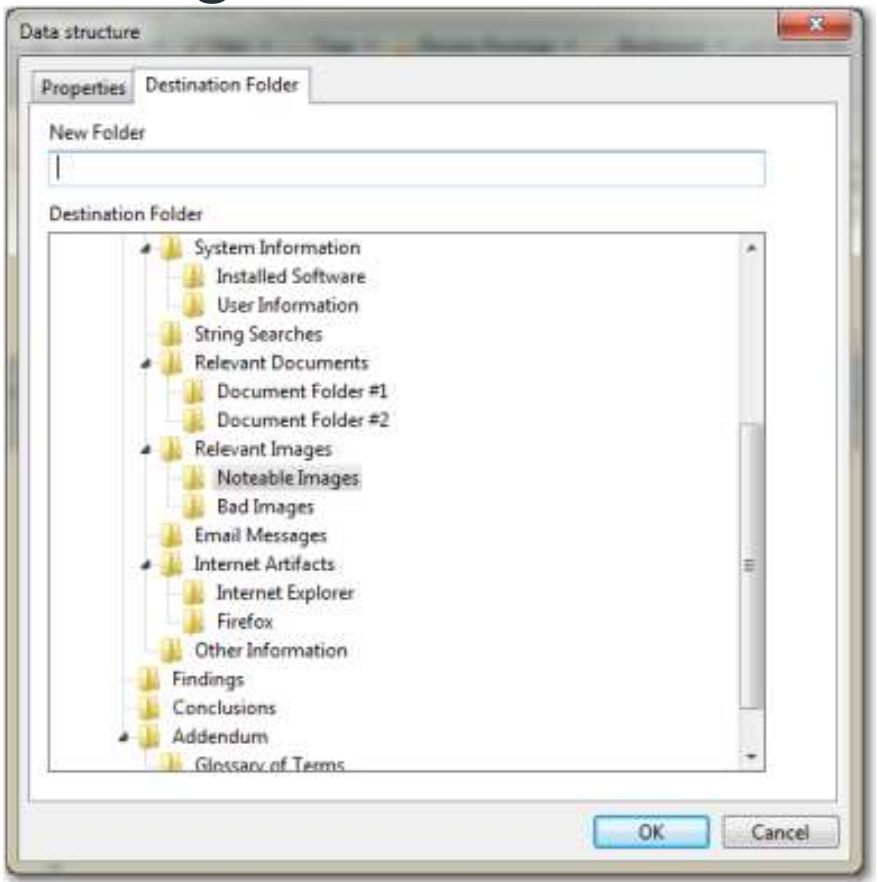

Viewing the Results
Go to Search
View Keyword Tab
EnCase Forensic
Case (ATACyber)
View
Tools
EnScript
Add Evidence
Home
Evidence
Results
Search
Split Mode
Condition
Filter
Searches
Tags
Index
Tags
Keywords
Table
Timeline
Selected 0/4
Selected 0/1
Expression
Items
Hits
1 jpg_header 0
2 \xFF\xD8\xFF\xED\xEE 1 21
3 skimmer 0
4 skimmer 120 2,055
1 Unallocated Clusters
Fields
Report
Text
Hex
Decode
Doc
Transcript
Picture
Review
Lock
Options
Codepage
Text Style
Find
Compressed View
Previous Item
Next Item
Next Hit (Ctrl-Down)
Canon Canon EOS-1D Mark II
Adobe Photoshop CS Macintosh 2010:12:14 15:1
JFIF
Adobe_CM
Adobe d
ATACyber\tepisang\MBP-500GB\E\Unallocated Clusters (FO 4473414 LE 4)


Decode and View Results
Decode Tab, Choose Picture Type
EnCase Forensic
Case (ATACyber)
View
Tools
EnScript
Add Evidence
Home
Evidence
Results
Search
Bookmarks
Split Mode
Condition
Filter
Searches
Index
Tags
Keywords
Table
Timeline
Selected 0/4
Selected 0/1
Expression
Items
Hits
1 jpg_header 0
2 \xFF\xD8\xF... 1 21
3 skimmer 0
4 skimmer 120 2,055
1 Unallocated Clusters
Fields
Report
Text
Hex
Decode
Doc
Transcript
Picture
Review
Lock
Zoom In
Zoom Out
100%
View Types
Text
Picture
Picture
Base64 Encoded Picture
UUE Encoded Picture
Integers
Dates
Windows
ATACyber\tepisangMBP-500GB\E\Unallocated Clusters (FO 4473414 LE 4)

Bookmark the Results,
Right-click the Picture, Bookmark it as Data Structure

Select the Destination

- Go to the Data Structure menu destination tab
- Under Relevant Images, choose Notable Images



EnCase Forensic

Case (ATACyber) ▾ View ▾ Tools ▾ EnScript ▾ Add Evidence ▾

Home | Reports | Evidence | Results | Search | Bookmarks

Examination Report

Go to template | Go to bookmark | Edit bookmark | Zoom In | Zoom Out | 100% ▾

Digital Movies

Computer generated animation or "digital movies" come in various standard formats. Sor
and AVI files.

Relevant Images

The following images were discovered during the examination and are potentially relevant to

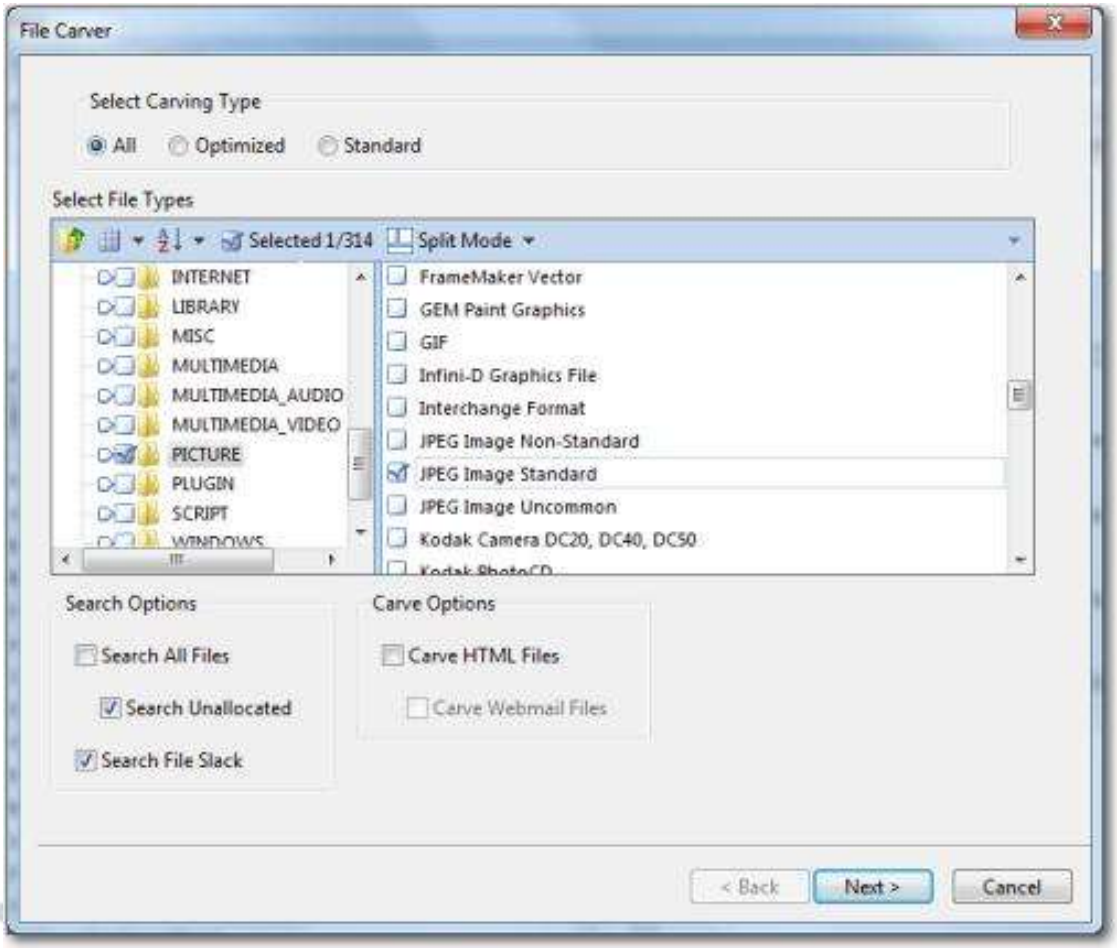
1) Unallocated Clusters

ATACyber\tepirang\MBP-500GB\E\Unallocated Clusters (FO 4473414 LE 4)

View the Report

Automated File Carver

- **Easier than the manual method**
- **Select options, click OK, and view the results**

