

# EnCase v7 Essential Training

---

# What's in this course

---

Explore the most notable features of the new version.

Everything you need to know about EnCase v7 to conduct basic investigations.

- Create Cases
- Acquire Mobile phones and Storage Devices
- Add existing evidence to cases
- Browse and explore evidence
- Process evidence and conduct analysis
- Export findings and Write reports.

# Acknowledgment

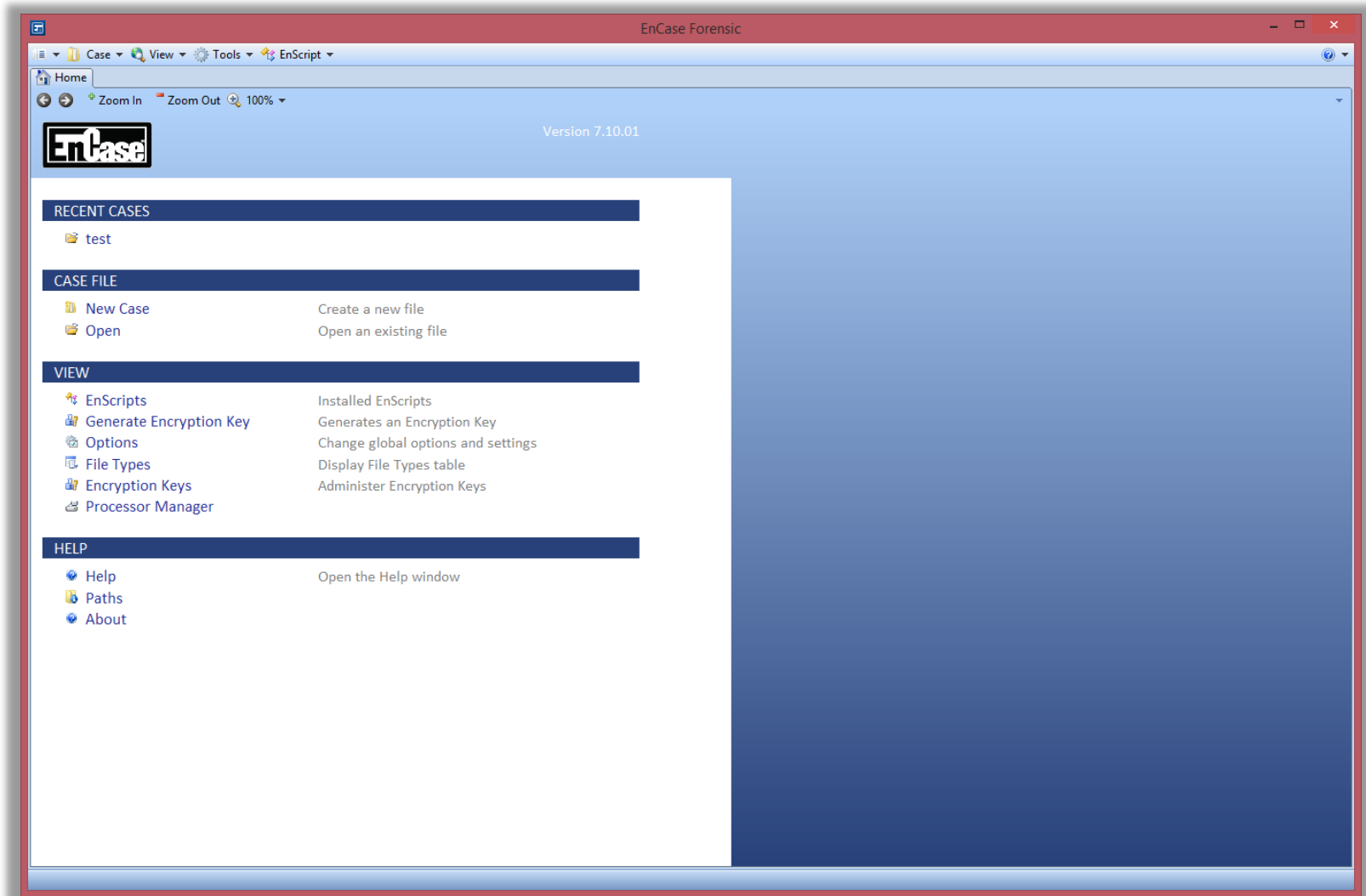
---

The Computer Evidence sample we shall use is “TDurden evidence file”, which Guidance Software provides for free; get it from:

- [http://media.johnwiley.com.au/product\\_ancillary/63/04709010/DOWNLOAD/tdurdenex01.html](http://media.johnwiley.com.au/product_ancillary/63/04709010/DOWNLOAD/tdurdenex01.html)
- <https://www.4shared.com/file/aa3BYubz/TDurden.htm>

Few screenshots in this presentation are taken from “EnCase® Version 7.10 User 's Guide”

# EnCase v7 new UI



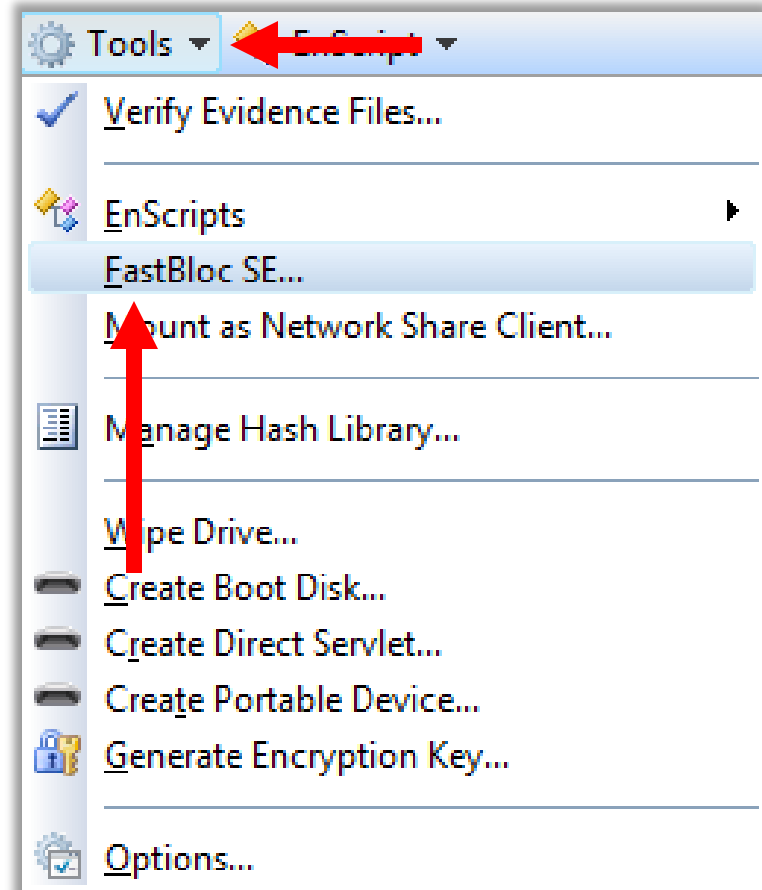
# Evidence Acquisition

---

# FastBloc SE

FastBloc SE is the first commercial software write-blocking solution that allows EnCase to take full control of IDE, SATA and SCSI channels on particular PCI controller cards, as well as the FireWire and USB ports from Windows, permitting a forensically sound acquisition without the use of hardware write-blocking devices.

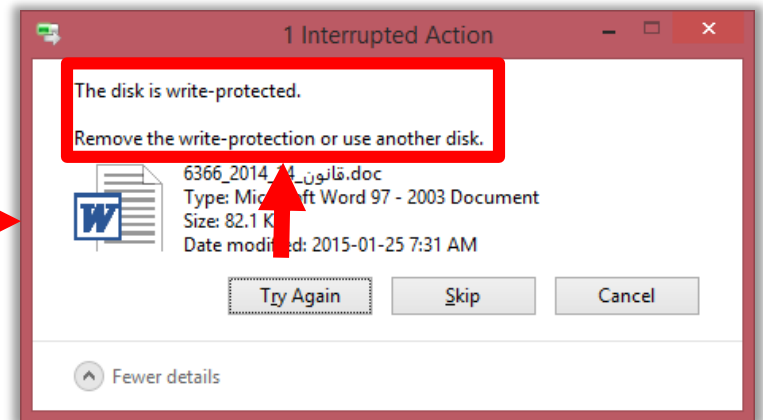
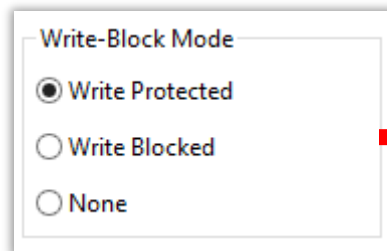
Tools -> `FastBloc SE`



# FastBloc SE modes

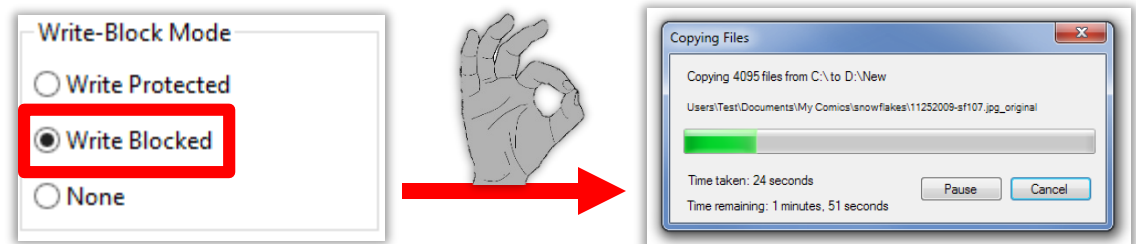
All modes protect the evidence from actual modifications.

**Write Protected:** Operating system will not allow any modifications (copy to / delete / modify) and will throw an error. **Use this mode for imaging!**



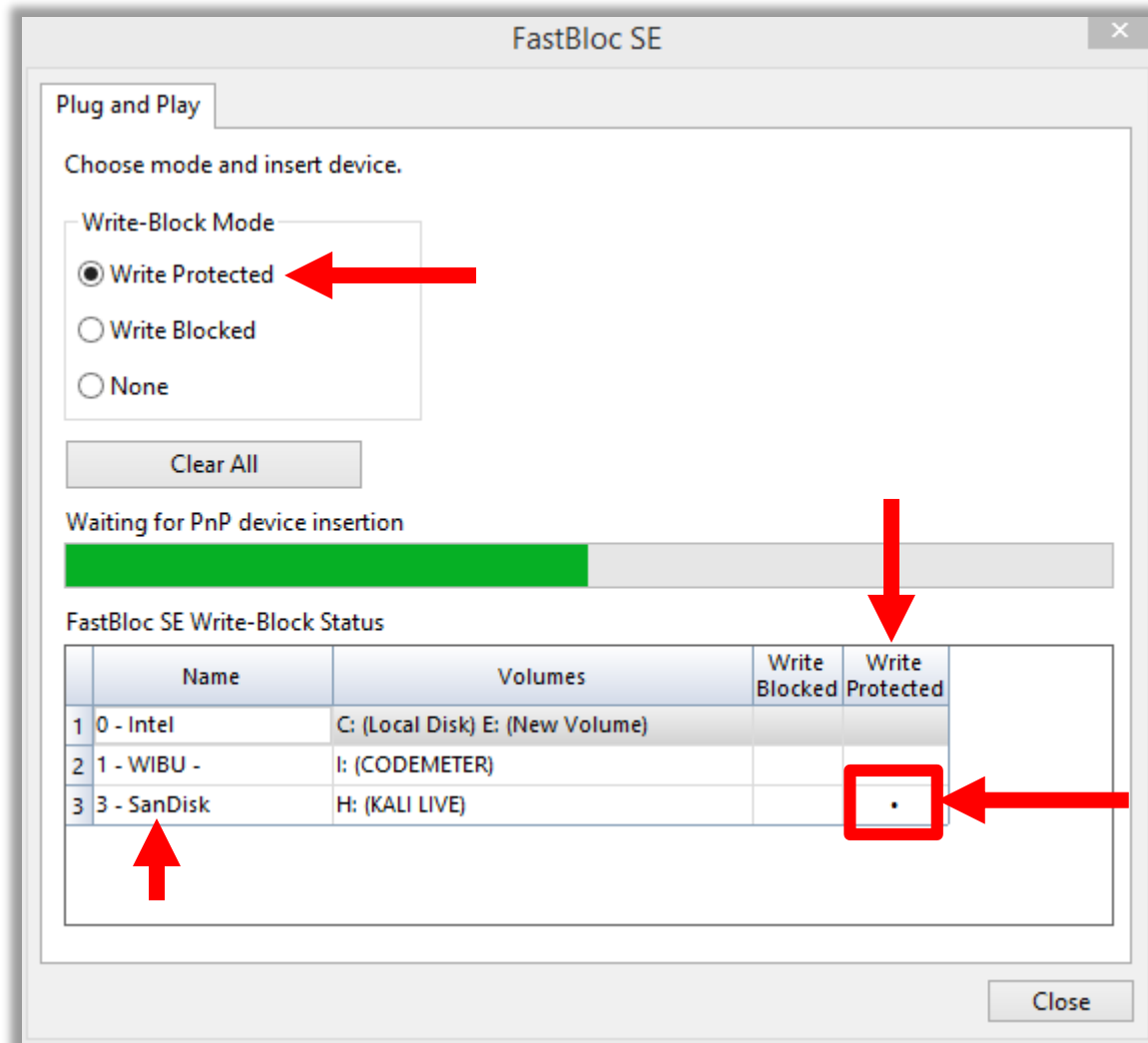
# FastBloc SE modes

**Write Blocked:** OS will act as if the device is not write blocked at all, and will allow changing security permissions of files “use this mode for casual `browsing` where sometimes access is not permitted due to security permissions. (if you unplugged and plugged device again, it will lose all modifications).





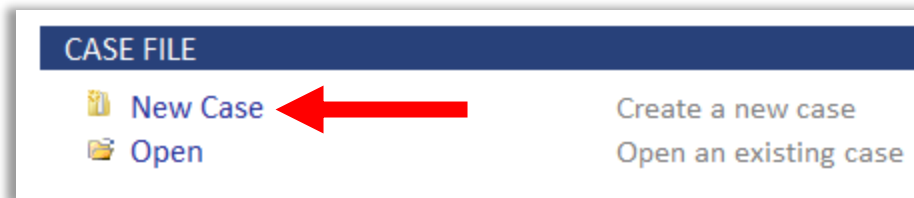
# Pick a mode, plug a device



# Create a new case

---

With the evidence write-blocked and attached, we have to create a case for evidence acquisition.



# Create a new case

The screenshot shows the 'Options' dialog box in EnCase, titled 'Options' with a close button (X) in the top right corner. The dialog is divided into several sections:

- Templates:** A list of templates on the left, including '#1 Basic', '#2 Forensic', '#3 Basic (UK)', '#4 Forensic (UK)', '#5 Flexible', and 'None'. The 'None' template is currently selected.
- Name and location:** Fields for 'Name' (containing 'EnCaseTraining'), 'Full case path' (containing 'C:\Users\USER\Documents\EnCase\Cases\EnCaseTraining\EnCaseTraining.Case'), and 'Base case folder' (containing 'C:\Users\USER\Documents\EnCase\Cases').
- Evidence cache locations:** A section with a checked checkbox 'Use base case folder for primary evidence cache'. Below it, 'Primary evidence cache' is set to 'C:\Users\USER\Documents\EnCase\Cases\EnCaseTraining\EvidenceCache', and 'Secondary evidence cache' is empty.
- Backup settings:** A section with a checked checkbox 'Backup every' set to '30 minutes', 'Maximum case backup size (GB)' set to '50', and 'Backup location' set to 'C:\Users\USER\Documents\EnCase\CaseBackup'.

At the bottom of the dialog are 'OK' and 'Cancel' buttons. On the left side, under 'Case information', there is a 'Split Mode' dropdown set to 'New' and a table with columns 'Name' and 'Value'.

# Add Evidence

## SEARCH

 Search

Search your case for matching items

## EVIDENCE

 Add Evidence

Add items to the Case

 Processor Manager

## BROWSE

 Evidence

Evidence in the case

 Records

Processed data, such as email and Internet artifacts

 Case Analyzer

Analyze processed metadata

 EnScripts

Installed EnScripts


## REPORT

 Reports

Reports created from report templates

 Bookmarks

A bookmark

 Report Templates

A template for a report

## CASE

 Options

Case options and settings

 Hash Libraries

Change hash libraries settings

 Save

Save this case to disk

 Close

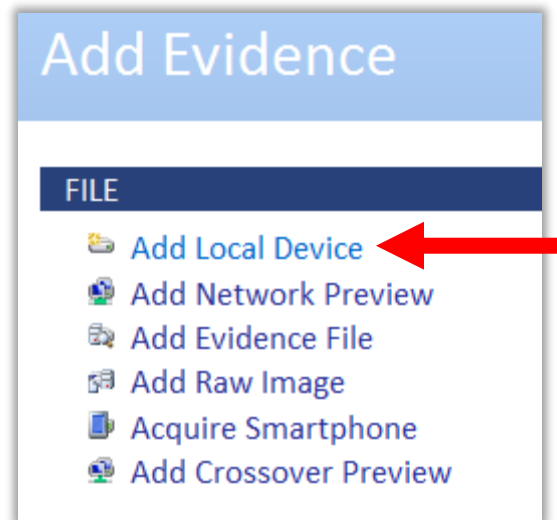
Close this case

# Add Evidence

---

Since the evidence is attached as a USB device, we pick `Add local device`.

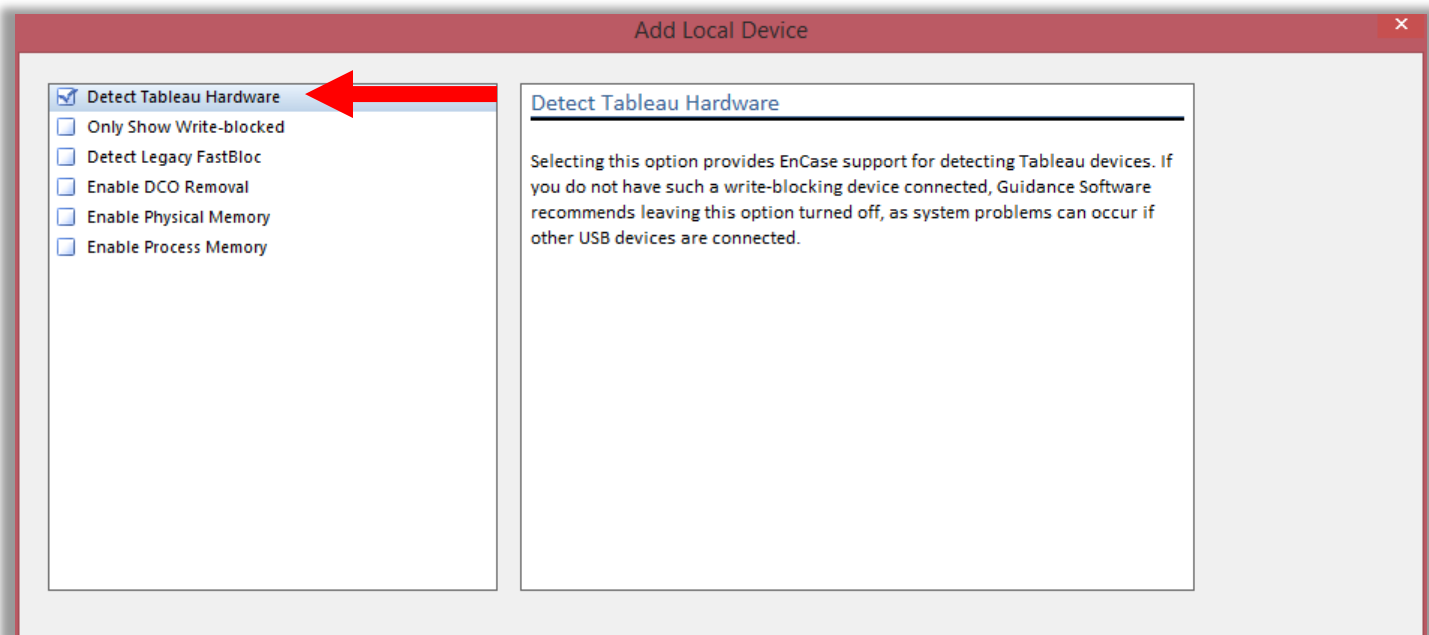
... we will explore the other options later, God willing.



# Add local device

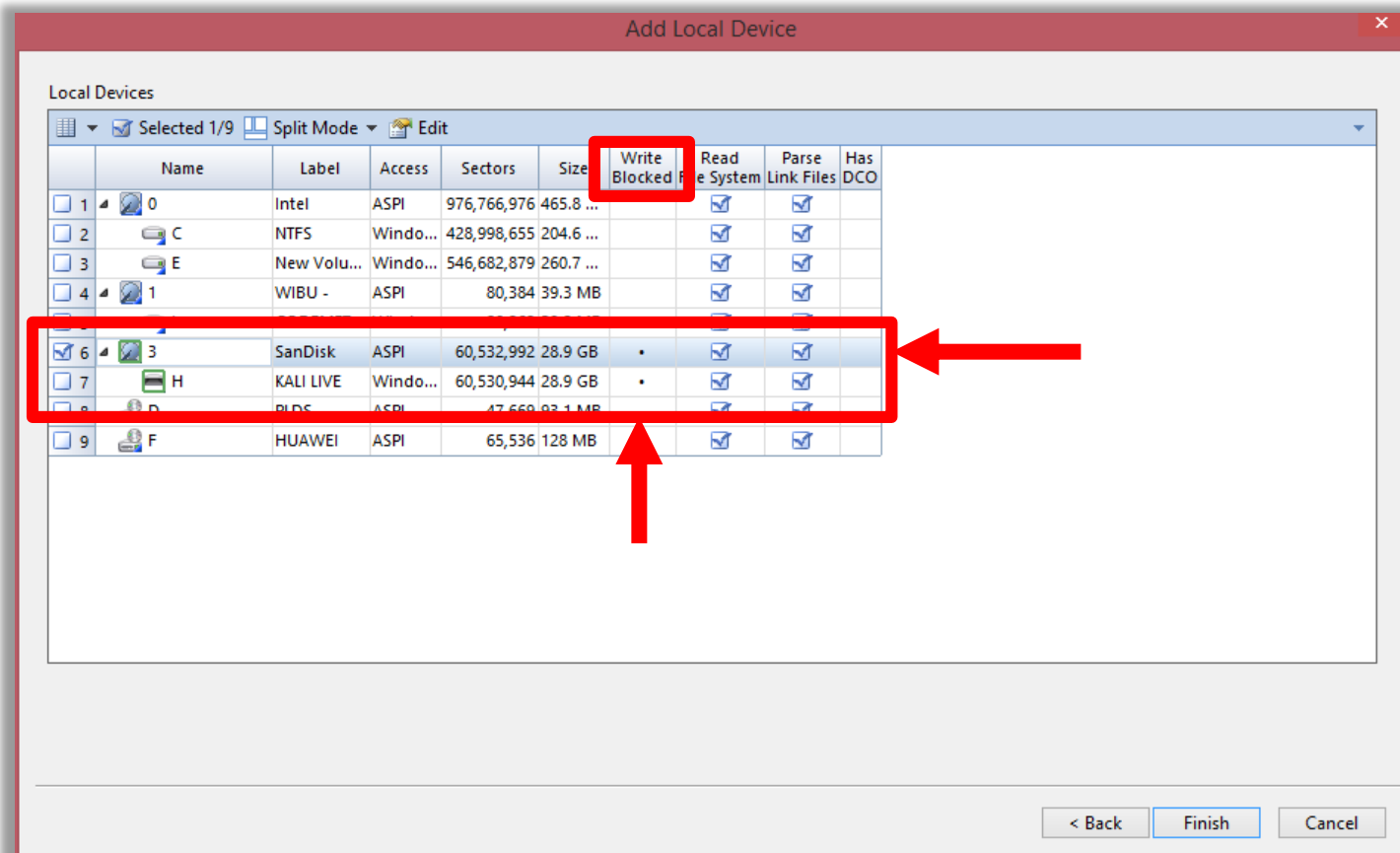
**UNSELECT** “Detect Tableau HW” if you have none attached! “it might/will cause problems”

Next ...



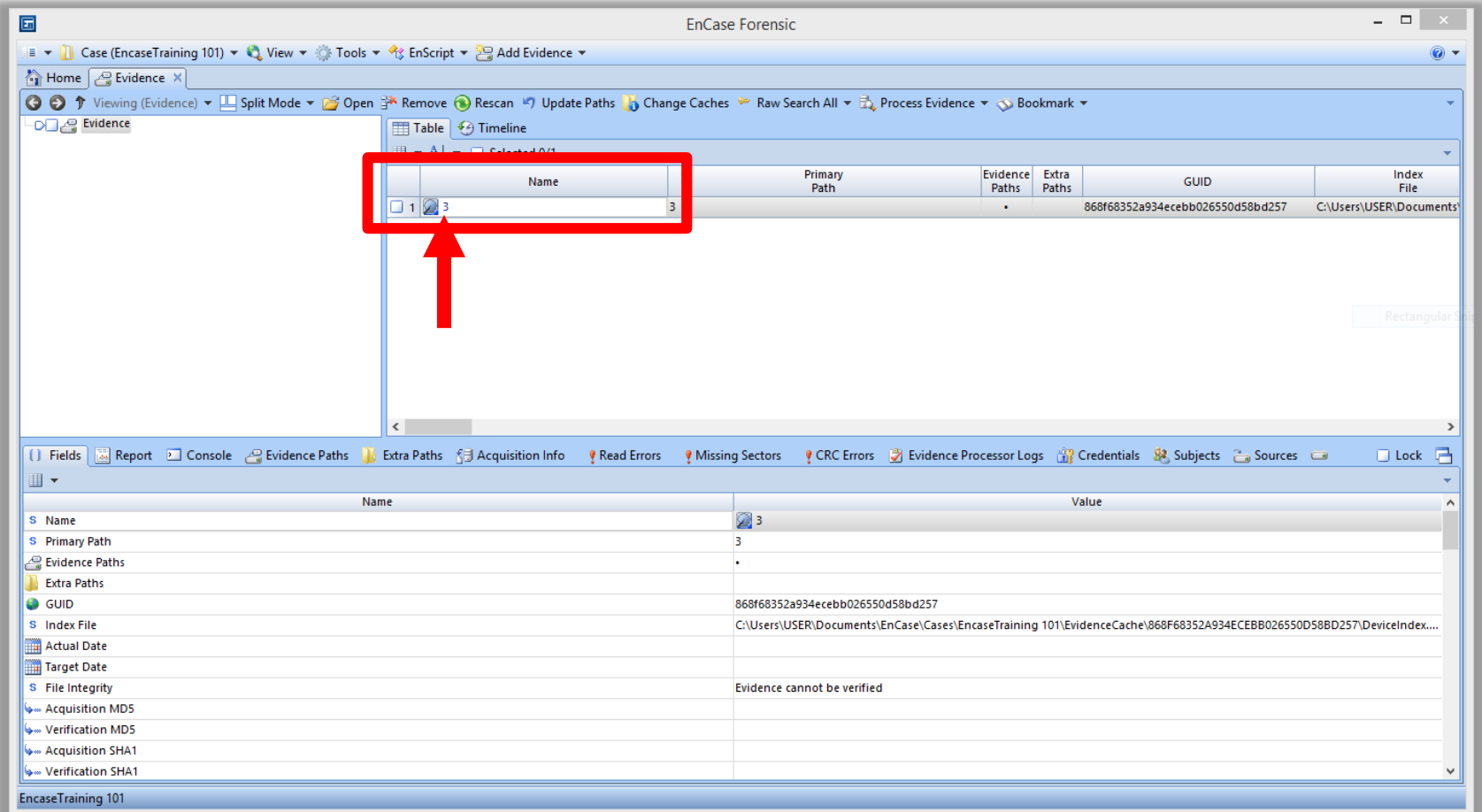
# Add local device

Detected, write-blocked and good to go



# Selecting the evidence

Click on the evidence name ...





# Browsing the evidence

The screenshot displays the EnCase Forensic application window. The top menu bar includes 'Case (EncaseTraining 101)', 'View', 'Tools', 'EnScript', and 'Add Evidence'. The left pane shows a tree view of the evidence structure, with folders like '.disk', 'boot', 'dists', 'firmware', 'install', 'isolinux', 'live', 'pool', 'System Volume Information', and 'tools'. The main pane shows a table of files and folders. The bottom pane shows a detailed view of the selected file, '.disk'.

	Name	Re	Re	Re	Re	File Ext	Logical Size	Category	Signature Analysis	File Type	Protected
1	.disk					disk	0	Folder			
2	boot						0	Folder			
3	dists						0	Folder			
4	firmware						0	Folder			
5	install						0	Folder			
6	isolinux						0	Folder			
7	live						0	Folder			
8	pool						0	Folder			
9	System Volume Information						0	Folder			
10	tools						0	Folder			
11	KALI LIVE						0	Unknown			
12	ldlinux.sys					sys	69,572	Executable			

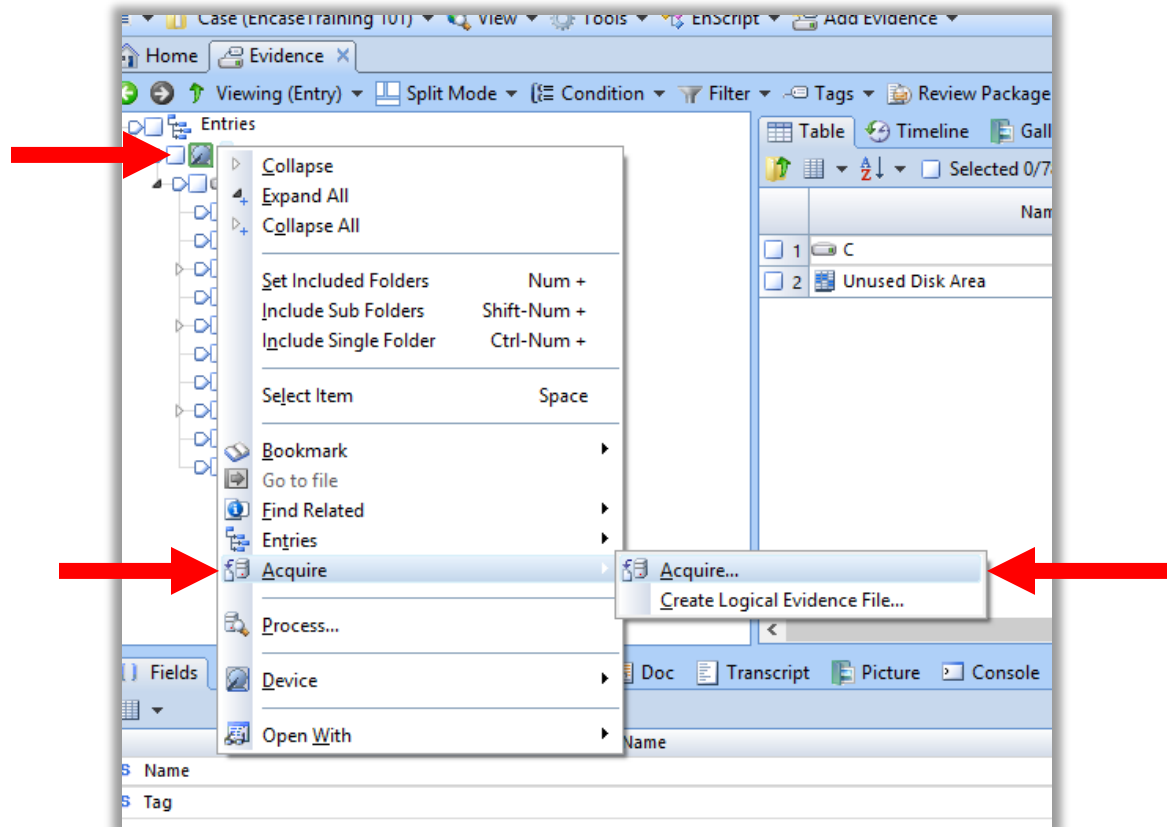
  

Name	Value
S Name	.disk
S Tag	
S File Ext	disk
i Logical Size	0
i Category	Folder
i Signature Analysis	
S File Type	
S Protected	
i Protection complexity	
Last Accessed	01/22/15
File Created	01/22/15 12:44:01 PM

EncaseTraining 101\3\C\disk

# Acquiring evidence

Right click on evidence name -> Acquire -> Acquire...



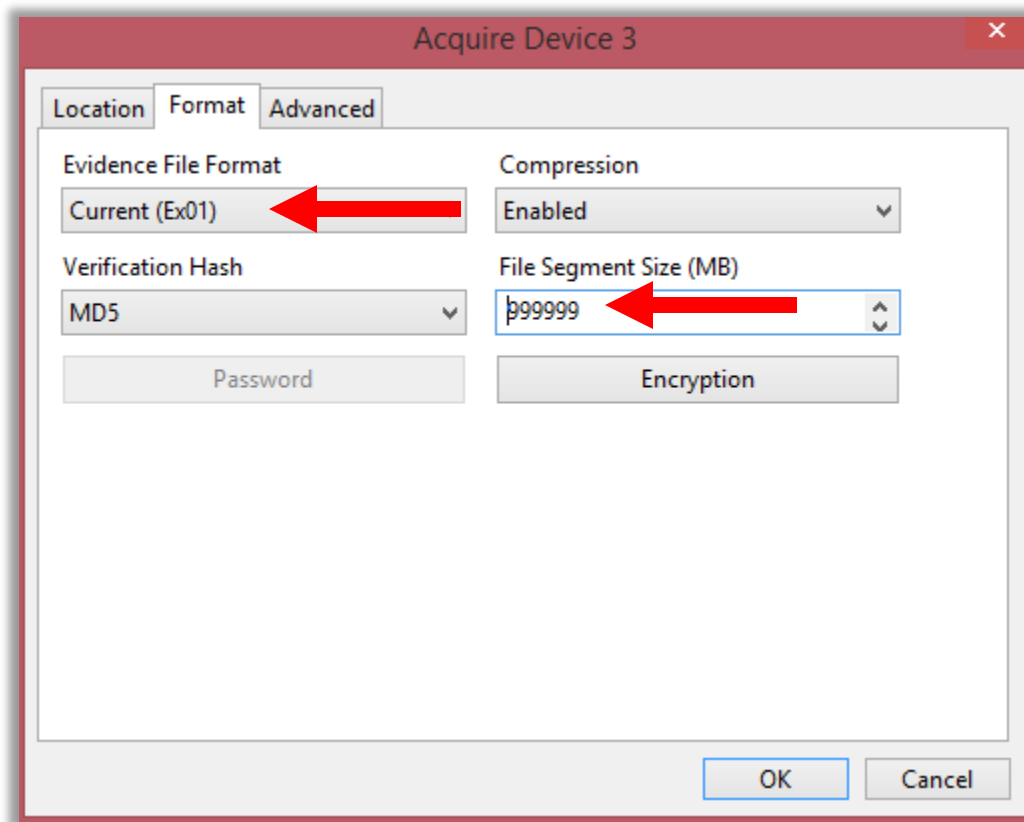
# Location & Name

The screenshot shows the 'Acquire Device 3' dialog box with the 'Location' tab selected. The 'Name' field contains 'USB Flash Drive - sandins' and the 'Evidence Number' field contains '2015-123-001'. The 'Case Number' field contains '2015-123' and the 'Examiner Name' field contains 'Shareef'. The 'Notes' field contains 'Found in suspect's Car'. The 'Restart Acquisition' and 'Remote acquisition' checkboxes are unchecked. The 'Output Path' field contains 'E:\USB Flash Drive - sandins.Ex01' and the 'Alternate Path' field is empty. Red arrows point to the 'Name' and 'Output Path' fields.

