SANS

www.sans.org

FORENSICS 408

COMPUTER FORENSIC ESSENTIALS

408.2

Evidence Acquisition and Analysis

The right security training for your staff, at the right time, in the right location.

SANS

www.sans.org

FORENSICS 408

COMPUTER FORENSIC ESSENTIALS

408.2

Evidence Acquisition and Analysis

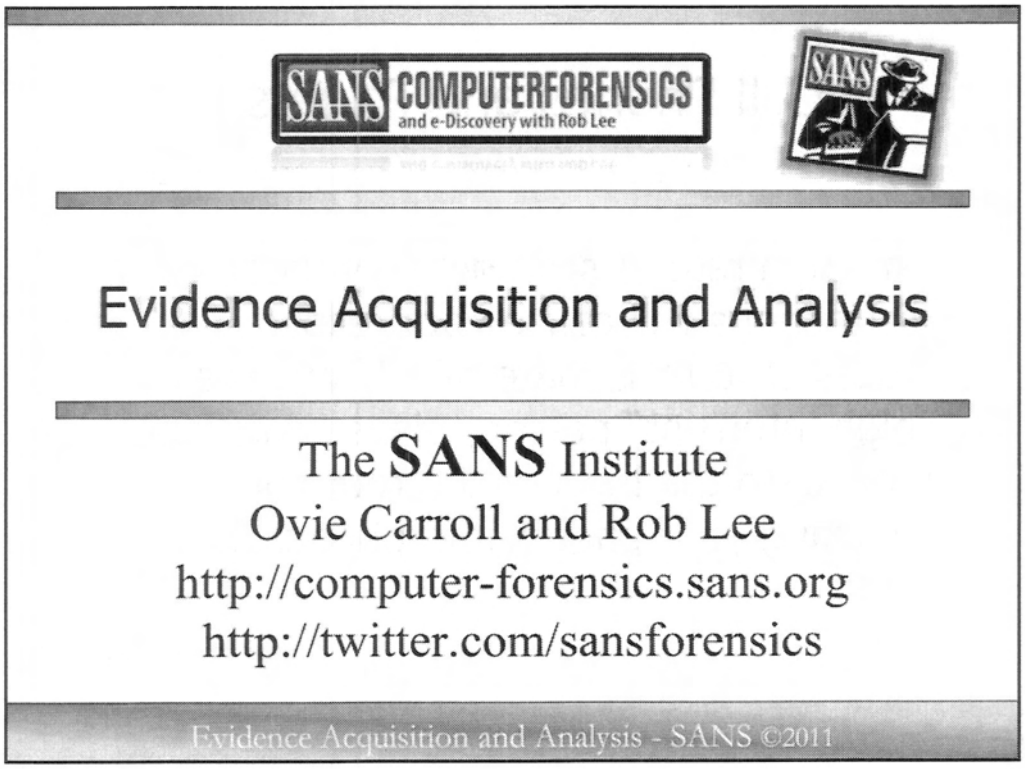
The right security training for your staff, at the right time, in the right location.

IMPORTANT-READ CAREFULLY:

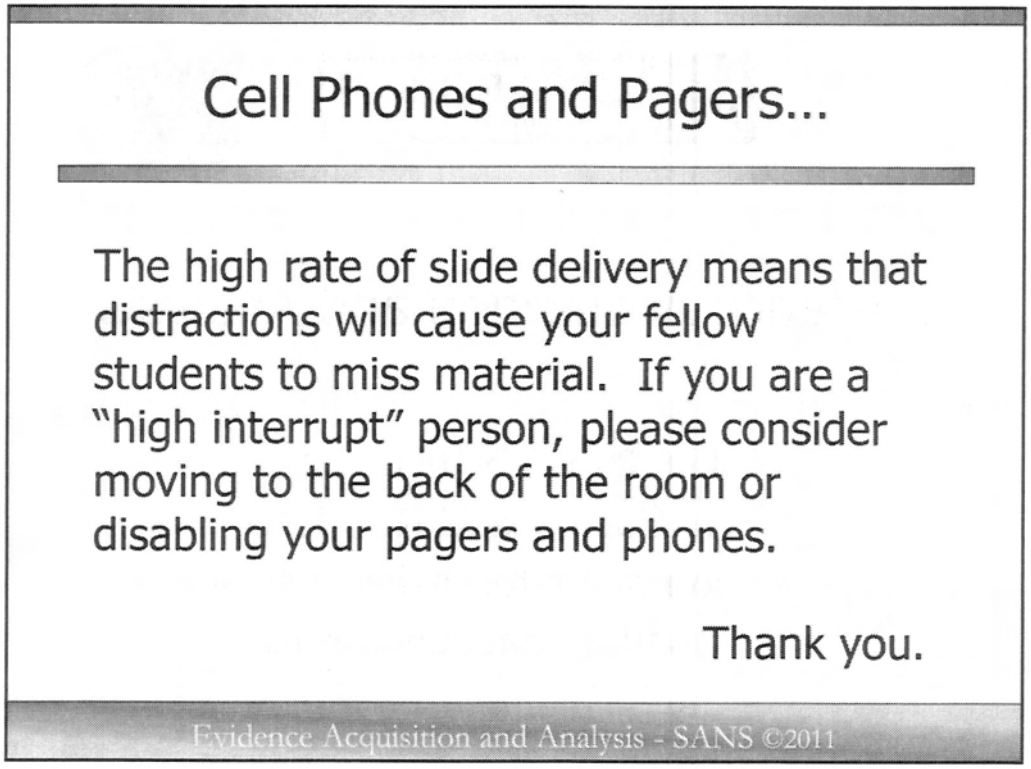
This Courseware License Agreement ("CLA") is a legal agreement between you (either an individual or a single entity; henceforth User) and the SANS Institute for the personal, non-transferable use of this courseware. User agrees that the CLA is the complete and exclusive statement of agreement between The SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA. If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this courseware. BY ACCEPTING THIS COURSEWARE YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. IF YOU DO NOT AGREE YOU MAY RETURN IT TO THE SANS INSTITUTE FOR A FULL REFUND, IF APPLICABLE. The SANS Institute hereby grants User a non-exclusive license to use the material contained in this courseware subject to the terms of this agreement. User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of this publication in any medium whether printed, electronic or otherwise, for any purpose without the express written consent of the SANS Institute. Additionally, user may not sell, rent, lease, trade, or otherwise transfer the courseware in any way, shape, or form without the express written consent of the SANS Institute.

The SANS Institute reserves the right to terminate the above lease at any time. Upon termination of the lease, user is obligated to return all materials covered by the lease within a reasonable amount of time.