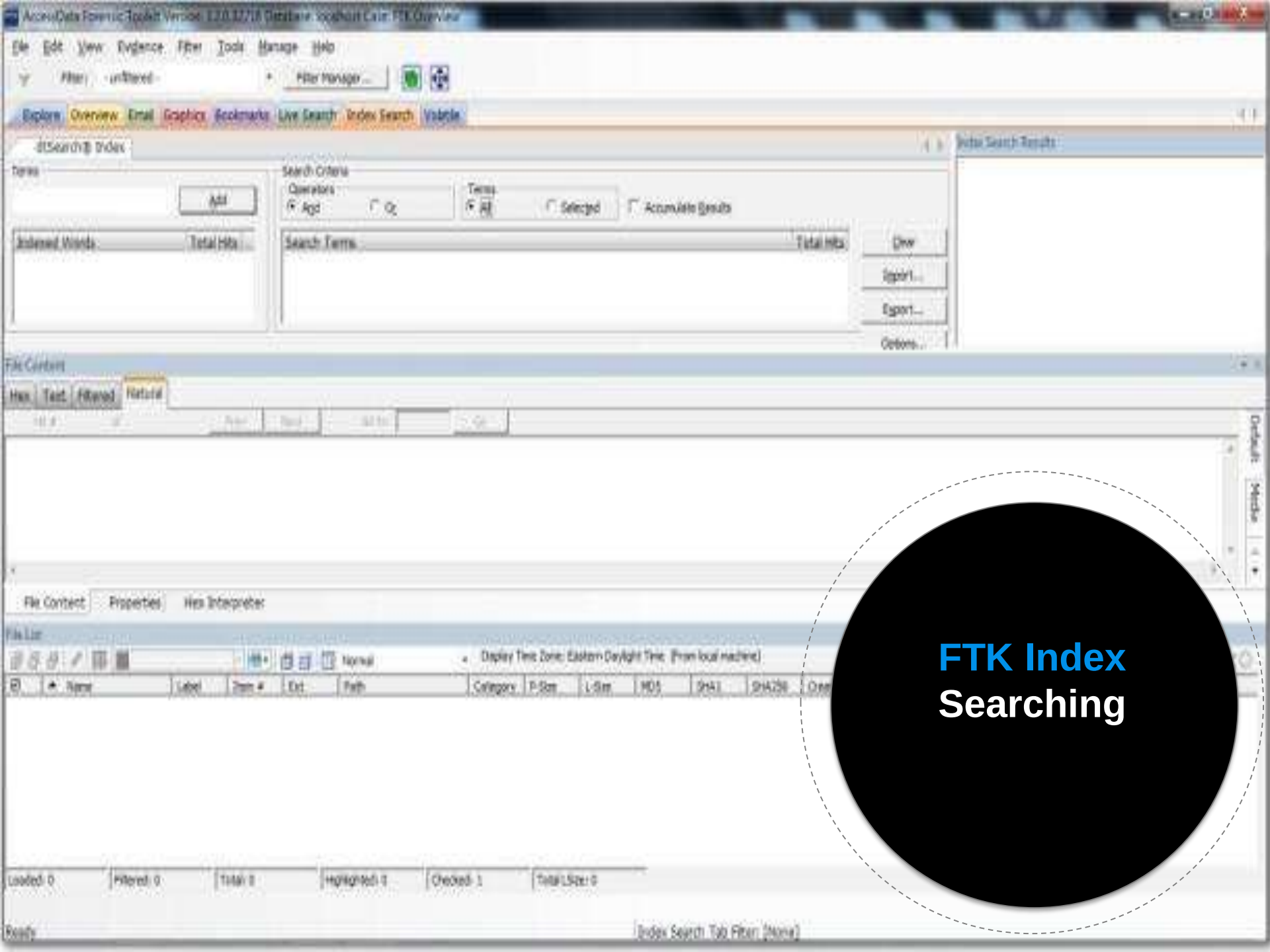


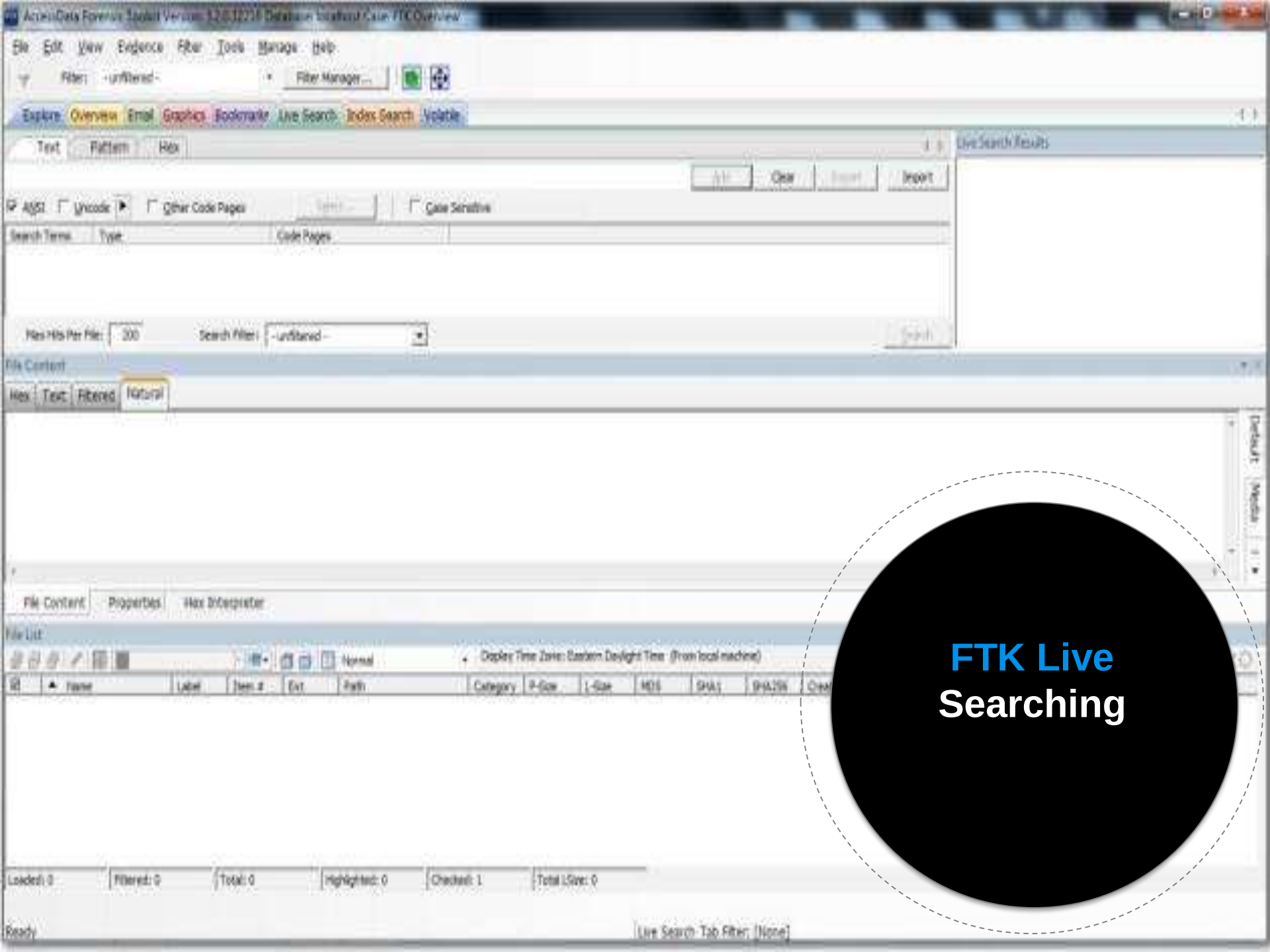
FTK

Search Techniques

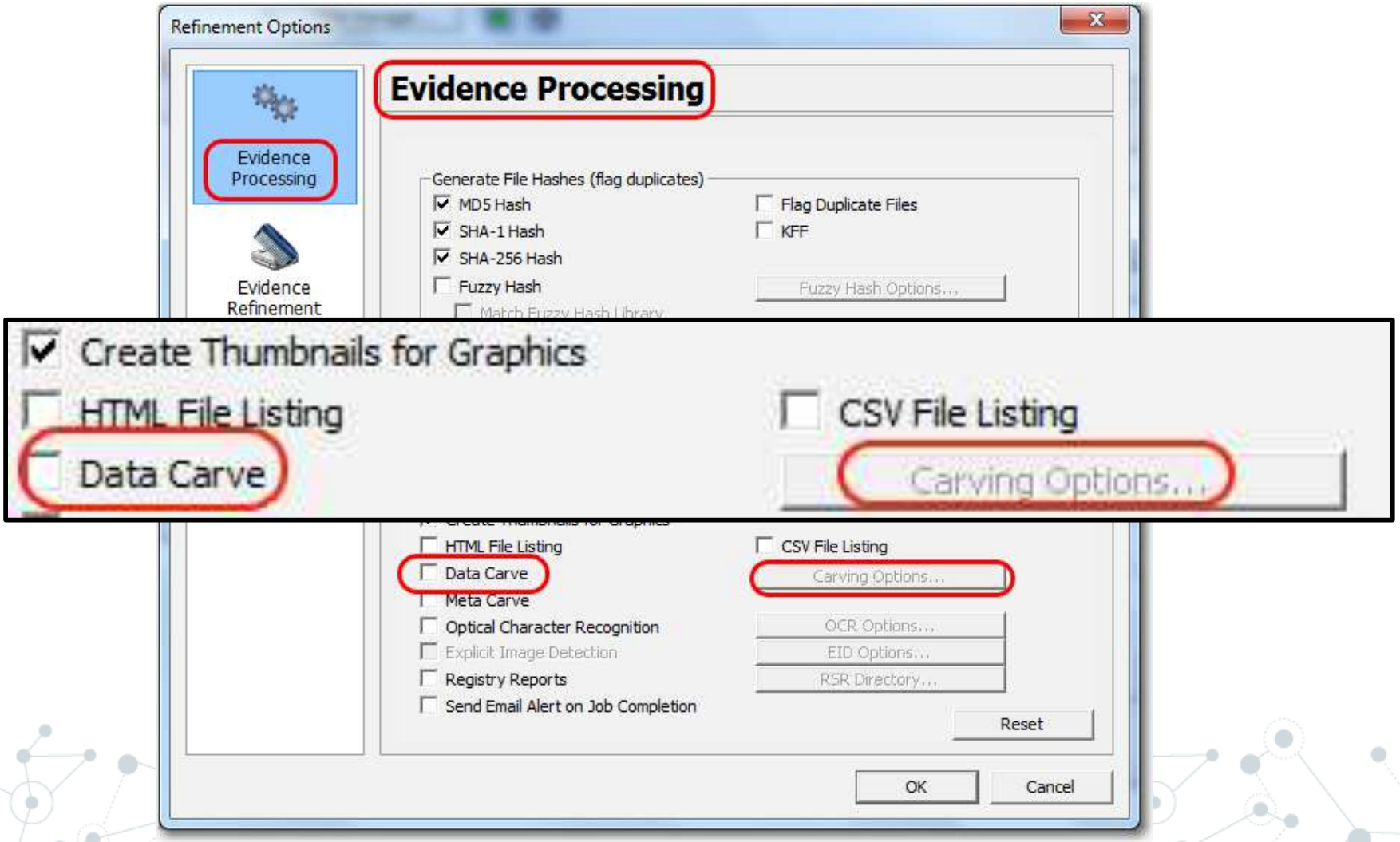
FTK Searching Features

- **FTK supports:**
  - **Indexed searches**
  - **Raw searches, including regular expressions**
  - **Data carving through its evidence processing feature set**
  - **Unicode character sets**


FTK Index
Searching


FTK Live
Searching

FTK Data Carving Feature



Summary

- **You should now be familiar with:**
  - **Storage and search of ASCII and Unicode text**
  - **Types of keyword searches**
  - **Index, live or raw keyword, and GREP searches**
  - **Data carving based on file signatures**
  - **Foreign language views and searches**

Thanks!

Any questions?

Windows Artifacts Forensic

Objective

- By the end of this module, participants will be able to analyze artifacts common to windows 7 operating system.

What is an Operating System ?

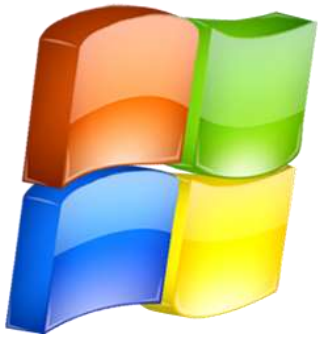
What Is an Operating System?

- The largest and most important application
- An interface between applications, hardware, and users
- Support for many hardware configurations

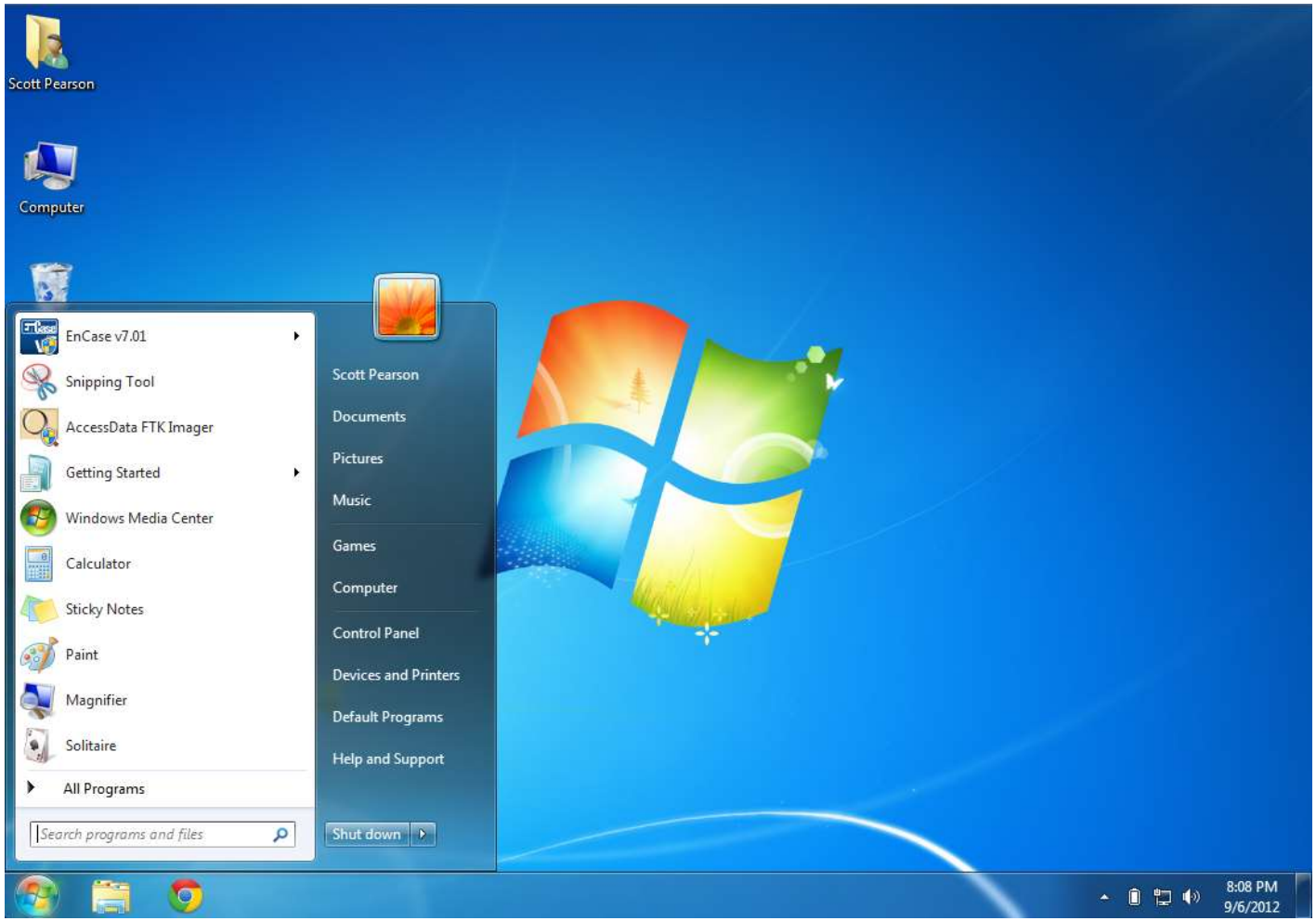
Windows Operating System

- Microsoft Windows is the most prevalent and widely used operating system

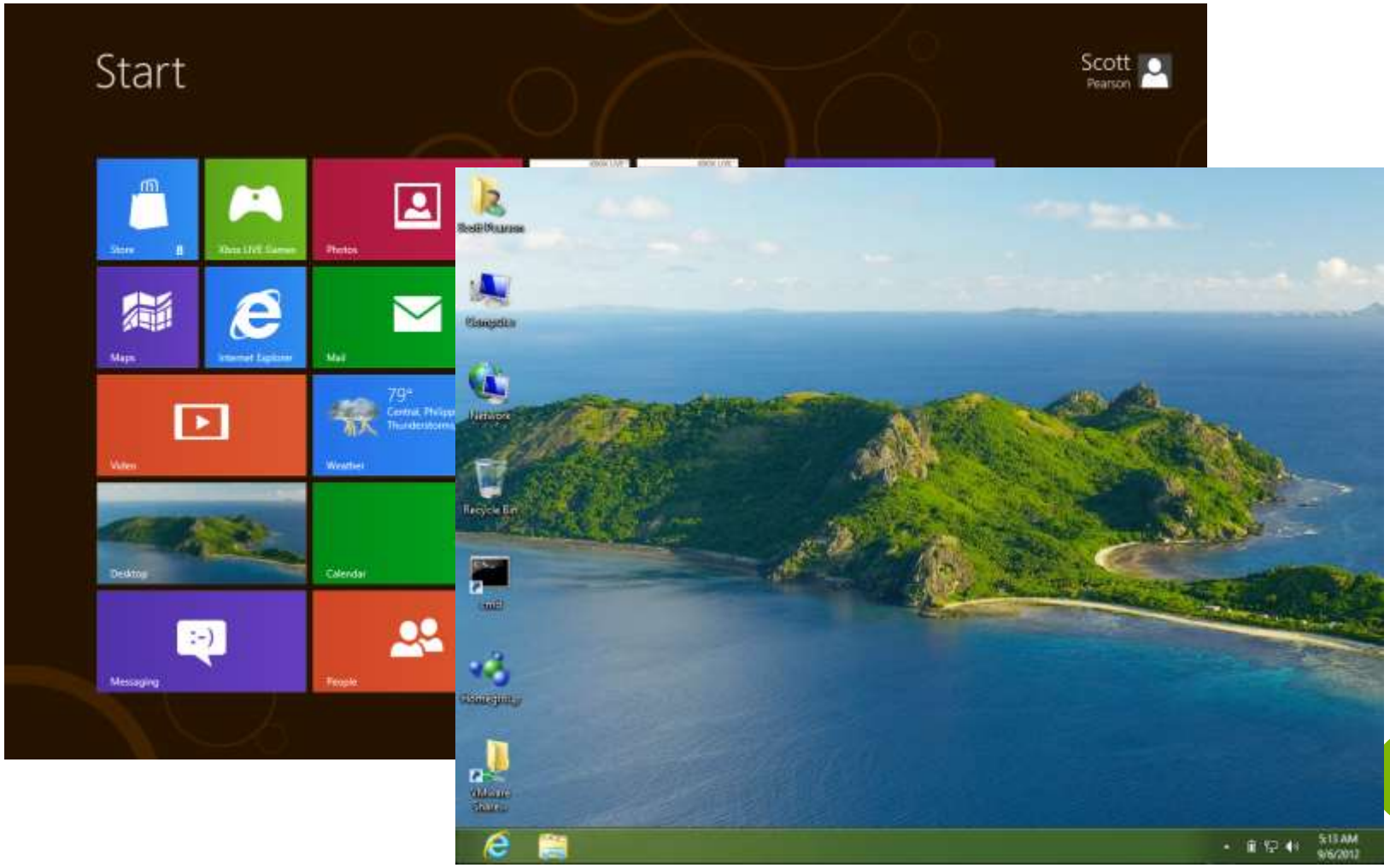
- Examiners must be aware of how Windows is used and where pertinent artifacts could be stored



Windows 7 Desktop



Windows 8 Desktop



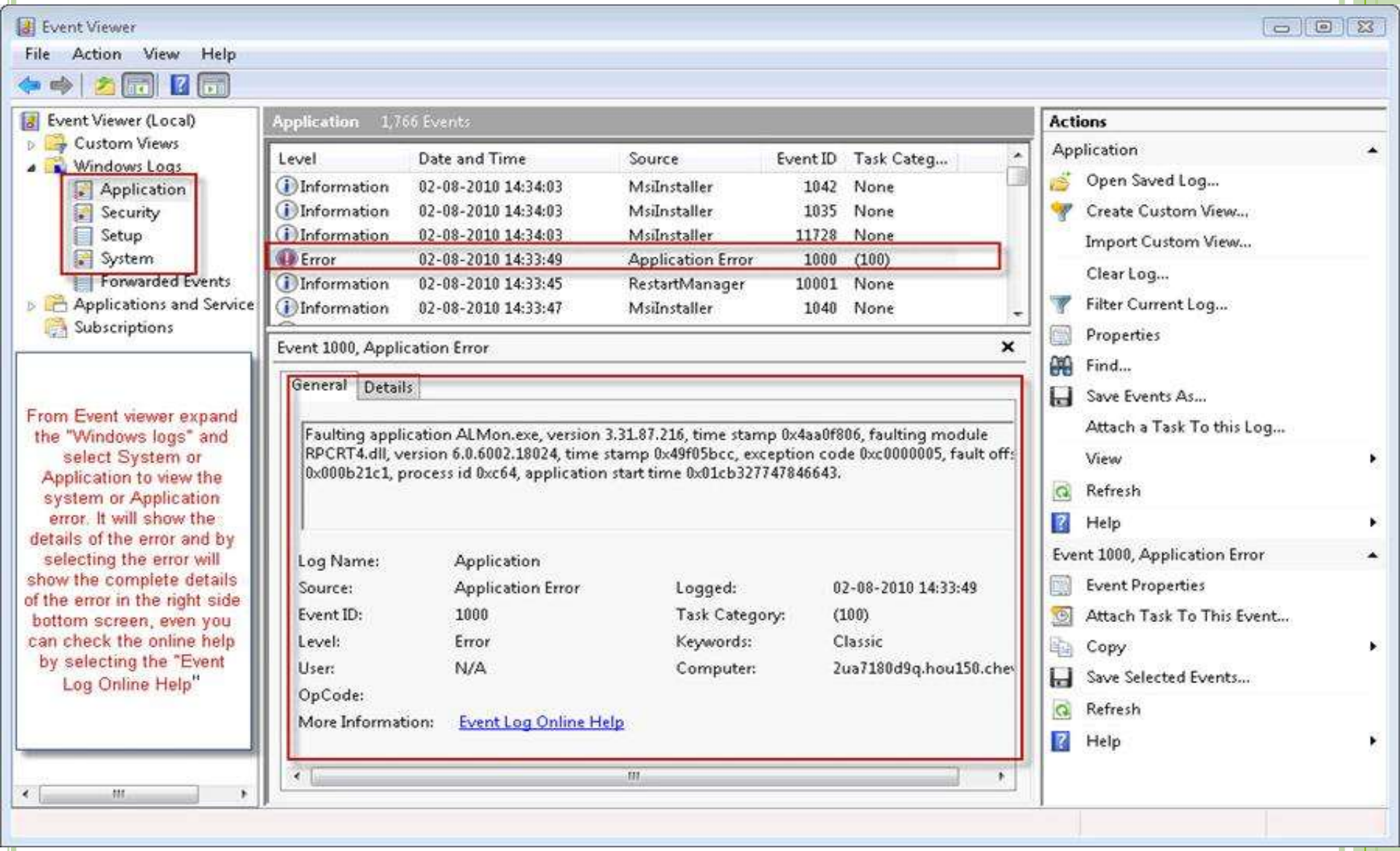
Common Windows Artifacts

Windows Event Logs

- An event is a notable incident that generates a log entry or user notification
- An event log:
  - Is a collection of events categorized by function
  - Provides a historical reference