Acquire Device 3	
Location   Format   Advanced	
Name	Evidence Number
USB Flash Drive - sandins	2015-123-001
Case Number	Examiner Name
2015-123	Shareef
Notes	
Found in suspect's Car	
<input type="checkbox"/> Restart Acquisition <input type="checkbox"/> Remote acquisition	
Output Path	
E:\USB Flash Drive - sandins.Ex01	
Alternate Path	
OK Cancel	

# Format

`Current` format is NOT compatible with v6!!

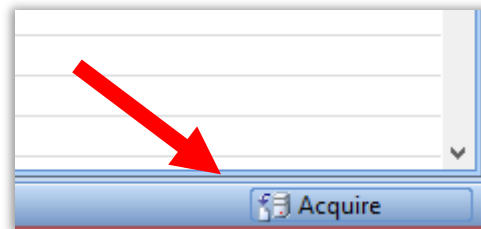


# Acquisition will start

---

Press `OK`

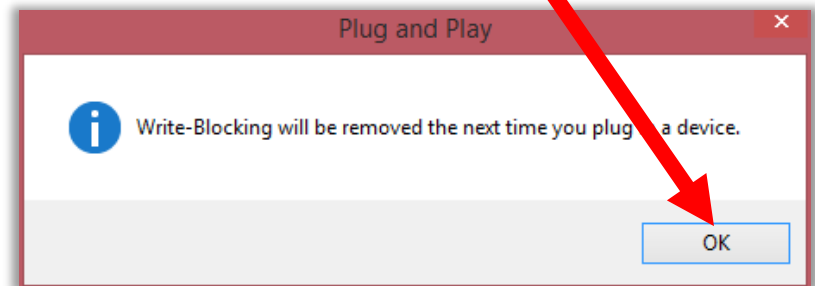
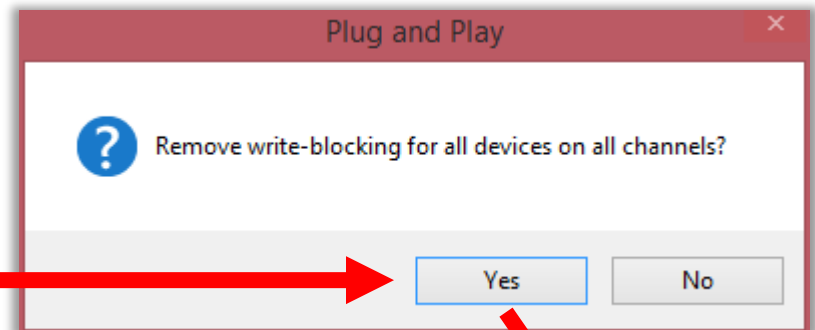
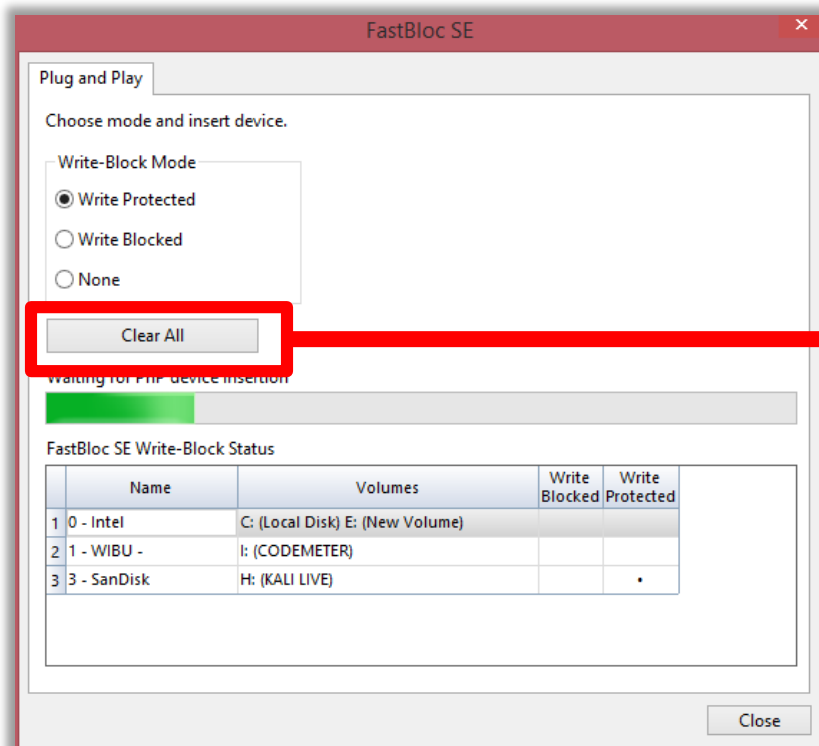
Wait for it to finish ... then you'll have the evidence file in `.ex01` format



Next section we will learn how to add an existing evidence file to a case.

# Stopping FastBloc SE

The USB device(s) will remain write-blocked till FastBloc SE is stopped “Clear All”

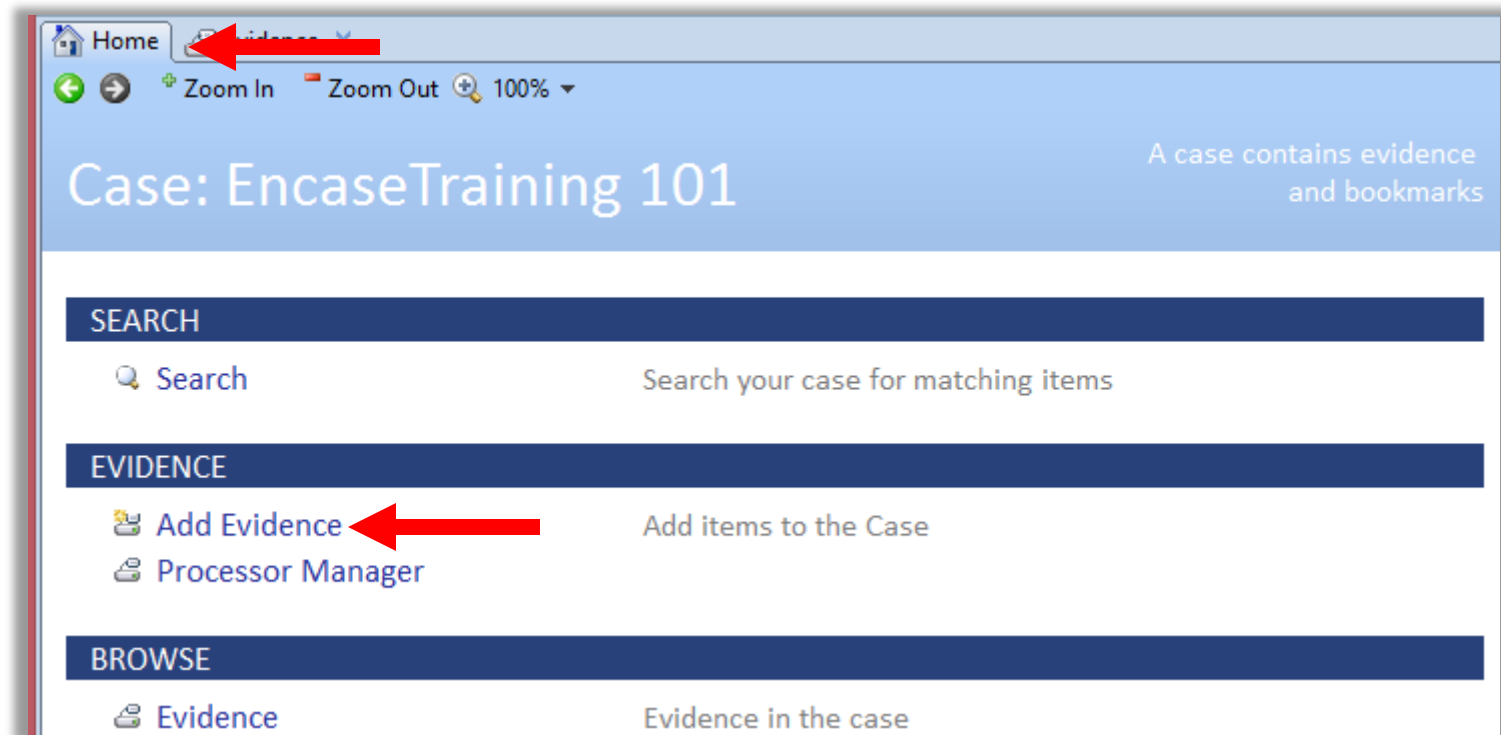


# Adding Evidence Files

---

# Adding `Evidence Files`

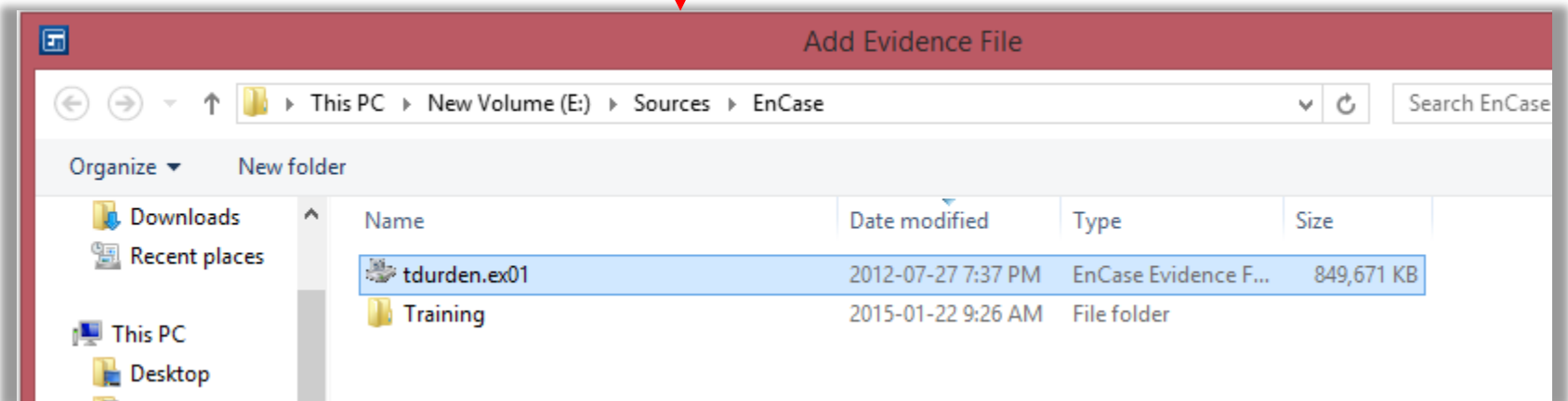
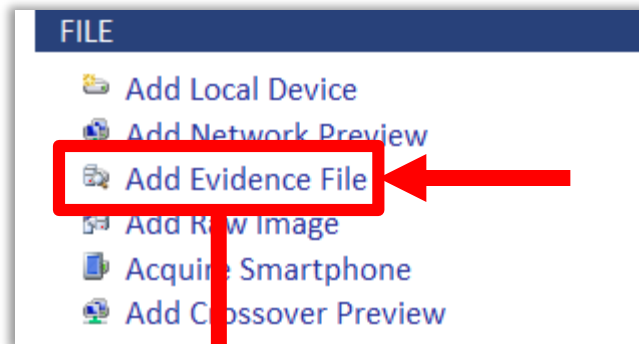
Go to `Home` tab -> Add Evidence





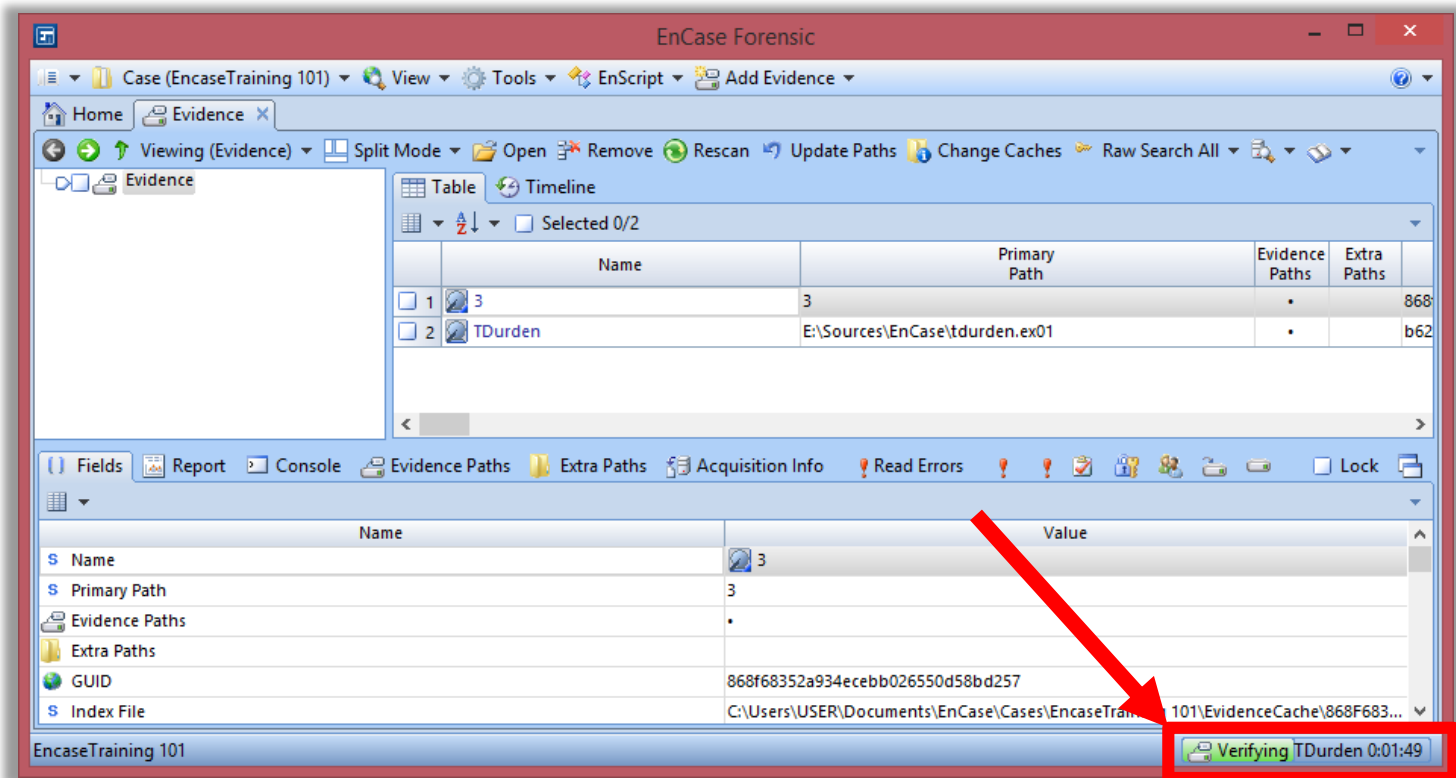
# Adding `Evidence Files`

`Add Evidence File` -> select file



# Adding `Evidence Files`

You can cancel the `Verification` process if you want by double clicking here



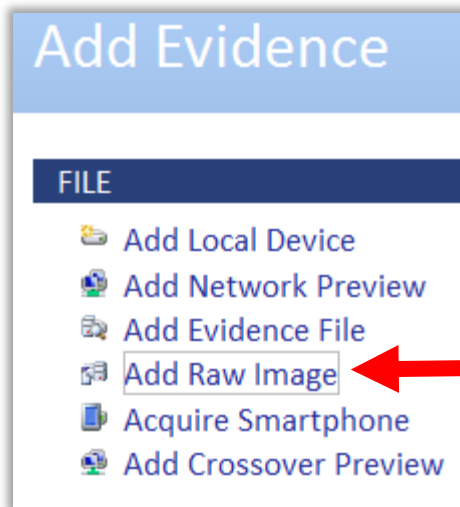
# Adding Raw image files `DD`

---

# Adding `Raw DD Files`

---

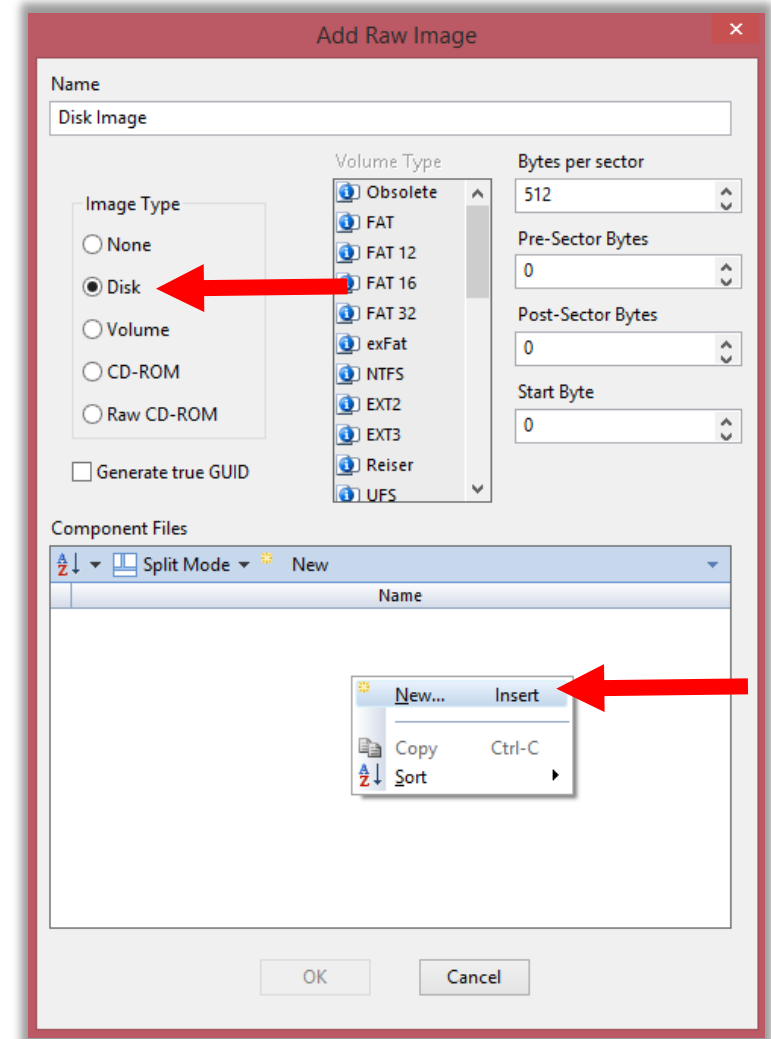
Home -> Add Evidence -> `Add Raw Image`



# Adding `Raw DD Files`

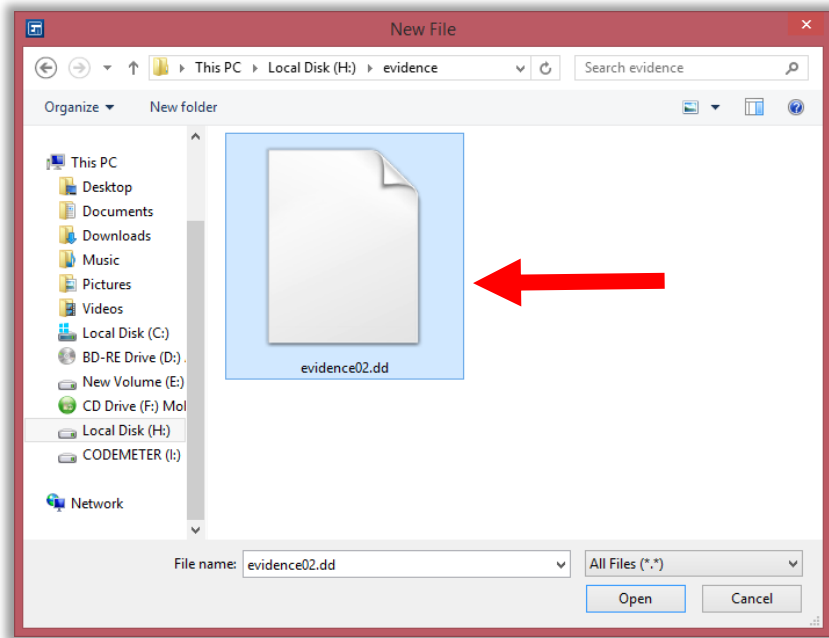
Image type -> Disk

Right-Click -> New...



# Adding `Raw DD Files`

Pick the file -> Open -> OK



A screenshot of the Encase V7 Timeline window. The 'Table' tab is active, showing a list of items. A red arrow points from the 'evidence02.dd' file in the File Explorer to the 'Disk Image' entry in the timeline table.

	Name	Primary Path
<input type="checkbox"/> 1	3	3
<input type="checkbox"/> 2	TDurden	E:\Sources\EnCase\tdurden.ex01
<input type="checkbox"/> 3	Disk Image	H:\evidence\evidence02.dd

# Acquiring Mobile Phones

---

PRE-REQUISITES AND IMPORTANT  
CONSIDERATIONS

# Mobile Phone Support

---

EnCase v7 supports acquiring data from smartphones and tablets directly.

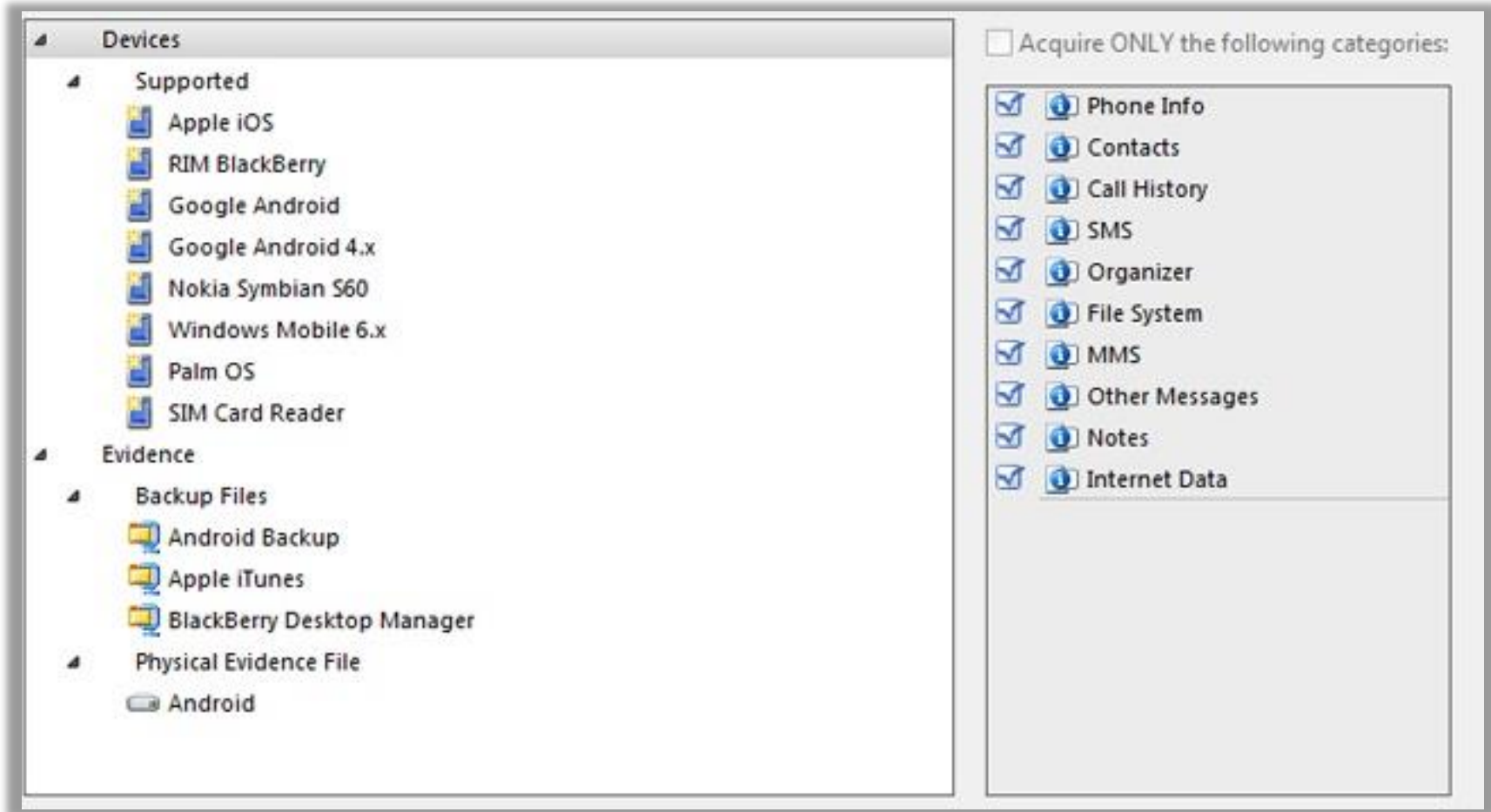
Evidences could be acquired from the device itself, or a backup file located on the suspect Computer.

Allows exporting geo-tags and other location data which can then be loaded into google maps!

Creating a report is very easy!



# Supported devices & Data



# Physical v.s. Logical Acquisition

---

For some devices (like Android) it is possible to perform `Physical Acquisition`, that enables recovery of more data, including deleted files which will not possible otherwise.

Logical acquisition is like “copying” the data from the device, yet deleted data will not be available for parsing.

Physical acquisition requires that the device is rooted (Google that if you are unfamiliar with the term).

# IMPORTANT!!!

---



Few things needs to be considered before acquiring evidence from mobile devices:

- Examination environment considerations
- Computer-side preparation and necessary drivers installation.
- Preparing target mobile device for acquisition

# Use a faraday Bag/Cage!!!

All smart phones have a `Remote Wipe` capability, if the suspect “or someone related to him” managed to initiate/schedule a remote wipe, we lose big time.

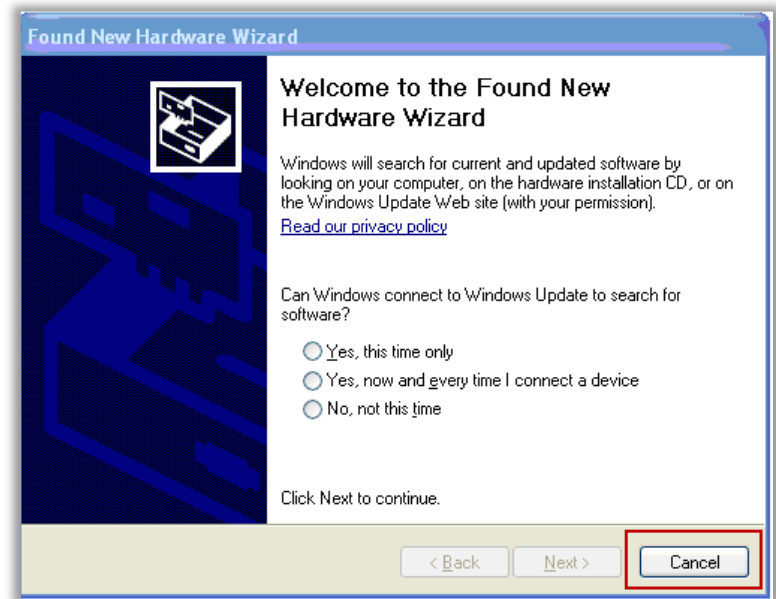


# Install drivers

For EnCase to be able to acquire evidence from mobile devices, appropriate drivers need to be installed the computer needs to recognize them correctly first.

This means installing

iTunes for apple devices,  
and appropriate drivers  
for others.

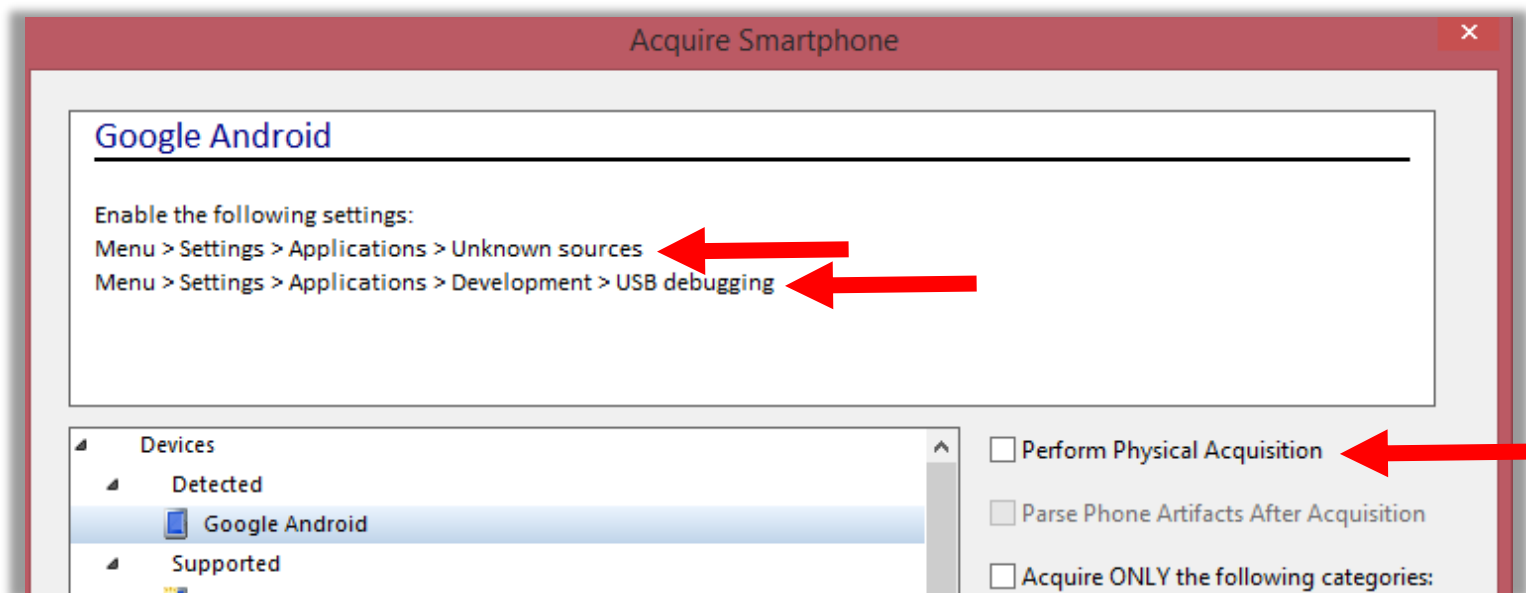


# Android: Prerequisites

---

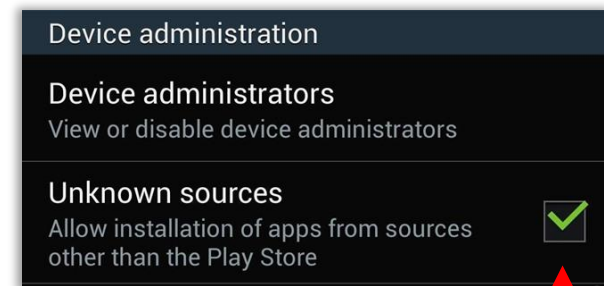
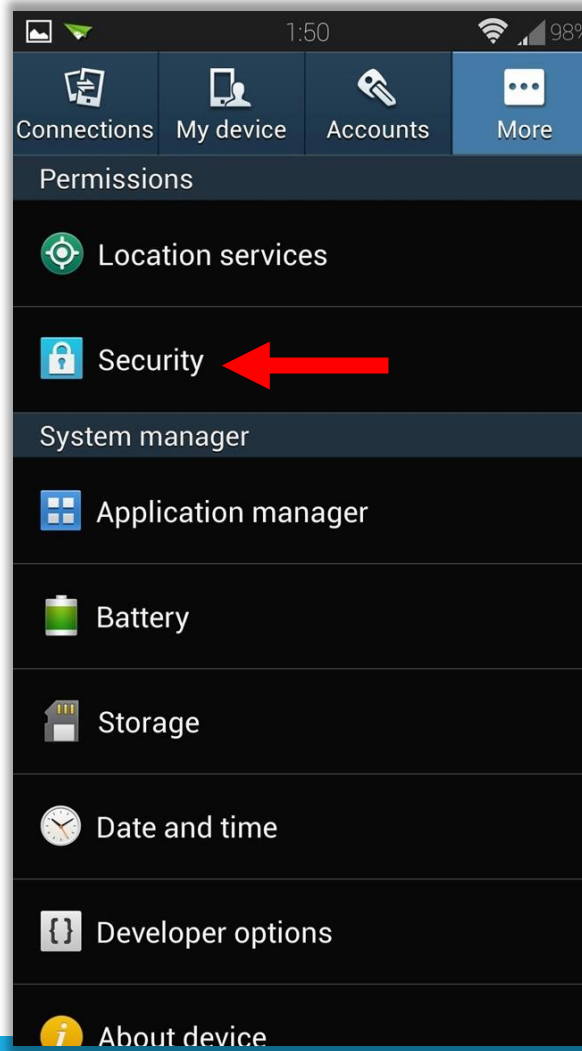
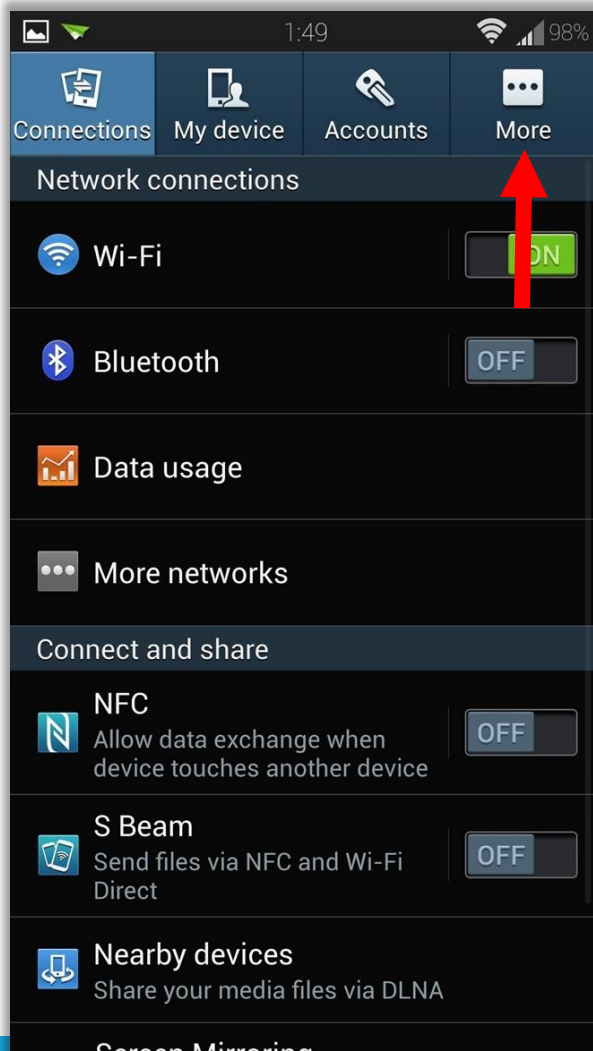
# Requirements

As per Encase, we need to do the following **ON THE PHONE** before acquiring evidence (don't forget to document your actions):



+ For Physical acquisition, we need root.