V2011_0228

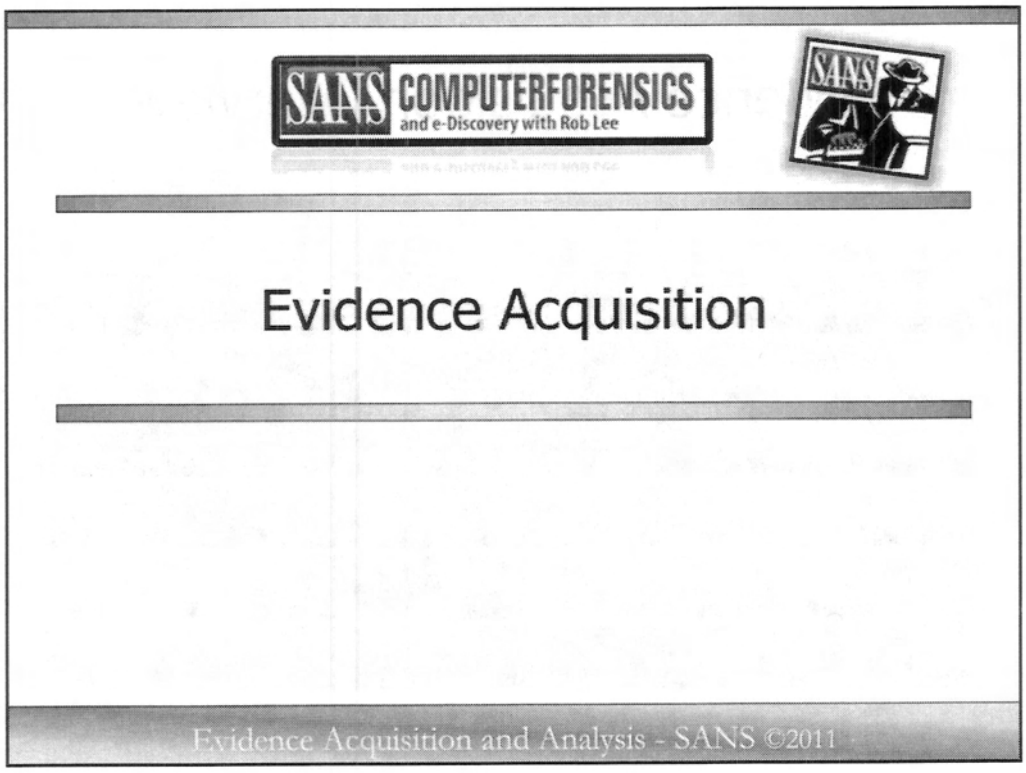


Rob Lee
rlee@sans.org
http://twitter.com/robtlee
http://twitter.com/sansforensics