C:/Windows/System32/Winevt/Logs

Windows Event Logs

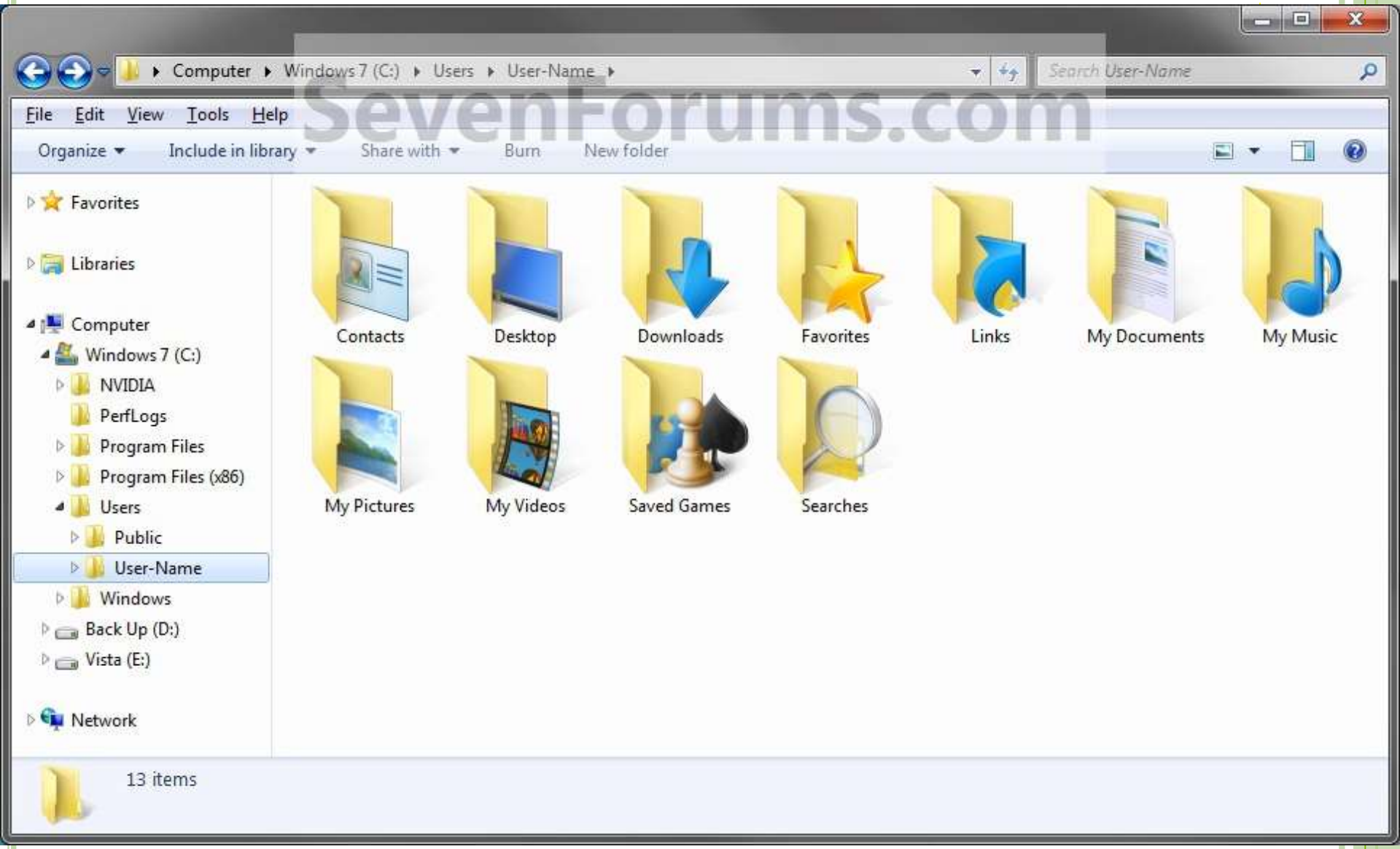


Windows User Profile

- The user profile is a default collection of folders to store user-generated data
- Every user with a Windows account has their own user profile

Windows 7 location → C:\Users\<UserID>

Windows User Profile

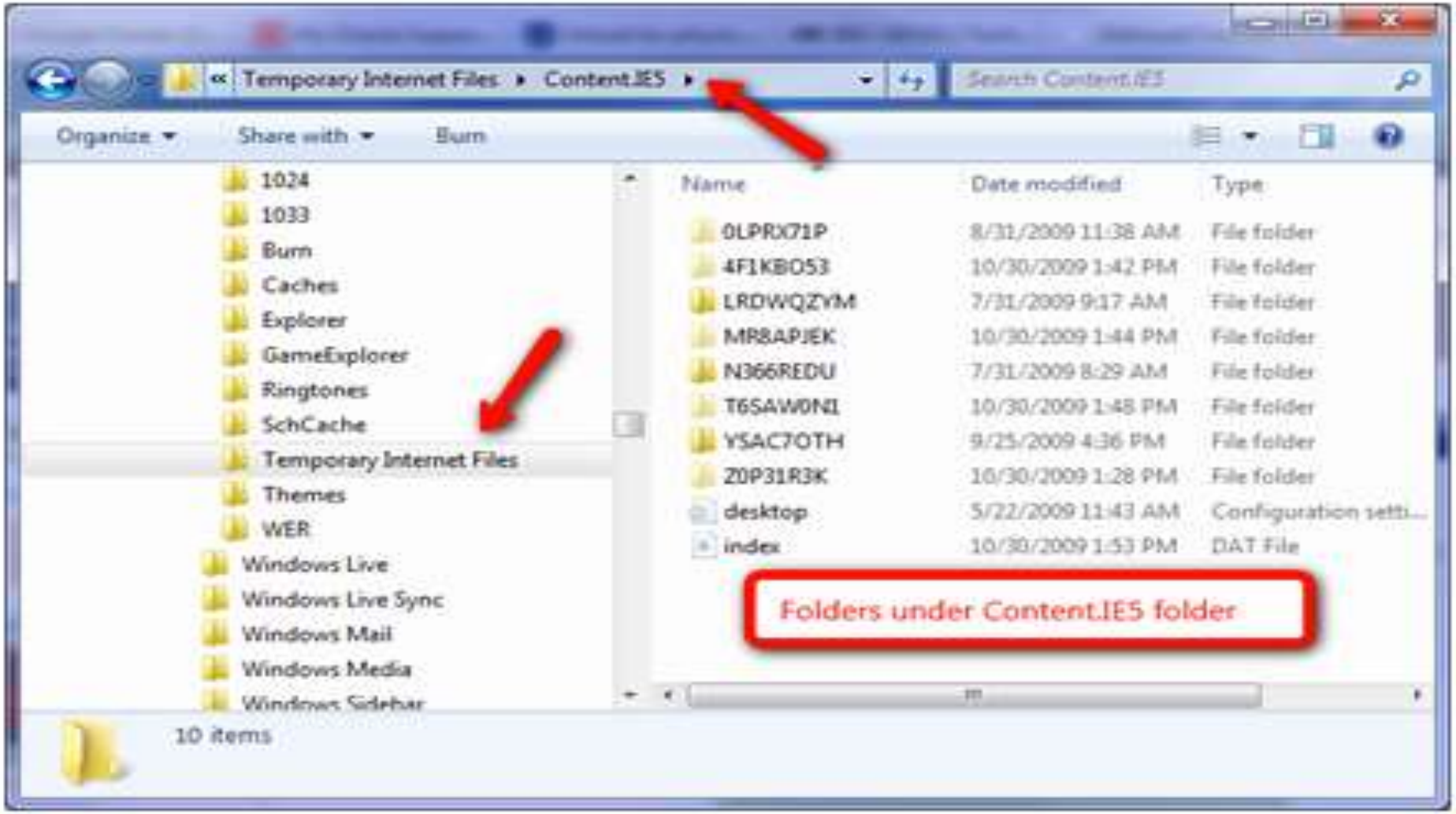


Temporary Internet Files

- Serves as the browser cache,
  - Cache pages and other multimedia content, such as video and audio files, from websites visited by the user.
- This allows websites to load more quickly the next time they are visited.

%userprofile%\AppData\Local\Microsoft\Windows\Temporary Internet Files

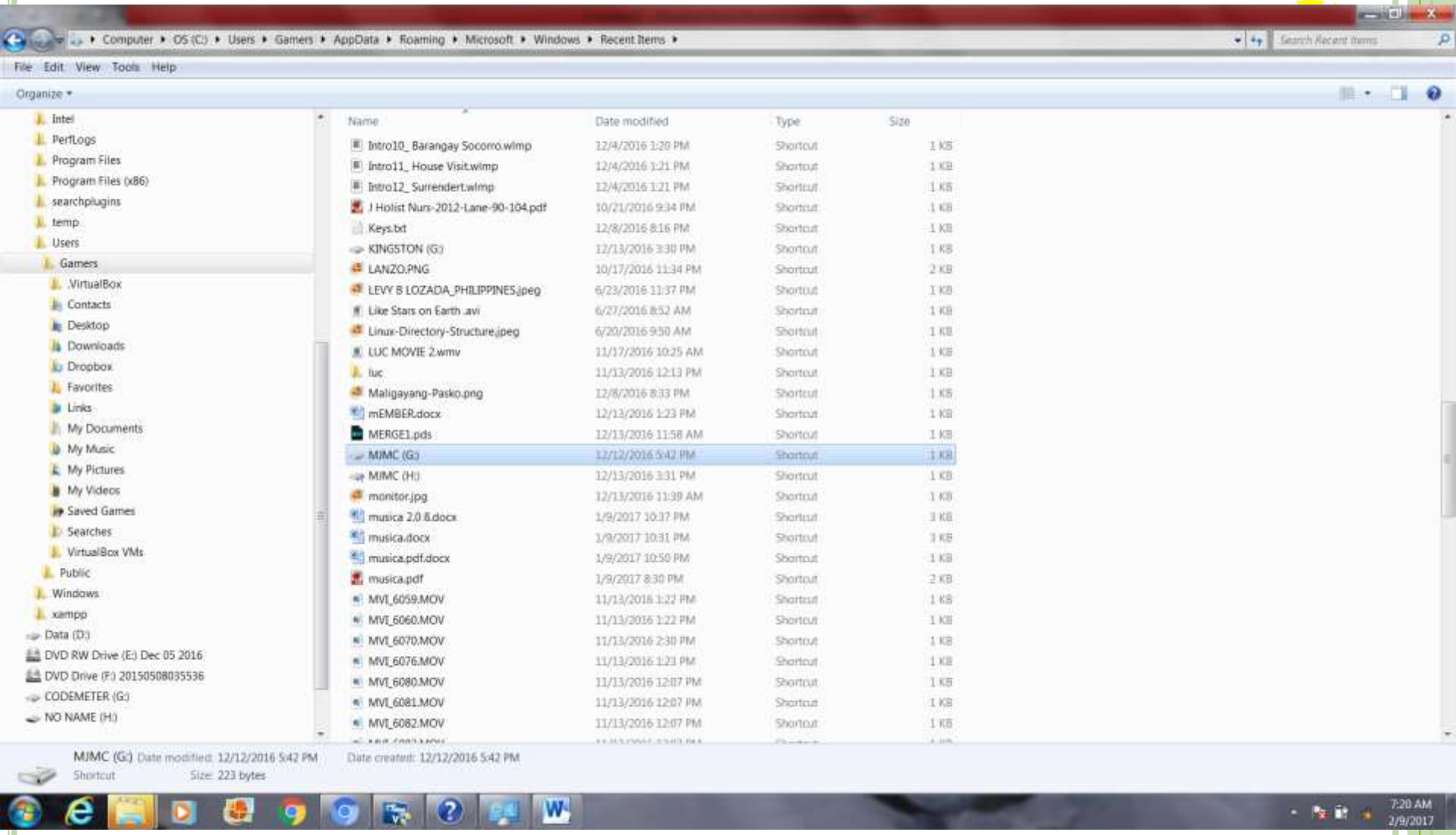
Temporary Internet Files



Recent Items Folder and Link Files

- **Recent Items;**
  - The Recent Items folder is used by Windows to record what documents have been opened.
- **Link Files:**
  - Is a shortcut to a file stored within the file system
  - Provides quick access to commonly used files
  - May contain valuable clues to the actual location and/or prior existence of files on the computer

Recent Items Folder and Link Files



Recycle Bin

- Is temporary storage for deleted files
- Will not contain files deleted from devices with removable storage
- Is unique to every Windows user

\$Recycle.Bin\%SID%,

- %SID% is the SID of the user that performed the deletion.

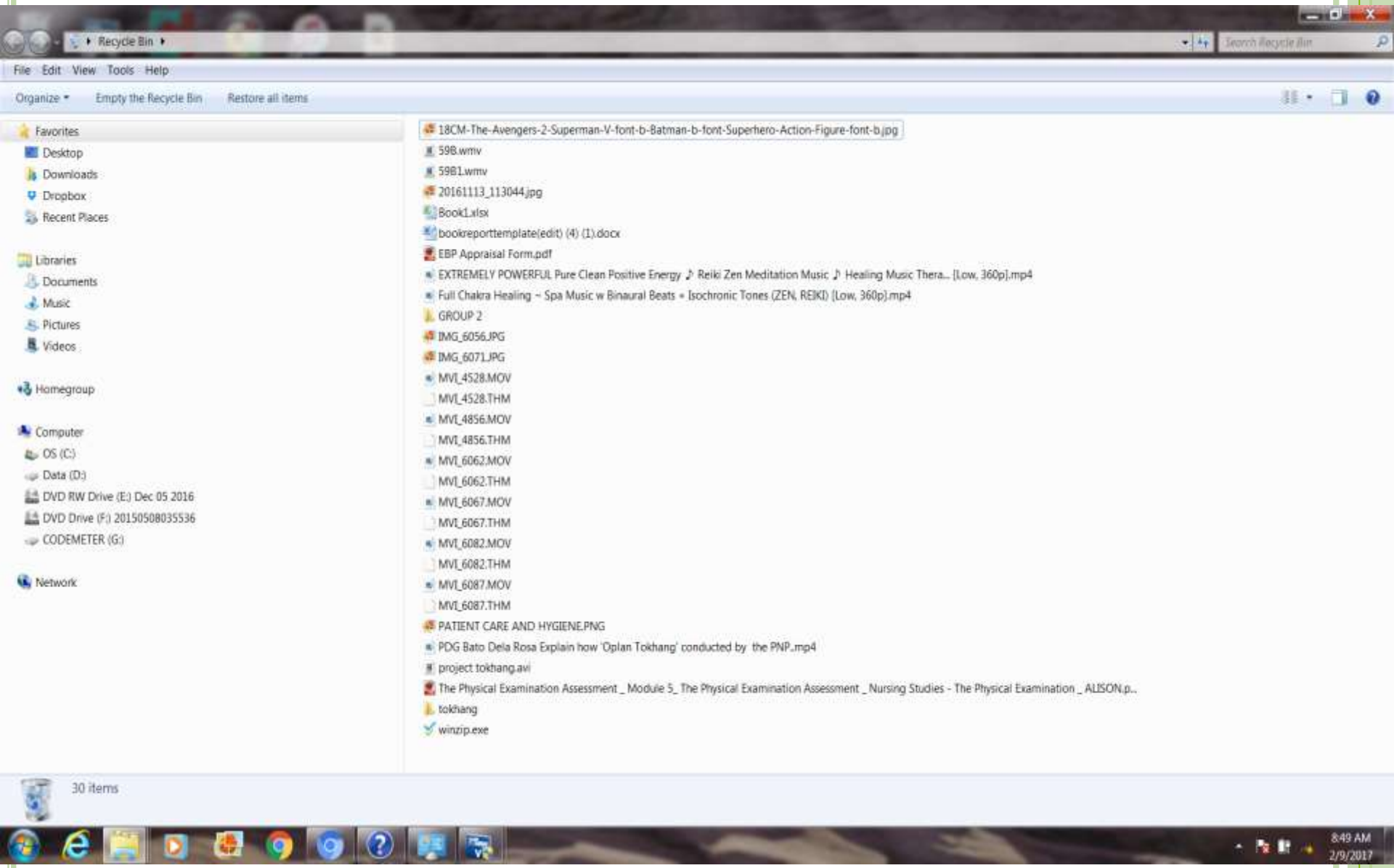
Recycle Bin

- Recycle bin files can:
  - Be restored to their original file system location
  - Be emptied from the file system
  - Provide clues about files the user tried to remove

\$Recycle.Bin\%SID%,

- %SID% is the SID of the user that performed the deletion.