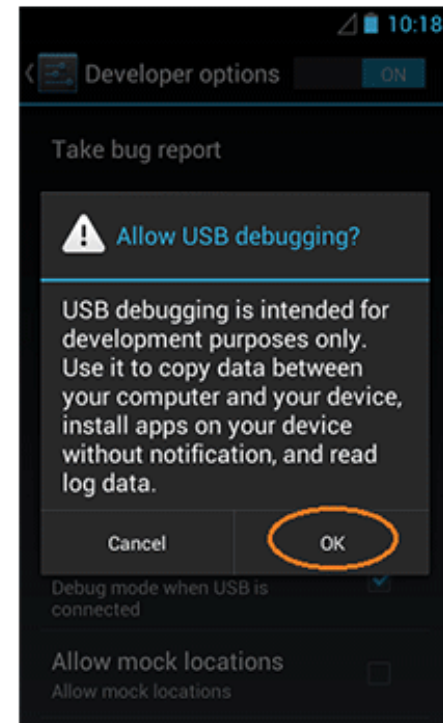
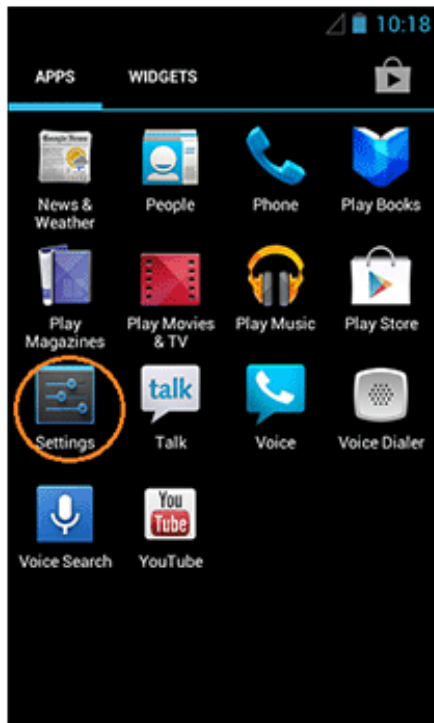
# Enable unknown sources



- Settings might change slightly
- Google is your best friend, just find how to enable this setting and do it!



# Enable USB Debugging

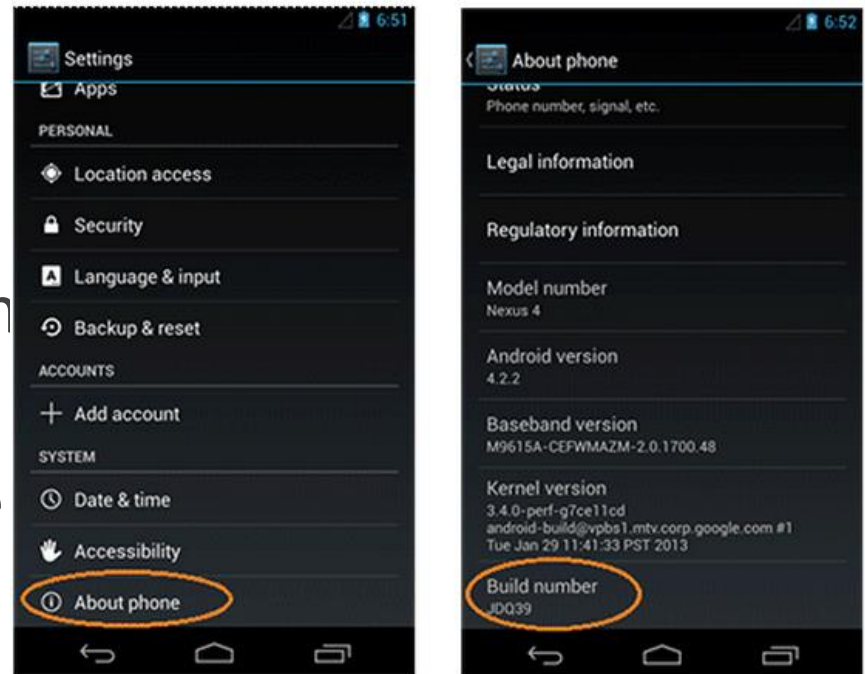


# Enable USB Debugging(!)

In Recent Android versions ( $\geq 4.2$ ), the Developer Options menu and USB Debugging option have been hidden, and needs to be enabled first.

- `About Phone`
- Click `Build number`  
10 times

Now Developer options are available, then continue as prev. slide



# Rooting the phone

---

As mentioned earlier, physical acquisition (and recovery of deleted data) requires the device to be `Rooted`.

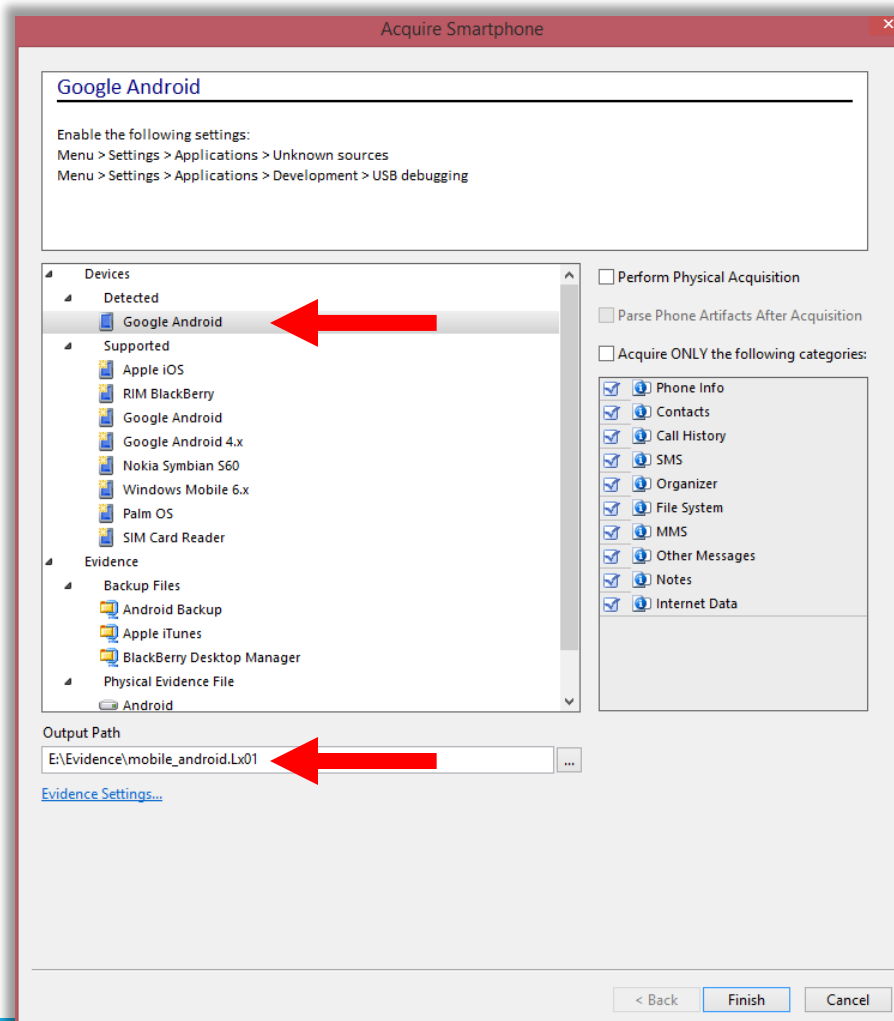
If it is already rooted, you're in good shape, if it is not, please note that there is a very high probability that the device gets fully erased, or irrecoverably damaged!

Short answer, don't ever root a device in course of examination!!! `unless authorized, and after "authority" understands the risk`

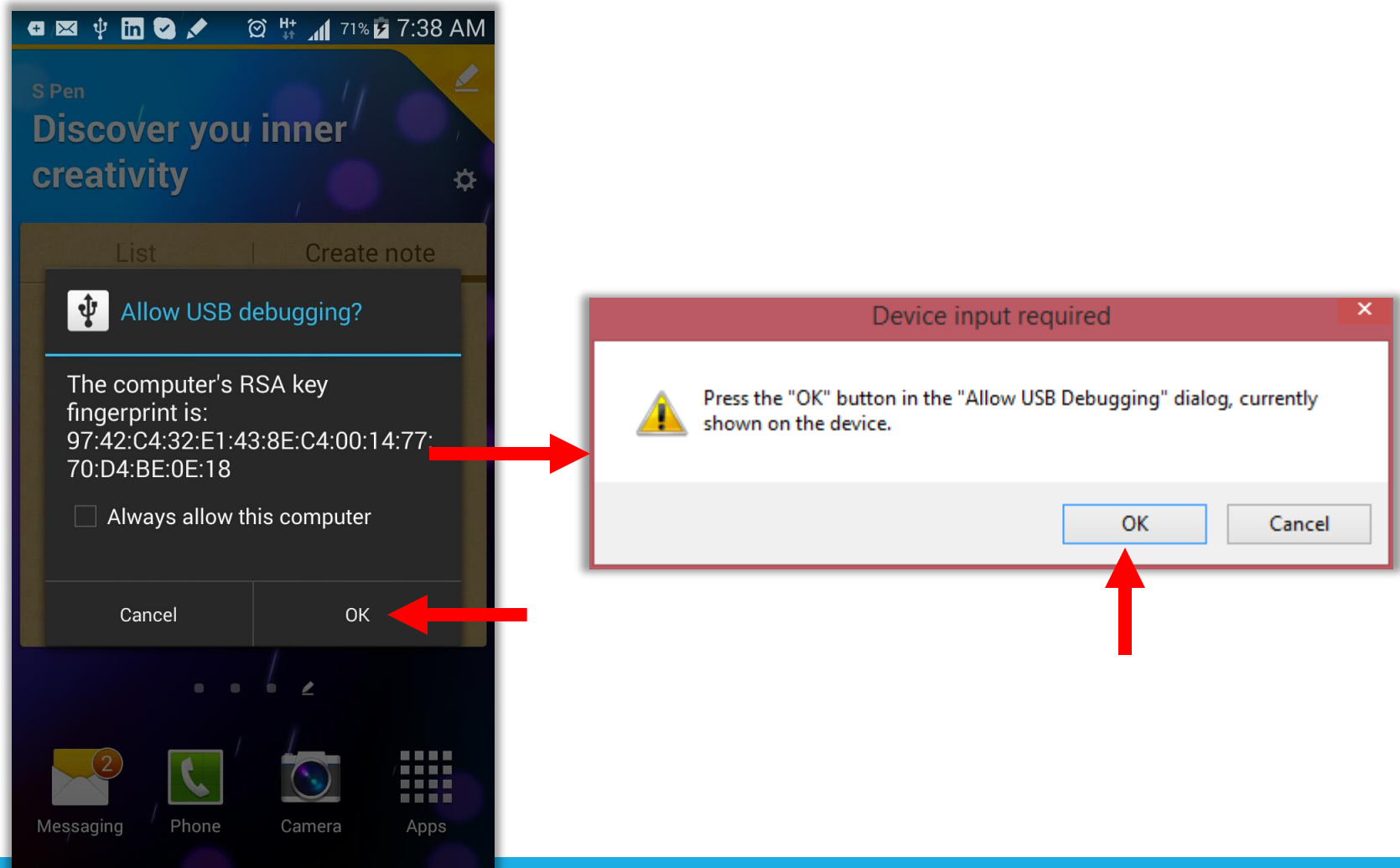
# Android: Acquisition Demo

---

# Once all is set ...

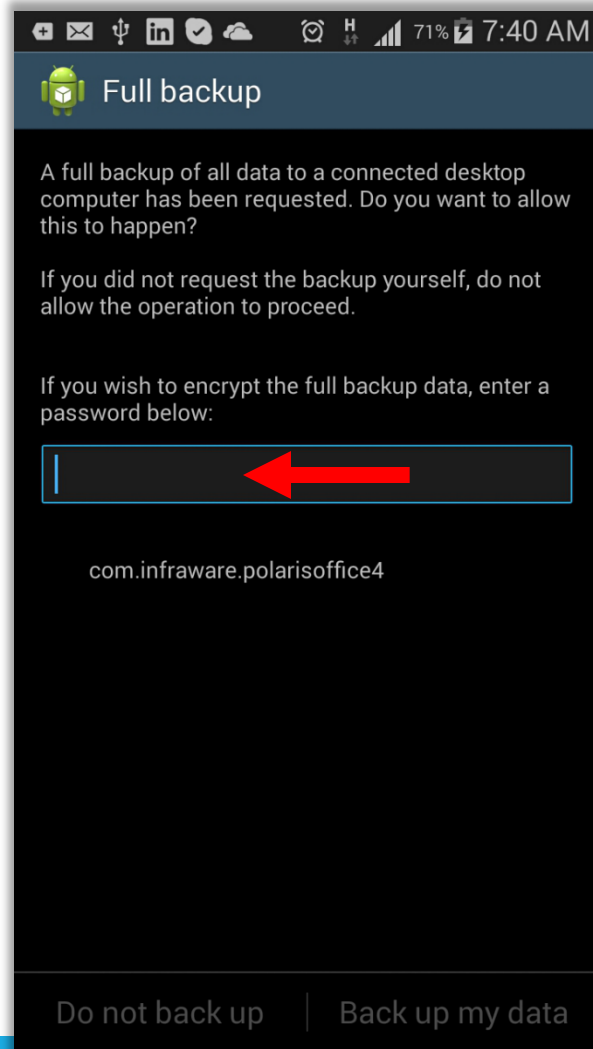


# Press OK on phone first ...



# Set Password if you wish

---



# Wait ... and keep waiting

---

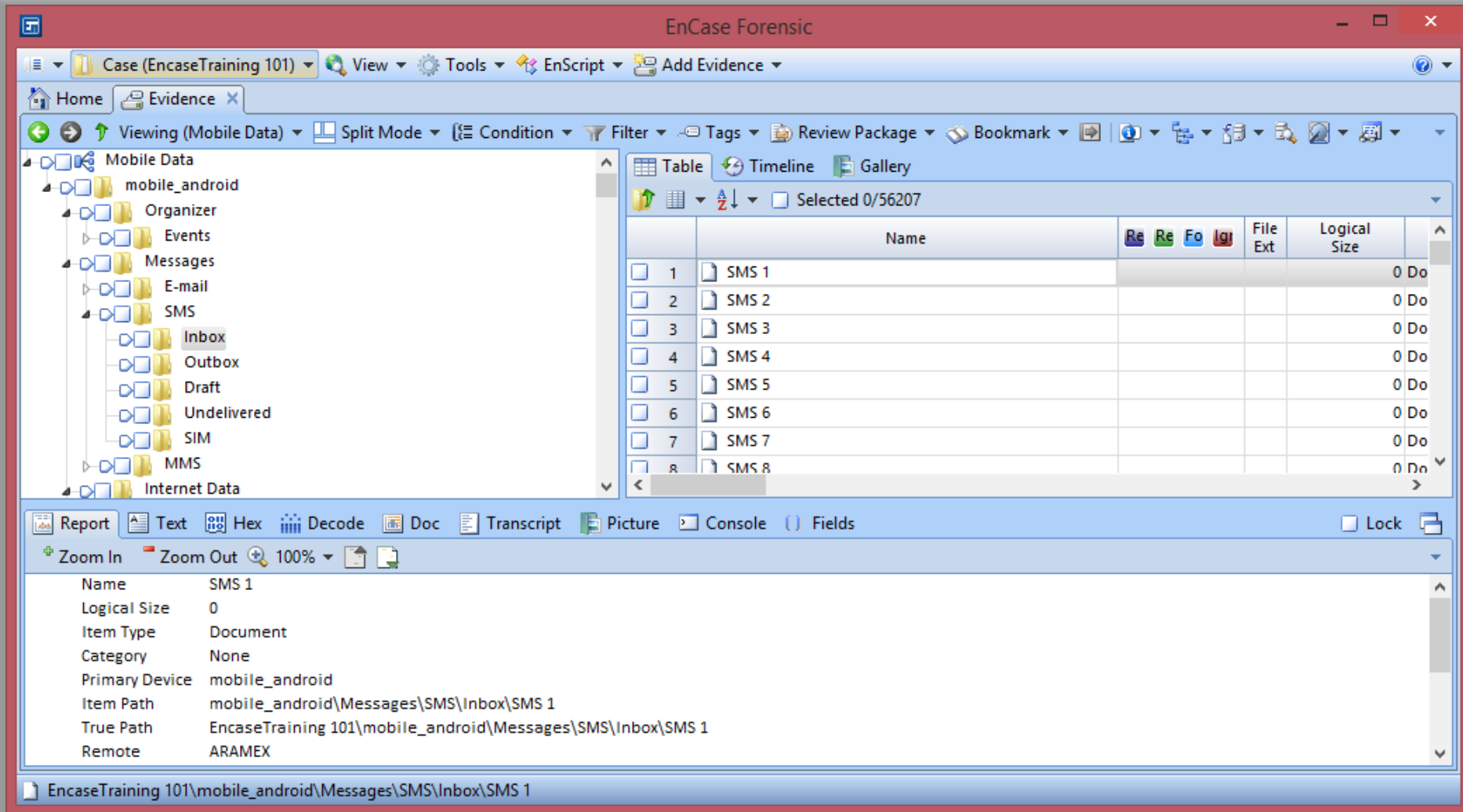
It took us around 1½ hours to acquire a 16GB Note2, problem is the progress bar is not moving, and there's no indication on the mobile!

Have faith `it works` & have patience `it will take time`.





# Acquisition done!



The screenshot displays the EnCase Forensic software interface. The main window is titled "EnCase Forensic" and shows a case named "Case (EncaseTraining 101)". The left pane shows a tree view of the mobile data structure, including "Mobile Data", "mobile\_android", "Organizer", "Events", "Messages", "E-mail", "SMS", "Inbox", "Outbox", "Draft", "Undelivered", "SIM", "MMS", and "Internet Data". The right pane shows a table of SMS messages. The bottom pane shows the details of the selected SMS message.

	Name	Re	Re	Fo	lgr	File Ext	Logical Size	
1	SMS 1						0 Do	
2	SMS 2						0 Do	
3	SMS 3						0 Do	
4	SMS 4						0 Do	
5	SMS 5						0 Do	
6	SMS 6						0 Do	
7	SMS 7						0 Do	
8	SMS 8						0 Do	

Report Text Hex Decode Doc Transcript Picture Console Fields

Zoom In Zoom Out 100%

Name SMS 1  
Logical Size 0  
Item Type Document  
Category None  
Primary Device mobile\_android  
Item Path mobile\_android\Messages\SMS\Inbox\SMS 1  
True Path EncaseTraining 101\mobile\_android\Messages\SMS\Inbox\SMS 1  
Remote ARAMEX

EncaseTraining 101\mobile\_android\Messages\SMS\Inbox\SMS 1

# Note!

---

For some reason, photos taken by camera (the ones usually in DCIM) were not included in the evidence file when we acquired it ...

We didn't check why, but you may copy the files from the phone storage directly and take appropriate notes (MD5 hashes ... etc.)

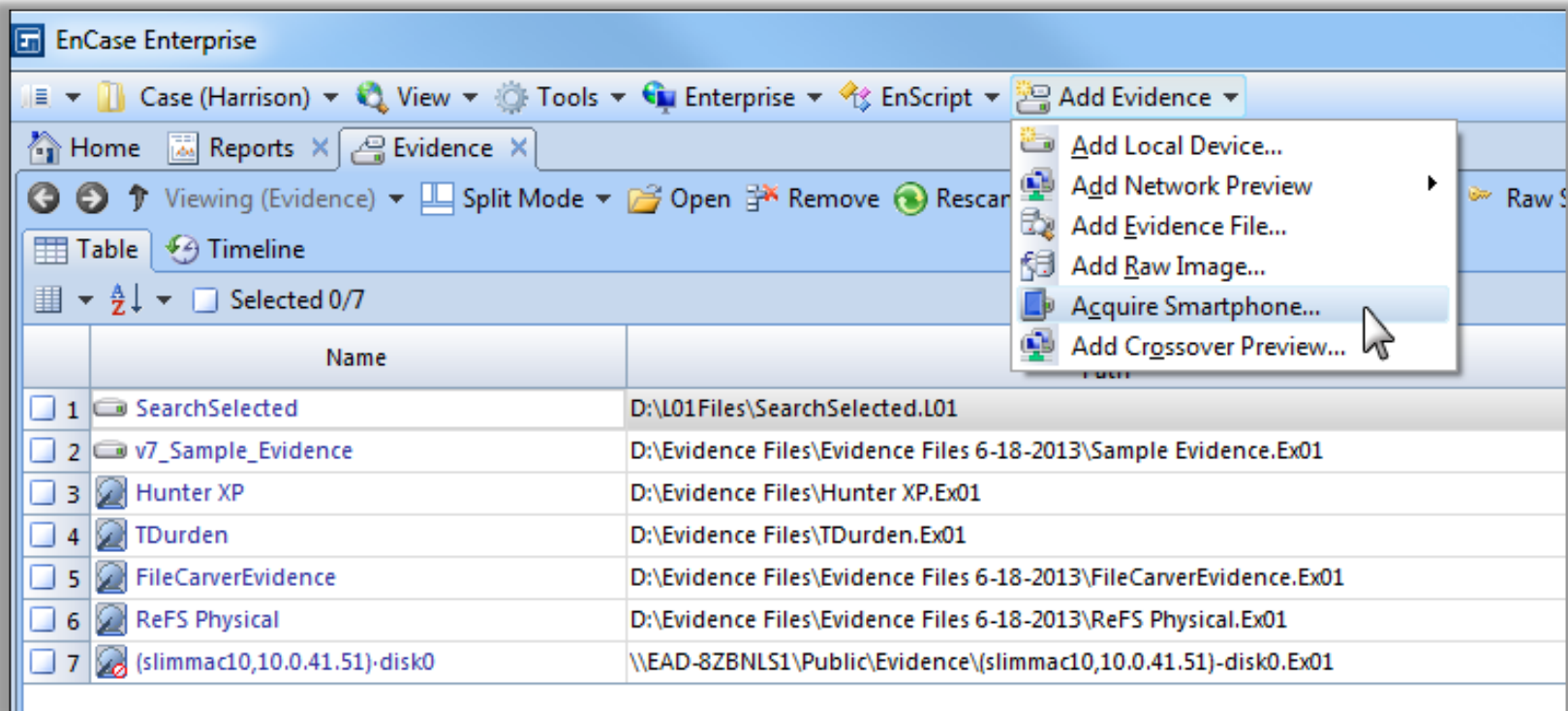
- Or make a logical evidence file which includes the images.

# iTunes Backup Files

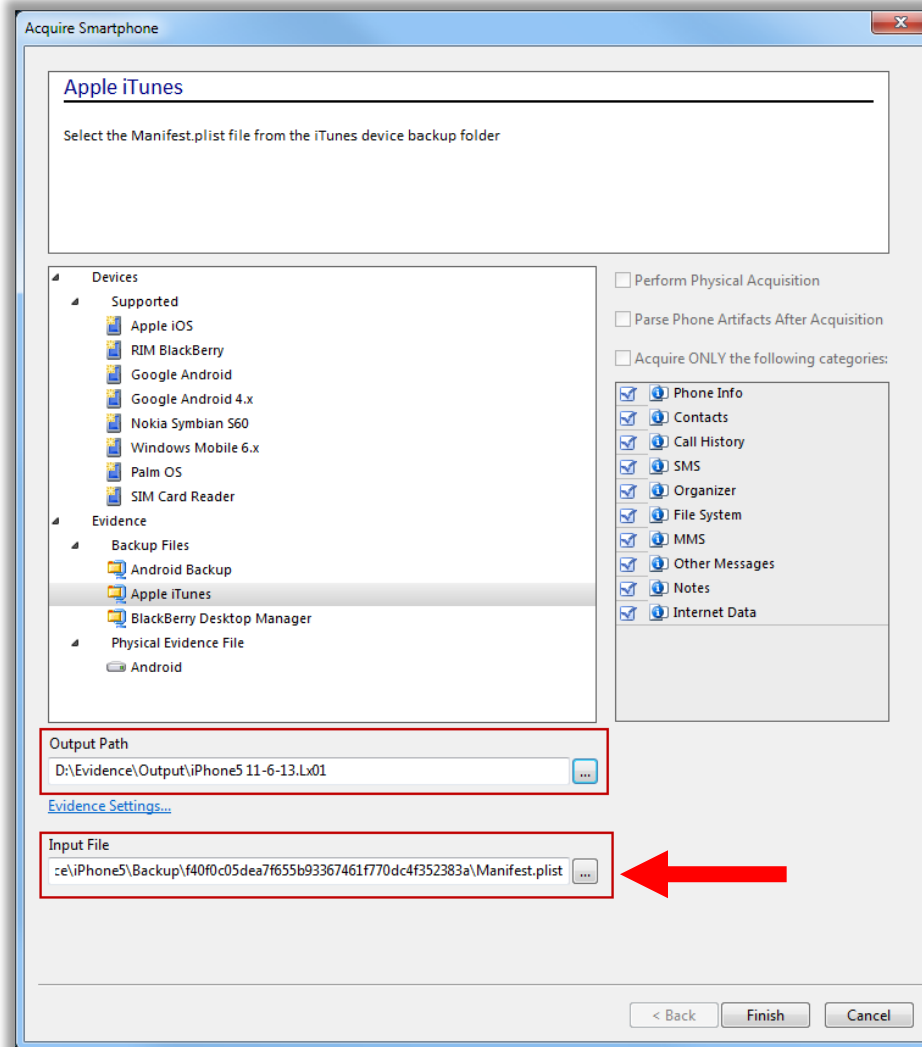
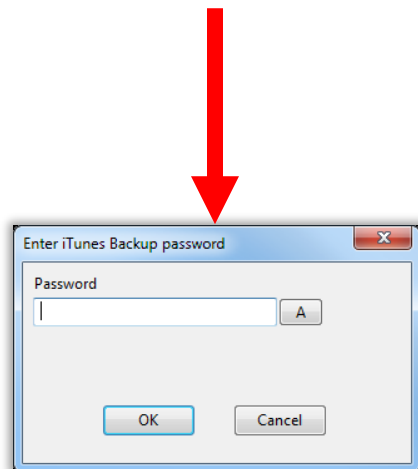
---

# Acquiring iTunes Backup

To acquire an iTunes backup file: Open a case and click Add Evidence > Acquire Smartphone.



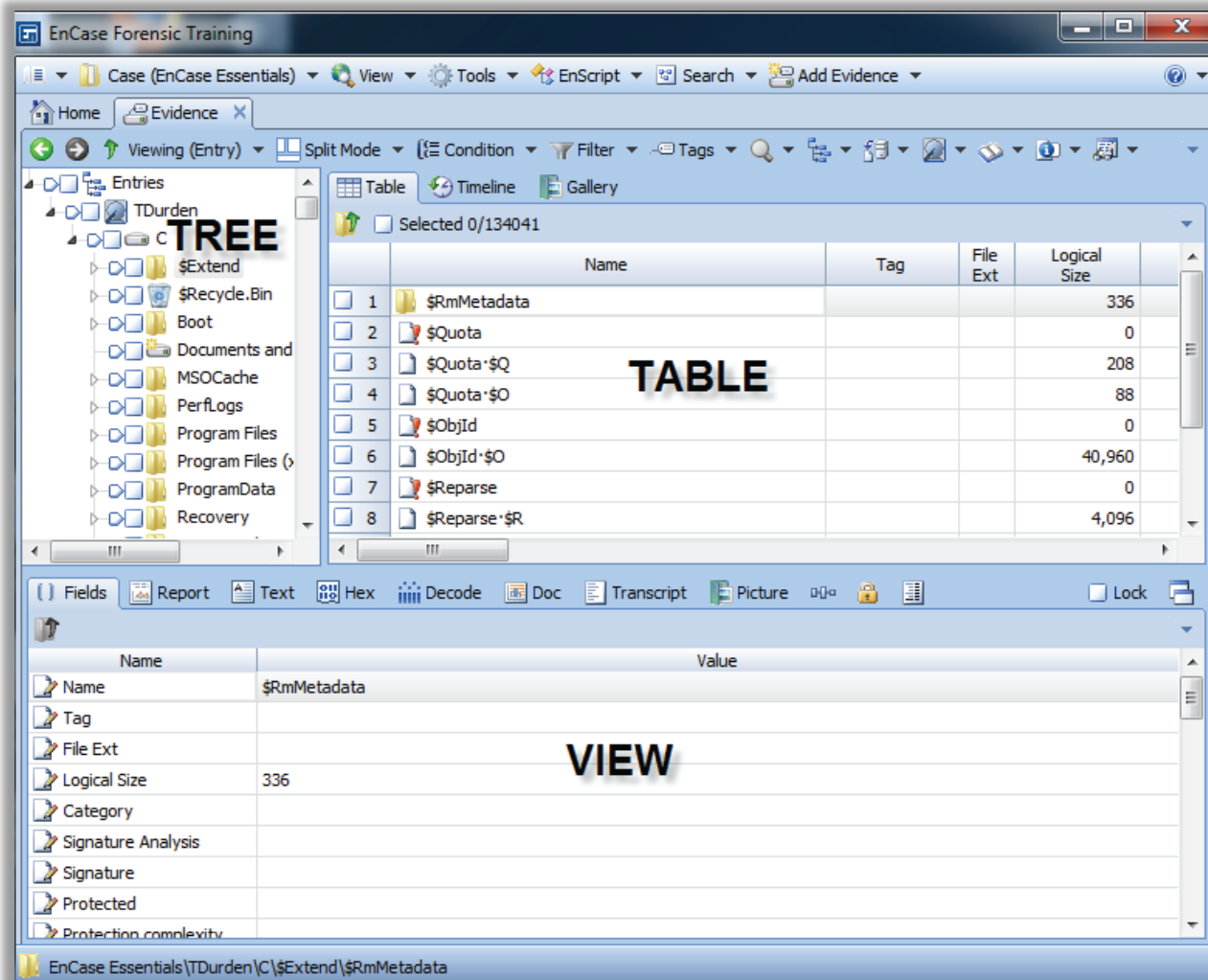
# Point to `Manifest.plist`



# Browsing and Viewing Evidence

---

# Tree, Table, Traeble & View



# Tree, Table, Traeble & View

The screenshot displays the EnCase Enterprise Training interface. The top menu bar includes options like Case, View, Tools, EnScript, Search, and Add Evidence. Below the menu, there are tabs for Home, Evidence, and Records. The main window is divided into two sections: a file tree on the left and a detailed view on the right.

**File Tree (Tree View):** The tree shows a hierarchy starting with 'TDurden' (selected), followed by 'C', and then a list of folders and files. The 'Admin' folder is highlighted.

	Name	Tag	File Ext	Logical Size	Category	Signature Analysis	Signature	Protected
1	TDurden			0				
2	C			4,096				
3	\$Extend			552				
4	\$Recycle.Bin		Bin	4,096	Windows			
5	Boot			4,096				
6	Documents and Settings			48				
7	MSOCache			25				
8	PerfLogs			144				
9	Admin			48				
10	Program Files			8,192				
11	Program Files (x86)			4,096				
12	ProgramData			4,096				
13	Recovery			312				
14	System Volume Information			4,096				
15	Users			4,096				
16	Windows			16,384				
17	\$MFT			110,886,912				

**Detailed View (View):** The bottom section shows a detailed view of the selected 'Admin' file. It includes fields for Name, Tag, File Ext, Logical Size, Category, Signature Analysis, Signature, Protected, and Protection complexity.