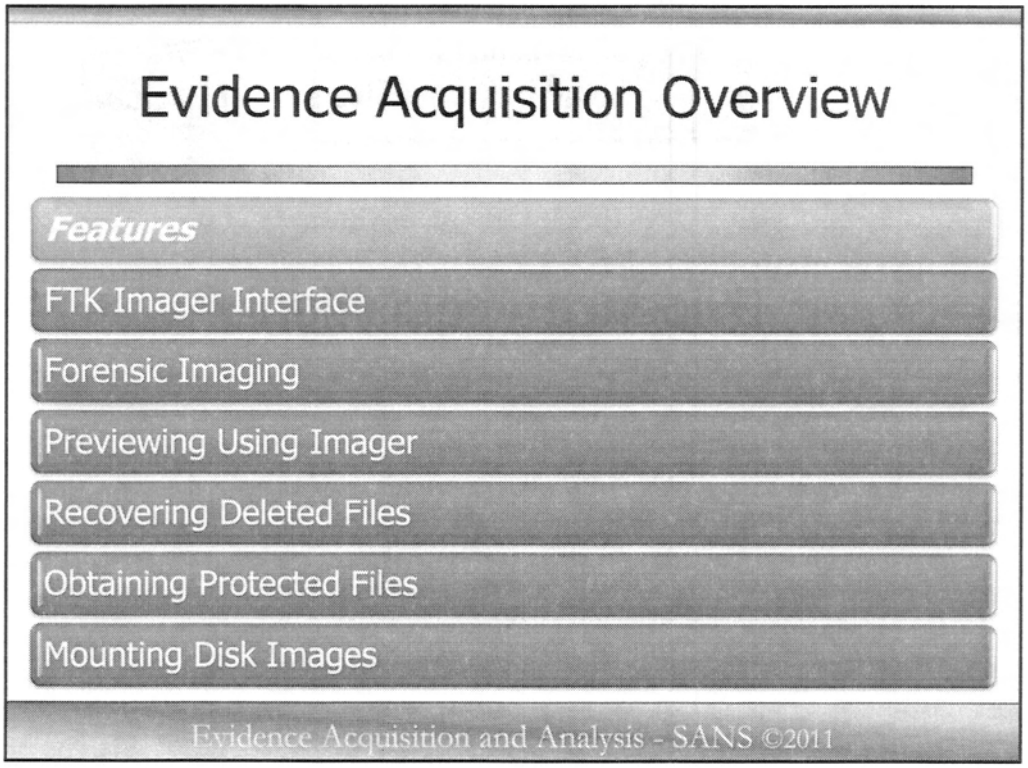


Please know that I understand the need to stay "connected", especially in the positions that we hold. However, we will be covering quite a bit of material today, and cell phone/pager interruptions do cause your neighbor to miss material. Most pagers and cell phones have a "vibrate" setting. Please use this feature during your class time at SANS. If you must answer an important call, the best way to do it is to quietly go out into the hallway and conduct business there.

I thank you, and the person sitting next to you does too! ☺



This page intentionally left blank.



In many cases when you are first assigned to a computer crime lab or office, one of the first duties you will be assigned to is the imaging team. This is because imaging is the foundation of incident response and computer forensic analysis. So in this session we are going to be discussing the FTK Imager.

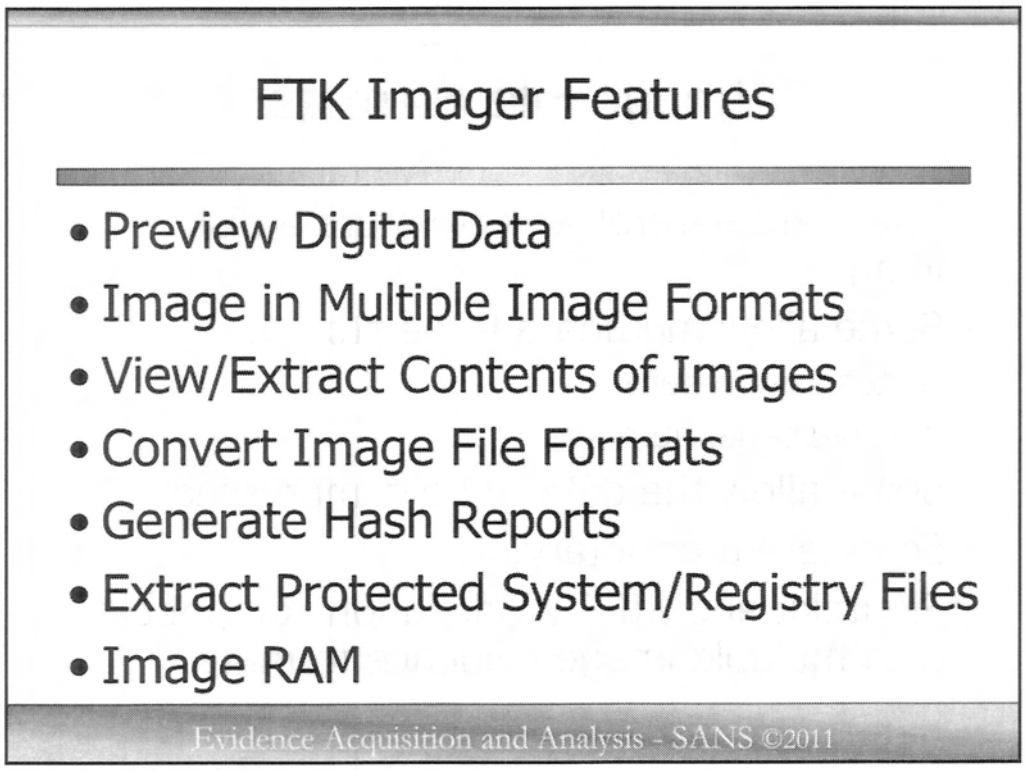
There are many forensic imaging tools available to the forensic investigator, but one of the leaders in this field is Access Data's FTK Imager.

The FTK imager is a free download. What makes FTK Imager such a powerful, yet light weight tool (not to mention my favorite imaging tool) are the capabilities it has in such a small package.