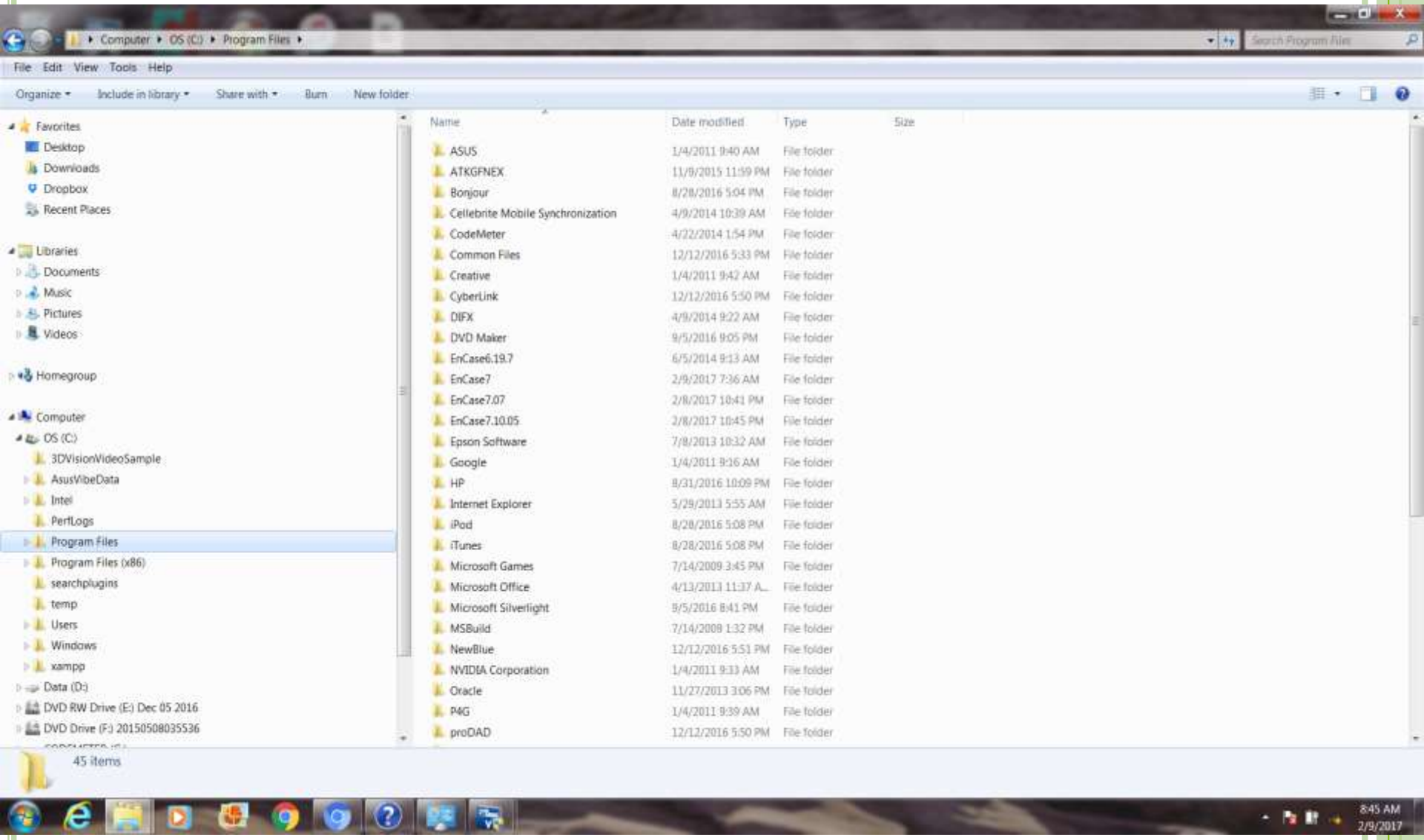
RECYCLE BIN


Recycle Bin
Search Recycle Bin
File Edit View Tools Help
Organize
Empty the Recycle Bin
Restore all items
Favorites
Desktop
Downloads
Dropbox
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
OS (C:)
Data (D:)
DVD RW Drive (E:) Dec 05 2016
DVD Drive (F:) 20150508035536
CODEMETER (G:)
Network
18CM-The-Avengers-2-Superman-V-font-b-Batman-b-font-Superhero-Action-Figure-font-b.jpg
598.wmv
5981.wmv
20161113_113044.jpg
Book1.xlsx
bookreporttemplate(edit) (4) (1).docx
EBP Appraisal Form.pdf
EXTREMELY POWERFUL Pure Clean Positive Energy ♪ Reiki Zen Meditation Music ♪ Healing Music Thera... [Low, 360p].mp4
Full Chakra Healing ~ Spa Music w Binaural Beats + Isochronic Tones (ZEN, REIKI) [Low, 360p].mp4
GROUP 2
IMG_6056.JPG
IMG_6071.JPG
MVI_4528.MOV
MVI_4528.THM
MVI_4856.MOV
MVI_4856.THM
MVI_6062.MOV
MVI_6062.THM
MVI_6067.MOV
MVI_6067.THM
MVI_6082.MOV
MVI_6082.THM
MVI_6087.MOV
MVI_6087.THM
PATIENT CARE AND HYGIENE.PNG
PDG Bato Dela Rosa Explain how 'Oplan Tokhang' conducted by the PNP..mp4
project tokhang.avi
The Physical Examination Assessment _ Module 5_ The Physical Examination Assessment _ Nursing Studies - The Physical Examination _ ALISON.p...
tokhang
winzip.exe
30 items
8:49 AM
2/9/2017

Installed Applications

- Allow the users to interact with the computer system
- Generate specific types of output
- Leave unique footprints that can assist the examiner to understand how the system was used

Volume Shadow Copy



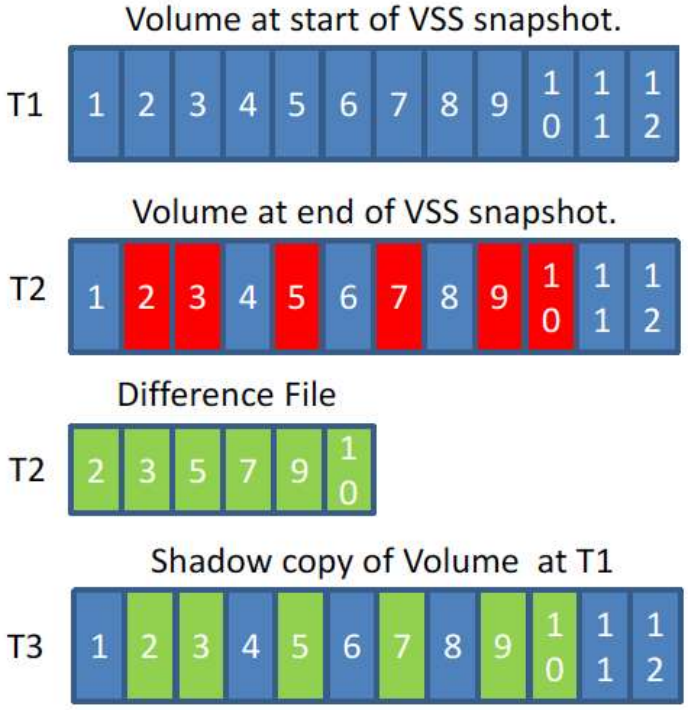
Volume Shadow Service (VSS)

- Creates a snapshot image of application data on a volume
- Enables reliable backups even while the system is actively running
- Enables examiners to access previous versions of files

Volume Shadow Copy

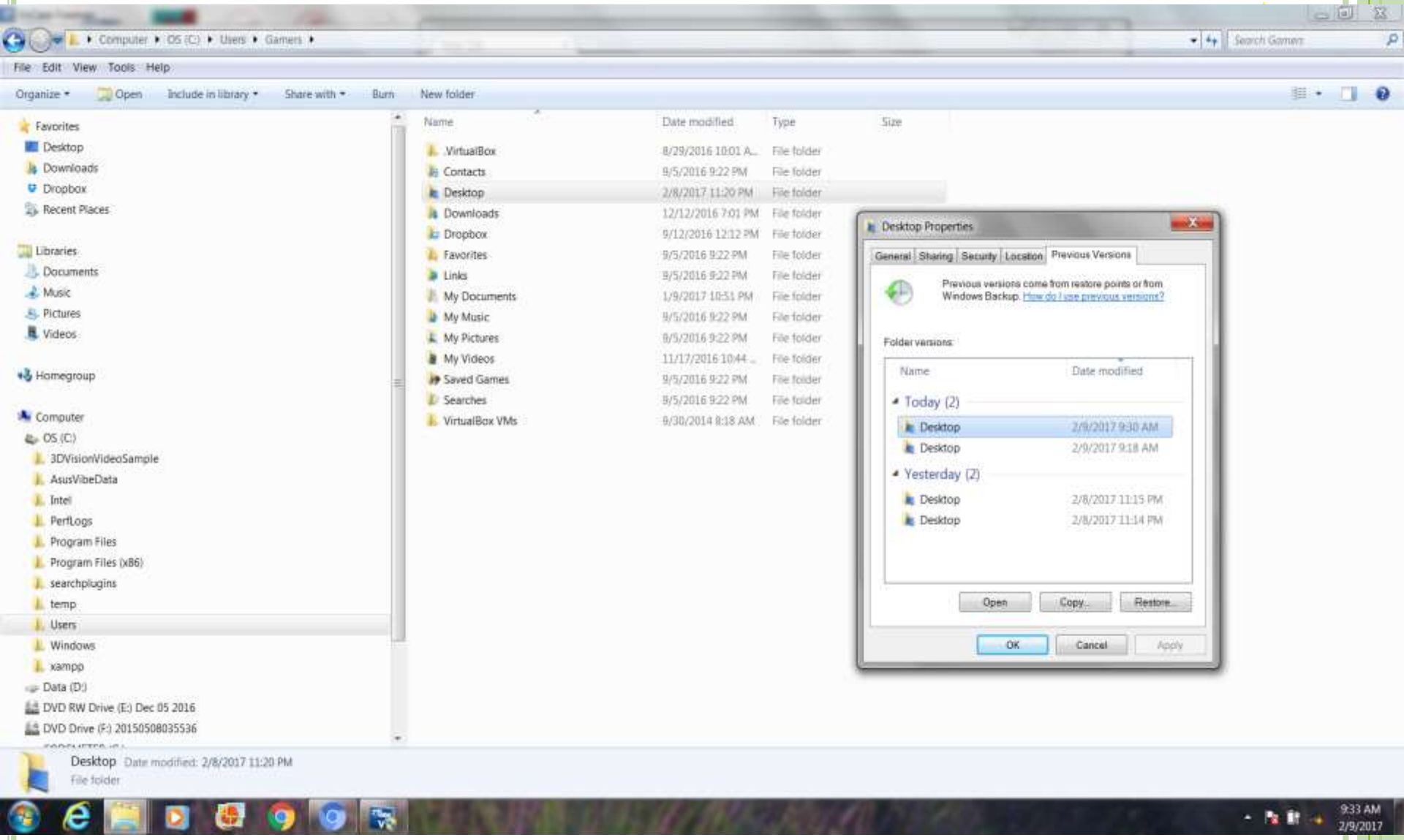
- Volume shadow copies are bit level differential backups of a volume.
  - -16 KB blocks.
  - -Copy on write.
  - -Volume Shadow copy files are “difference” files.

Volume Shadow Copy

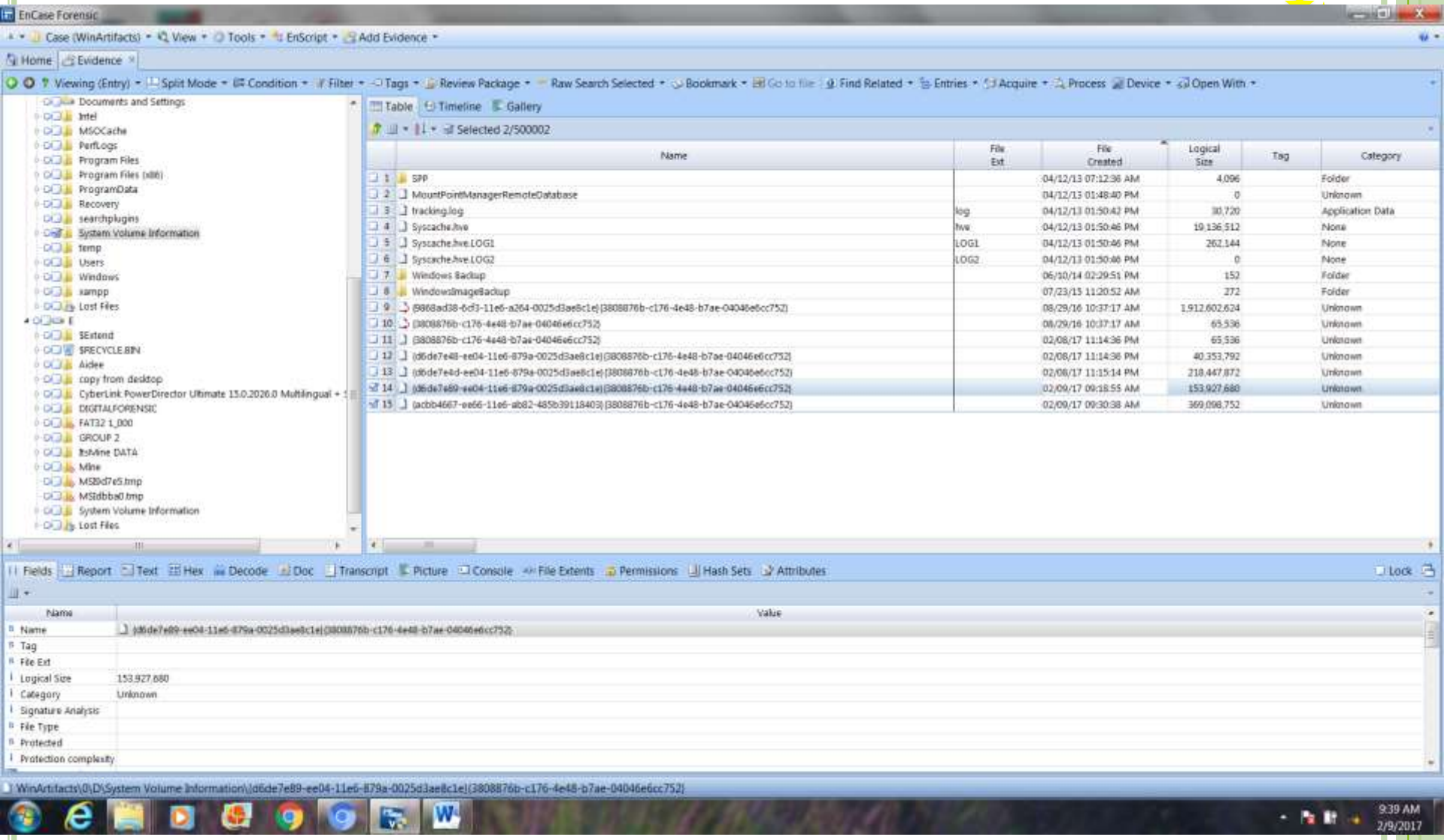


- ***Copy on Write:*** Before a block is written to, it is saved to the difference file.
- When a Shadow Copy is read, the "volume" consists of the live, unchanged blocks, and the saved blocks from the difference file.