Name	Value
Name	Admin
Tag	
File Ext	
Logical Size	48
Category	
Signature Analysis	
Signature	
Protected	
Protection complexity	

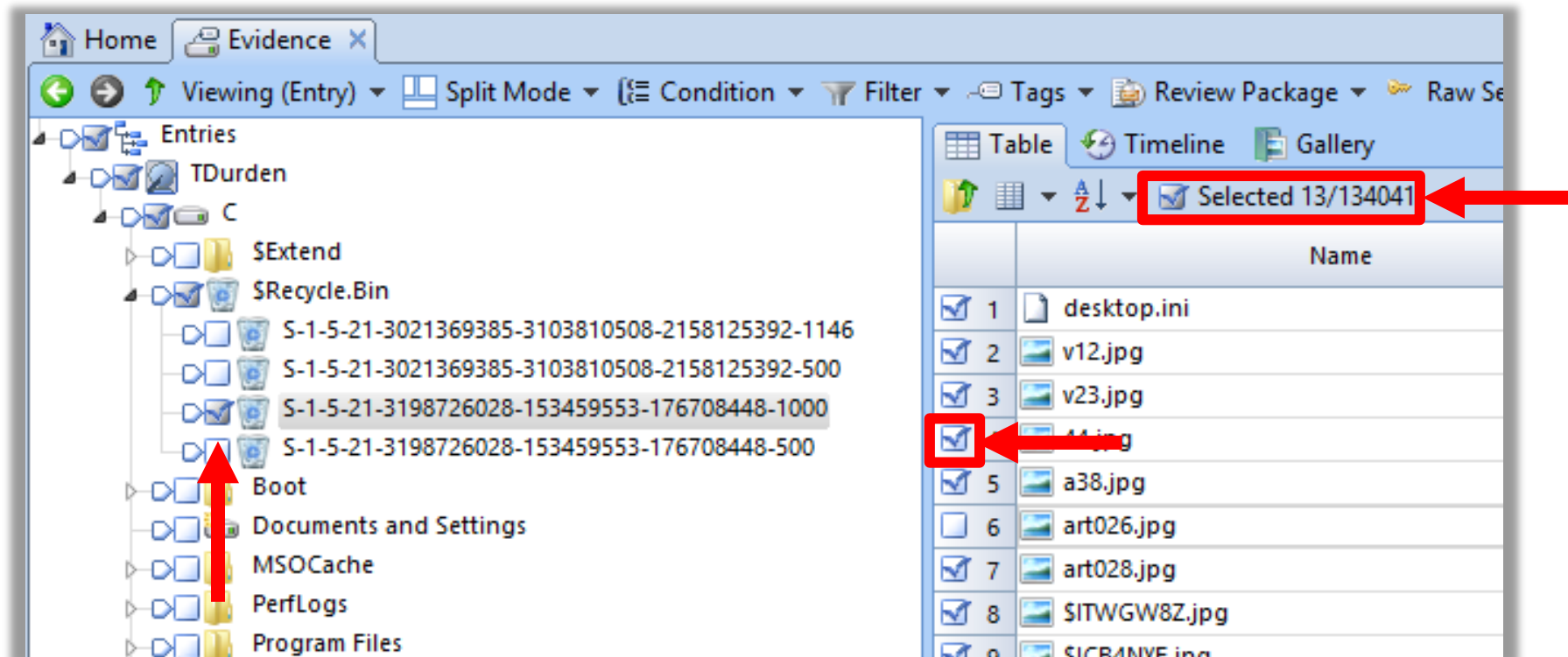
The status bar at the bottom indicates the current path: new new new case again\TDurden\C\PerfLogs\Admin.



# Selection and Displaying

Selection is different than viewing

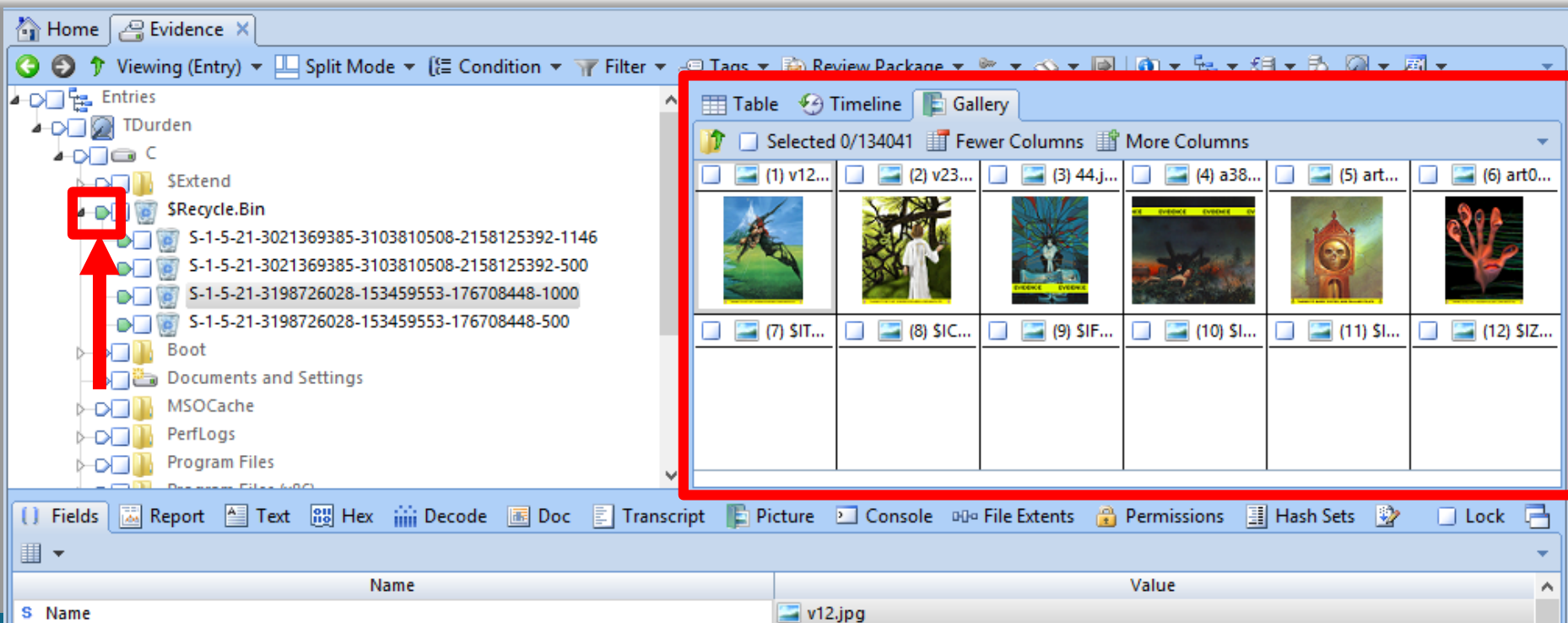
To select, tick the box



# Selection and Displaying

To display only a subset, tick the

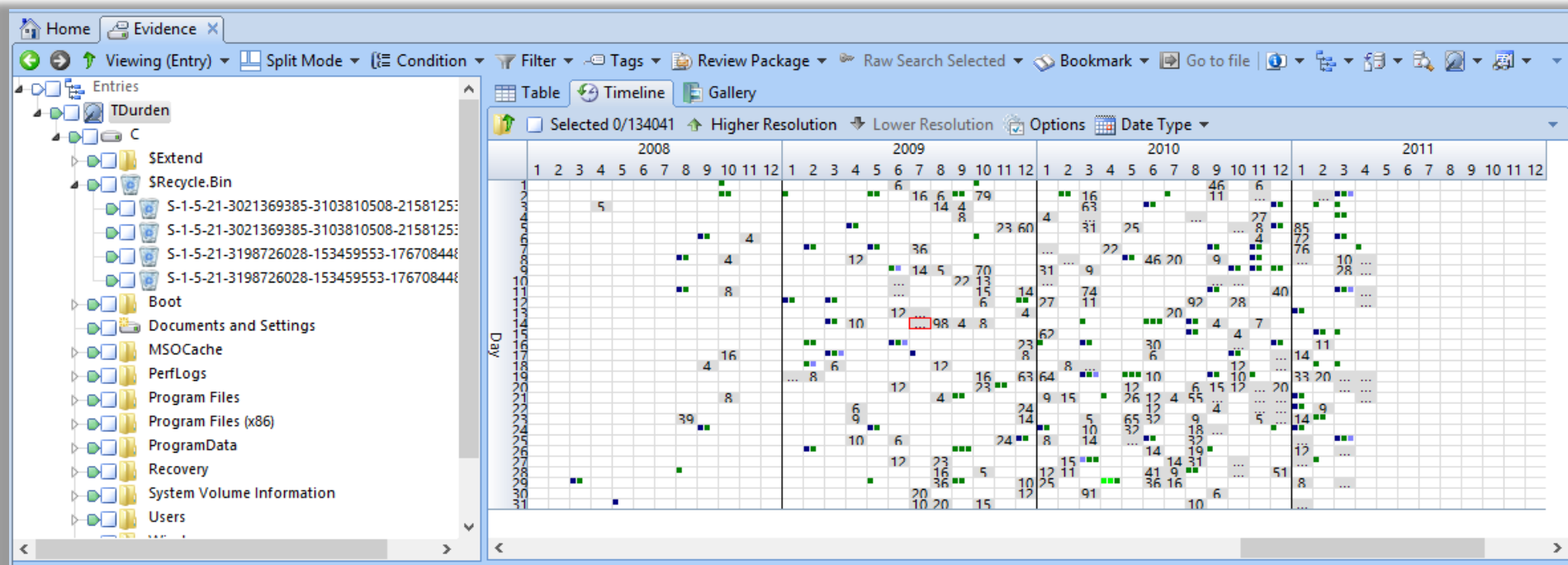
Very useful to focus on specific files or folders



# Timeline

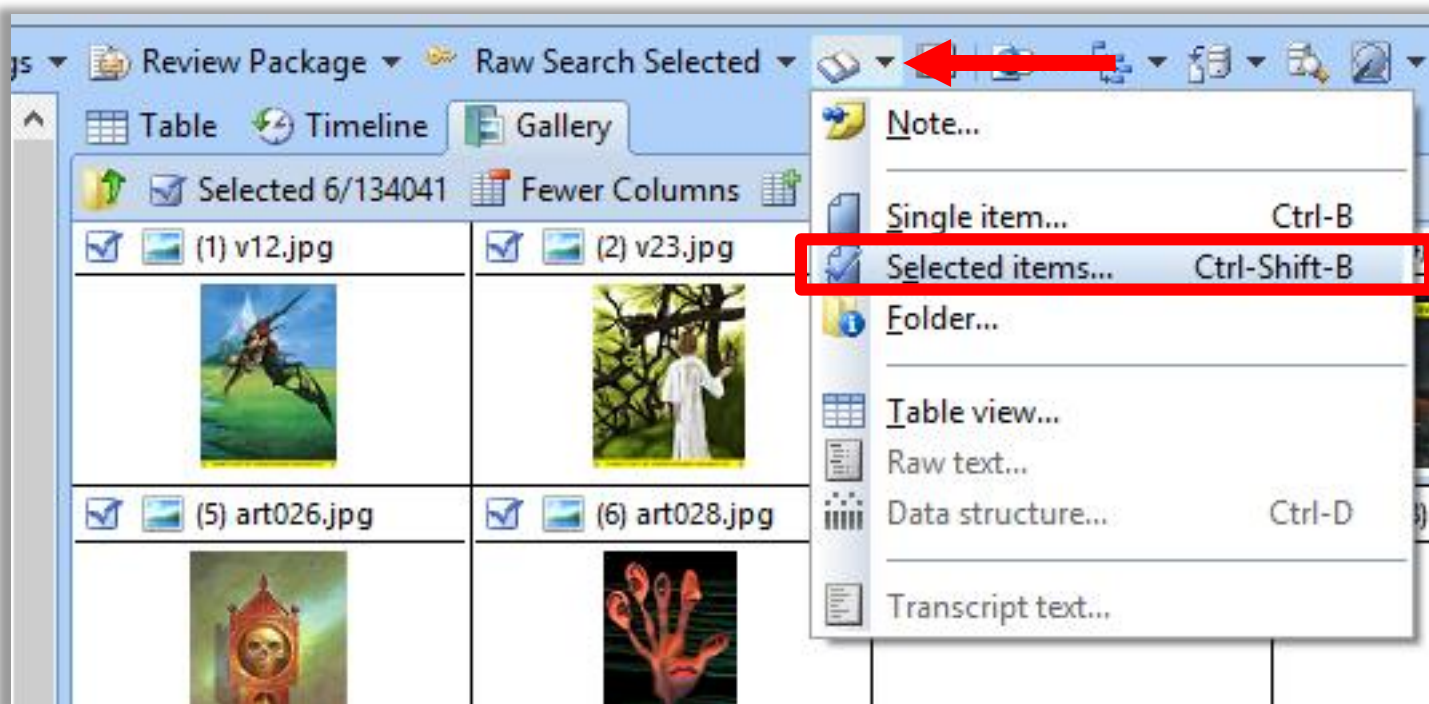
Tick from the left, display on the right

Easier focusing on finding what happened in a specified time range



# Something looks interesting?

Select it, then Bookmark it!



# Other features to consider

---

Consider them on your own! Covering them here can take forever ...

Take a look at Chapter 7 in the user manual.

Filtering & conditions.

Searching.

# Mounting Evidence

---

# Mounting evidence

---

Evidence could be mounted as local, or network mounted drives.

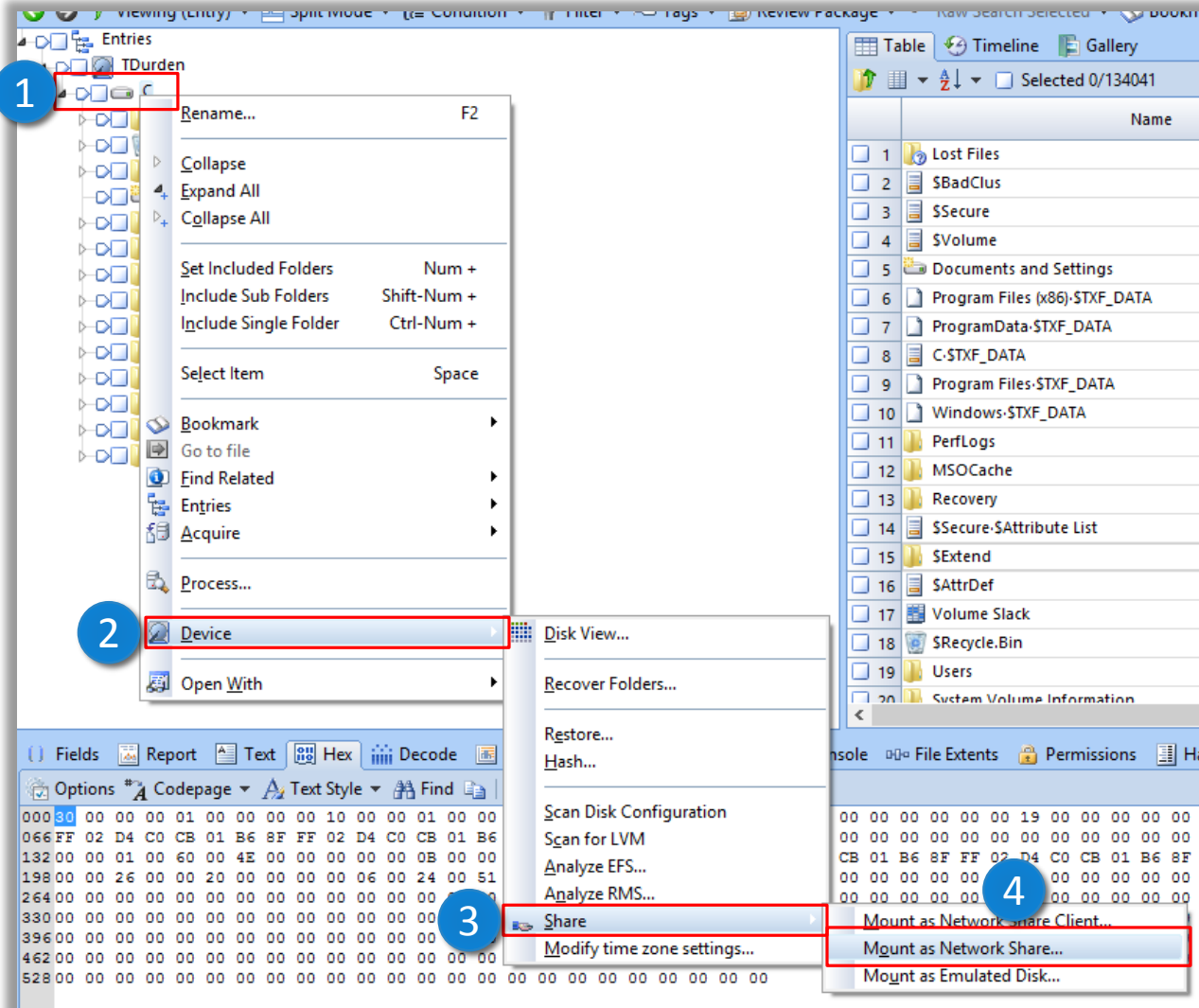
This will enable casually “browsing” the evidence, or perform a virus scan.

Virtual Machines could be created from evidence if mounted as local drive.

This also enables to view all file systems even those not supported by windows “e.g. evidence from Linux or Mac computers”

# Mounting evidence: VFS

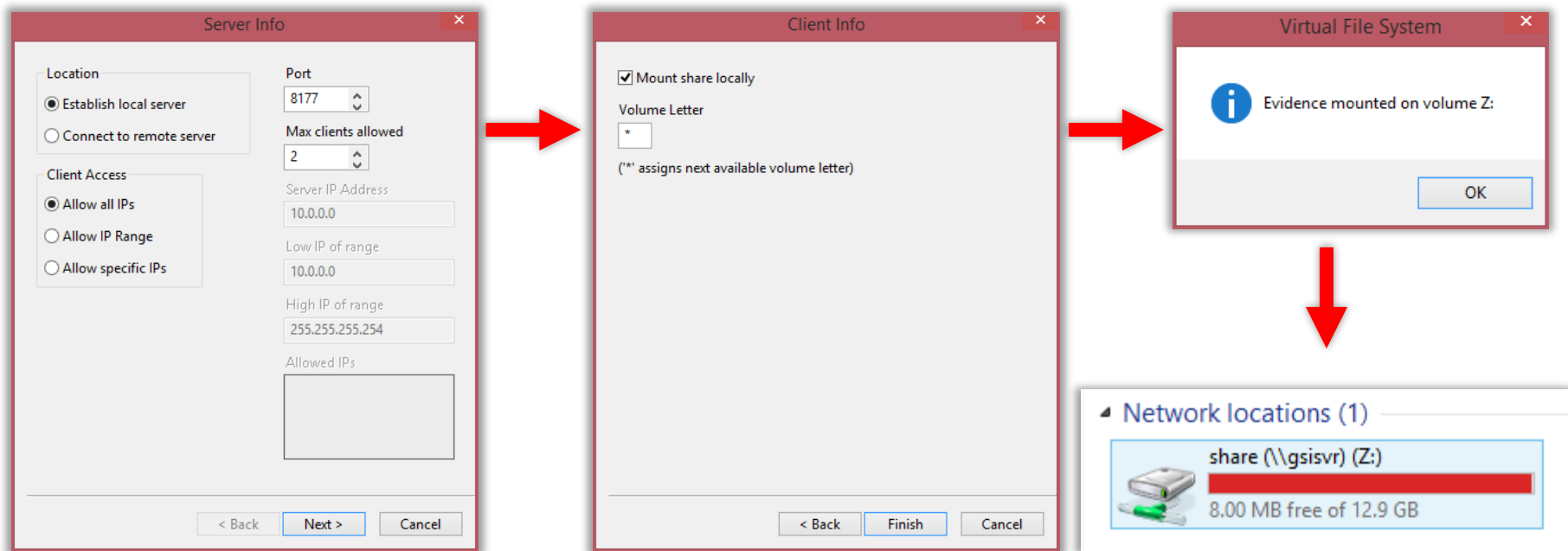
Virtual File System (VFS) mounts a drive, volume or folder as read-only offline network share.





# Mounting evidence: VFS

Next → Finish → Ok

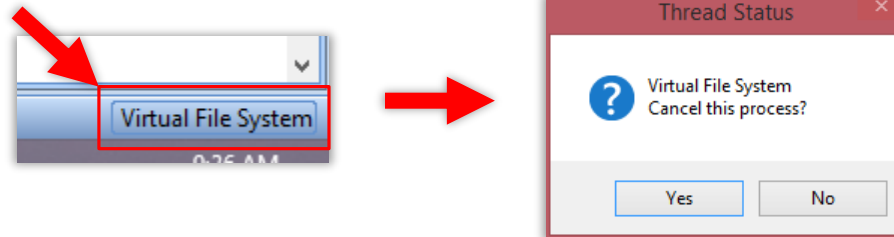


# Mounting evidence: VFS

VFS shows evidence as EnCase “sees” it (e.g. deleted files, alternate streams, unallocated clusters will show up as files)

Program Files (x86)\$.TXF_DATA	System file	1 KB
Program Files\$.TXF_DATA	System file	1 KB
ProgramData\$.TXF_DATA	System file	1 KB
Unallocated Clusters	File	1,001,568 KB
Volume Slack	File	4 KB
Windows\$.TXF_DATA	System file	1 KB

To stop the VFS service, double click “Virtual File System” in lower-right corner



# Mounting evidence: PDE

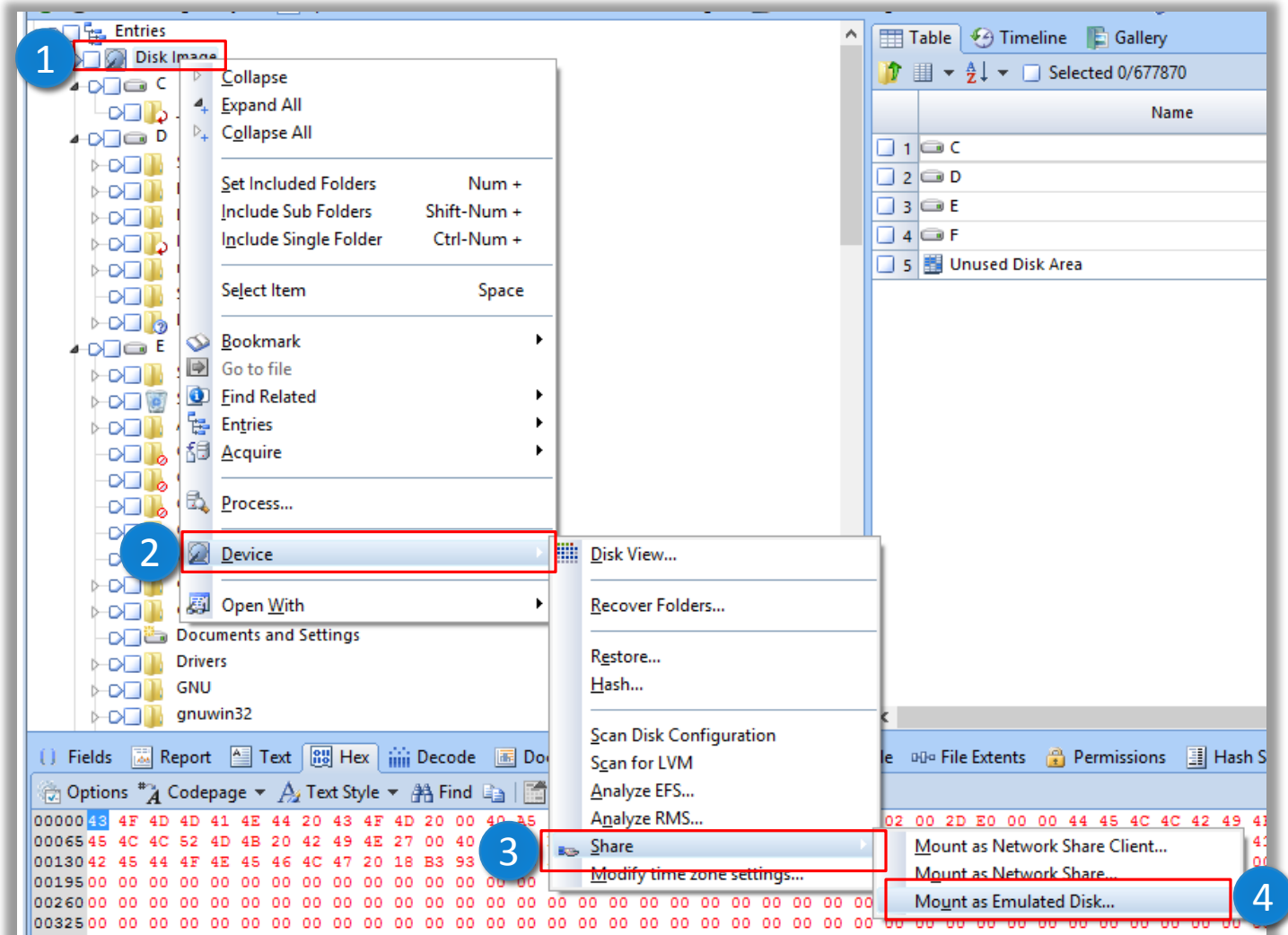
---

Another way to mount evidence is Physical Disk Emulator (PDE), which “tricks” windows into thinking that the evidence is an actual physical disk attached to the examiner machine.

This enables analysis of the evidence using other forensic tools, or use it to boot into a virtual machine.

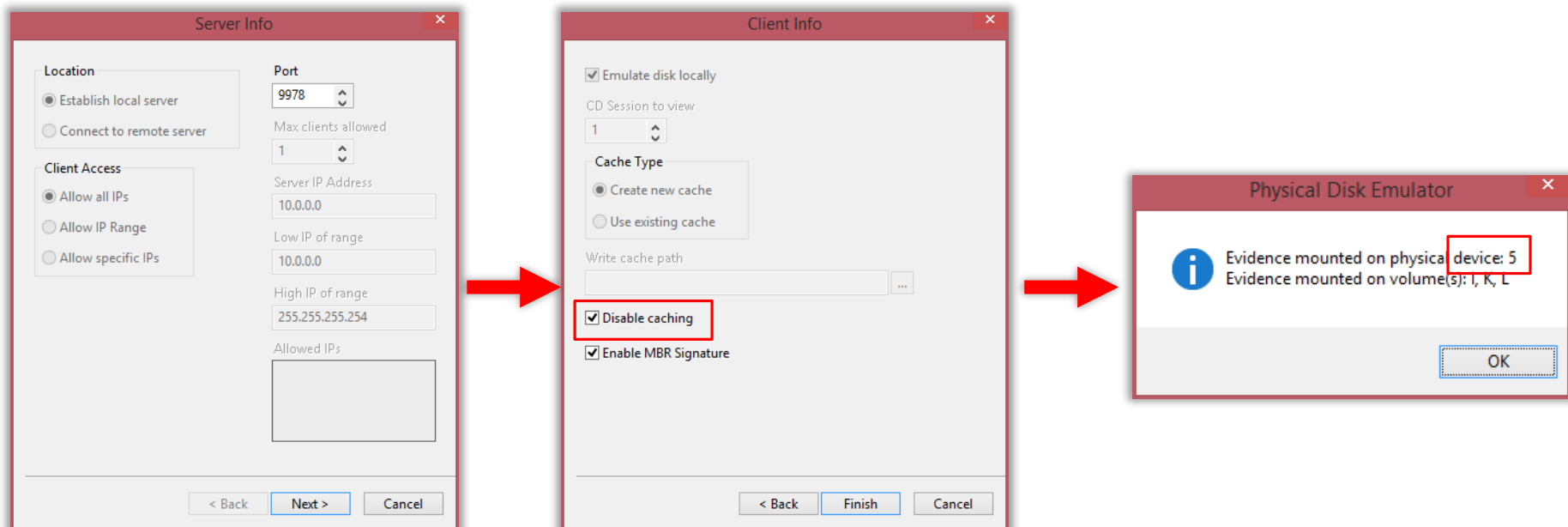
But this limits the supported file systems for casual browsing to those supported by windows (i.e. FAT & NTFS)

# Mounting evidence: PDE



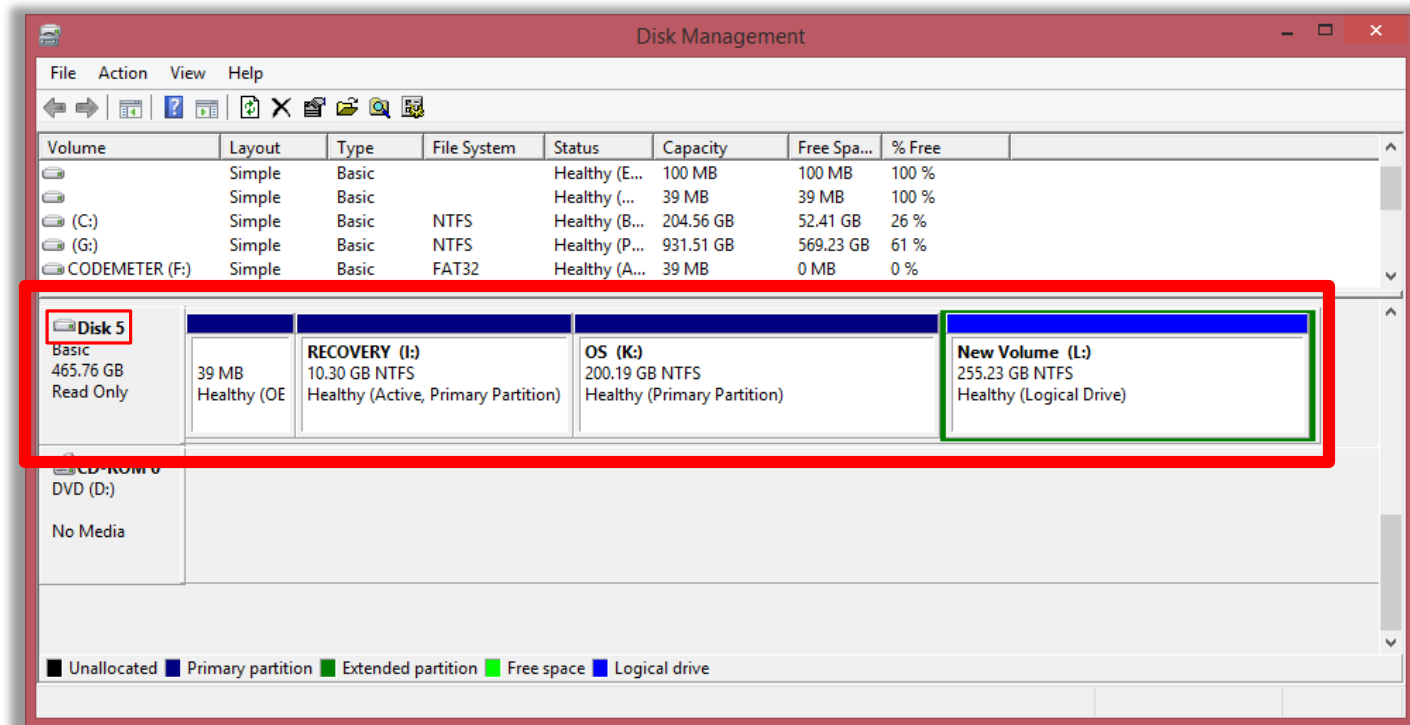
# Mounting evidence: PDE

Removing “Disable Cache” enables write-emulation “i.e. programs will believe they are able to modify files on evidence” ... only that changes are sent to cache folder of course



# Mounting evidence: PDE

Mounted Evidence recognized as a locally attached physical drive.

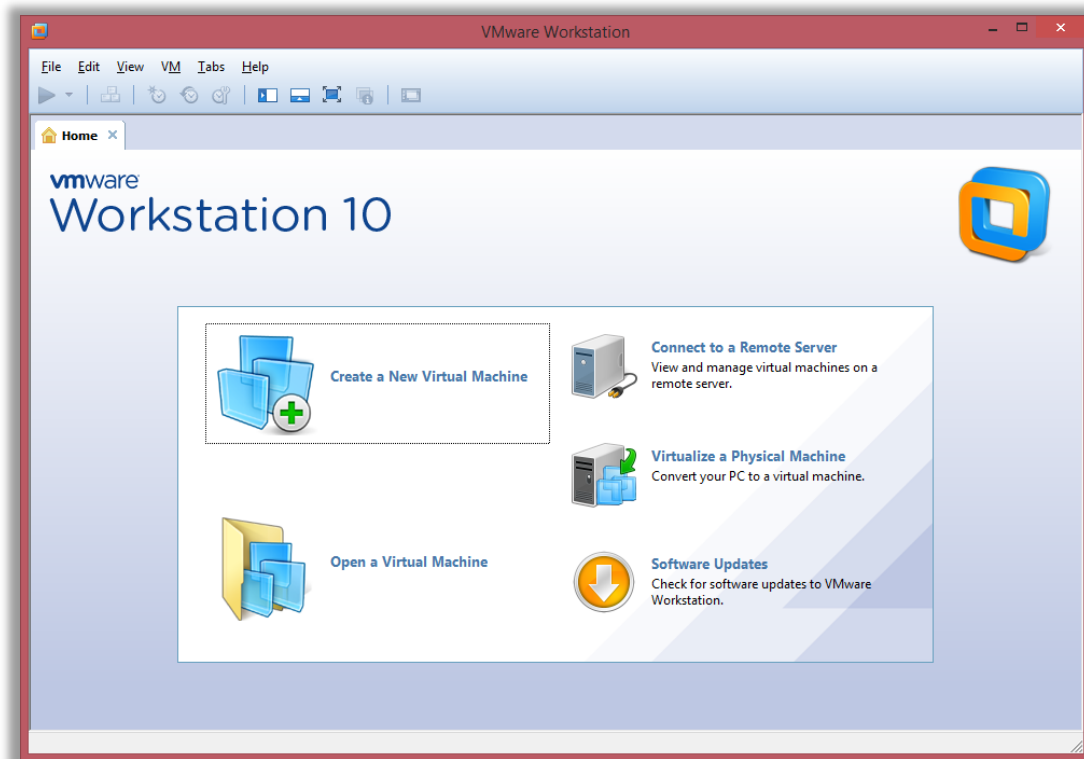


# Running evidence as a Virtual Machine

---

# Running evidence as a VM

Once mounted using PDE, we can create a virtual machine which boots as the evidence.





# Running evidence as a VM

Create a new VM, custom (advanced)



# Next, next ... next

**New Virtual Machine Wizard**

**Choose the Virtual Machine Hardware Compatibility**  
Which hardware features are needed for this virtual machine?

Virtual machine hardware compatibility

Hardware compatibility: Workstation 10.0

Compatible with: ☒ ESX Server

Compatible products:

- Fusion 6.0
- Workstation 10.0

Limitations:

- 64 GB memory
- 16 processors
- 10 network adapters
- 8 TB disk size

**New Virtual Machine Wizard**

**Name the Virtual Machine**  
What name would you like to use for this virtual machine?

Virtual machine name:

Case #2015-XXXX

Location:

C:\Users\USER\Documents\Virtual Machines\Case #2015-XXXX

The default location can be changed at Edit > Preferences.

< Back Next > Cancel

**New Virtual Machine Wizard**

**Guest Operating System Installation**  
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

☐ Installer disc:

BD-RE Drive (D:)

☐ Installer disc image file (iso):

E:\Downloads\ubuntu-14.04-desktop-1386.iso

Browse...

☒ I will install the operating system later.