Volume Shadow Copy



Volume Shadow Copy



Windows Prefetch

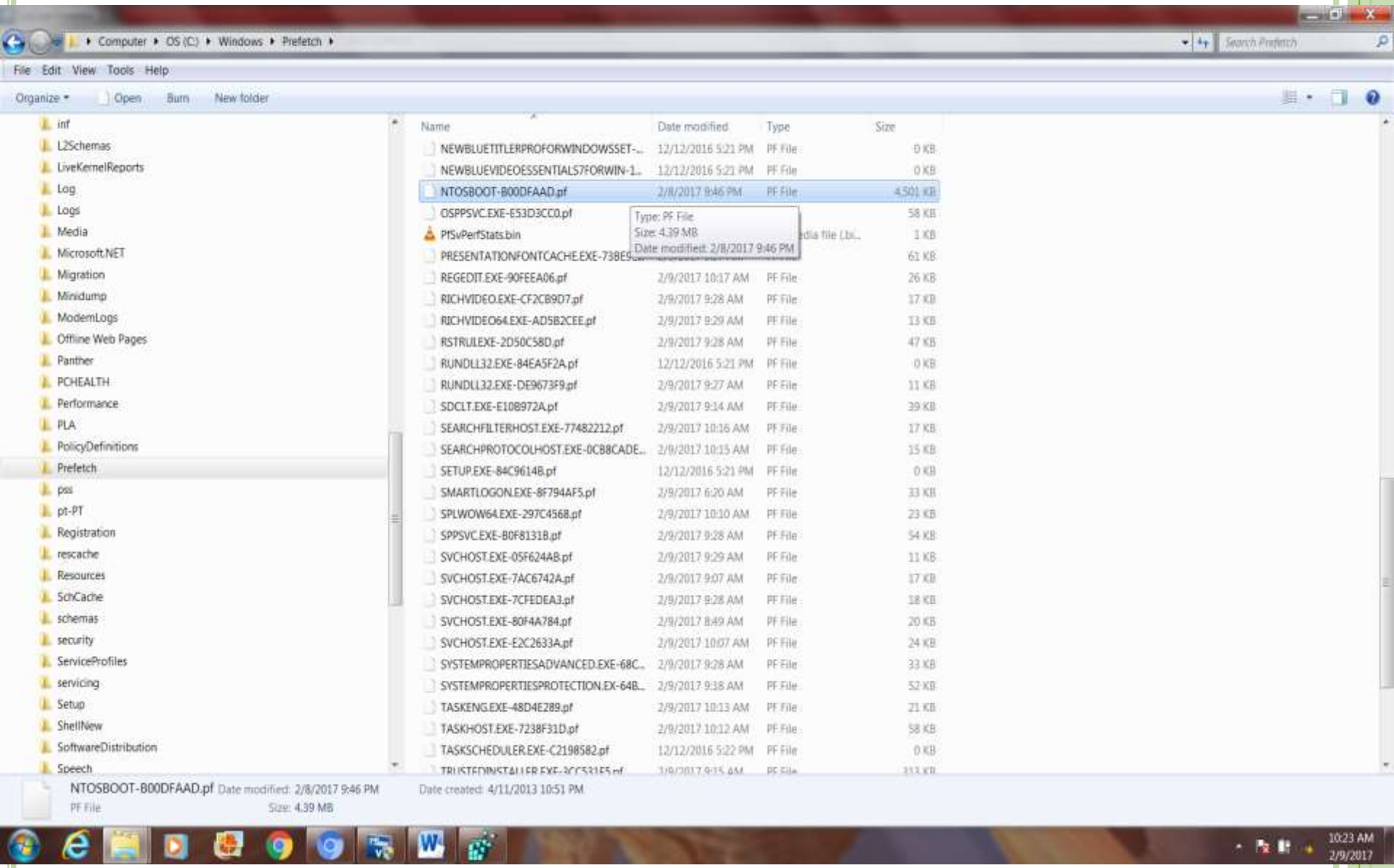
- Boosts performance by preloading data into RAM based on cache history
- Provides clues about frequently-used applications and when they were last used

Location = C:\Windows\Prefetch

.PF extension

NTOSBOOT-B00DFAAD.PF

Windows Prefetch



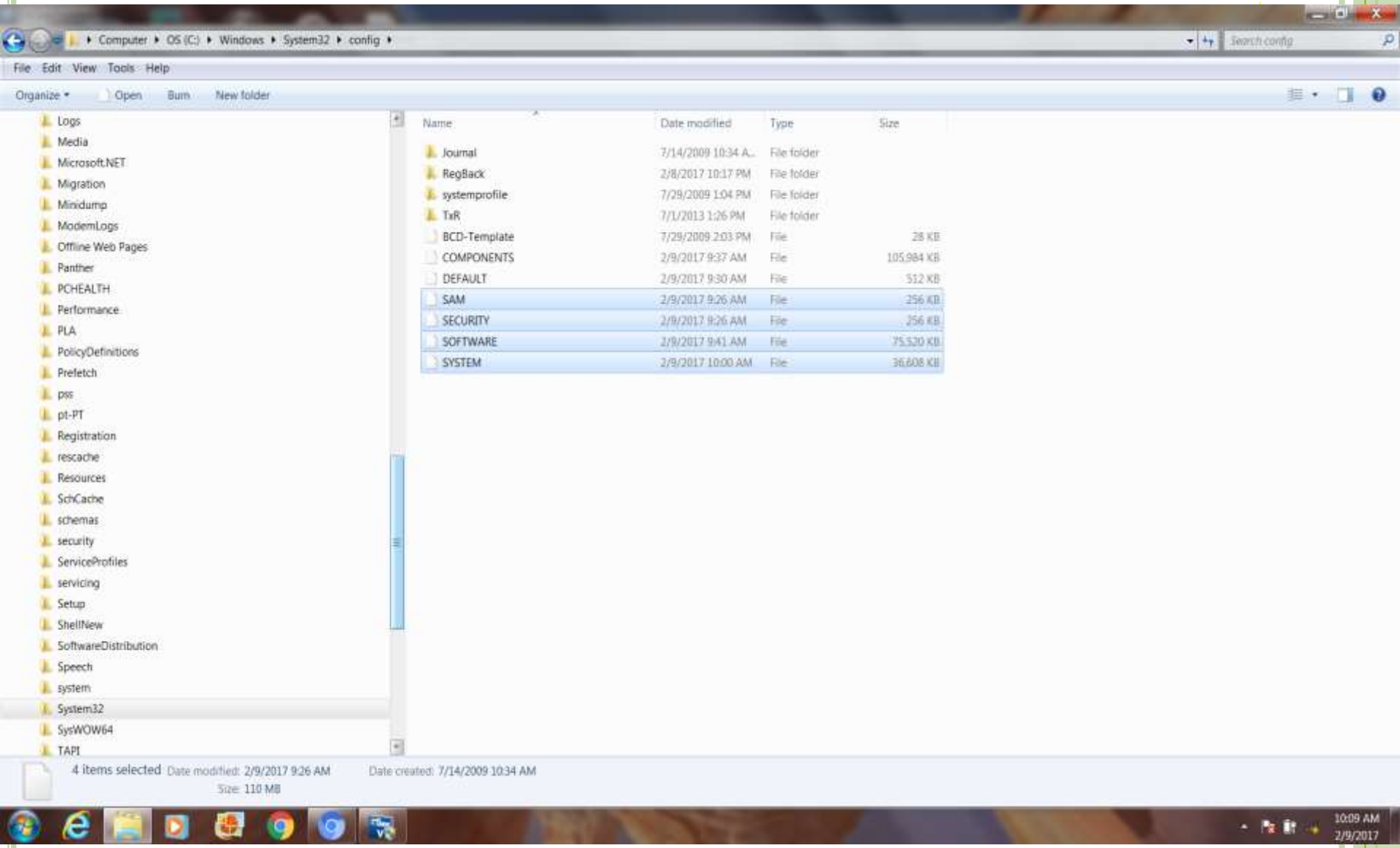
Windows Registry

- Is a database of operating system, installed application, and user configuration settings
- Provides valuable clues about how the computer system was used since installation time

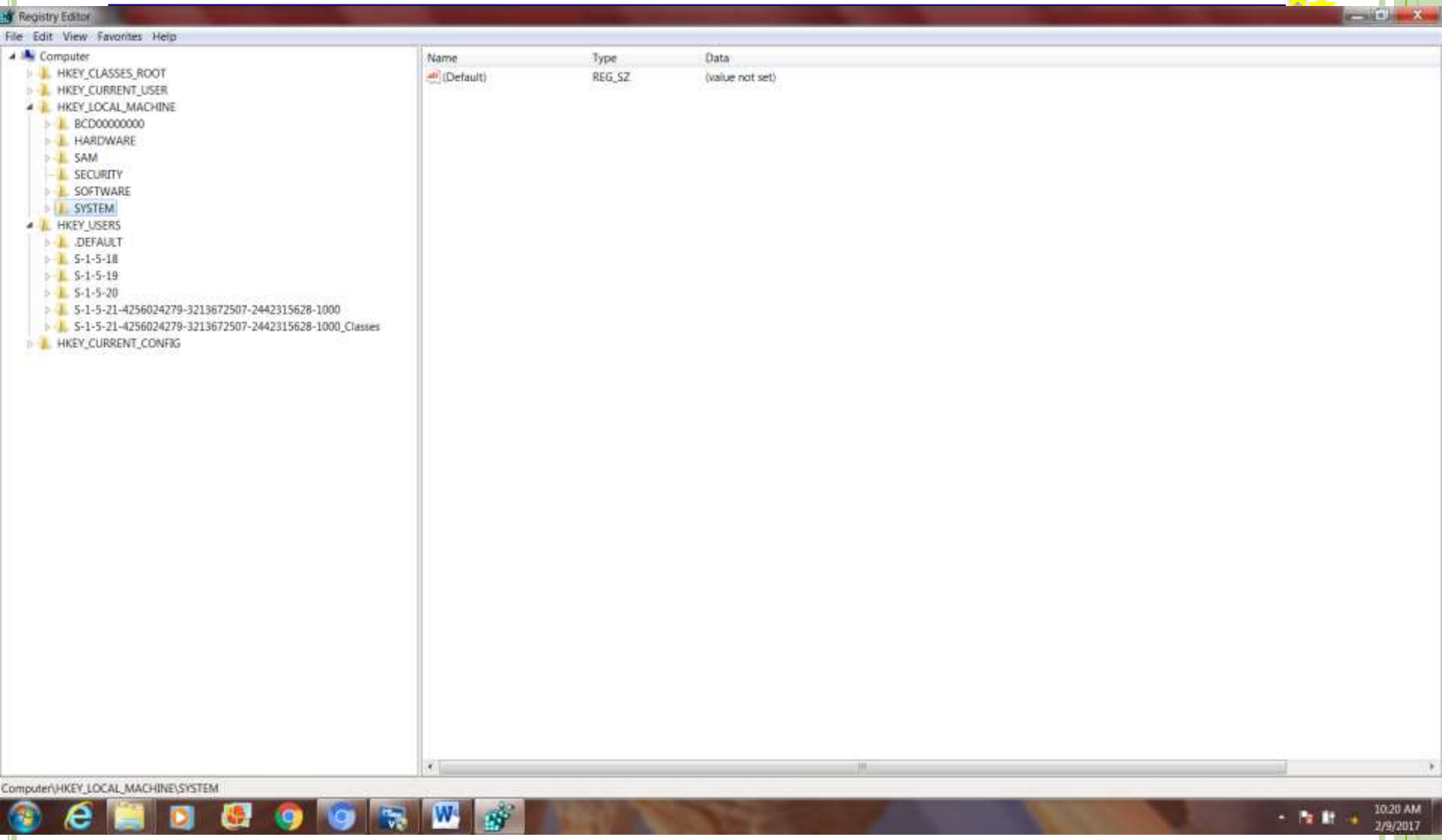
The location of these registry hives are as follows:

* HKEY_LOCAL_MACHINE \SYSTEM : \system32\config\system HKEY_LOCAL_MACHINE \SAM : \system32\config\sam HKEY_LOCAL_MACHINE \SECURITY : \system32\config\security HKEY_LOCAL_MACHINE \SOFTWARE : \system32\config\software
* HKEY_USERS \UserProfile : \winnt\profiles\username HKEY_USERS.DEFAULT : \system32\config\default

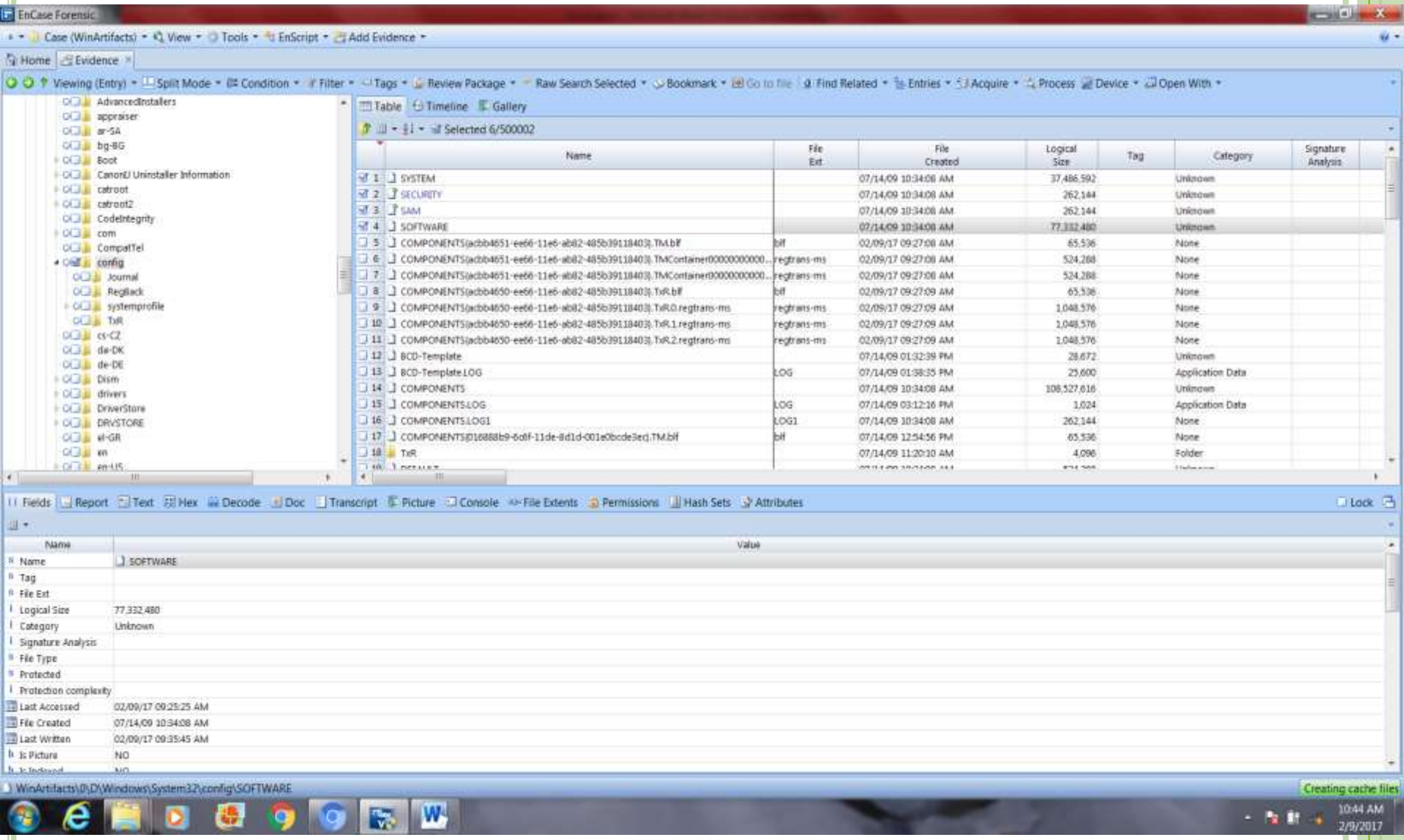
Windows Registry



Windows Registry



Windows Registry



End

Thank you
and
Good day …

Email Artifacts

Objective

- By the end of this module, participants will be able to search emails using industry-standard tools for forensic investigations

Introduction to Email

- **Internet-based applications have changed how people communicate**

- **Traditional communication methods have been enhanced**

  - **Contact anyone at anytime, anywhere in the world – in real time**
  - **Instant sharing of files**

What Is Email?