**New Virtual Machine Wizard**

**Processor Configuration**  
Specify the number of processors for this virtual machine.

Processors

Number of processors: 1

Number of cores per processor: 1

Total processor cores: 1

Help < Back Next > Cancel

**New Virtual Machine Wizard**

**Select a Guest Operating System**  
Which operating system will be installed on this virtual machine?

Guest operating system

☒ Microsoft Windows

☐ Linux

☐ Novell NetWare

☐ Solaris

☐ VMware ESX

☐ Other

Version

Windows 7 x64

**New Virtual Machine Wizard**

**Memory for the Virtual Machine**  
How much memory would you like to use for this virtual machine?

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 2048 MB

Maximum recommended memory: 6008 MB

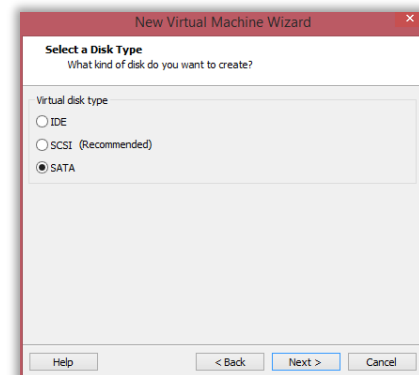
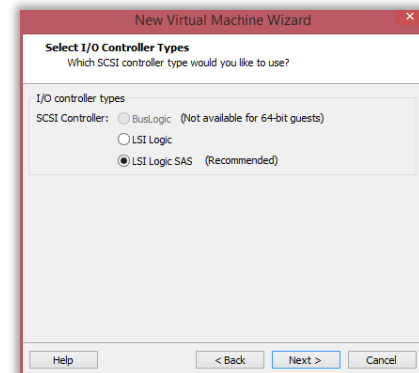
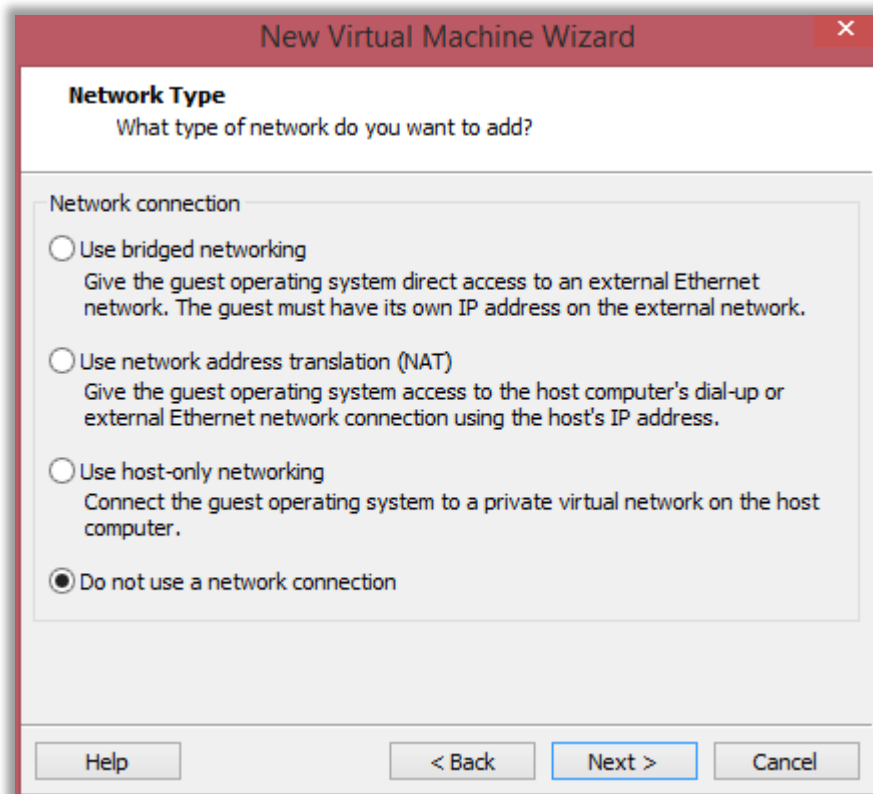
Recommended memory: 2048 MB

Guest OS recommended minimum: 1024 MB

Help < Back Next > Cancel

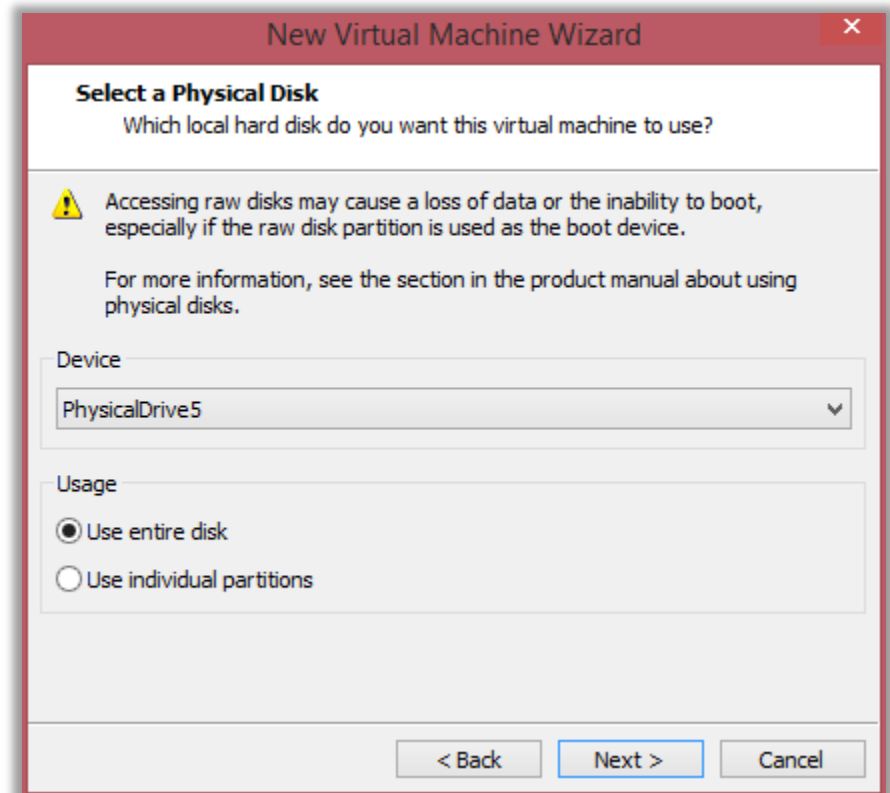
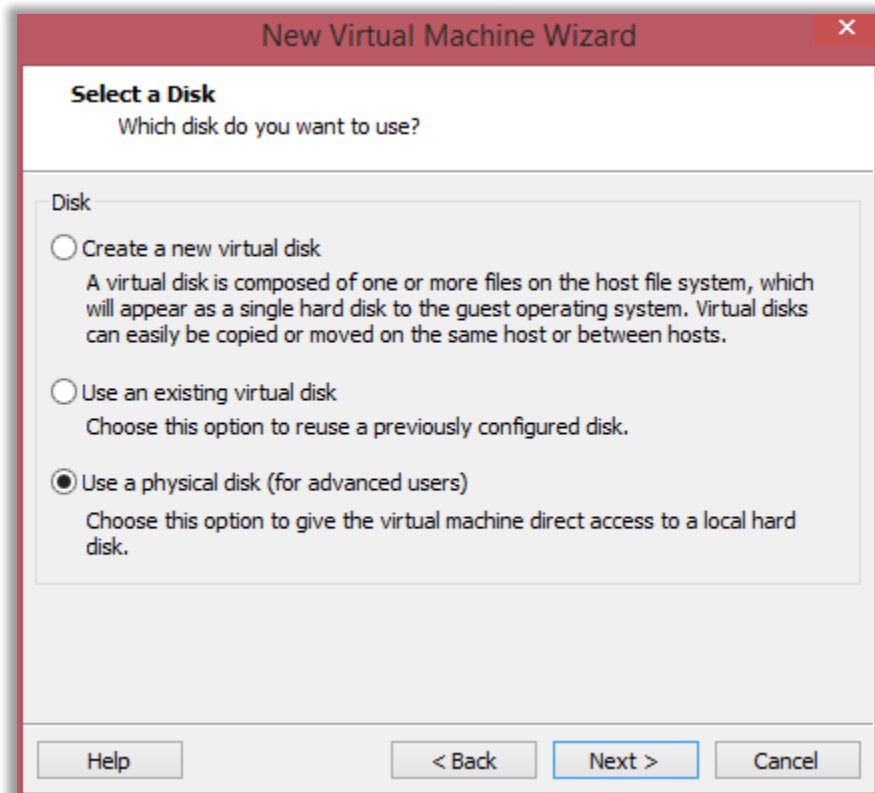
# No network!!

Or else bad things might happen ... then continue clicking through.

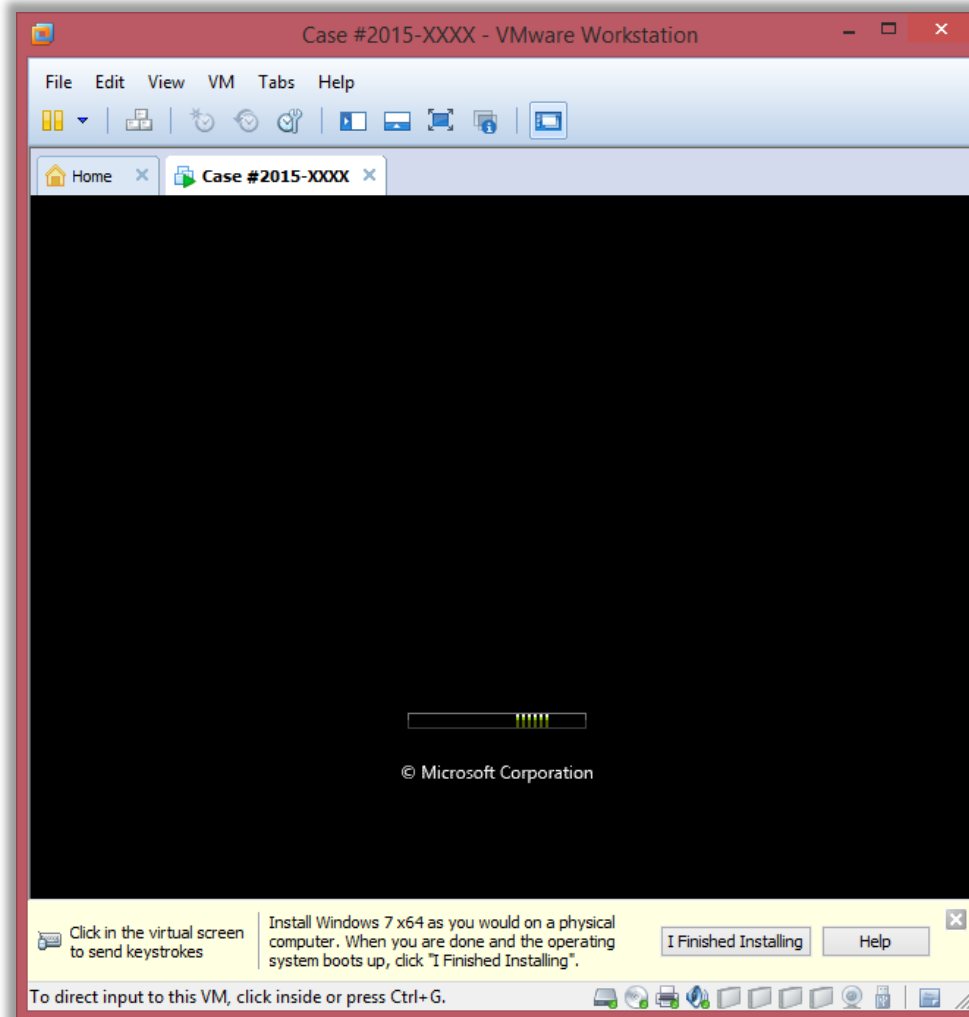


# Specifying a Disk for the VM

“Use a physical disk (for advanced users) ... then pick the emulated device ...



# Finish, then VM should start ...

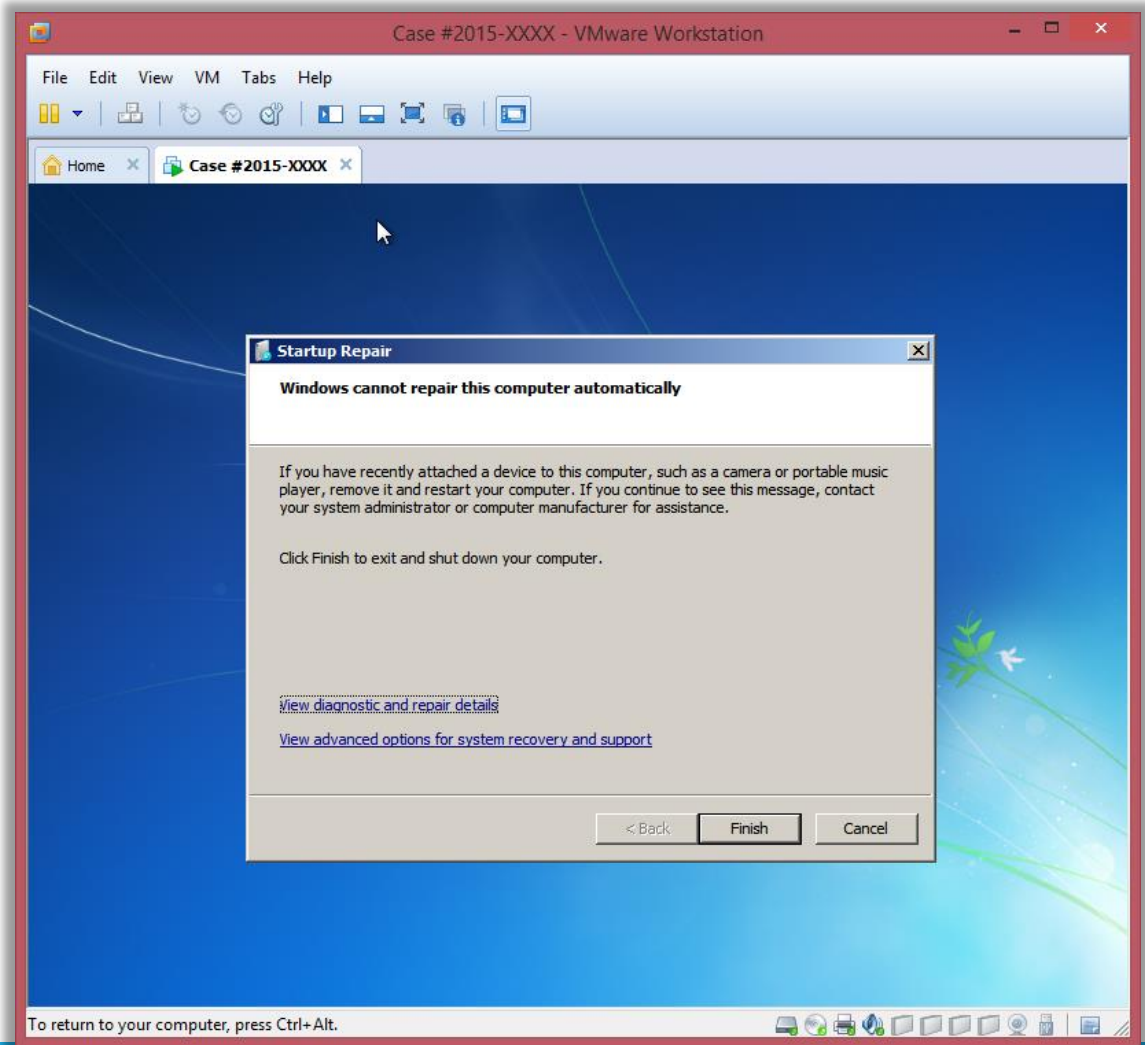


# Or not ...

Most probably  
windows won't  
start without  
manual fix

...

YMMV.



# Processing Evidence

---

.... WHERE THE FUN BEGINS

# What is `Evidence Processing`?

---

The Evidence Processor runs, in a single automated session, a collection of potent analytic tools against the case data.

Examples include: File carving, Internet artifact extraction, history of connected USB devices, network info (IP address & MAC addresses), System info, Instant messaging parser, Recovery of deleted files ... and much more!



# Evidence Processing

---

Some tasks take very, very ... very long time.

It is recommended that you pick what you are looking for only.

It has two pre-requisites:

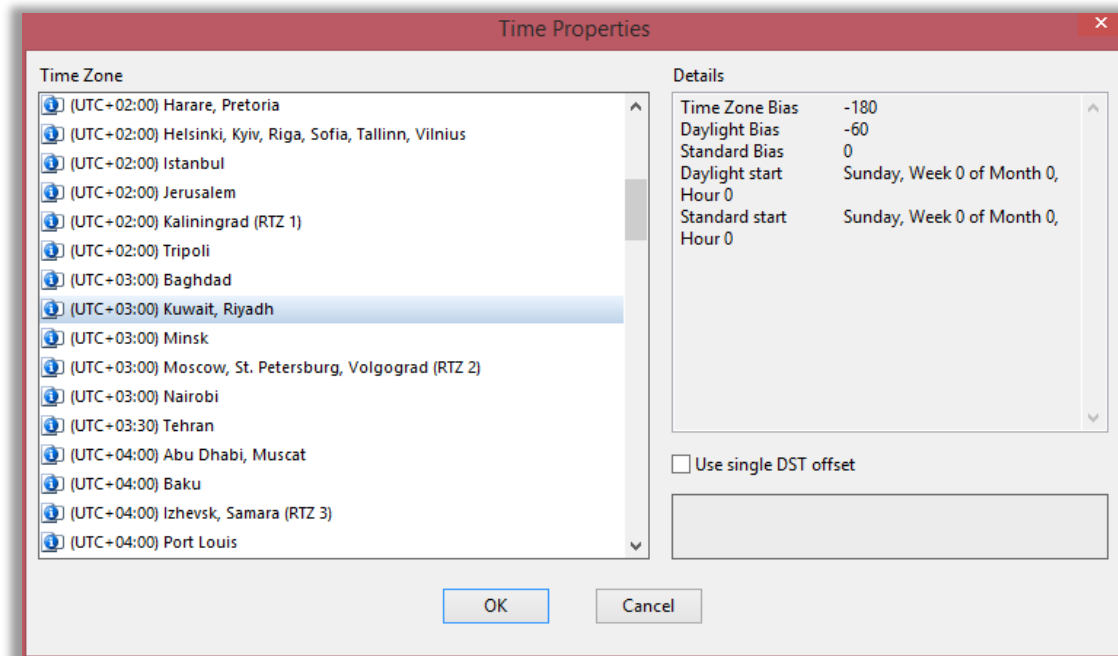
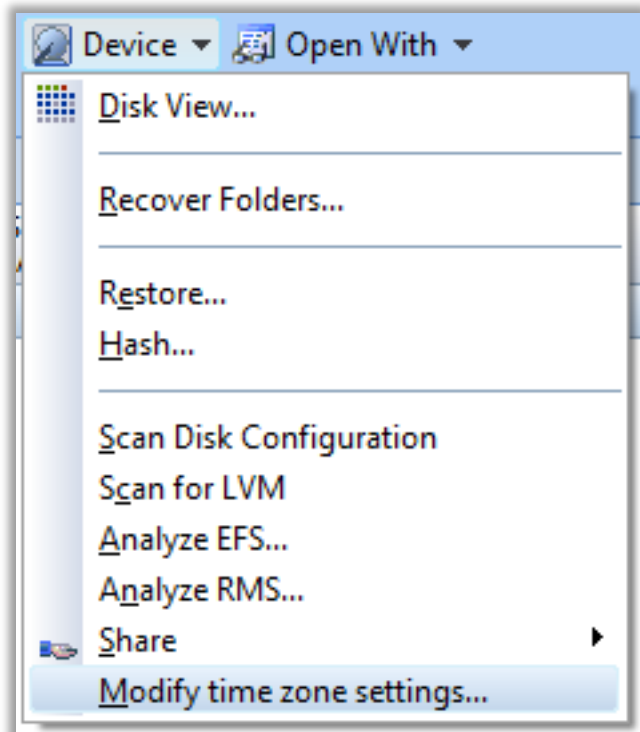
- Evidence must have been Acquired.
- Set the time zones of the evidence.

... let's see how to get the time zone of the evidence and configure EnCase appropriately

# Setting right time zone

If you know the time zone, set it directly.

Device -> Modify time zone settings



# If you don't know the Time Zone

---

If we don't know the time zone “like in many cases we get the evidence from overseas”, we have to know from which time zone it came.

In windows computers, Time Zone information is stored in the registry in the following key:

```
HKEY_LOCAL_MACHINE\System\ControlSet001\Control\TimeZoneInformation\TimeZoneKeyName
```

Which is stored in the following registry file:

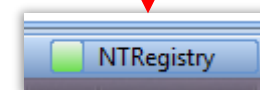
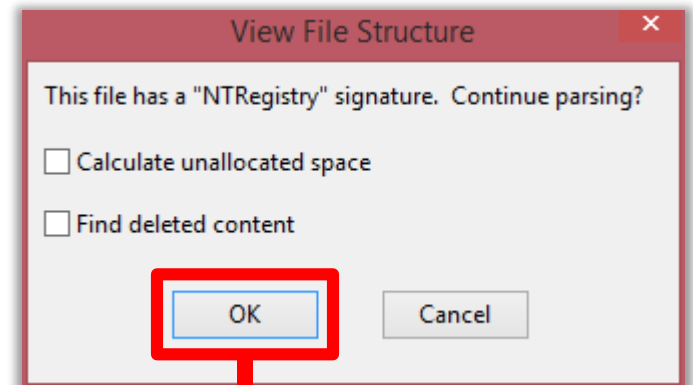
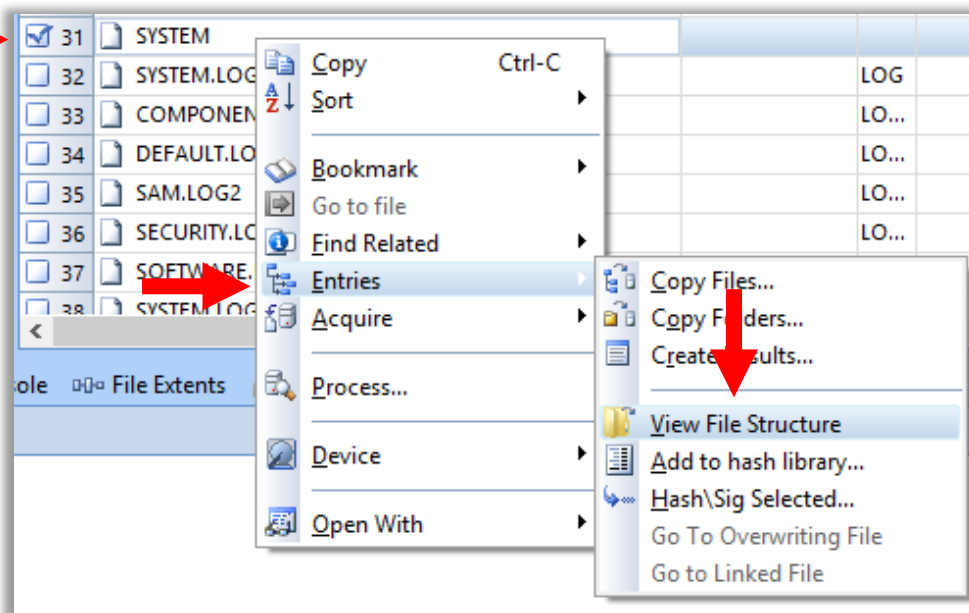
**\windows\system32\config\SYSTEM**

Browse to that file in the left pane ...

# If we don't know the Time Zone

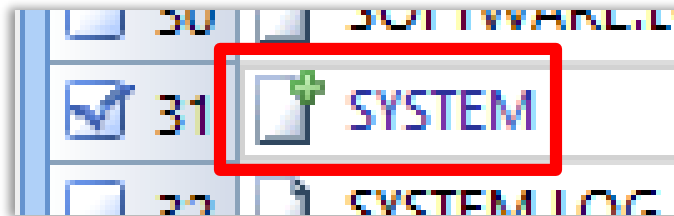
Right click -> Entries -> View file Structure

Wait for parsing to finish.

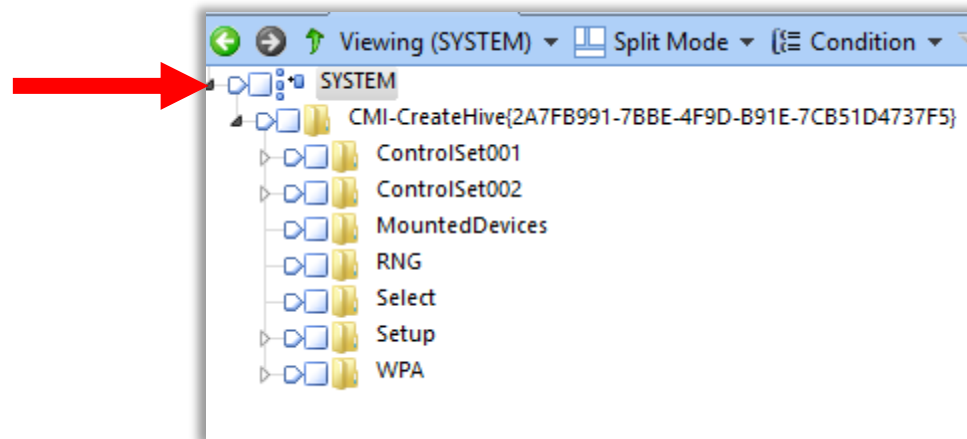


# If we don't know the Time Zone

When processing is finished, there will be a little green “+” beside the SYSTEM name

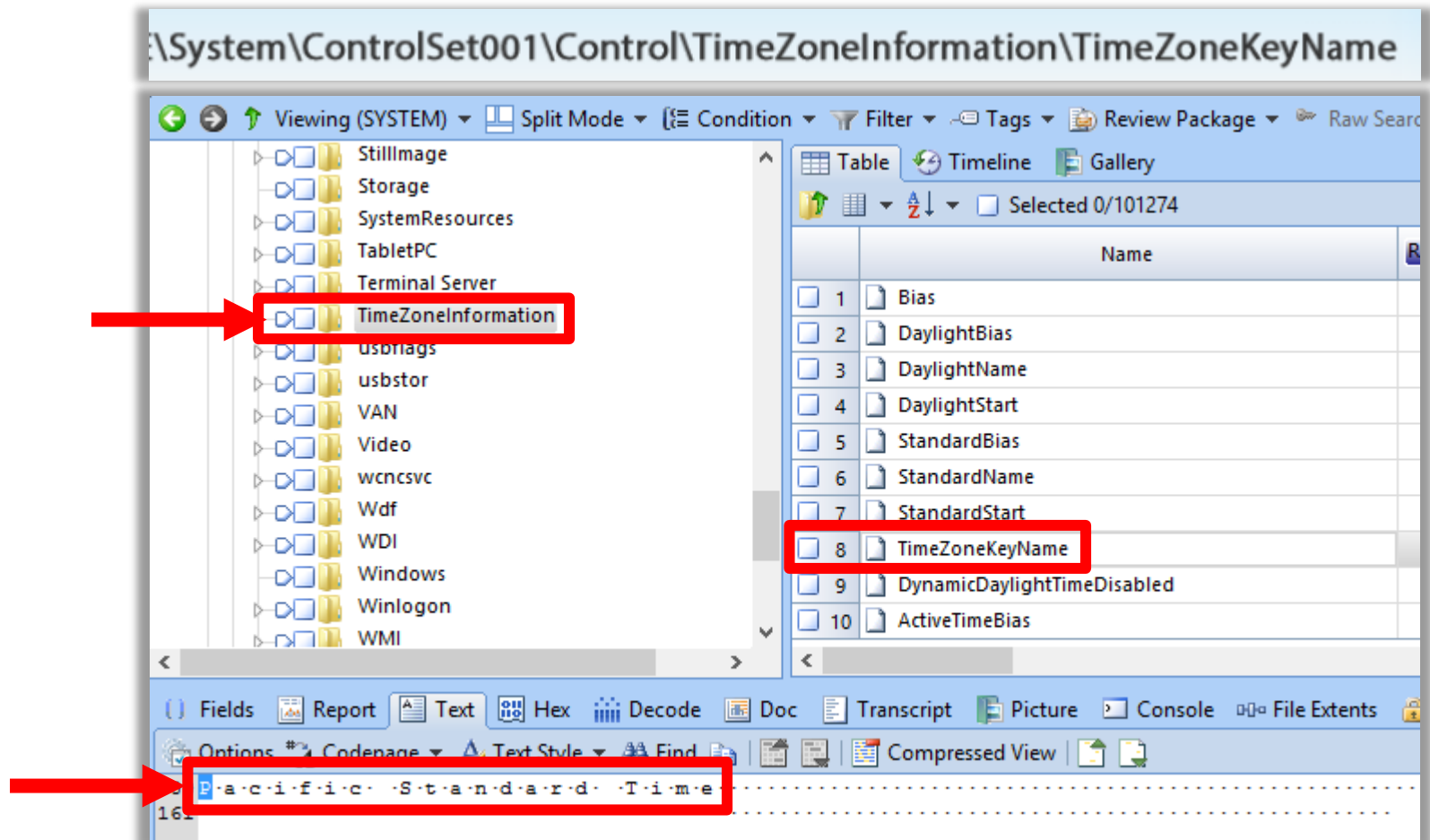


Now click the SYSTEM file, it will expand



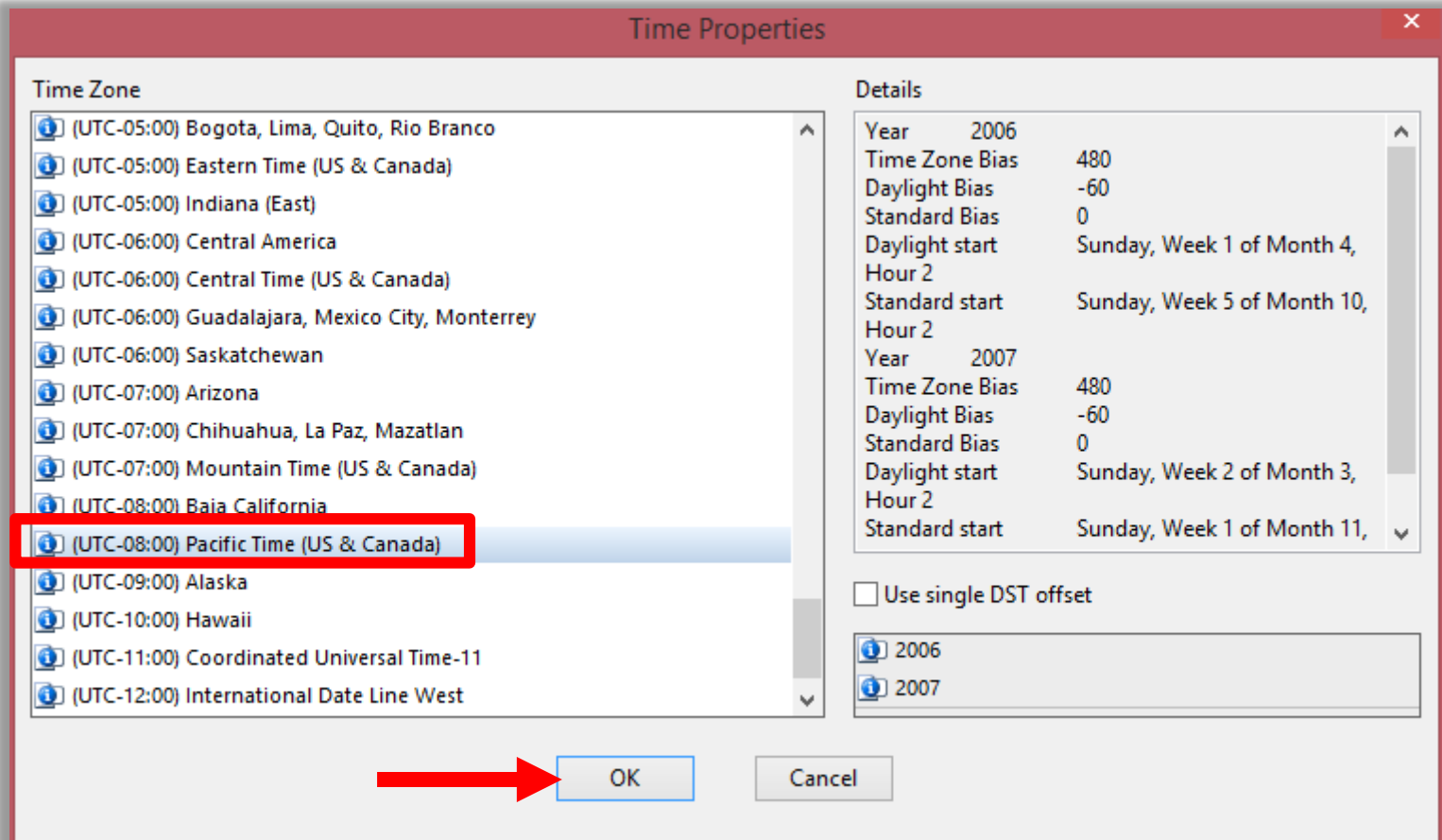
# If we don't know the Time Zone

## We go to that key



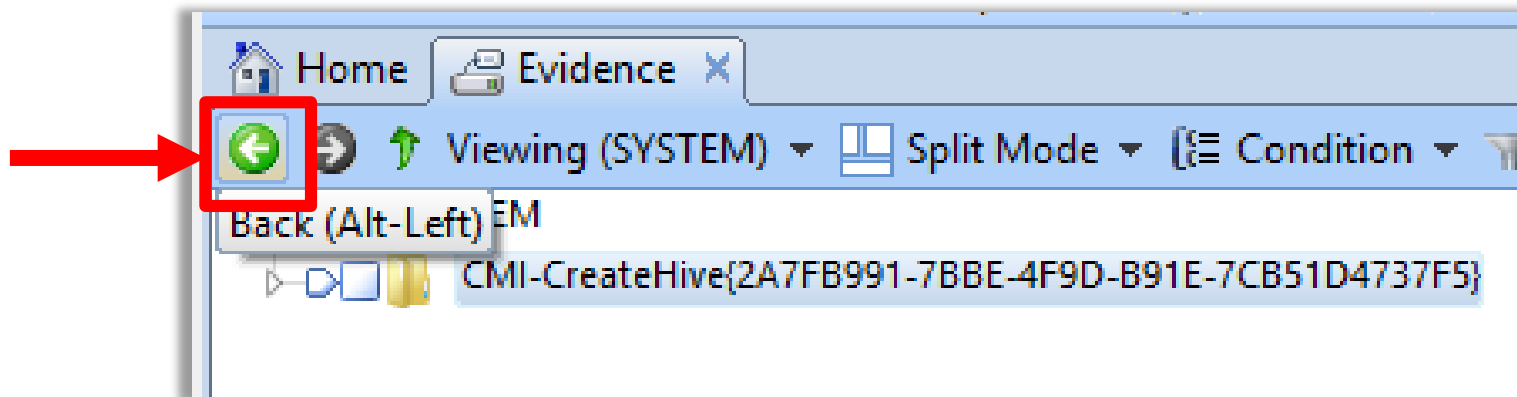
# If we don't know the Time Zone

It's `Pacific Standard Time` ... let's reconfigure



# If we don't know the Time Zone

To get back to the main evidence area “i.e. exit from the SYSTEM hierarchy”, Press the `Back` green button





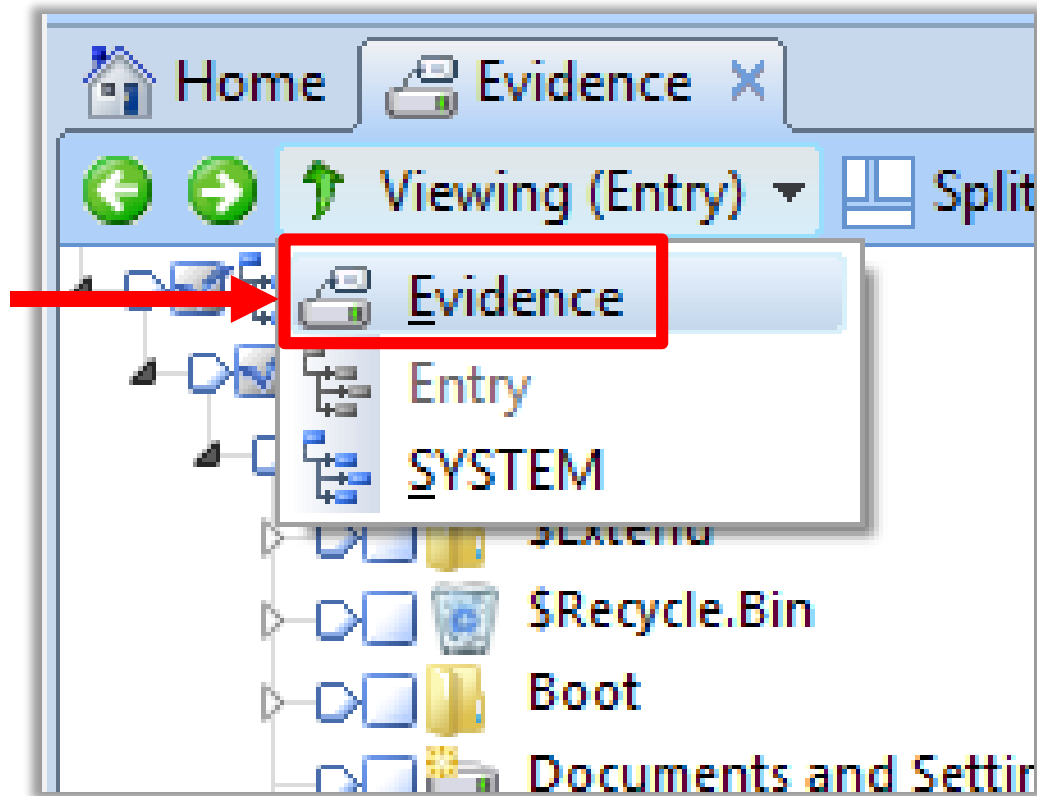
# Processing Evidence

---

...CONTD.