- **Internet-based application enabling users to send and receive messages with guaranteed delivery**
- **Messages can be accessed from many devices**
  - **Cell phones**
  - **Tablets**
  - **Computer systems**

Client-Based Versus Web-Based Email

Client-Based	Web-Based
• Installed by the Operating System • Configured according to the user's preferences and server settings	• Are typically accessed via an Internet browser • Store user content on a remote server

How Does Email Work?

- **Messages are sent and received over the Internet to an email address using specific network protocols**
- **Delivery to recipient is guaranteed**

Host and Domain

Host:

- **A member given access to use network resources**

mmouse@gmail.com

Domain:

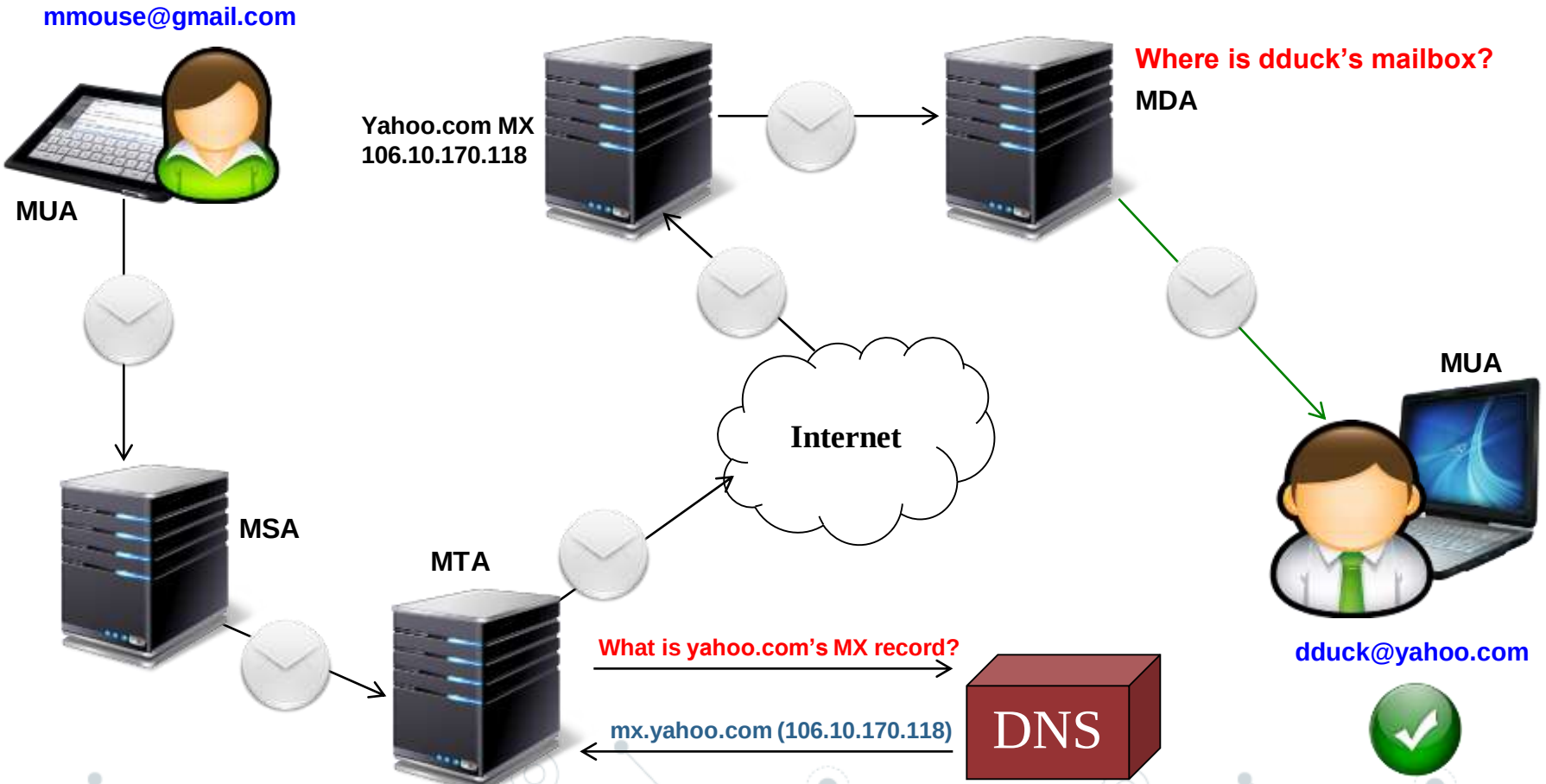
- **Collection of shared network resources**

Internet Protocols

- **Simple Mail Transfer Protocol (SMTP)**
- **Post Office Protocol (POP)**
- **Internet Message Access Protocol (IMAP)**
- **Hyper Text Transfer Protocol (HTTP)**

Email Delivery

From: mmouse@gmail.com
To: dduck@yahoo.com



Client-Based Email Applications

- **Installed on Internet-capable devices**
  - **Microsoft Outlook**
  - **Mozilla Thunderbird**
  - **Apple Mail (Macintosh OS X)**
- **User email data stored and managed in locally accessible databases**
  - **Contacts**
  - **Inbox**
  - **Sent Items**

Locating Email Artifacts: MS Outlook

- **Proprietary database format → Personal Storage Table (*.pst extension)**
  - **Contacts**
  - **Messages**
  - **Calendar**
- **MS Outlook 2010 database default location → C:\Users\<username>\Documents\Outlook Files**

Locating Email Artifacts: Thunderbird

- **User data stored in open database format → MBOX**
- **Email messages stored in plaintext in one file**
  - **Inbox**
  - **Sent Mail**
- **Mozilla Thunderbird database default location → C:\Users\<username>\AppData\Roaming\Thunderbird\Profiles*.default**

Web-Based Email Applications

- **Email content is accessed via an installed Internet browser on device → Webmail**
  - **Google Mail (Gmail)**
  - **Windows Live Mail (Hotmail)**
  - **Yahoo! Mail**
- **User data is maintained at the server level**
  - **Inbox/Sent Items**
  - **Contacts**
  - **Trash**

Locating Email Artifacts: Webmail

- **Some artifacts can be recovered**
  - **Temporary Internet Files**
  - **Pagefile.sys / Hiberfil.sys**
  - **NTFS metadata ($MFT, $LOGFILE)**
  - **Registry**

Email Message Headers

- **Detail journey of message from sender to recipient**
  - **Could provide clues on network identity of sender**
  - **Google Mail (when accessed via the browser) hides senders' network identity**
- **Stored as header of original email message**
- **Typically manually accessed by user/analyst**
  - **Hidden by most email clients**

Analyzing Email Message Header

Recipient's email address

```
Delivered-To: spearson47@gmail.com
Received: by 10.60.42.104 with SMTP id n8csp11154oel;
        Wed, 4 Jul 2012 00:17:29 -0700 (PDT)
Received: by 10.68.234.104 with SMTP id ud8mr15438560pbc.163.1341386249321;
        Wed, 04 Jul 2012 00:17:29 -0700 (PDT)
Return-Path: <kfamily_r@yahoo.cn>
Received: from mail.jkgroupbd.com (mail.jkgroupbd.com. [203.76.153.242])
        by mx.google.com with ESMTP id ms9si28256705pbb.132.2012.07.04.00.16.40;
        Wed, 04 Jul 2012 00:17:29 -0700 (PDT)
Received-SPF: neutral (google.com: 203.76.153.242 is neither permitted nor denied by best
guess record for domain of kfamily_r@yahoo.cn) client-ip=203.76.153.242;
Authentication-Results: mx.google.com; spf=neutral (google.com: 203.76.153.242 is neither
permitted nor denied by best guess record for domain of kfamily_r@yahoo.cn)
smtp.mail=kfamily_r@yahoo.cn
Received: by mail.jkgroupbd.com (Postfix, from userid 48)
        id AA8A12EE8204; Wed,  4 Jul 2012 04:27:50 +0600 (BDT)
Received: from 213.136.113.78
        (SquirrelMail authenticated user marketing)
        by 203.76.153.242 with HTTP;
        Wed, 4 Jul 2012 04:27:50 +0600 (BDT)
Message-ID: <39060.213.136.113.78.1341354470.squirrel@203.76.153.242>
Date: Wed, 4 Jul 2012 04:27:50 +0600 (BDT)
Subject: From Raphael Kamara
From: "Raphael Kamara" <kfamily_r@yahoo.cn>
Reply-To: rfamily_r@yahoo.cn
User-Agent: SquirrelMail/1.4.8-5.el5.centos.13
MIME-Version: 1.0
Content-Type: text/plain;charset=iso-8859-1
Content-Transfer-Encoding: 8bit
X-Priority: 3 (Normal)
Importance: Normal
To: undisclosed-recipients:;
```

Received tags show each hop

Could be sender's <u>actual</u> IP address

→ *traceable to ISP

Summary

- **You should now be able to**

  - **Access different types of mail files**
  - **Sort mail using defined fields**
  - **Filter mail types by keyword**
  - **Analyze an email header**

Thanks!

Any questions?

Computer Forensics Process

Godwin S. Monserate

21/09/2022

Objectives of the Session(1)

- **Sources of Evidence**
- **Acquire evidence using forensic techniques**
- **Use of forensic tools**
- **Digital evidence analysis**

Objectives of the Session(2)

- **Solving a Case**

- **Apply and use forensic techniques**

Digital Forensics

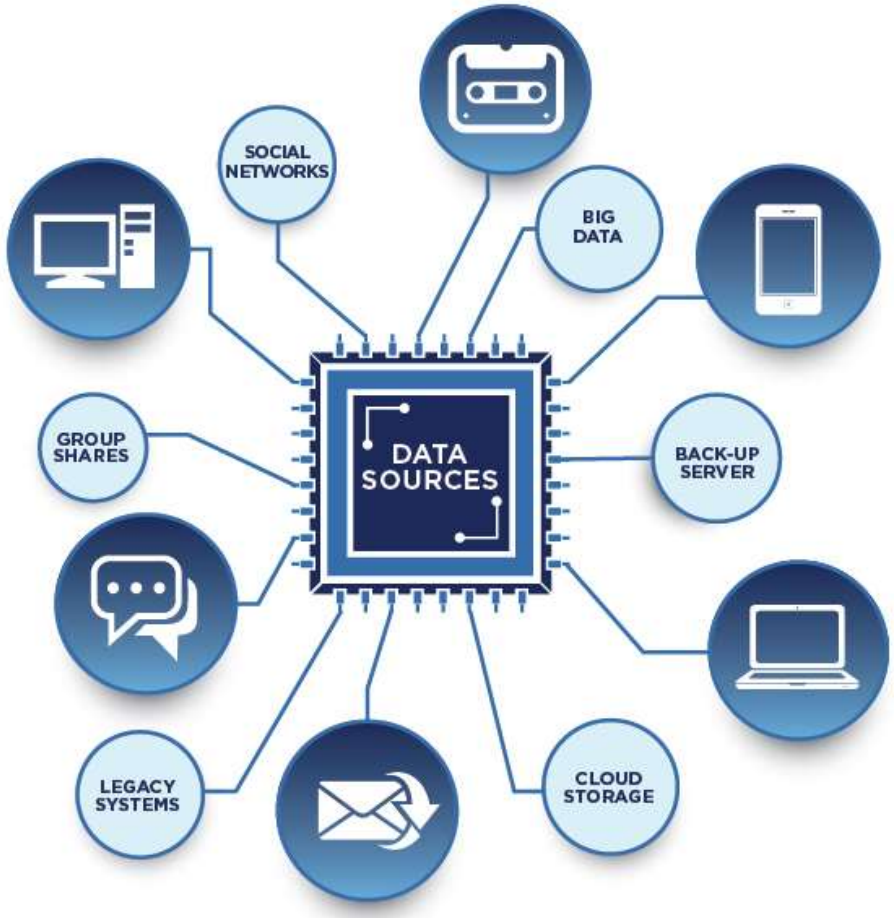
- Also known as Computer Forensics
- Considered to be the use of analytical and investigative techniques to identify, collect, examine and preserve evidence/information which is magnetically stored or encoded
- The objectives are:
  - Main objective is to find the criminal which is directly or indirectly related to cyber world
  - To find out digital evidences
  - Presenting evidences in a manner that leads to legal action of the criminal in the court of law

21/09/2022

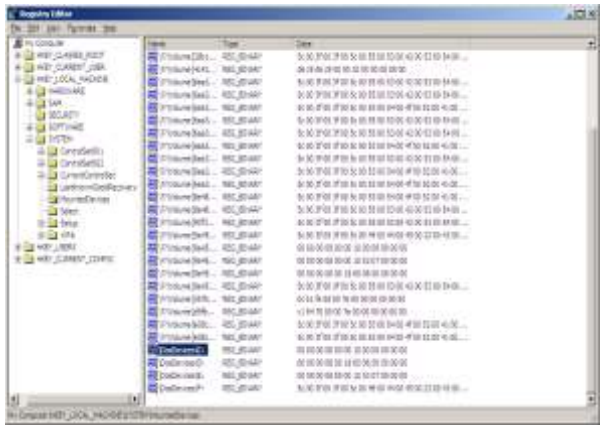
4

Digital Evidences

- Any data that is recorded or preserved on any medium in or by a computer system or other similar device, that can be read or understand by a person or a computer system or other similar device.
- Information and data of value to an investigation that is stored on, received, or transmitted by an electronic device.
- In the legal world, Evidence is EVERYTHING
- Evidence is used to establish facts



Types of Digital Evidence



- **Persistent Data**

  Data that remains intact when the computer is turned off.

  E.g. hard drives, disk drives and removable storage devices(such as USB drives or flash drives)

- **Volatile Data**

  Data that would be lost if the computer is turned off.

  E.g. deleted files, computer history, the computer's registry, temporary files and web browsing history.

Sources of Evidence

- Computers
- External hard drives
- CD's and DVD's
- Thumb drives
- Floppy disks
- Cell phones
- Voice over IP phones
- Answering machines
- iPods
- Electronic game devices
- Digital video recorders
- Digital cameras
- PDAs
- GPSs
- Routers
- Switches
- Wireless access points

21/09/2022

Forensic Phases:

- Acquisition
- Identification
- Evaluation
- Presentation

Computer Forensics Process(1)

Computer Forensics

- Identification
  - Identify Evidence
  - Identify type of information available
  - Determine how best to retrieve it





21/09/2022

9

Handling Digital Evidence at the Scene(1)

- First responders may follow the steps listed below to guide their handling of digital evidence at an electronic crime scene:
  - Recognize, identify, seize and secure all digital evidence at the scene.
  - Document the entire scene and the specific location of the evidence found.
  - Collect, label, and preserve the digital evidence
  - Package and transport digital evidence in a secure manner

- **Before collecting evidence at a crime scene, first responders should ensure that –**
  - Legal authority exists to seize evidence.
  - The scene has been secured and documented.
  - Appropriate personal protective equipment is used.

First thing to be done at the crime scene

- When seizing a stand alone computer at the crime scene:
  - If the computer is “POWERED OFF”, do not turn it ON(turning it “OFF” could activate lockout feature)

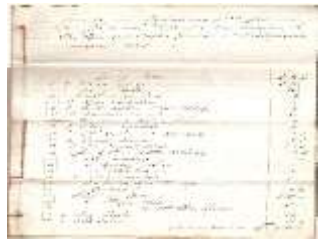
  - If the computer is “POWERED ON”, do not turn it OFF and do not allow any suspect or associate to touch it(turning it “ON” could alter evidence on device)

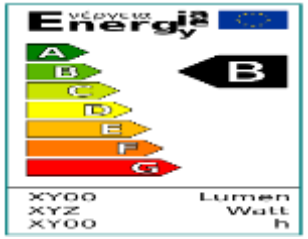
Tools and Materials for Collecting Digital Evidence

- Aside from tools for processing crime scenes in general, first responders should have the following items in their digital evidence collection toolkit:
  - Cameras(photo and video)
  - Cardboard boxes
  - Notepads
  - Gloves
  - Evidence inventory logs
  - Evidence tape
  - Evidence stickers, labels, or tags
  - Crime scene tape
  - Antistatic bags
  - Permanent markers
  - Nonmagnetic tools







Acquisition/Preservation(2)

- Taking images of the drives/partition belonged to the identified system.
- Physically or remotely obtaining possession of the computer and external physical storage devices.
- Imaging is a bit for bit copy of the original evidence.
- It is much different than a simple copy and paste, because it maintains file structure present on the disk.
- Imaging can be time consuming process for a digital investigation, it is a step that cannot be avoided.
- Reasons why digital evidence needs to be imaged.
  - Most important reason is to uphold the integrity of the original media that was seized from the crime scene or suspect
  - Allows investigator to add multiple evidence items to a single analysis tool
  - Allows investigator to process all of the digital evidence for a case at one time, which will speed up the analysis process

EnCase®

13

Number of Images Needed

- While the process of imaging can be different depending on the examiner or office procedure, the number of images should be a standard that is maintained for most investigations.
- Recommended is a two image standard.
- The first image that is created is considered the backup image.
- The backup image is an image that is used to create any additional images that are needed.
- When not in use, the backup image should be kept in a secure location to avoid outside manipulation of the evidence.
- From the backup images a second image is created, which is referred to as the working image. The working image is what will be analyzed by the examiner.




Ways of Imaging/Mirroring

- Hardware Imaging/Mirroring
  - There are hardware duplicators that take a hard drive and mirror it on another hard drive.
  - One of their big advantages is the speed and the safety.
  - Example, the Logicube places the capturing disk (the destination) within the encasing and connects the suspect drive at the outside, preventing the most important mistake that the forensics examiner can make, namely to write in the wrong direction and destroy the evidence.
- Software Based Forensics Duplication
  - A number of software products are available that create qualified forensics duplicates.

    UNIX dd - The dd utility in UNIX is certified to make forensic duplicates. dd is a UNIX tool, so the original drive needs to be mounted in UNIX. Raw dd duplicates need to be verified with a hashing (signatures), but there are specialized version of dd or scripts that include the verification.

    Encase is a very expensive, but very impressive Windows based Forensics suite that includes the making of qualified forensics duplicates

UNIX®

Guidance Software | EnCase

Computer Forensics

- Preservation
  - Preserve evidence with least amount of change possible
  - Must be able to account for any change
  - Chain of custody

3 Different Types of Imaging Process

- Disk to disk imaging is used when the investigator needs an exact duplicate or clone of the original storage media.
  - Integrity of the original can be maintained throughout the course of the investigation
- Disk to file imaging is much like disk to disk imaging.
  - Main difference it that instead of a clone of the original a single file is created that represents the original media.
  - If multiple items are seized from a scene it is possible to image multiple pieces of evidence at one time. This allows the examiner to set up the imaging process and step away.
  - Multiple file formats that can be used in Disk to File Imaging
    - dd
      - This format is a raw data format. Native to Linux/Unix
      - Very beneficial because many free tools are linux/unix based.
      - Every bit (0 or 1) that is on the original media is stored in the file.
      - If the original is a 20 GB hard drive, the result will be a 20 GB dd file.
- Files to File imaging is same thing as disk to file imaging except the input is files instead of an entire disk. This type of imaging is mainly used when the scope is limited or the disk has extremely large capacity such as a RAID setup. Files to file imaging is rarely used, but it is essential for the examiner to understand when it should be used.

3 Different Types of Imaging Process

- Multiple file formats that can be used in Disk to File Imaging
  - dd
    - This format is a raw data format. Native to Linux/Unix
    - Very beneficial because many free tools are linux/unix based.
    - Every bit (0 or 1) that is on the original media is stored in the file.
    - If the original is a 20 GB hard drive, the result will be a 20 GB dd file.
  - e01
    - A file format that was created by the developer of the commercial forensics tool Encase.
    - While the format was developed by the developers of Encase, it can be interpreted by other commercial tools.
    - Main benefit of E01 over DD is that the image file is compressed in a manner that is forensically sound.
    - Allows the examiner to save space on the destination storage media.

2 Categories of Software Imagers

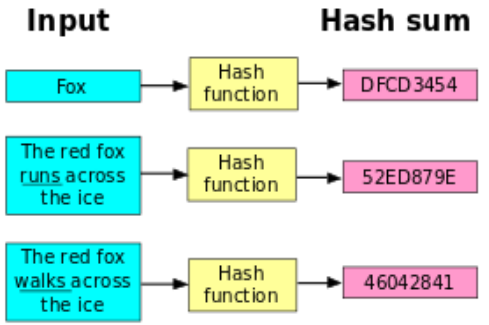
- Imagers that use a command line interface.
  - The most common command line interface is DD or data dump.
  - Most command line interfaces used today are linux based.
  - There are multiple versions of DD, some of which include the hashing function, such as DCFLDD.
  - The benefit of command line tools is that the user will usually have more control over the tool.
- Imagers that use a graphical style interface.
  - The graphical interface is much easier to use than command line.
  - Most commercial software imagers on the market will include a graphical style interface.
  - Example is FTK Imager by Access- Data.
  - Like most commercial software imagers FTK Imager supports multiple formats, has hashing capabilities, and generates an imaging report.
  - Like other forms of imaging it is essential that an examiner practice with the tools that he or she is going to use to ensure that they fully understand the capability and procedure of the tools they are using.

Commercial vs Open-Source Tools

- Some advantages Commercial tools have over Open-Source tools:
  - Better Documentation
  - Commercial Level Support
  - Slick GUI (Graphical User Interface), user-friendly
  - In some cases, complete report generation which is accepted in court of law
- However, for anything a commercial forensics application can do, there are open-source applications which can do the same thing.

Authentication

- Important to continue proper documentation throughout the entire investigation process.
- Digital evidence can easily change.
- Authentication, supported by proper documentation, can ensure that the evidence does not change once it was acquired and can ensure that the examination machine did not manipulate the original media.
- To provide proper authentication, verification takes place using hashing algorithms on both evidence and images.
- Hardware write blockers will prevent any change to the original media.



Create Proof of Non-Alteration(Hashing)

- For this reason, it is common practice to calculate cryptographic hash of an evidence file and to record that hash elsewhere, usually in an investigator's notebook, so that one can establish at a later point in time that the evidence has not been modified since the hash was calculated.
- Hashing is a one-way function that computes a fixed length output from a variable input.
- Any change in the input results in a completely different output due to the avalanche effect.
- The input of a hashing function can be any digital stream of data.
- This can range from individual files to large storage devices.
- The only limitation is that the device must be able to be read by a computer. Items such as cell phones may require some type of data cable or specialized software.

Create Proof of Non-Alteration(Hashing)

- The output of a hashing function is usually represented in hex or base 16.
- This hash value can be looked at as a digital fingerprint.
- A benefit of using hash values to compare files is that there is no way to reverse from the hash to digital media.
- This helps maintain the integrity of the evidence while comparing it to other known files or devices.
- There are many different known hashing algorithms.
- The ones that are used the most for digital forensics today are MD5, SHA 1, and SHA 256.
- The MD5 hash algorithm returns a 128 bit output.
- The SHA 1 hash algorithm returns a 160 bit output. The SHA 256 hash algorithm returns a 256 bit output.

Chain of Custody

- "Chain of Custody" is a fancy way of saying "The ability to demonstrate who has had access to the digital information being used as evidence".
- Special measures should be taken when conducting a forensic investigation if it is desired for the results to be used in a court of law.
- One of the most important measures is to assure that the evidence has been accurately collected and that there is a clear chain of custody from the scene of the crime to the investigator – and ultimately to the court of law.

Forensic Techniques

- **Cross-drive analysis:**
- forensic technique that correlates information found on multiple hard drives.
- can be used to perform anomaly detection.

- **Live analysis:**
- The examination of computers from within the operating system using custom forensics to extract evidence.

Forensic Techniques

- **Deleted files:**
- recovery of deleted files
- Use of forensic software tools for recovering or carving out deleted data.

- **Example of Software Tools:**
- EnCase
- WinHex
- ProDiscover
- S-tool

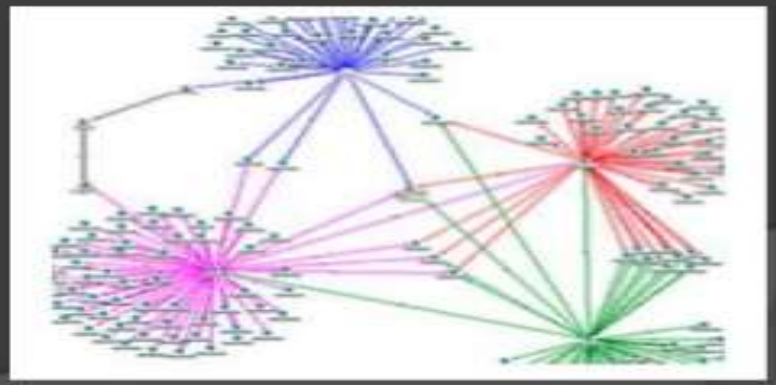
Forensic Techniques

- **Steganography:**
- concealing a message, image, or file within another message, image, or file.
- detection of steganographically encoded packages is called steganalysis.
- the simplest method to detect modified files is to compare them to known originals.

Computer Forensics Process(3)

Computer Forensics

- Analysis
  - Extract
  - Process
  - Interpret



Computer Forensics Process(3)

- The third stage is Analysis.
- Analysis is the examination of all digital evidence that has been acquired and authenticated.
- The analysis process will be dictated by the examiner and types of digital evidence.
- In most situations the analysis will require specialized tools and skills. The tools requires be both software and hardware based.
- The goal of the analysis stage is to identify all evidence contained in the digital device and report the results.
- Each examiner will have their own approach to analysis.
- A collection of tools that you are comfortable with is important.
- There are both commercial and open source tools available.

Computer Forensics Process(3)

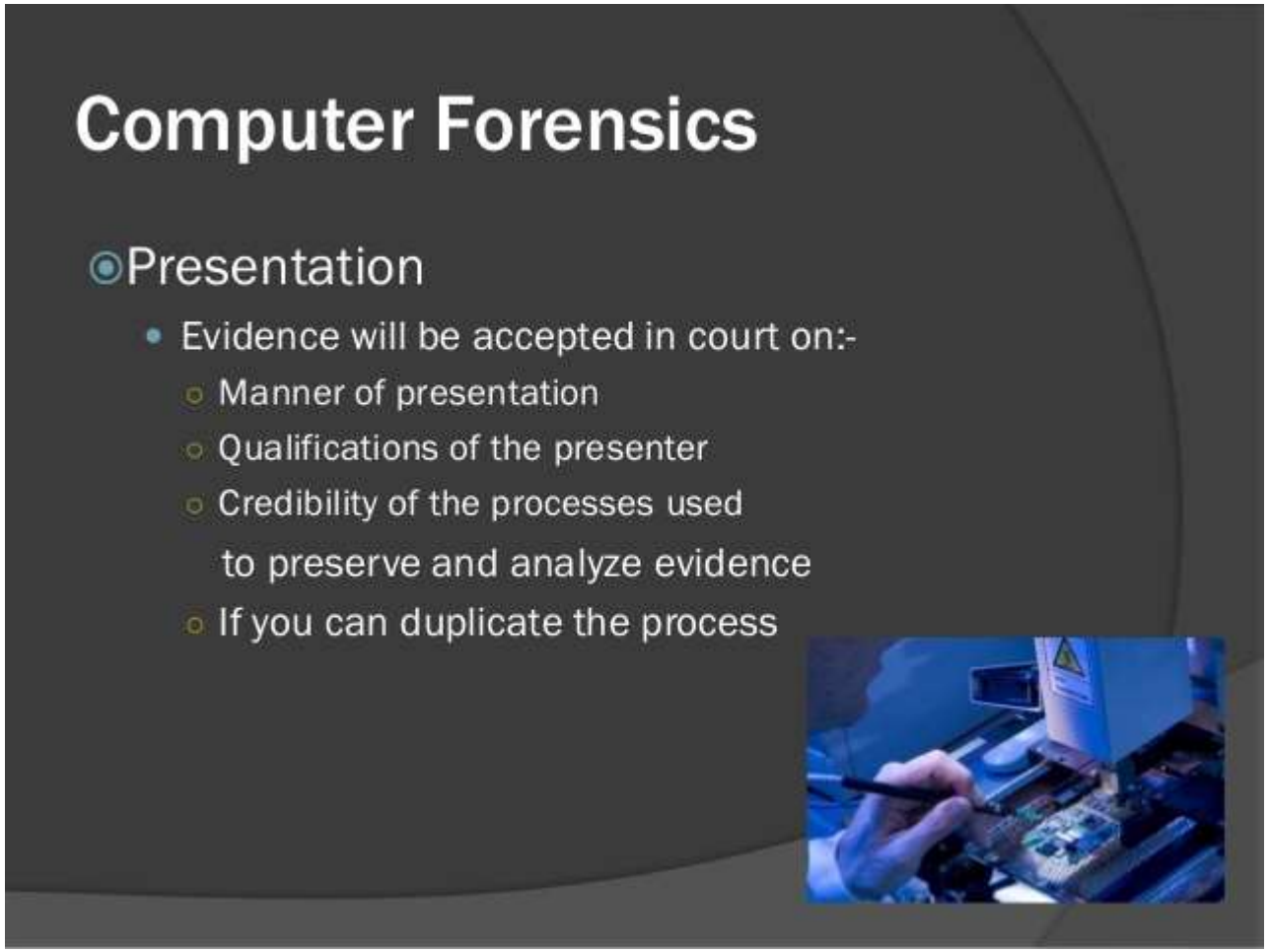
- There are two leading commercial manufacturers of computer forensics software today.
- They are AccessData and Guidance Software. In addition to commercial software there are free options such as Linux and other free tools.
- Free tools should only be used for examination by someone who has tested and practiced with the tool.
- The next logical step refers to when you are done with an investigation.
- How do you know that you have found all the evidence related to the case? Do you need to look at every file?
- What if you can't find anything?

Computer Forensics Process(3)

- It is unreasonable to assume that you can look at every bit of data on the disk.
- Depending on your workload and policies, you want to at least look at most of the disk.
- The goal is to determine three things.
  - What is present on the disk?
  - What is the most likely and supported reason that information is present or absent?
  - Are there any plausible alternative explanations? Use the data to rule them out.

Computer Forensics Process(4)

The final step is to prepare a report that details both your procedure and your findings. Reporting is covered in Advanced Comp Forensic.