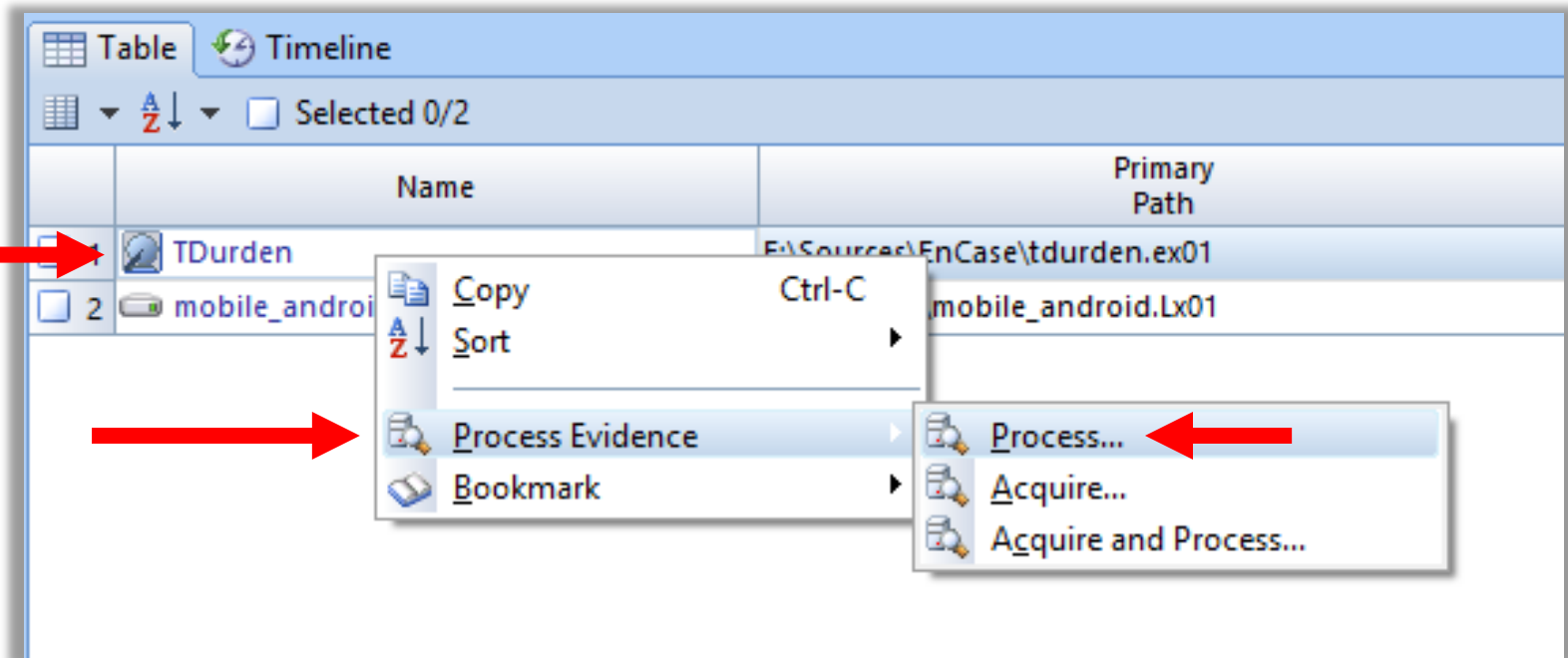
# Change view to `Evidence`

Change view to `Evidence` instead of `Entry`

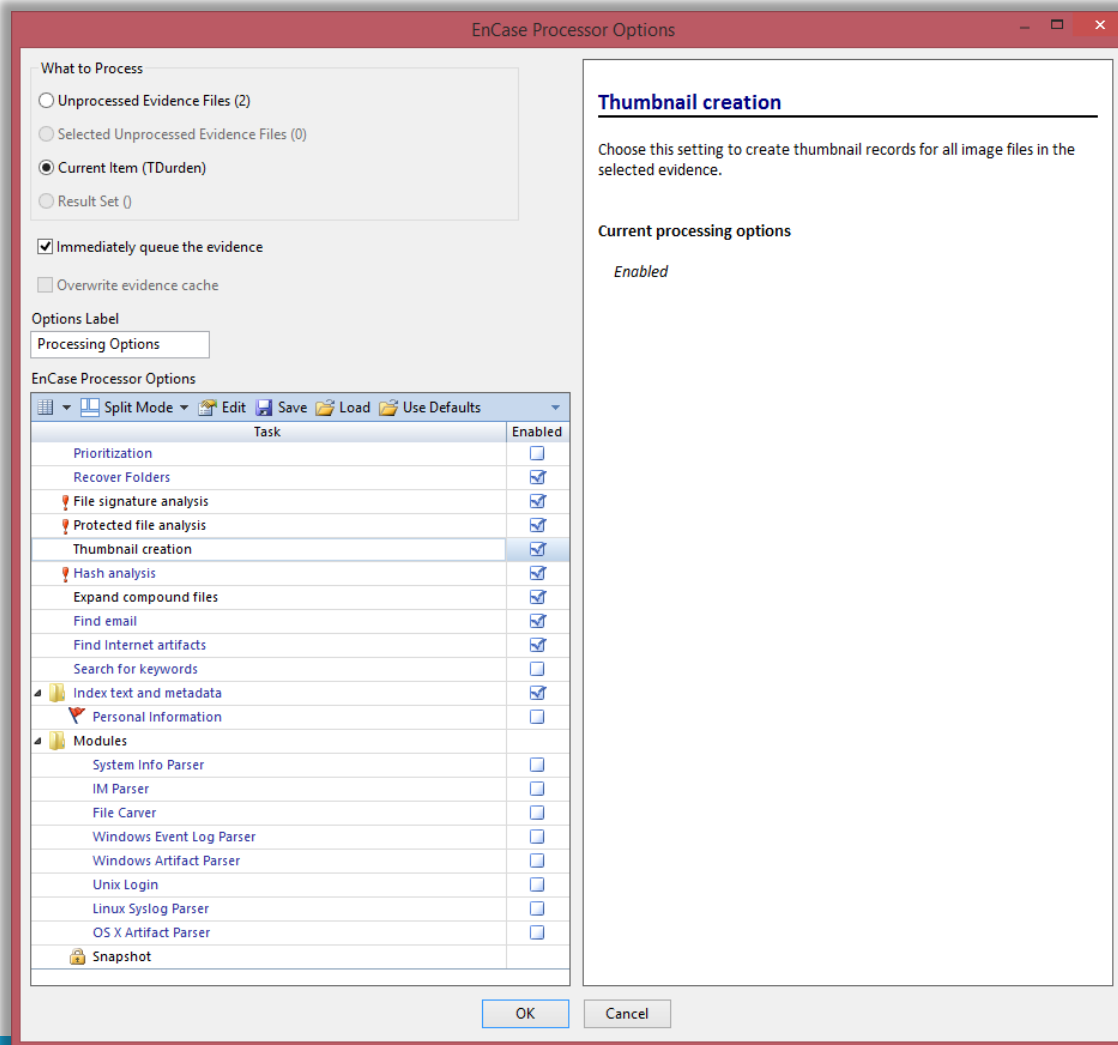


# Process ...

Right click on Evidence -> Process Evidence -> Process...



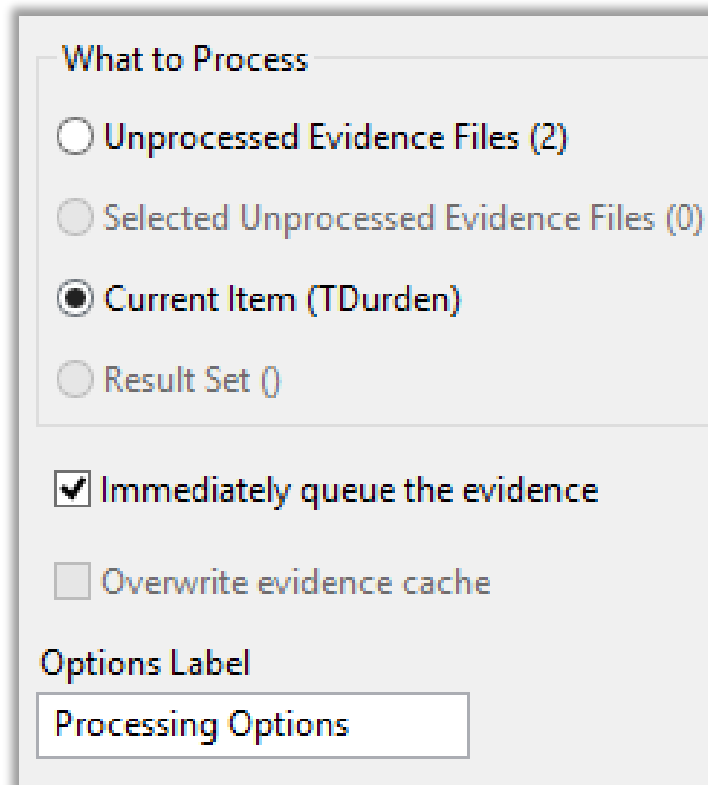
# Processor Options



# Processor Options

---

Process all evidence files? Or just current?



The screenshot shows a dialog box titled "What to Process" with the following options:

- ☐ Unprocessed Evidence Files (2)
- ☐ Selected Unprocessed Evidence Files (0)
- ☒ Current Item (TDurden)
- ☐ Result Set ()








Below the radio buttons, there are two checkboxes:

- ☒ Immediately queue the evidence
- ☐ Overwrite evidence cache

At the bottom, there is a section labeled "Options Label" containing a text box with the text "Processing Options".

# Processor Options

If it is [blue](#), it's a hyperlink and it has more options.

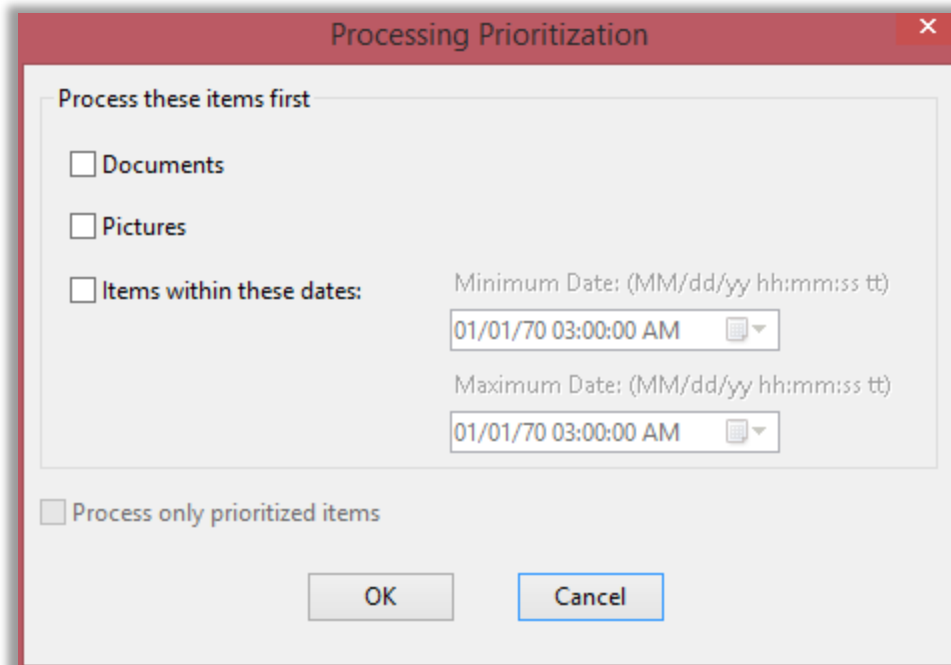
<a href="#">Prioritization</a>	<input type="checkbox"/>
<a href="#">Recover Folders</a>	<input checked="" type="checkbox"/>
 <a href="#">File signature analysis</a>	<input checked="" type="checkbox"/>
 <a href="#">Protected file analysis</a>	<input checked="" type="checkbox"/>
Thumbnail creation	<input checked="" type="checkbox"/>
 <a href="#">Hash analysis</a>	<input checked="" type="checkbox"/>
Expand compound files	<input checked="" type="checkbox"/>
<a href="#">Find email</a>	<input checked="" type="checkbox"/>
<a href="#">Find Internet artifacts</a>	<input checked="" type="checkbox"/>
<a href="#">Search for keywords</a>	<input type="checkbox"/>
 <a href="#">Index text and metadata</a>	<input checked="" type="checkbox"/>
 <a href="#">Personal Information</a>	<input type="checkbox"/>
 <a href="#">Modules</a>	
<a href="#">System Info Parser</a>	<input type="checkbox"/>
<a href="#">IM Parser</a>	<input type="checkbox"/>
<a href="#">File Carver</a>	<input type="checkbox"/>
<a href="#">Windows Event Log Parser</a>	<input type="checkbox"/>
<a href="#">Windows Artifact Parser</a>	<input type="checkbox"/>
<a href="#">Unix Login</a>	<input type="checkbox"/>
<a href="#">Linux Syslog Parser</a>	<input type="checkbox"/>
<a href="#">OS X Artifact Parser</a>	<input type="checkbox"/>
 <a href="#">Snapshot</a>	

# Prioritization

---

What to process first?

To process only the types of selected items,  
Check **Process only prioritized items**



The image shows a 'Processing Prioritization' dialog box with a red title bar and a close button. It contains a section titled 'Process these items first' with three checkboxes: 'Documents', 'Pictures', and 'Items within these dates:'. The 'Items within these dates:' checkbox is selected, and it has two date pickers for 'Minimum Date' and 'Maximum Date', both set to '01/01/70 03:00:00 AM'. At the bottom, there is a checkbox labeled 'Process only prioritized items' which is also selected. Below this checkbox are 'OK' and 'Cancel' buttons.

Processing Prioritization

Process these items first

☐ Documents

☐ Pictures

☒ Items within these dates: Minimum Date: (MM/dd/yy hh:mm:ss tt)  
01/01/70 03:00:00 AM

Maximum Date: (MM/dd/yy hh:mm:ss tt)  
01/01/70 03:00:00 AM

☒ Process only prioritized items

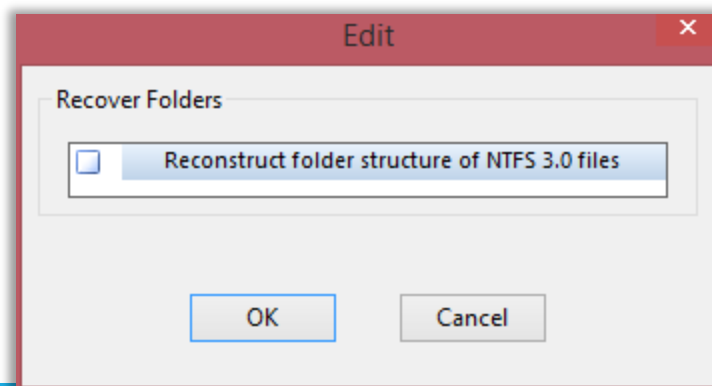
OK Cancel

# Recover Folders

---

Try to recover deleted files and folders

When you turn on the **Recover folder structure of NTFS 3.0 files** option, recovery will take longer, but will reconstruct (folder tree); if you left that unchecked, all found folders will be grouped together without tree structure.





# File Signature Analysis

---

A quite common technique for masking data is to rename a file and change its extension; for example, “image.jpg” might be renamed to “program.exe”.

Signature analysis verifies file type by comparing the file headers, or signature, with the file extension, and flag mismatches.



# Protected File Analysis

Relies on “Passware Kit” to be installed on examiner machine and properly configured



<http://www.lostpassword.com/encase.htm>

Identify password-protected files

This will take long, long time.

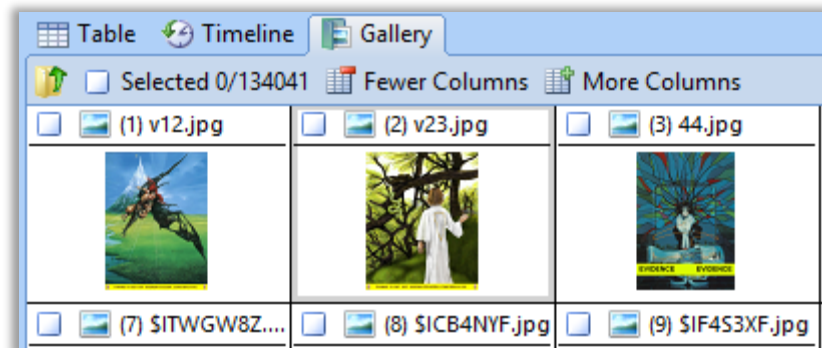


Protected file analysis



# Thumbnail creation

Will create “thumbnails” for all images to be viewed in the “Gallery” ... upfront.



Thumbnail creation



# Hash Analysis

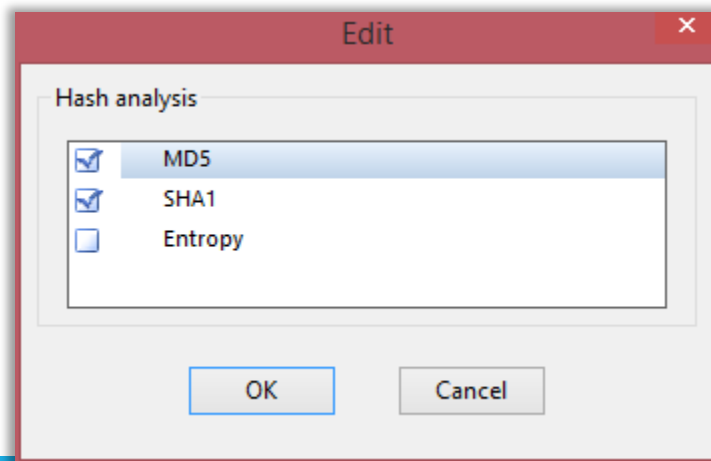
Calculate hash value for all files.



Is required for more advanced analysis.

“Entropy” -> high value indicates compression or encryption.

Takes time, if not required, unselect.



# Expand Compound Files

---

Will expand ZIP, RAR, BZIP2 and other compressed files, and make files within them available for processing.

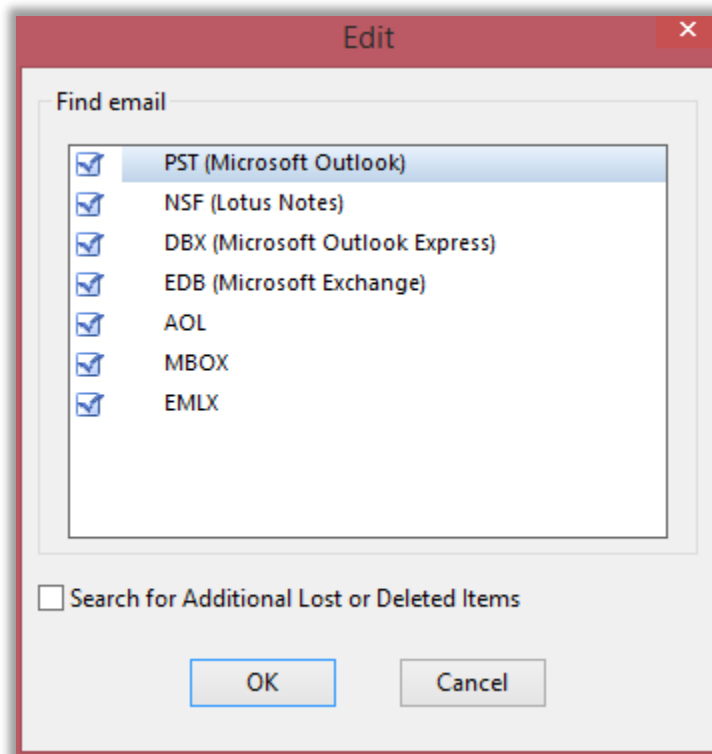
VERY USEFUL!

Expand compound files



# Find Email

Will extract messages (and attachments) from email archives (e.g. PST).



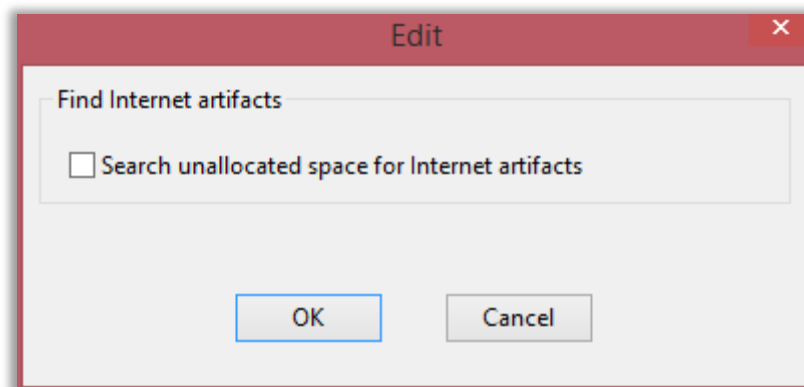
# Find Internet Artifacts

---

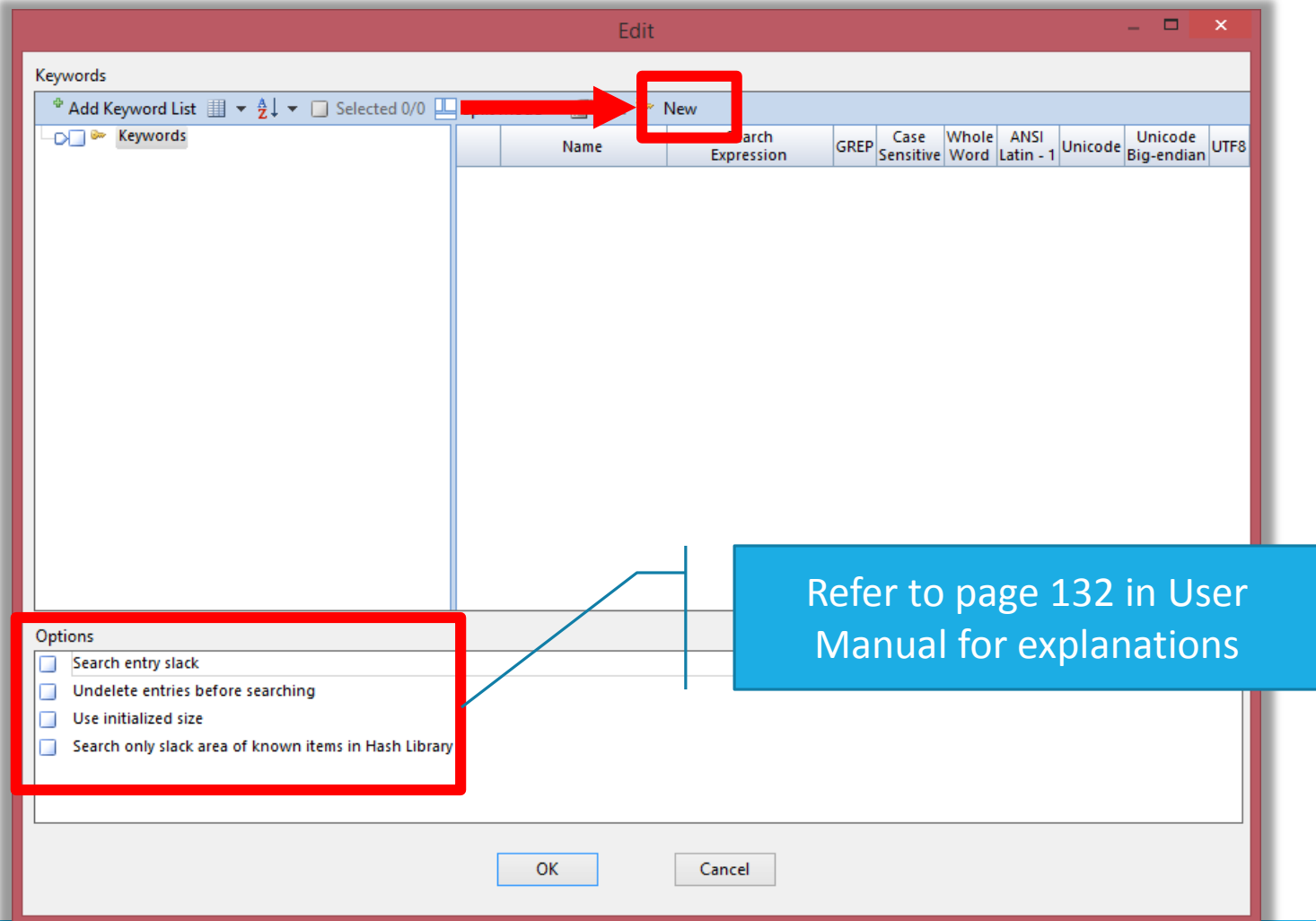
Browser History and cached web pages

Chrome & Firefox supports: cookies, downloads, keyword search, login data `users and passwords` and top visited sites.

Searching in unallocated space will take time



# Searching for Keywords





# Add new keyword

**New Keyword**

Search Expression   Code Page   Keyword tester

Search Expression  
Tyler

Name  
Tyler

Search Options

☒ ANSI Latin - 1   ☐ GREP  
☐ UTF8   ☐ Case Sensitive  
☐ UTF7   ☐ Whole Word  
☒ Unicode  
☐ Unicode Big-endian

GREP Symbols

\wFFFF	Unicode character
\xFF	Hex character
.	Any character
#	Any number [0-9]
?	Repeat zero or one time
+	Repeat at least once
[A-Z]	A through Z
*	Repeat zero+ times
[XYZ]	Either X, Y, or Z
[^XYZ]	Neither X nor Y nor Z
\[	Literal character
(ab)	Group ab together for ?, +, *,
{m,n}	Repeat m to n times
a b	Either a or b

Unicode View

[0054 0074][0059 0079][004C 006C][0045 0065][0052 0072]

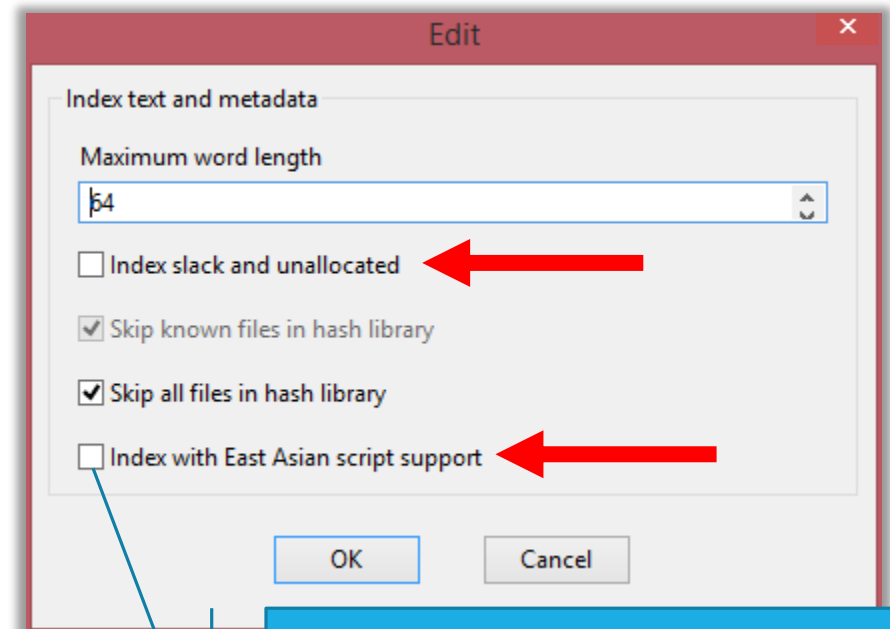
OK Cancel

# Creating an Index

An `index` is a list of all “text” in an evidence; create it once, search through it very quickly.



- Will enable searching across all types of information and view results in email, files, smartphones, and any other processed data in one search results view.



Enable this, if you enable  
“Index Slack and unallocated!”

# Personal Information

Credit cards, Phone numbers, Email addresses & USA Social security numbers ...

The 'Personal Information' dialog box is shown with the 'General' tab selected. It contains the following sections:

- Entry condition:** A checked checkbox and an 'Edit' button.
- Search Options:** A 'Hit Threshold' set to 1.
- Phone numbers:** Two checked checkboxes: 'With area code' and 'Without area code'.
- Email Addresses:** A checked checkbox for 'Email addresses'.

At the bottom are 'OK' and 'Cancel' buttons.

The 'Personal Information' dialog box is shown with the 'Credit Card' tab selected. It displays a list of credit cards with checkboxes:

- Visa
- MasterCard
- American Express
- Discover
- Diners Club
- InstaPayment
- JCB
- Maestro
- Laser
- Solo
- Switch
- BankCard

At the bottom are 'OK' and 'Cancel' buttons.

The 'Personal Information' dialog box is shown with the 'Government ID' tab selected. It displays a list with one item:

- Social Security Number

At the bottom are 'OK' and 'Cancel' buttons.

# Personal Information

Information about the Qatari ID number, and how to configure EnCase to look for them could be found at the following site:

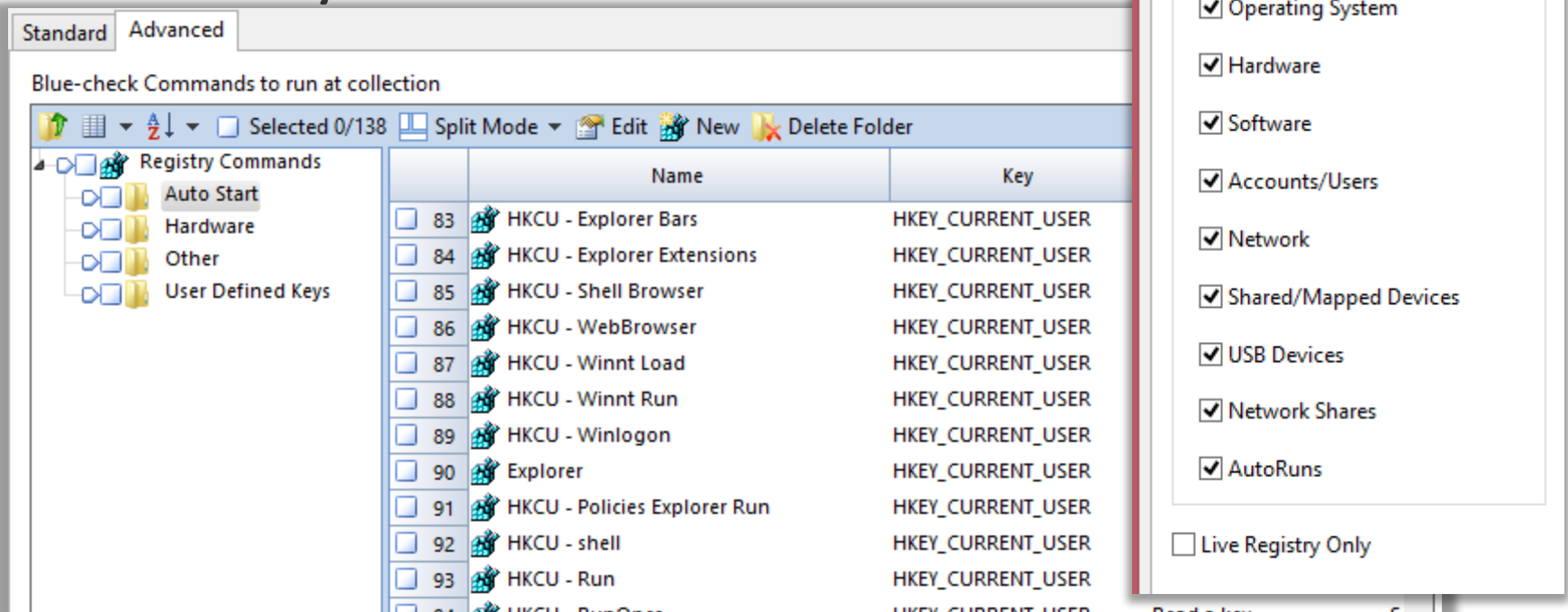
<https://eldeeb.net/wrdprs/?p=330>



# System Info Parser

Identify hardware, software, and user information.

Previously connected USB devices.

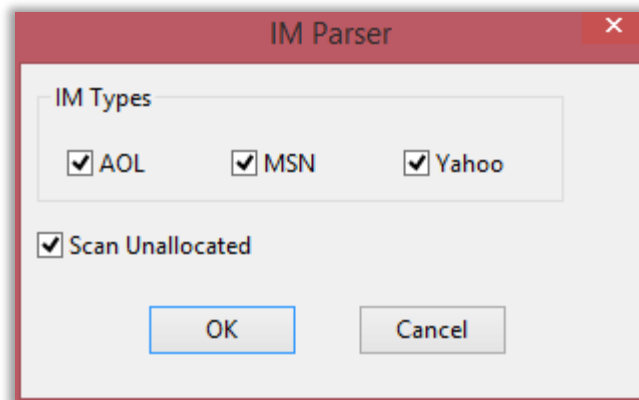


# IM Parser

Scans for AOL, MSN and Yahoo chat artifacts

Who is using those anyways :/ ... not very useful unless you're investigating an evidence acquired long, long time ago.

IM Parser



# File Carver

---

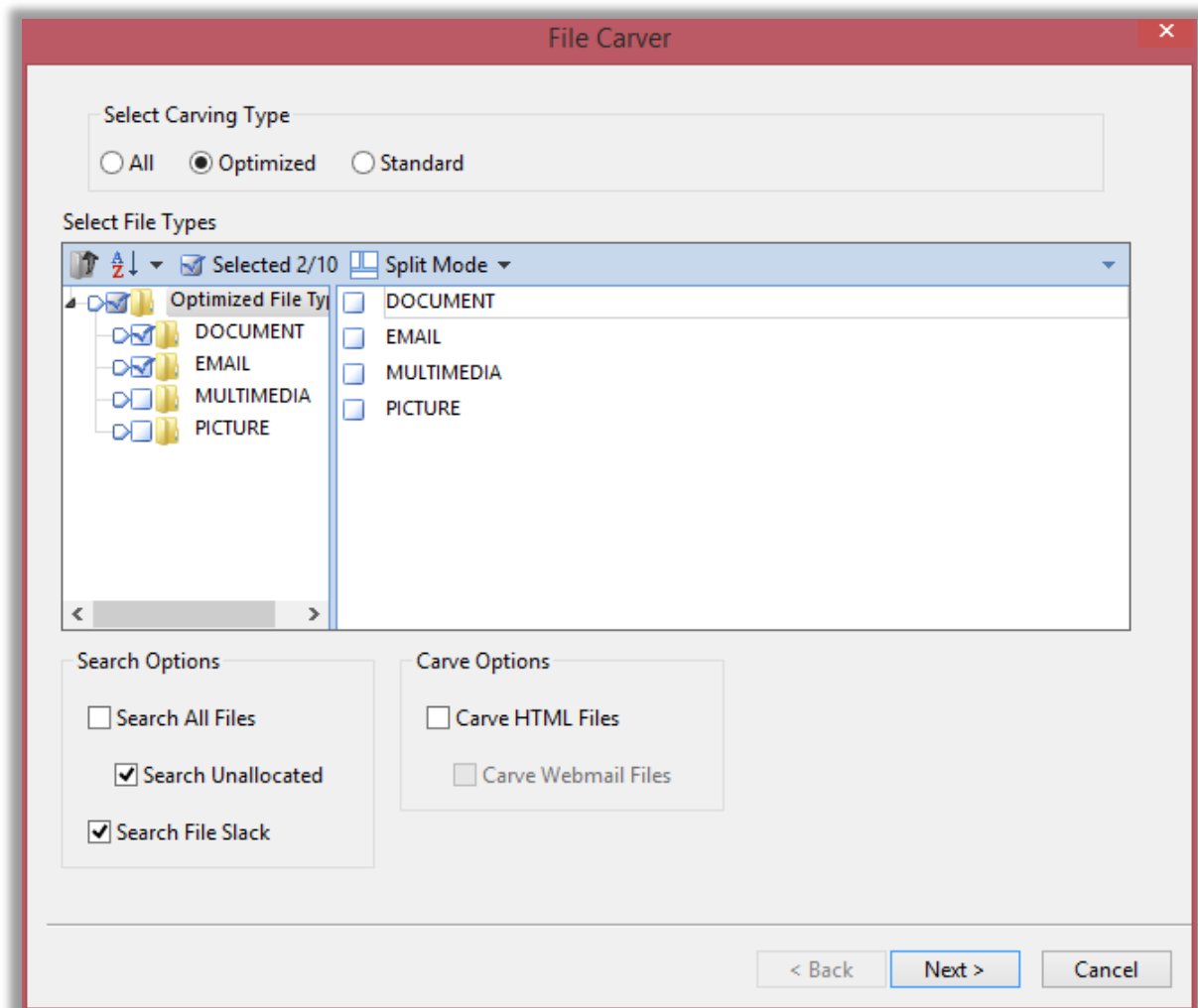
File carving is the process of reassembling files from fragments in the absence of filesystem metadata.

- e.g. there will be no file names or created time... only file data.

This should be able to recover deleted files which has not been overwritten, even if the metadata has been overwritten

Very useful for recovering deleted files, especially for relatively small files (images, audio ...etc.)

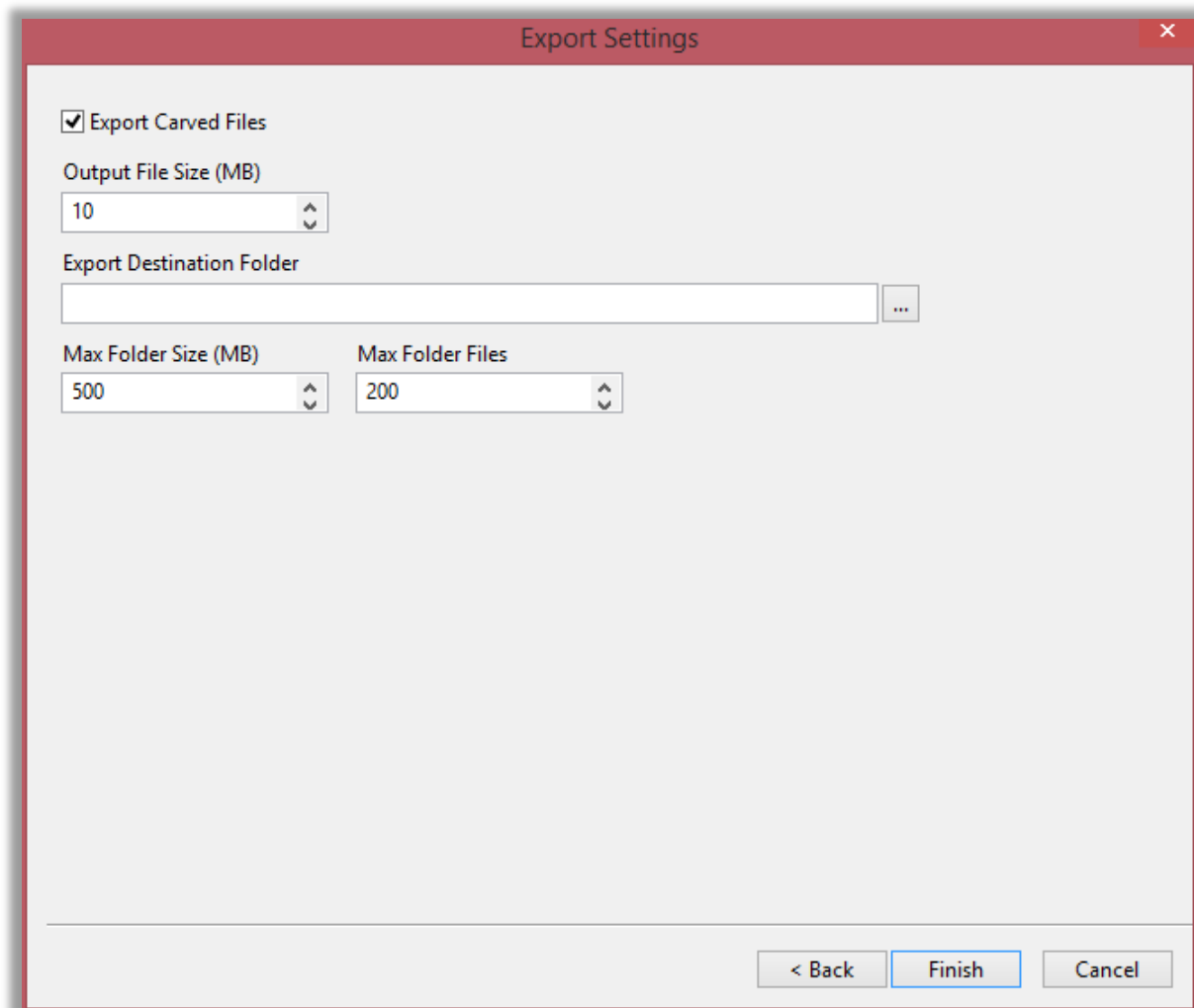
# File Carver





# File Carver

---



The screenshot shows the 'Export Settings' dialog box of File Carver. It has a red title bar with a close button. The settings are as follows:

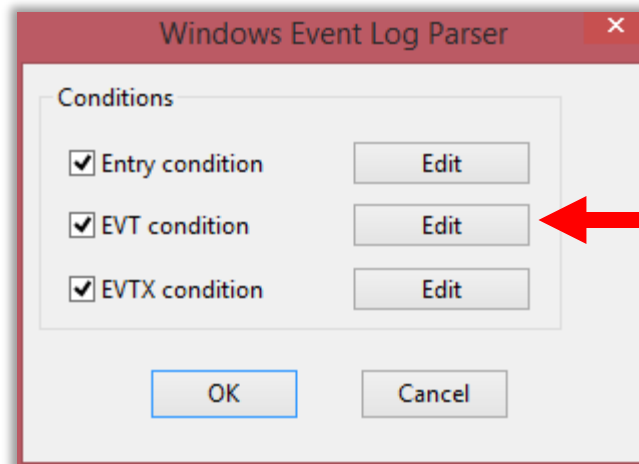
- ☒ Export Carved Files
- Output File Size (MB): 10
- Export Destination Folder: (empty text box with a browse button)
- Max Folder Size (MB): 500
- Max Folder Files: 200

At the bottom, there are three buttons: '< Back', 'Finish' (highlighted with a blue border), and 'Cancel'.

# Windows Event Log Parser

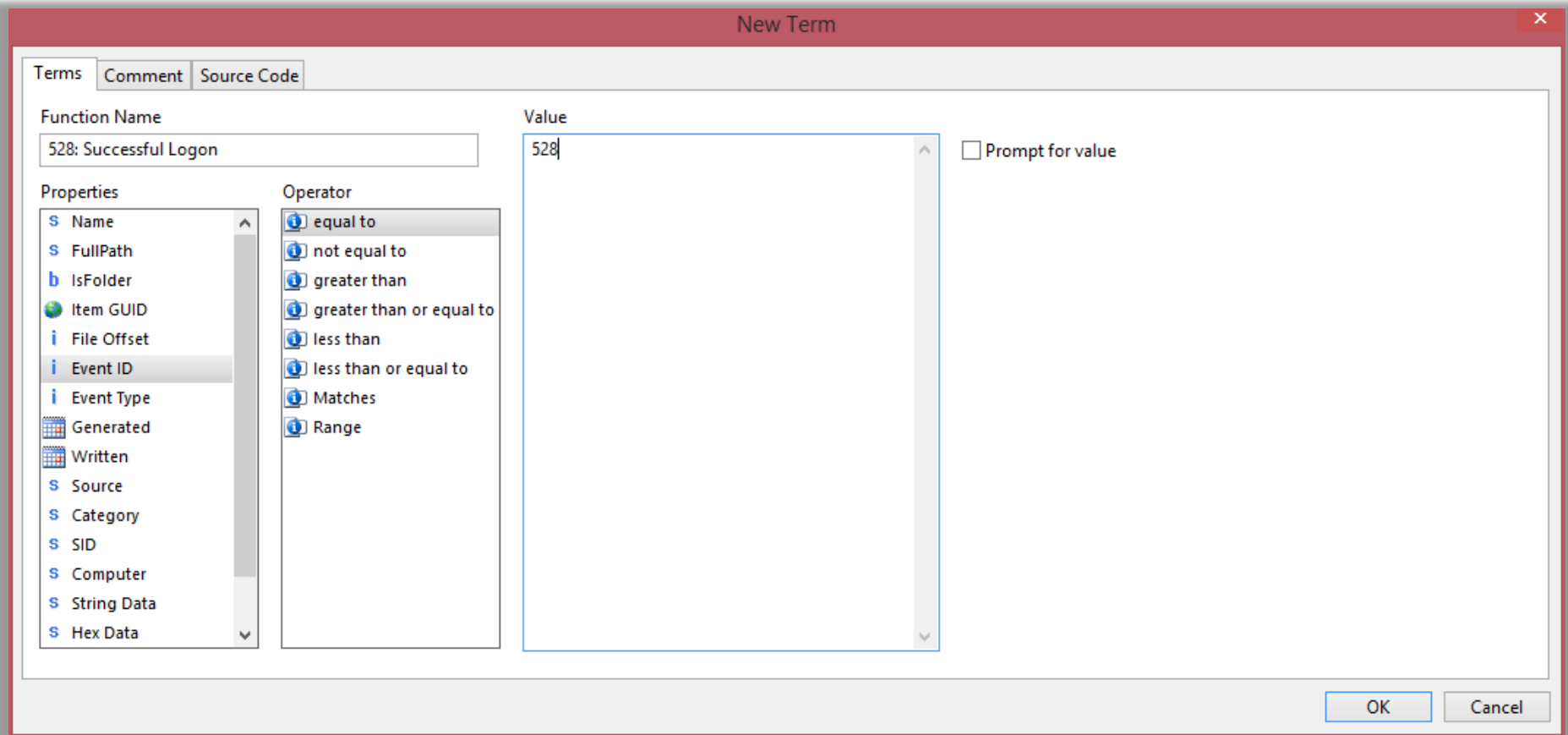
This module parses .evt and .evtx files for Windows Event Logs, and also allows for processing by condition (e.g. event id)

Windows Event Log Parser

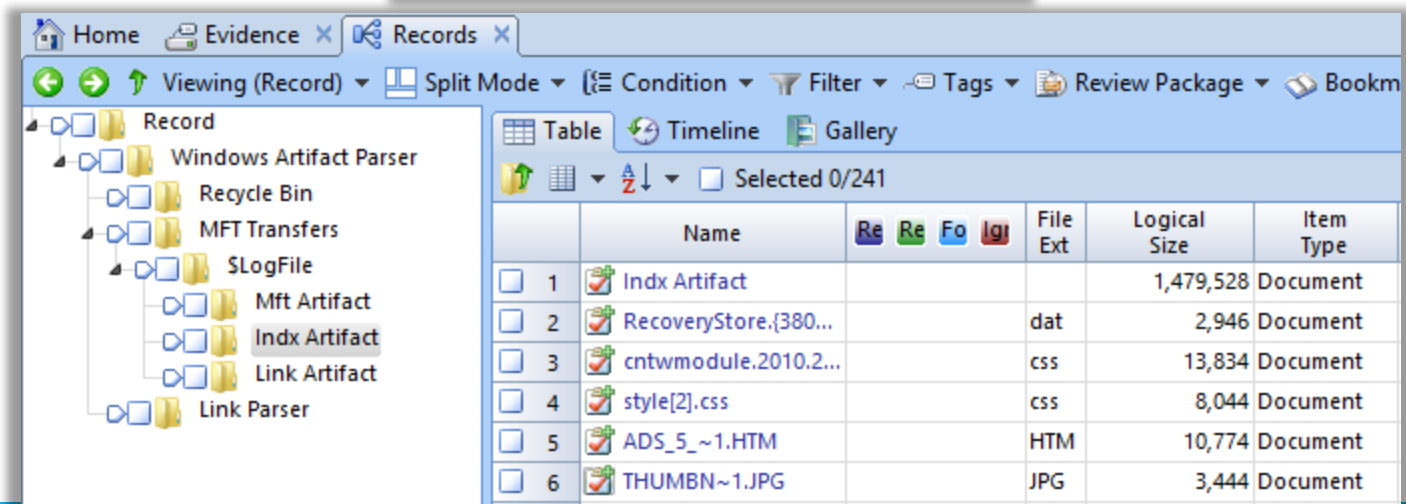
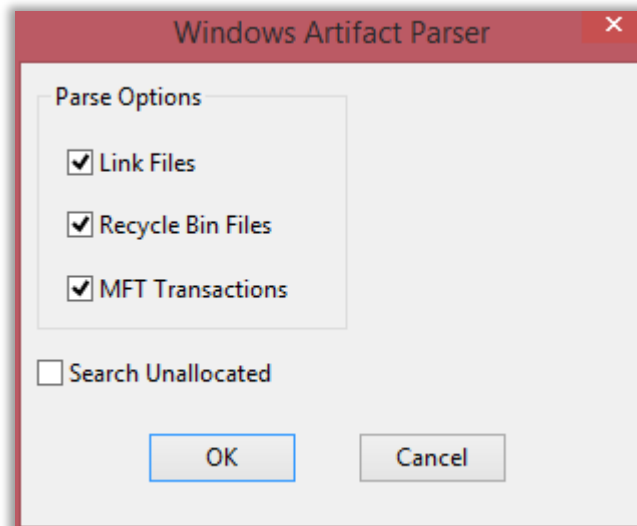


# Windows Event Log Parser

Example: only report log on events (ID = 528)



# Windows Artifact Parser

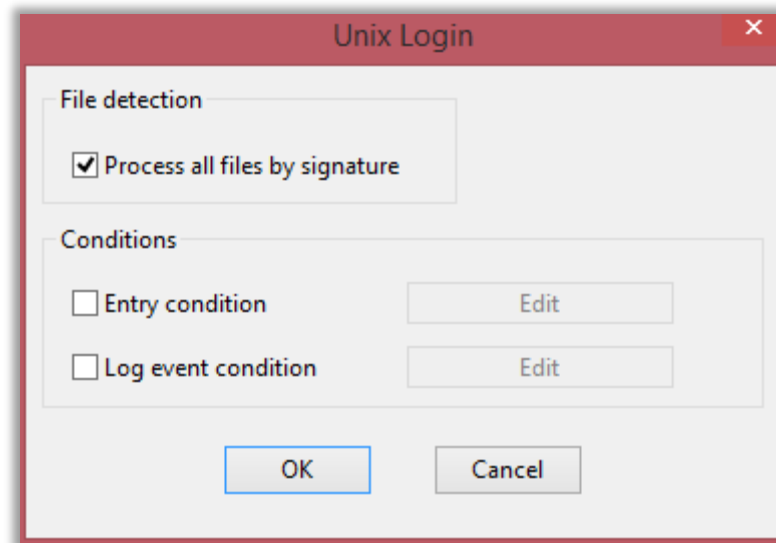


# Unix Login

---

This module parses files with the names “wtmp” and “utmp”

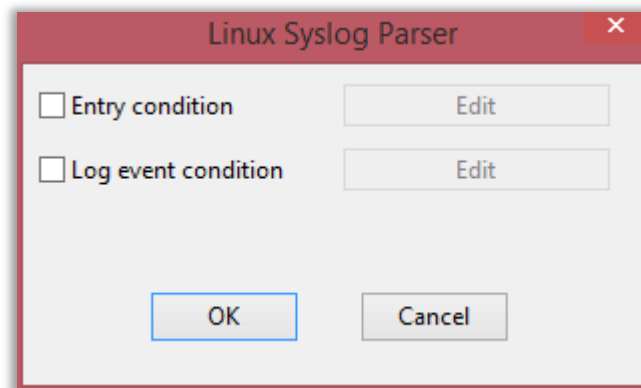
- Those files keep track of all logins and logouts to the system.



# Linux Syslog Parser

---

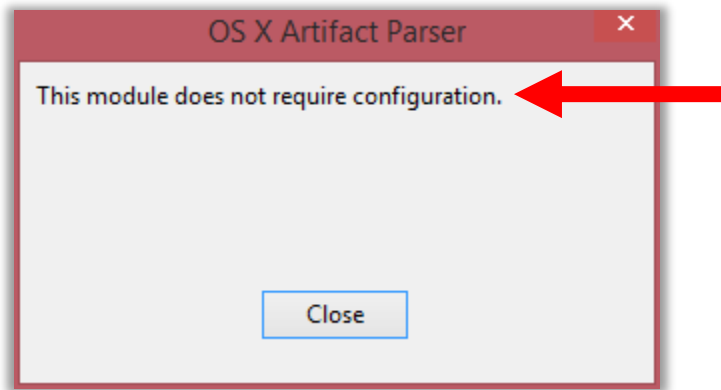
syslog is a widely used standard for message logging (you can think of it like Linux's equivalent of Windows Event logs ... sort of)



# Macintosh OS X Artifacts parser

---

Just like all other Apple products, there's not much you can do 😊



Collects Lots of very useful info: USB devices, OS version, Installation Date, Network info, User activity, Keychain (stored passwords), and many other.

# Processing Evidence

---

RESULT SETS: LIMITING THE CASE PROCESSING  
SCOPE



# Case Processing is slow...

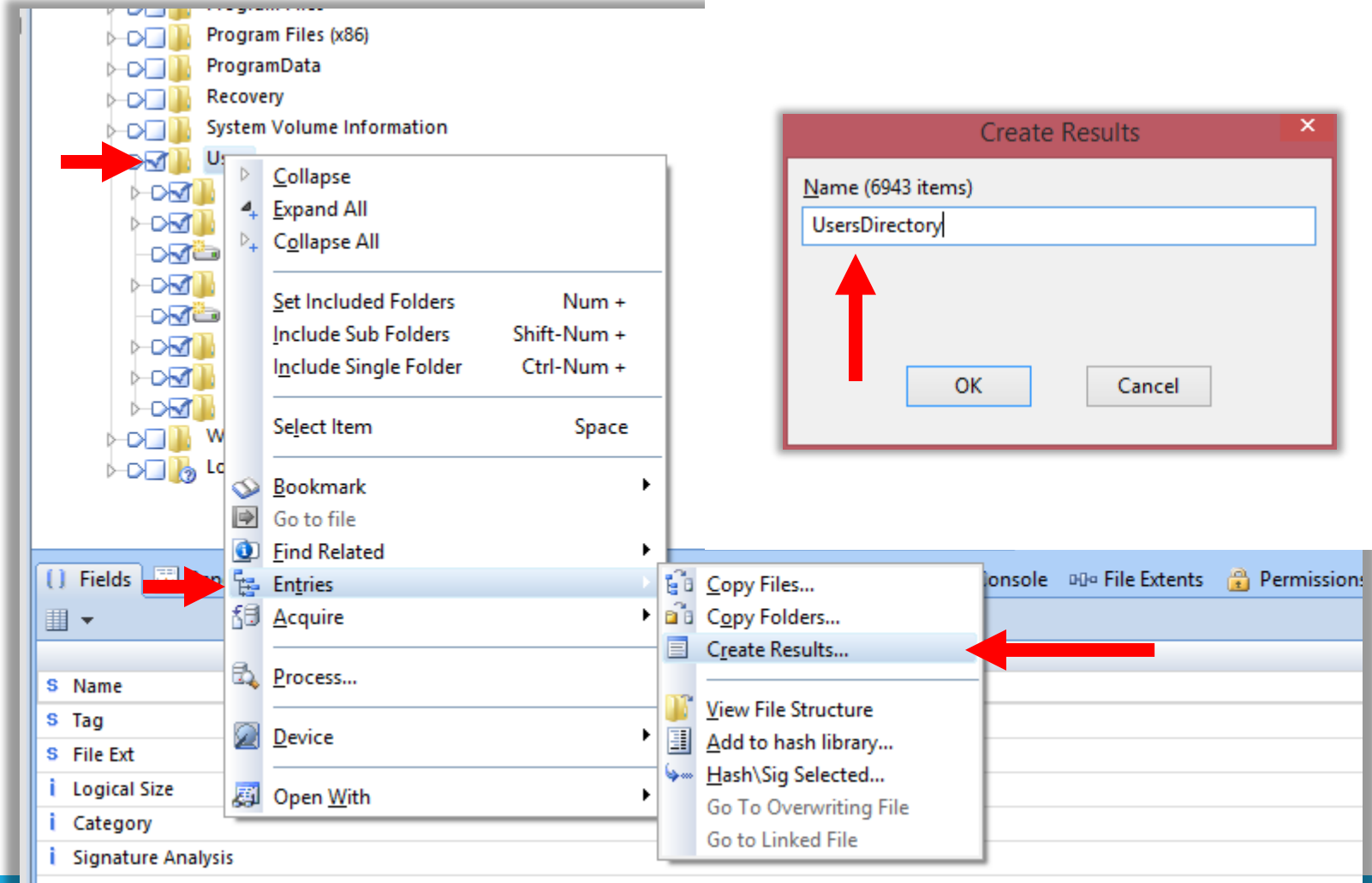
---

If you are only interested in specific items, or time frame, you can limit the “scope” of the case processor using “Result Sets”

To create a Result Set (see next slide)

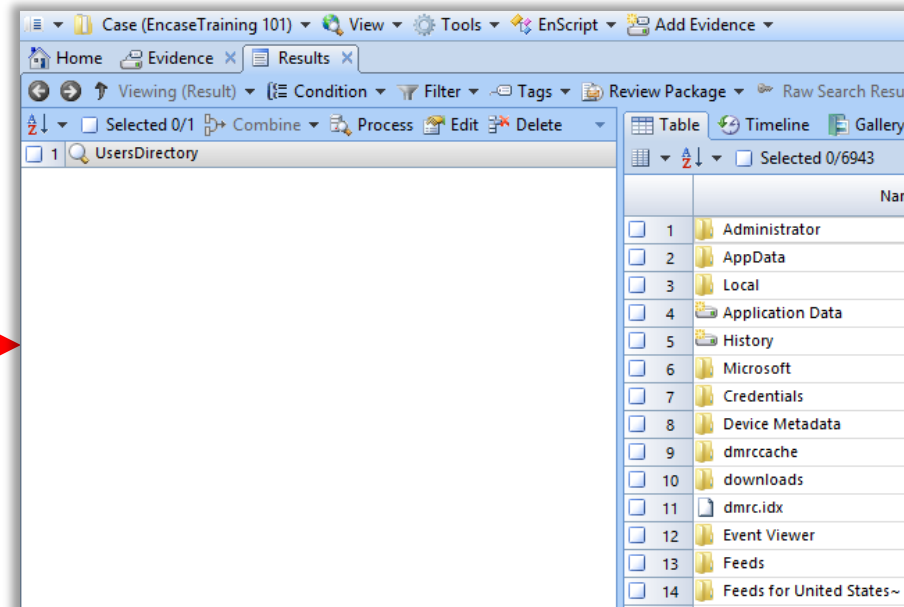
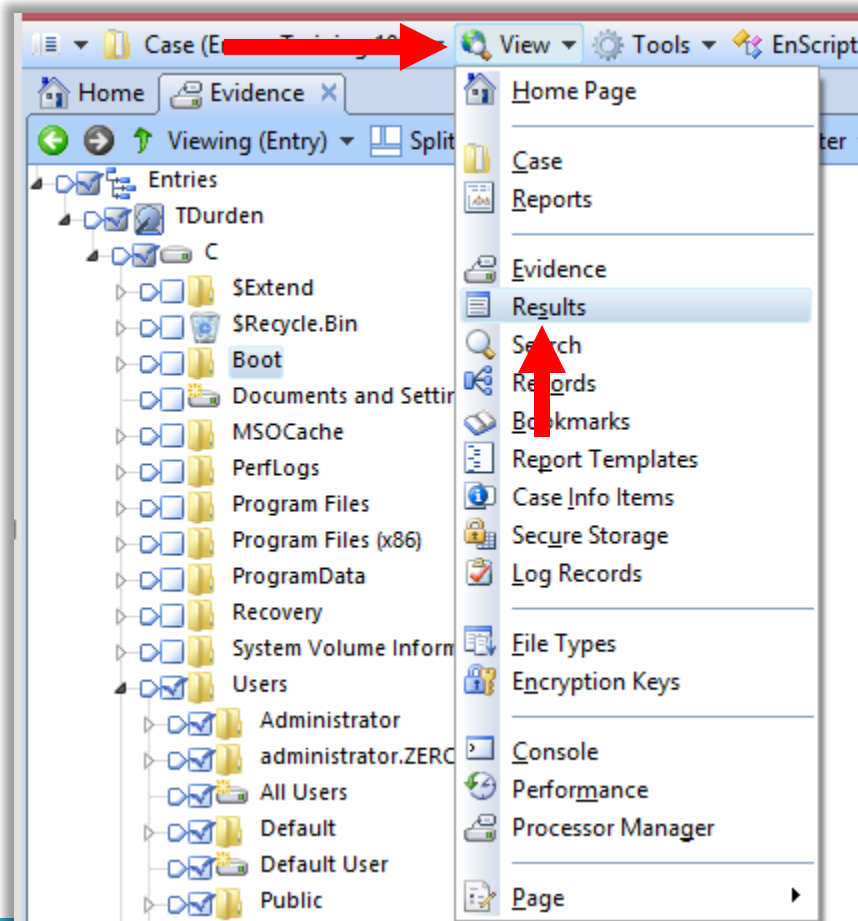
1. select the files
2. -> right click on any of them
3. -> Entries
4. -> Create Results ...
5. Call it something

# Creating Result Sets



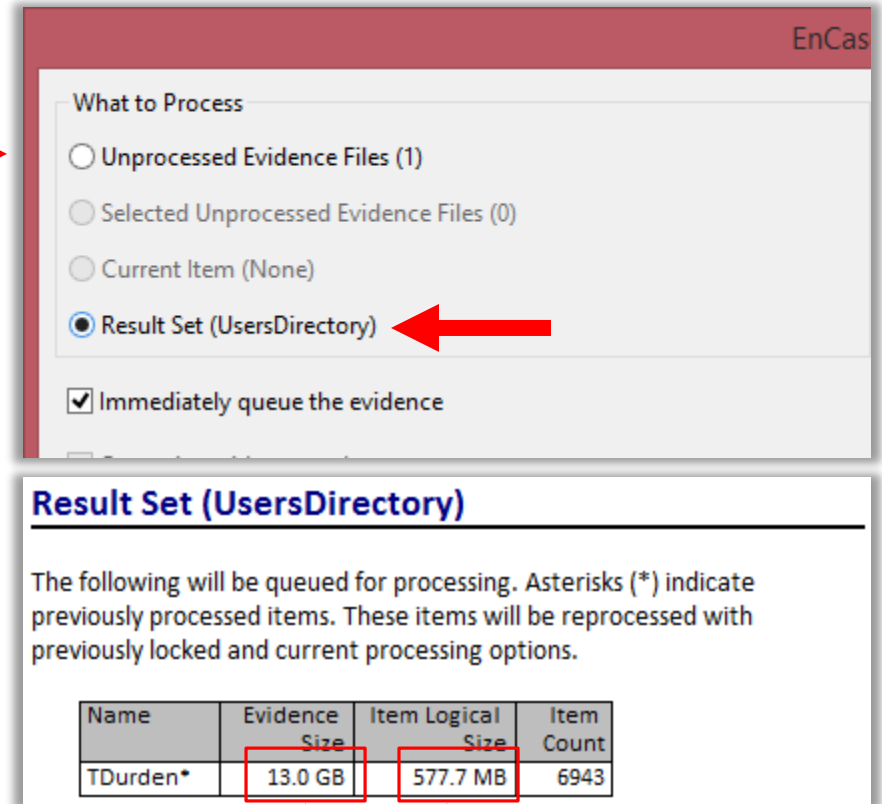
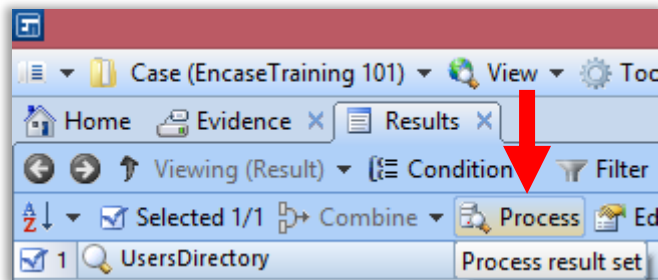
# Result Sets

To view the Result Set, click “view” -> Results



# Limit Processing to Result Sets

Select set -> Process



In this example, only 577MB out of 13GB will be processed

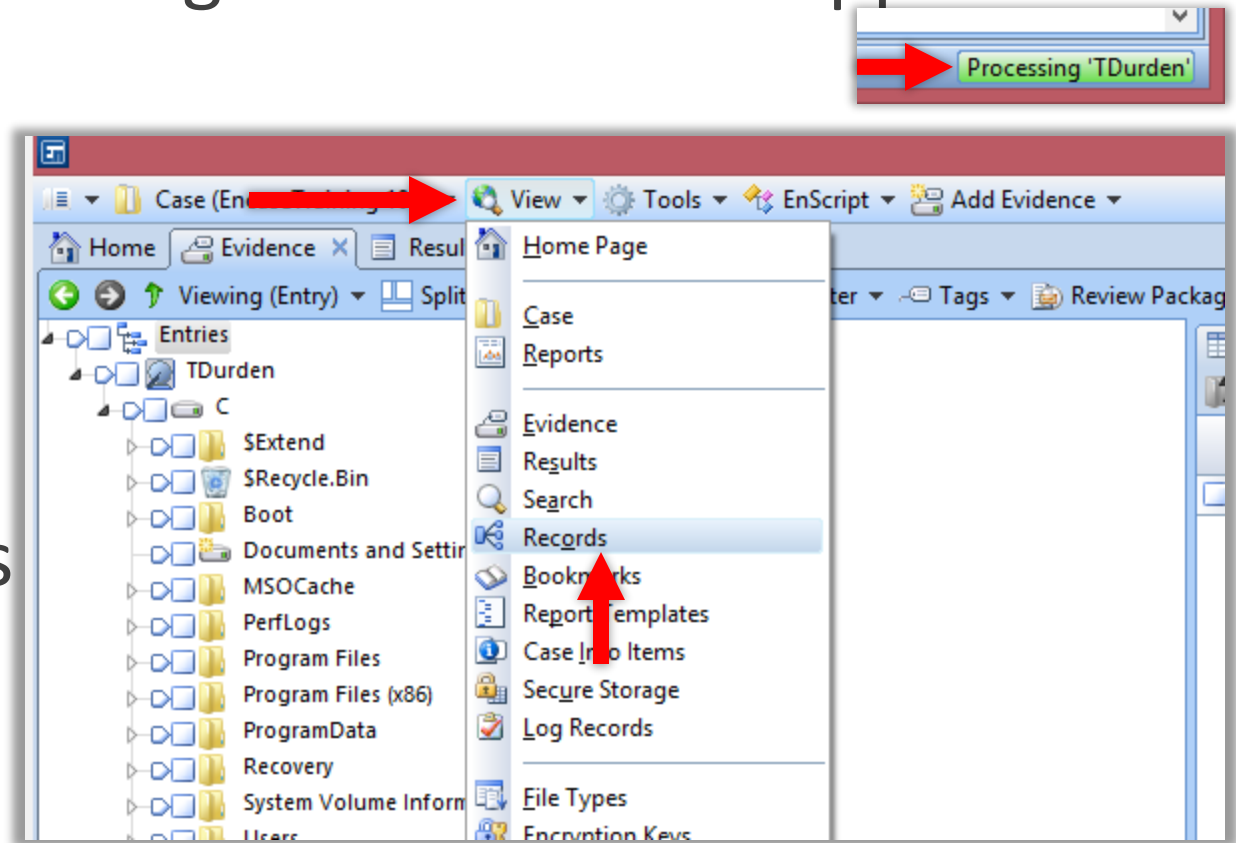
# Viewing Case Processor Results

---

# Viewing Case Processor Results

When the case is processed, an indication is at the bottom-right corner of the app.