COMPUTER FORENSIC REQUIREMENTS

- Hardware
  - Familiarity with all internal and external devices/components of a computer
  - Thorough understanding of hard drives and settings
  - Understanding motherboards and the various chipsets used
  - Power connections
  - Memory
- BIOS
  - Understanding how the BIOS works
  - Familiarity with the various settings and limitations of the BIOS

COMPUTER FORENSIC REQUIREMENTS

- Operation Systems
  - Windows 3.1/95/98/ME/NT/2000/2003/XP
  - DOS
  - UNIX
  - LINUX
- Software
  - Familiarity with most popular software packages such as MS Office
- Forensic Tools
  - Familiarity with computer forensic techniques and the software packages that could be used

COLLECTING EVIDENCE

- Make Exact copies of all hard drives & disks using computer software
  - Date and Time stamped on each file; used for timeline
- Protect the Computer system
  - Avoid deletion, damage, viruses and corruption
- Discover files
  - Normal Files
  - Deleted Files
  - Password Protected Files
  - Hidden Files
  - Encrypted Files
- Reveal all contents of hidden files used by application and operating system
- Access contents of password protected files if legally able to do so
- Analyze data
- Print out analysis
  - Computer System
  - All Files and data
  - Overall opinion
- Provide expert consultation/testimony

Conclusion

This field will enable crucial electronic evidence to be found, whether it was lost, deleted, damaged, or hidden, and used to prosecute individuals that believe they have successfully beaten the system.

CREATING A DIGITAL FORENSIC LABORATORY

Godwin S. Monserate

Cisco | Networking Academy®
Mind Wide Open™

CREATING A DIGITAL FORENSIC LABORATORY

- Creating a digital forensic laboratory is a responsible step. The effectiveness of the laboratory depends on what software, hardware and equipment will be purchased.

A FORENSIC WORKSTATION

- Choosing a workstation configuration is an important step. The effectiveness of digital examiners depends on the way the workstation is configured.
- However, we want to pay special attention to one point: the workstation should work as quietly as possible. Imagine an open space where several powerful computers are installed, each of which makes a noise like a server. The employees' headache and poor health are guaranteed. Silent workstation performance is achieved by using low-noise fans and passive cooling systems.
- Do not use top hardware. The idea to buy the most expensive processor, memory, motherboard for your new workstation is not the best one.

- This configuration is optimal today:
  - OS: Windows 10 Pro 64-bit
  - CPU (2): E5-2660 v4 (14 core)
  - RAM: 64 GB DDR-42133 ECC
  - OS Drive: 1 TB SSD
  - Temp/Cache/DB Drive: 256 GB SSD
  - Data Drive: 8 TB 7200rpm
  - RAID Drives: 5 × 4 TB 7200rpm
  - Video Card: GeForce GTX 1080

A FORENSIC WORKSTATION

- It is recommended to use two or more monitors for each workstation.
- The most effective work is achieved when a digital examiner uses two workstations in its work.
- Use Storages to store cases, forensic images, etc. Storages with a volume of 100-150 TB proved to be quite effective.
- Use 10Gbit Net Cards. They will allow you to transfer data from the workstation to storages quickly.

FORENSIC SOFTWARE

- It’s a good idea to have as more different forensic software in the digital laboratory.
- This will allow a forensic examiner to make cases as quickly and efficiently as possible. Also, this makes it possible to recheck the results of the research effectively.
- However, if you have a limited budget, we recommend buying this software:
- Windows 10 Pro, Office 365
- Antivirus software, X-ways Forensic
- AXIOM (Magnet Forensics)
- The rest of the tools can be purchased as the laboratory develops.

FORENSIC SOFTWARE

- Also, a lot of research can be done using freeware tools.
- Sometimes these tools outperform functionality of commercial tools.

CASE MANAGEMENT SOFTWARE

- The digital forensic laboratory in a government organization, for example in the police department, then most likely they have their own case management software and then your task is just to add a new laboratory to the network of existing ones.
- In other cases, you can use free and chargeable CRM systems. Besides, some CRM systems can be adapted to your management needs.
- Ex. **Kirjuri** (Kirjuri is a web application for managing cases and physical forensic evidence items.)
- Lima Forensic Case Management of all the specialized tools.

VIDEO FORENSICS

- Use a separate workstation for the production of video forensics cases. The following forensic tools are recommended for this task:
  - **DVR Examiner**
  - **Amped FIVE**
  - **Elecard**
- Very good results of recovering deleted videos can be obtained using X-ways Forensic.

MOBILE FORENSICS

- We recommend using a separate workstation to carry out mobile forensics research.
- There are a lot of tools for mobile forensics. That is why it is difficult for a beginner to understand what they need to carry out this research effectively. Using the following mobile forensic tools will help you achieve your objective:
  - UFED 4PC (with CHINEX, UFED Camera Kit)

Cellebrute UFED Touch

MOBILE FORENSICS

- **Oxygen Forensics DETECTIVE**
  - Oxygen Forensic Detective is an all-in-one forensic software platform built to extract, decode, and analyze data from multiple digital sources: mobile and IoT devices, device backups, UICC and media cards, drones, and cloud services. Oxygen Forensic® Detective can also find and extract a vast range of artifacts, system files as well as credentials from Windows, macOS, and Linux machines.
- **XRY**
  - **XRY** is a **digital forensics** and mobile device **forensics** product by the Swedish company Micro Systemation used to analyze and recover information from mobile devices such as mobile phones, smartphones, GPS navigation tools and tablet computers. It consists of a hardware device with which to connect phones to a PC and software to extract the data.
- **Elcomsoft Mobile Forensic Bundle**
  - includes a number of tools to acquire and analyze evidence from a number of mobile platforms. Physical and logical acquisition of iOS devices Extract evidence from 64-bit iOS devices with or without a jailbreak.

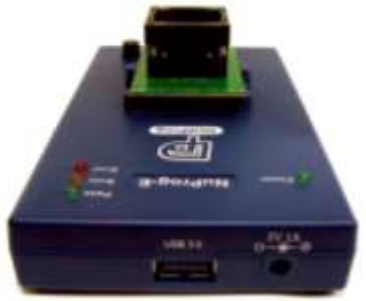
MOBILE FORENSICS

- **SP Flash tool to retrieve data from MTK based phones.**

  SP flash tool is an application which mainly helps you to flash Stock ROM, Custom recovery and fixing in some extreme cases (firmware update, Flash recovery, unbrick bricked Android device etc.).

  SmartPhone FlashTool is working with MediaTek Android smartphones (MTK based) You can Download SPFlashTool from our downloading section.

MOBILE DATA RECOVERY



- Use flashers for JTAG research:
  - Easy Z3x JTAG BOX
  - Octoplus Box
  - Samsung anyway S101
- For Chip-off we recommend using:
  - VISUAL NAND RECONSTRUCTOR (STARTER KIT, Rusolut)
  - SMARTPHONE KIT (Rusolut)
  - CHINESE SMARTPHONE KIT (Rusolut)
  - NuProg-E UFS/EMMC Programmer
  - IN-UFS-Socket BGA Opentop
  - N-UFS-065-BGA095-115130-02O BGA Opentop
  - N-UFS-050-FBGA153-115130-02O BGA Opentop

- Use Weller WHA 300 Hot Air Reworking Station or Ersa HR100 Hybrid Rework system for disordering chips.

CLOUD FORENSICS

- Use the following tools for Cloud forensics:
  - UFED Cloud Analyzer
  - Oxygen Forensics DETECTIVE
  - Elcomsoft Cloud eXplorer

DATA RECOVERY (HARD DRIVES, FLASH DRIVES, MEMORY CARDS)

- Use a separate workstation for the production of Data recovery. You will need special hardware and tools for data recovery:
  - PC-3000 Express Professional System (Acelab)
  - Data Extractor Express (Acelab)
  - PC-3000 Flash (Acelab)

DATA RECOVERY (HARD DRIVES, FLASH DRIVES, MEMORY CARDS)

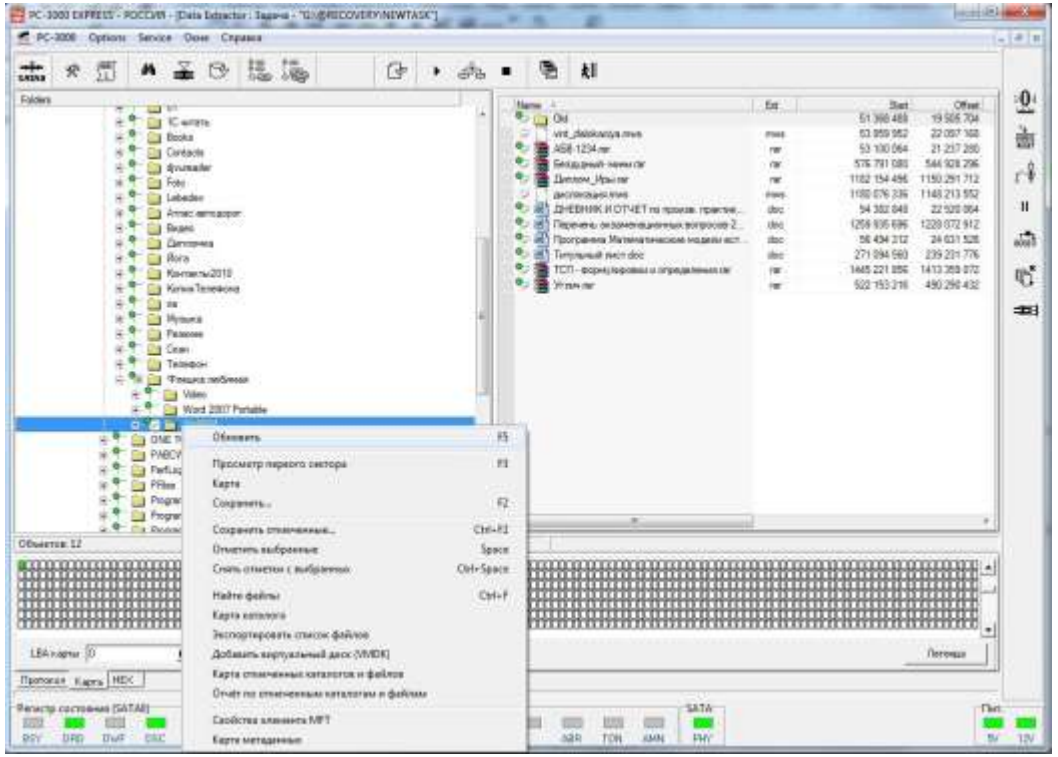
- Hardware and tools for data recovery:
  - PC-3000 Express Professional System (Acelab)
    - is the fastest, most efficient and most powerful hardware-software solution for recovering data from damaged HDDs based on SATA (Serial ATA) or PATA (IDE) interfaces for numerous vendors

DATA RECOVERY (HARD DRIVES, FLASH DRIVES, MEMORY CARDS)

Data Extractor Express (Acelab)

PC-3000 Flash (Acelab)

The **Data Extractor Express** is a specialized software product functioning in tandem with the PC-3000 Express hardware-software product.



FURNITURE

- Many people believe that it is enough to buy ordinary office desks and chairs to equip a digital forensic lab
- Tables must have abrasion resistant coatings.
- Office chairs should be as convenient as possible.
- The table where the electronic equipment is assembled and disassembled should be equipped with an antistatic mat and an antistatic bracelet.

What Is Digital Forensics?

- Digital forensic science is a branch of forensic science that focuses on the recovery and investigation of material found in digital devices related to cybercrime.
- The term digital forensics was first used as a synonym for computer forensics. Since then, it has expanded to cover the investigation of any devices that can store digital data.
- The first computer crime was reported in 1978, followed by the Florida computers act, it wasn’t until the 1990s that it became a recognized term. It was only in the early 21st century that national policies on digital forensics emerged.
- Digital forensics is the process of identifying, preserving, analyzing, and documenting digital evidence. This is done in order to present evidence in a court of law when required.

What Is Digital Forensics?

- “Digital forensics is the process of uncovering and interpreting electronic data. The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying, and validating the digital information to reconstruct past events.
- The context is most often for the usage of data in a court of law, though digital forensics can be used in other instances.”

-Techopedia

Steps of Digital Forensics

Steps of Digital Forensics

In order for digital evidence to be accepted in a court of law, it must be handled in a very specific way so that there is no opportunity for cyber criminals to tamper with the evidence.

1. Identification

First, find the evidence, noting where it is stored.

2. Preservation

Next, isolate, secure, and preserve the data. This includes preventing people from possibly tampering with the evidence.

3. Analysis

Next, reconstruct fragments of data and draw conclusions based on the evidence found.

4. Documentation

Following that, create a record of all the data to recreate the crime scene.

5. Presentation

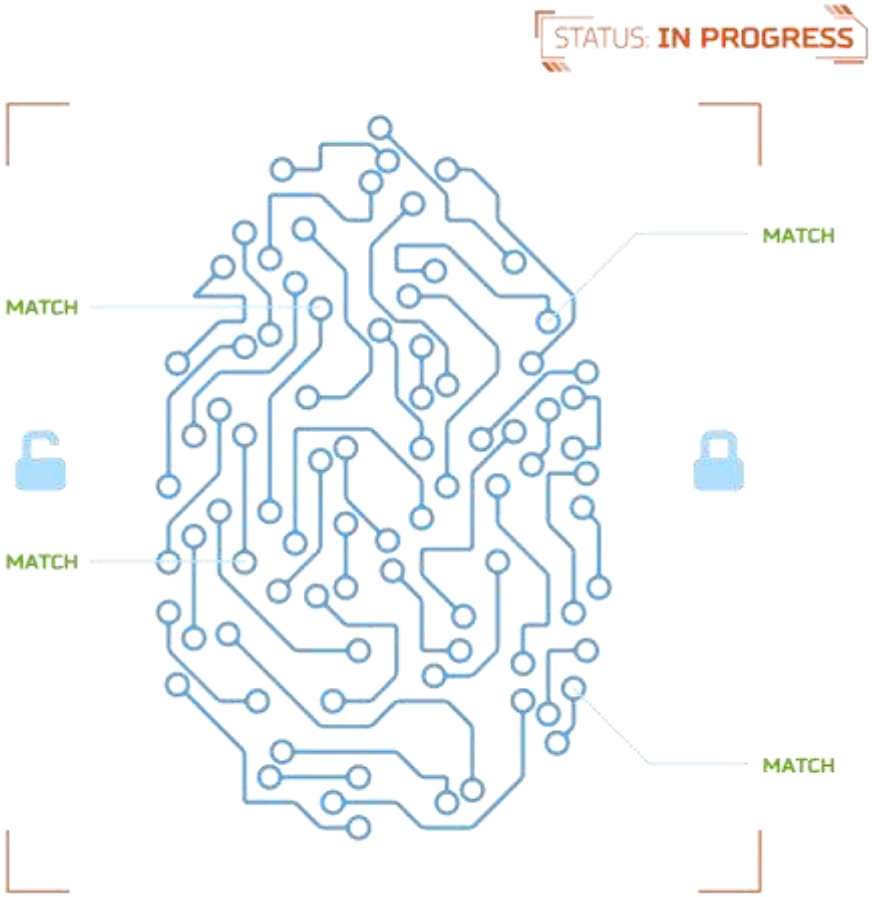
Lastly, summarize and draw a conclusion.

When Is Digital Forensics Used in a Business Setting?

- For businesses, Digital Forensics is an important part of the Incident Response process.
- Forensic Investigators identify and record details of a criminal incident as evidence to be used for law enforcement.
- Rules and regulations surrounding this process are often instrumental in proving innocence or guilt in a court of law.

Who Is a Digital Forensics Investigator?

- A Digital Forensics Investigator is someone who has a desire to follow the evidence and solve a crime virtually.
- Imagine a security breach happens at a company, resulting in stolen data.
- Under those circumstances, a digital forensic investigator's role is to recover data like documents, photos, and emails from computer hard drives and other data storage devices, such as zip and flash drives, with deleted, damaged, or otherwise manipulated.



How Is Digital Forensics Used in an Investigation?

- Digital footprint is the information about a person on the system, such as the webpages they have visited, when they were active, and what device they were using. By following the digital footprints, the investigator will retrieve the data critical to solving the crime case. To name a few –Matt Baker, in 2010, Krenar Lusha, in 2009, and more cases were solved with the help of digital forensics.
- Cyber forensic investigators are experts in investigating encrypted data using various types of software and tools. There are many upcoming techniques that investigators use depending on the type of cybercrime they are dealing with.
- Cyber investigators' tasks include recovering deleted files, cracking passwords, and finding the source of the security breach. Once collected, the evidence is then stored and translated to make it presentable before the court of law or for police to examine further.