After it is finished,  
results are under  
-> View  
--> Records



# Viewing Case Processor Results

The screenshot shows the EnCase Forensic interface. The 'Records' tab is active, displaying a table of records. The left sidebar shows the file tree with 'Internet Explorer (Windows)' > 'History' > 'Typed URL' selected. The bottom pane shows the details of the selected record.

	Name	Re	Re	Fe	Log	File Ext	Logical Size	Item Type	Categ
1	NTUSER.DAT					DAT	92	Document	Windows
2	NTUSER.DAT					DAT	50	Document	Windows
3	NTUSER.DAT					DAT	48	Document	Windows
4	NTUSER.DAT					DAT	92	Document	Windows
5	NTUSER.DAT					DAT	30	Document	Windows
6	NTUSER.DAT					DAT	38	Document	Windows

Details of the selected record (NTUSER.DAT):

- Primary Device: TDurden
- Item Path: Internet Explorer (Windows)\History\Typed URL\NTUSER.DAT
- True Path: EncaseTraining 101\TDurden\C\Users\administrator.ZEROBIT\Internet Explorer (Windows)\History\Typed URL\NTUSER.DAT
- Internet Artifact Type: History\Typed URL
- Title: url2
- Url Name: <http://cracks.am/>
- Url Host: cracks.am/
- Last Modification Time: 04/18/11 09:15:31 PM
- Browser Type: Internet Explorer (Windows)
- Profile Name: administrator.ZEROBIT
- Message Size: 38

Path: EncaseTraining 101\TDurden\C\Users\administrator.ZEROBIT\Internet Explorer (Windows)\History\Typed URL\NTUSER.DAT

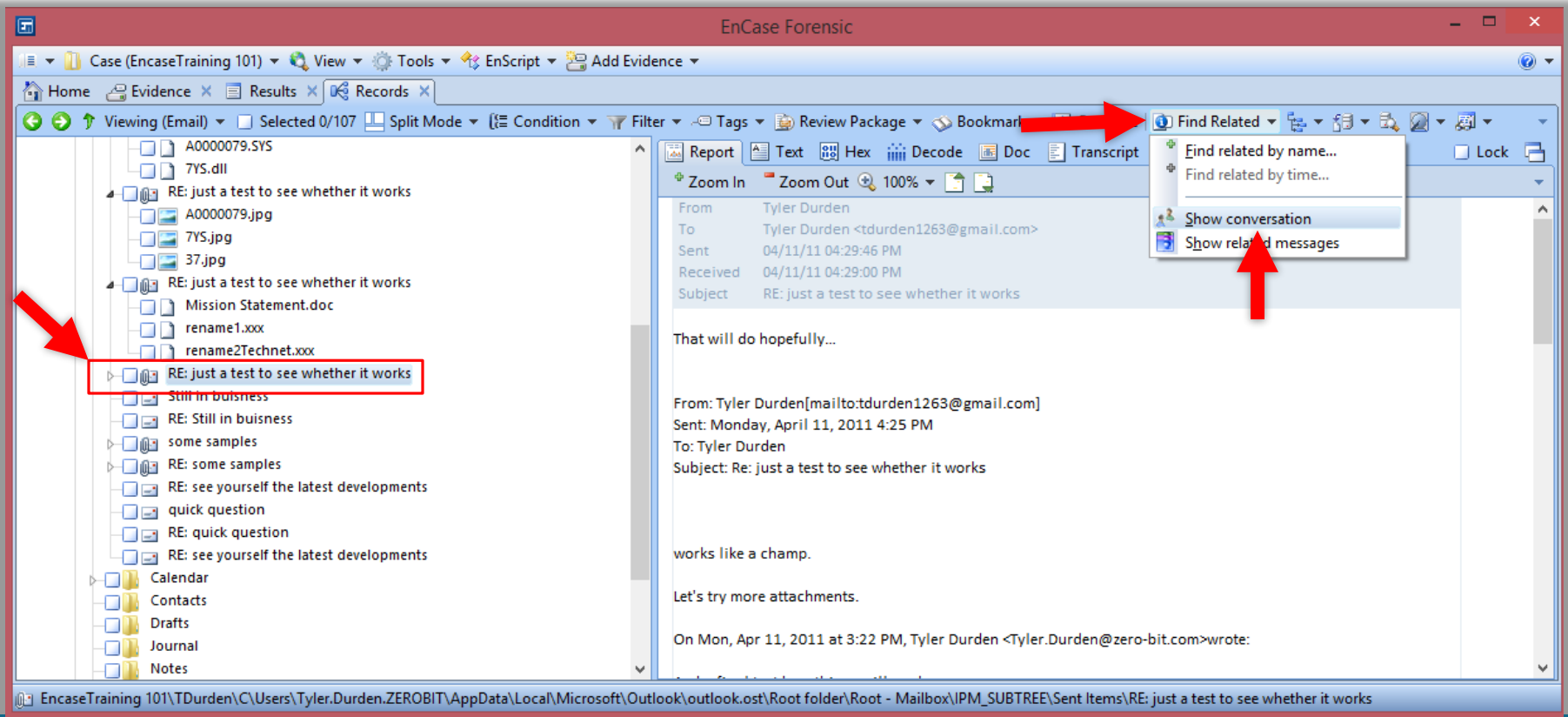
# General Useful Tricks

---

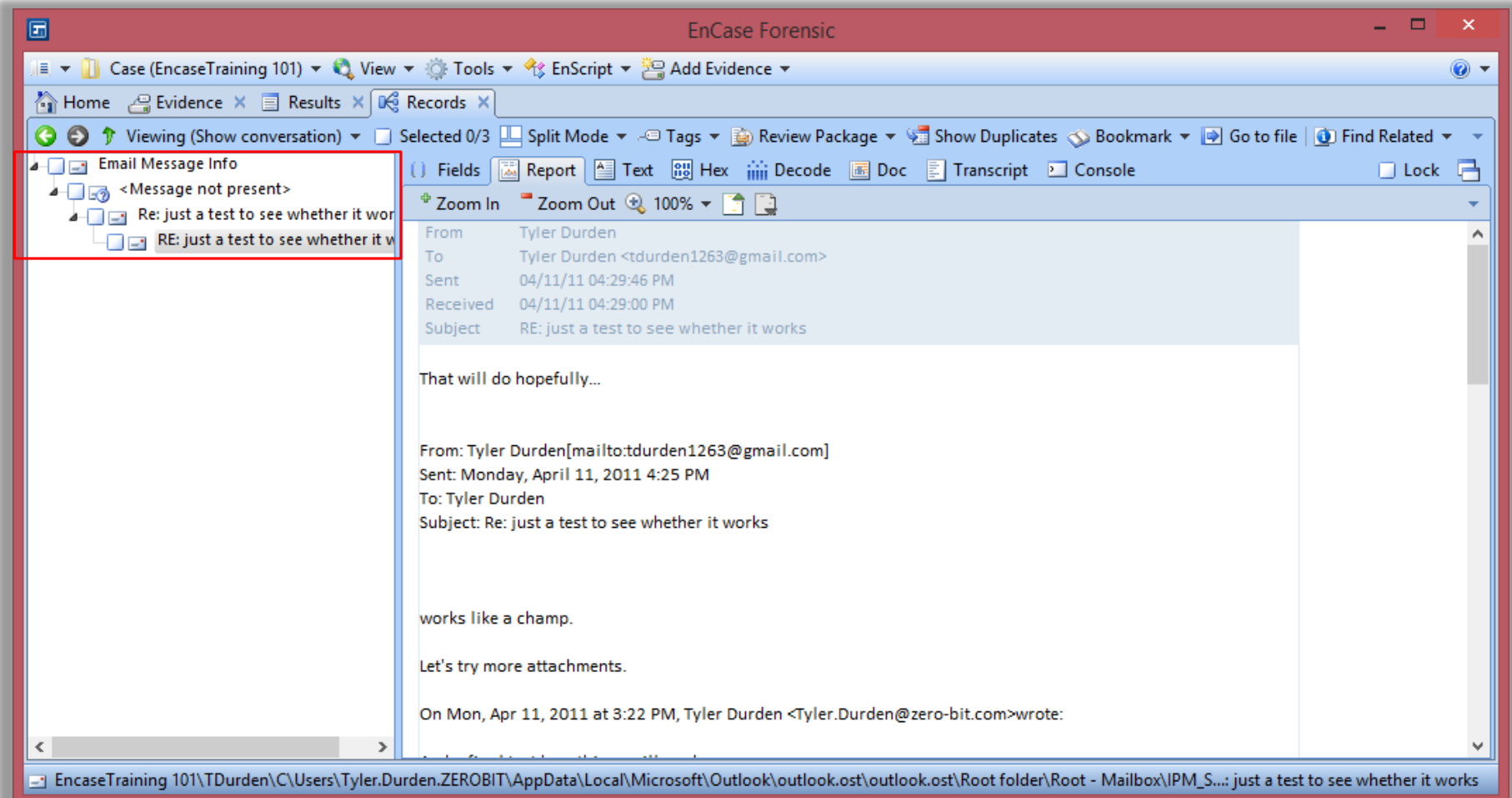


# Find Related Emails (Conversation)

You can check email “conversations” by going to “Find Related” -> Show Conversation

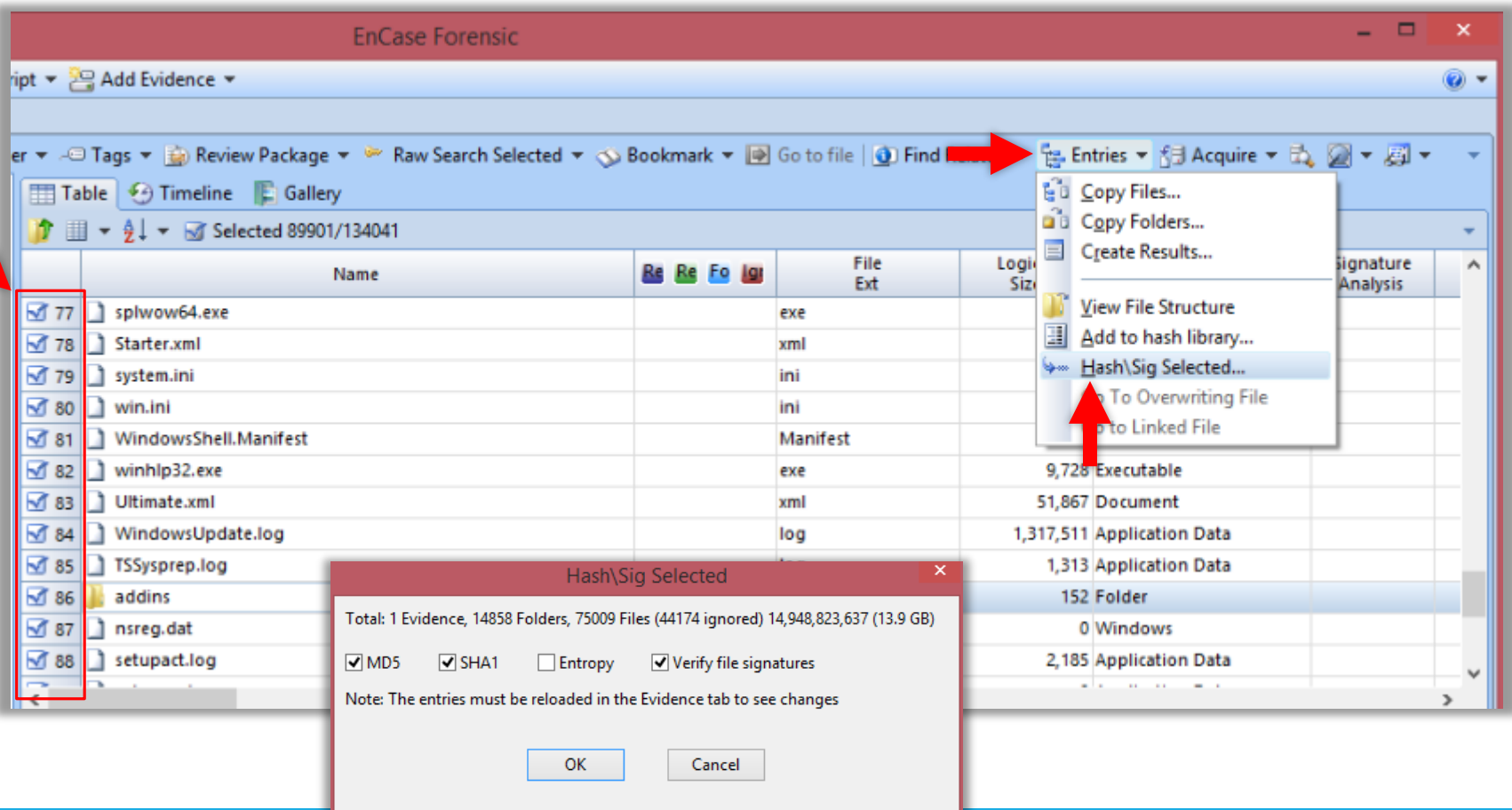


# Find Related Emails (Conversation)



# Hash only selected files

Select the files → “Entries” → “Hash\Sig Sel...”



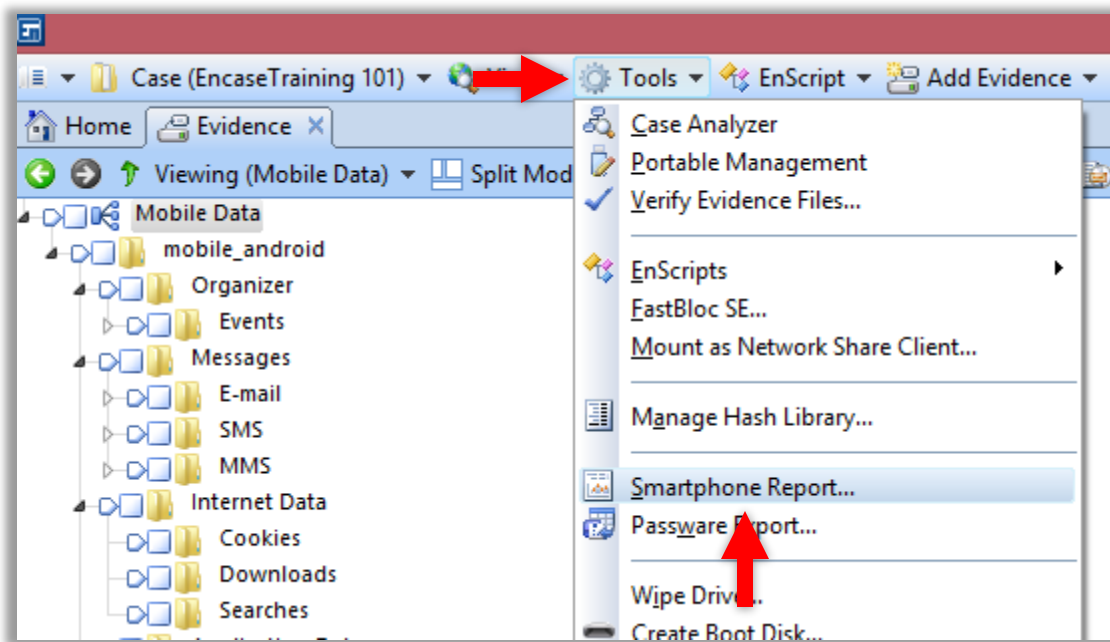
# Smartphone Reports

---

# Smartphone Reports

Creating reports for smartphone information using EnCase couldn't be easier

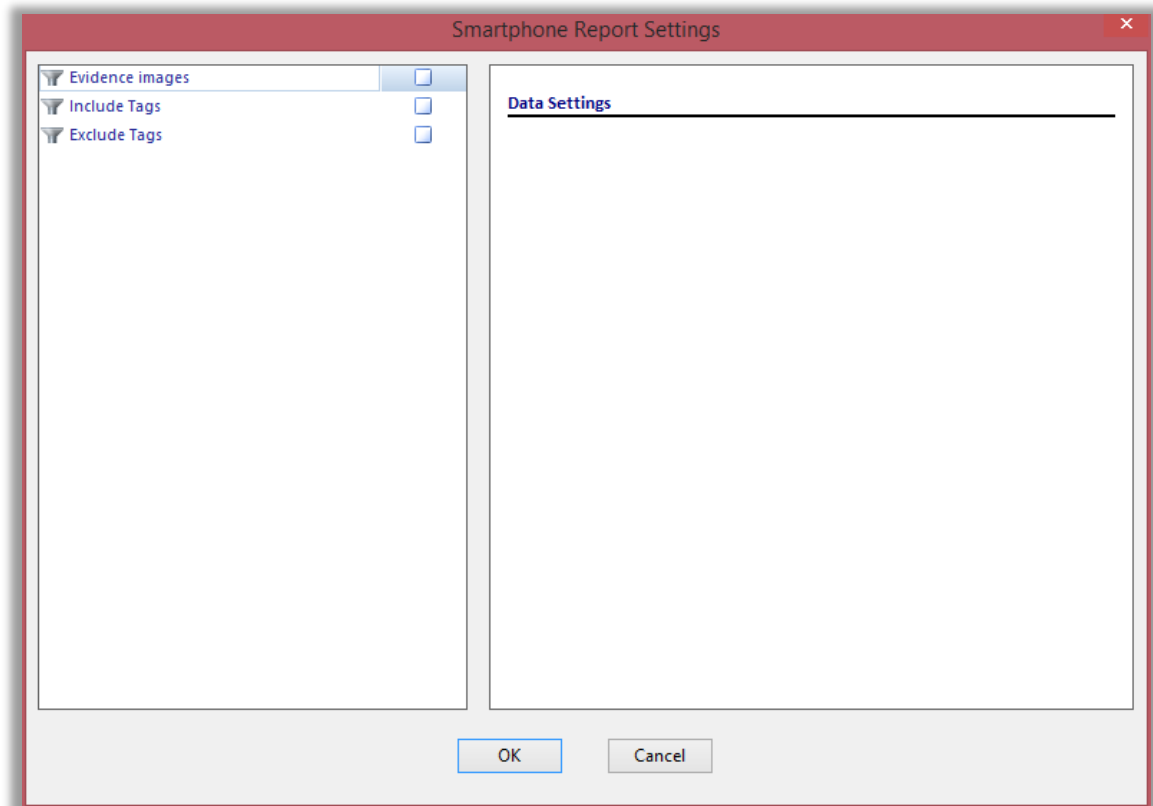
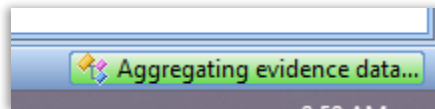
- Tools → Smartphone Report ...



# Smartphone Reports

`Tags` are explained in “Chapter 12” in user manual (and will be explained in next course, God willing)

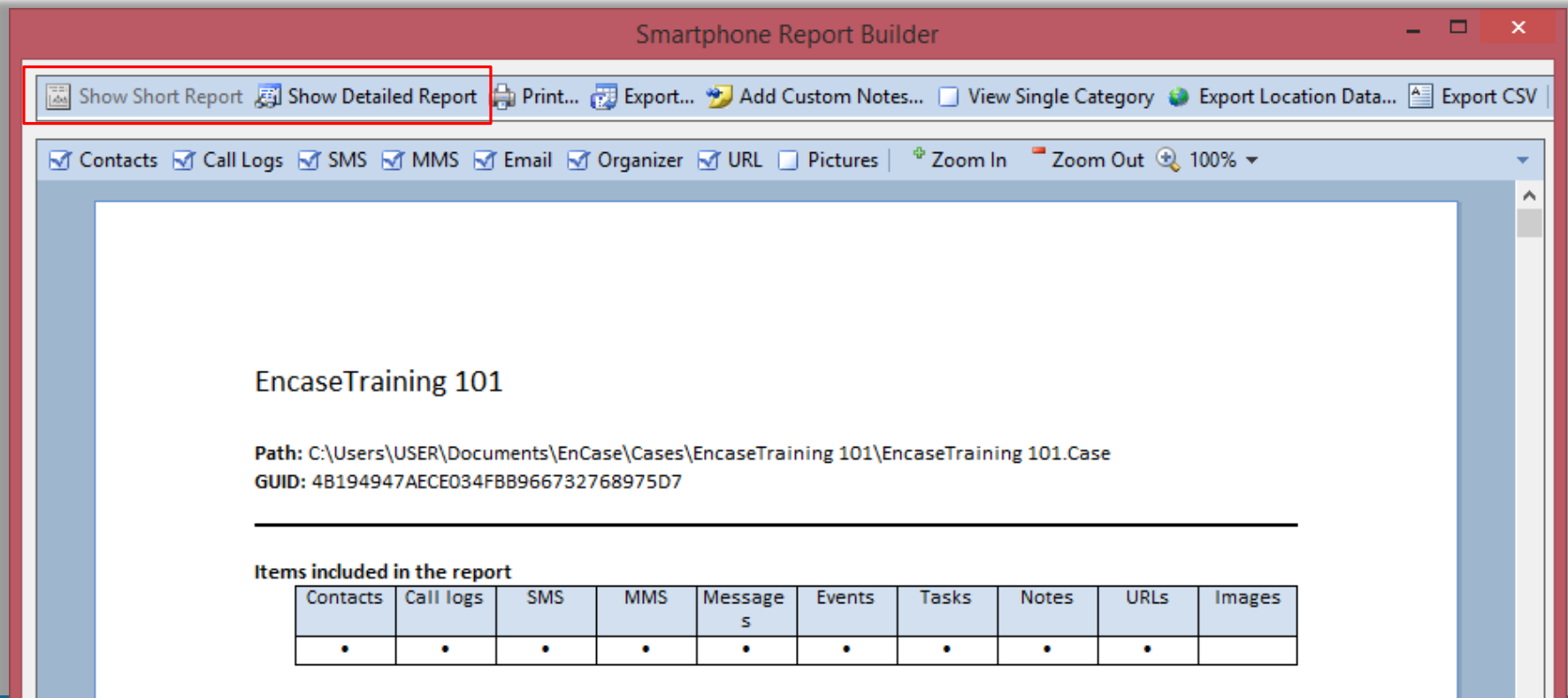
`OK` and it will work for a while.



# Smartphone Reports

Reports could be “Short” or “detailed”

You can pick what to be included



# Smartphone Reports


Smartphone Report Builder

Show Short Report Show Detailed Report Print... Export... Add Custom Notes... View Single Category Export Location Data... Export CSV

Contacts Call Logs SMS MMS Email Organizer URL Pictures Zoom In Zoom Out 100%

Title: My Contacts

Contact Name	Phone Numbers	E-mail
Pa [REDACTED]		p[REDACTED]@gmail.com(1)

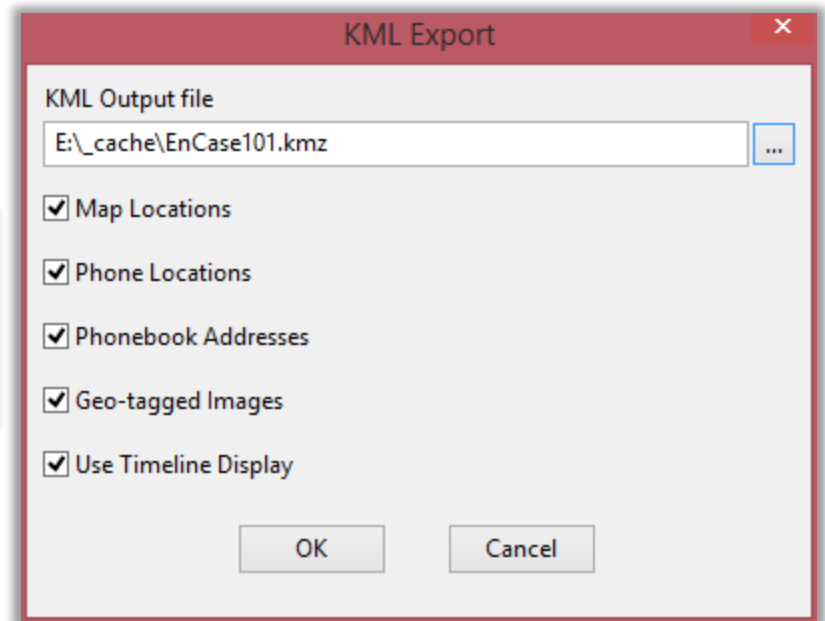
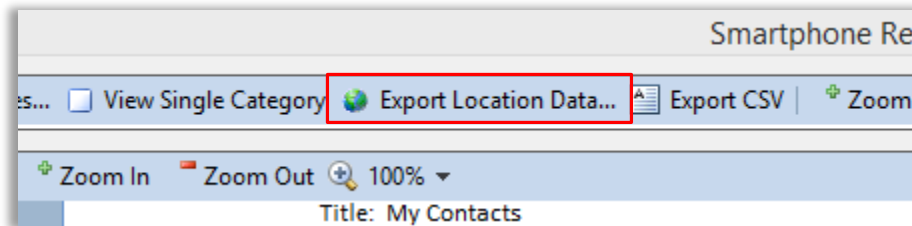


Name: Pa [REDACTED]  
INTERNET E-mail: ps[REDACTED]@gmail.com  
Times Contacted: 0  
Sync: [https://www.google.com/m8/feeds/contacts/\[REDACTED\]base2\\_property-android\\_linksto-gprofiles\\_highresphotos/22fa7f70e69d89a](https://www.google.com/m8/feeds/contacts/[REDACTED]base2_property-android_linksto-gprofiles_highresphotos/22fa7f70e69d89a)  
Given Name: P[REDACTED]  
Surname: [REDACTED]  
Name: Pa [REDACTED]  
Title: My Contacts  
File Name: Picture.jpg  
File Length: 7216  
File Type: File



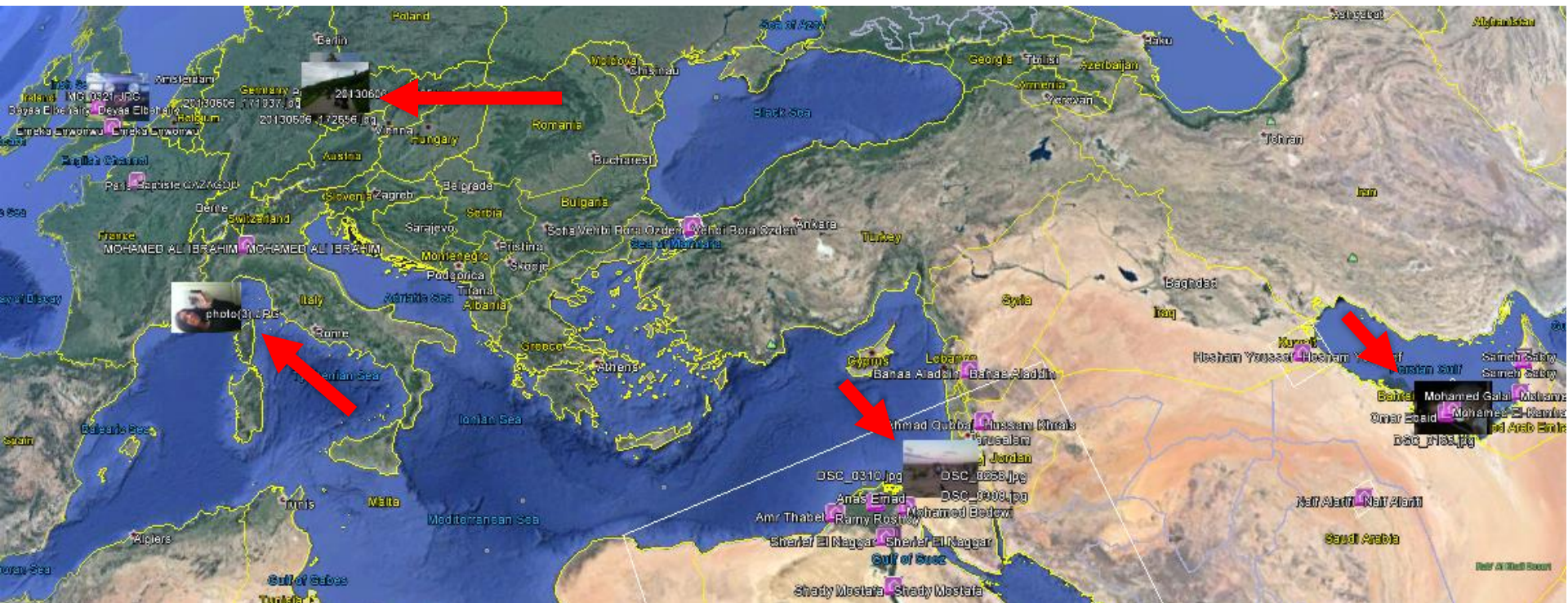
# Geo Location Data

EnCase parses all location-related information from several sources, then allows for export to KMZ file which can be viewed on Google Earth



# Geo Location Data

Photos and icons will be placed on their exact locations



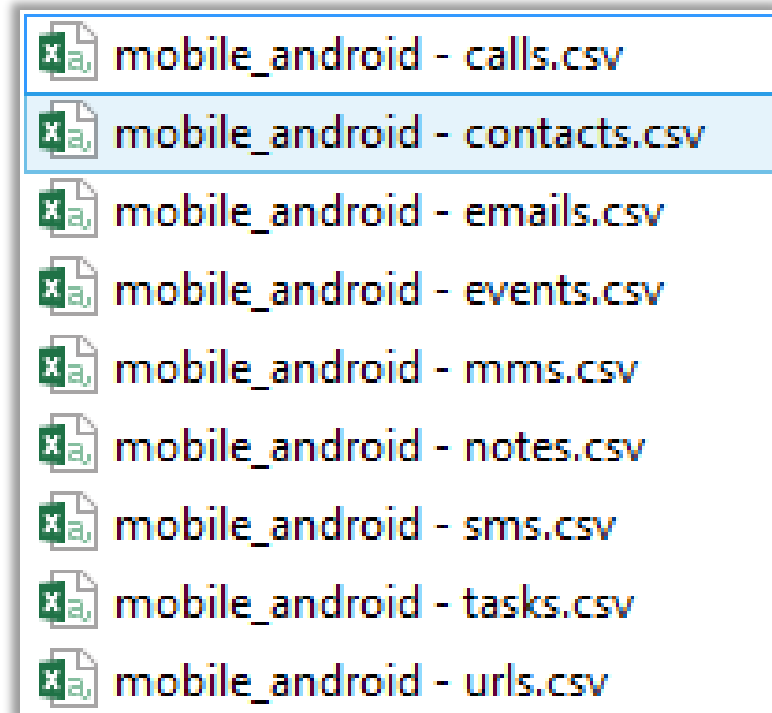
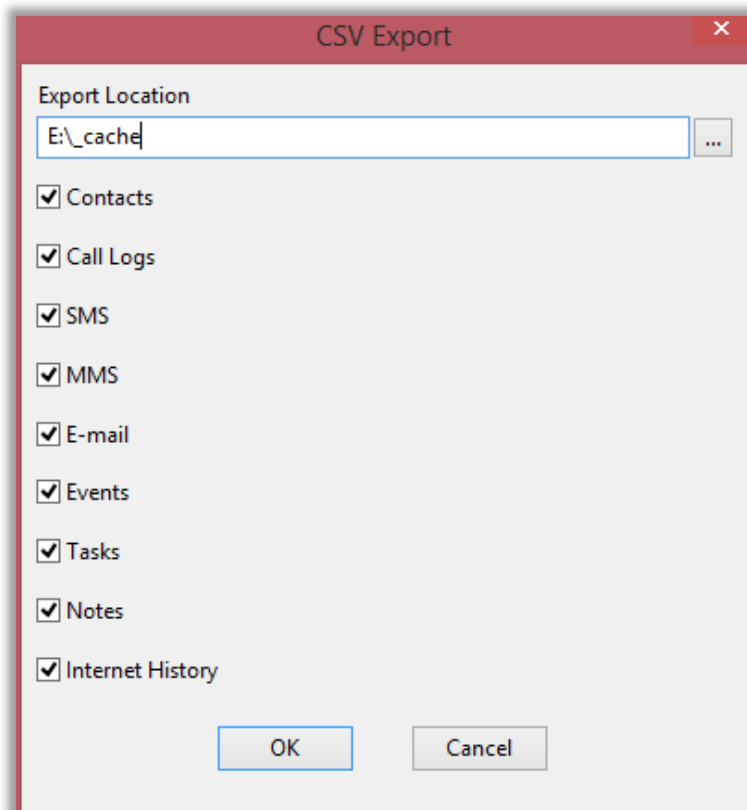
# Geo Location Data

Clicking on a picture/link reveals more info



# Export to CSV

Data could be exported as CSV for further dissemination using other tools



# The forensic challenge

---



تم بحمد الله

---

Sherif Eldeeb

<https://eldeeb.net>

@SheriefEldeeb