The installation of FTK Imager is very straightforward. You simply accept all the defaults. Rather than having you install FTK Imager, we have already installed it inside your SANS Investigative Forensic Toolkit (SIFT).

In a few minutes we will go over and discuss the most popular features of FTK Imager version 3.0, we will then show you how to use FTK Imager as a lightweight forensic recovery tool you can use on scene or back at the lab.

As you would expect, we will also go through the process of creating a forensic image and finally, we will show you how you can obtain protected registry files on a running computer.

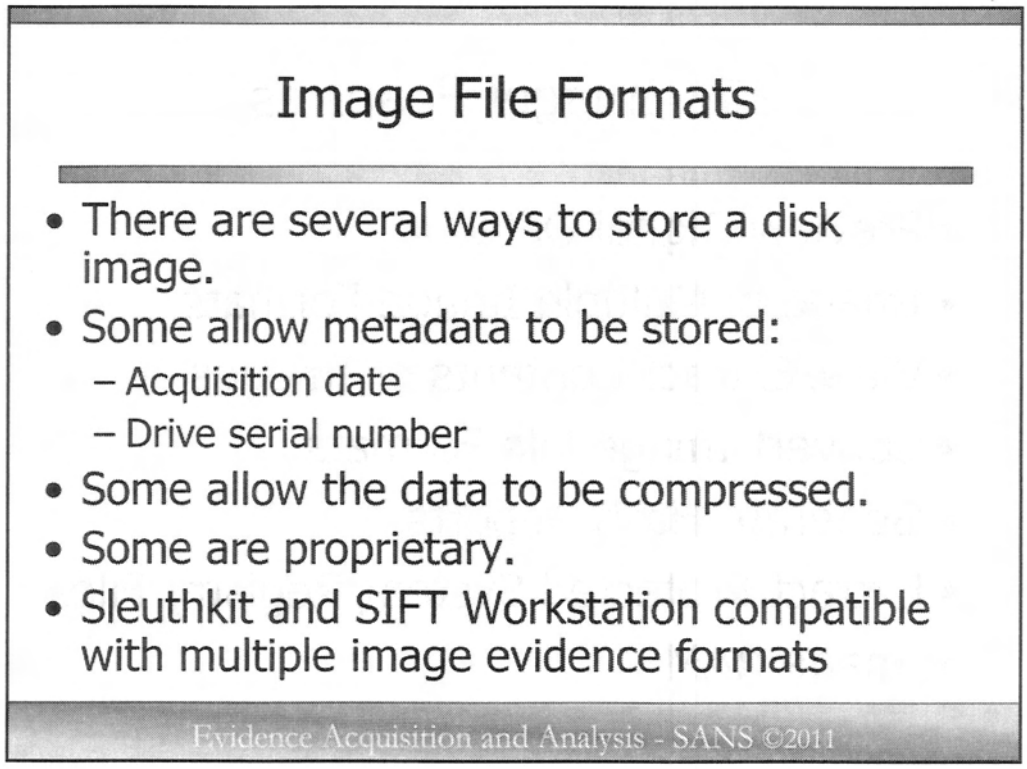


What makes FTK Imager my favorite forensic imaging tool is that it is so feature rich while being very compact and portable. The full version of FTK Imager 3.0 is only 60.5 MB and FTK Imager Lite Version 2.9.0 is only 44.2 MB.

The first of FTK Imager's features is its ability to review digital evidence. This powerful preview feature gives the investigator the ability to:

- Triage digital evidence
- View and extract deleted files
- Determine if the digital device warrants being imaged and a full analysis conducted.
- FTK Imager can convert other image file formats such as converting an EnCase E01 to a DD or SMART image
- Extract protected system files such as Registry Files or System Volume Information (location of the restore point files) directory from live system
- Image RAM on Windows 32 bit operating system

FTK Imager runs standalone, full-featured without a dongle.



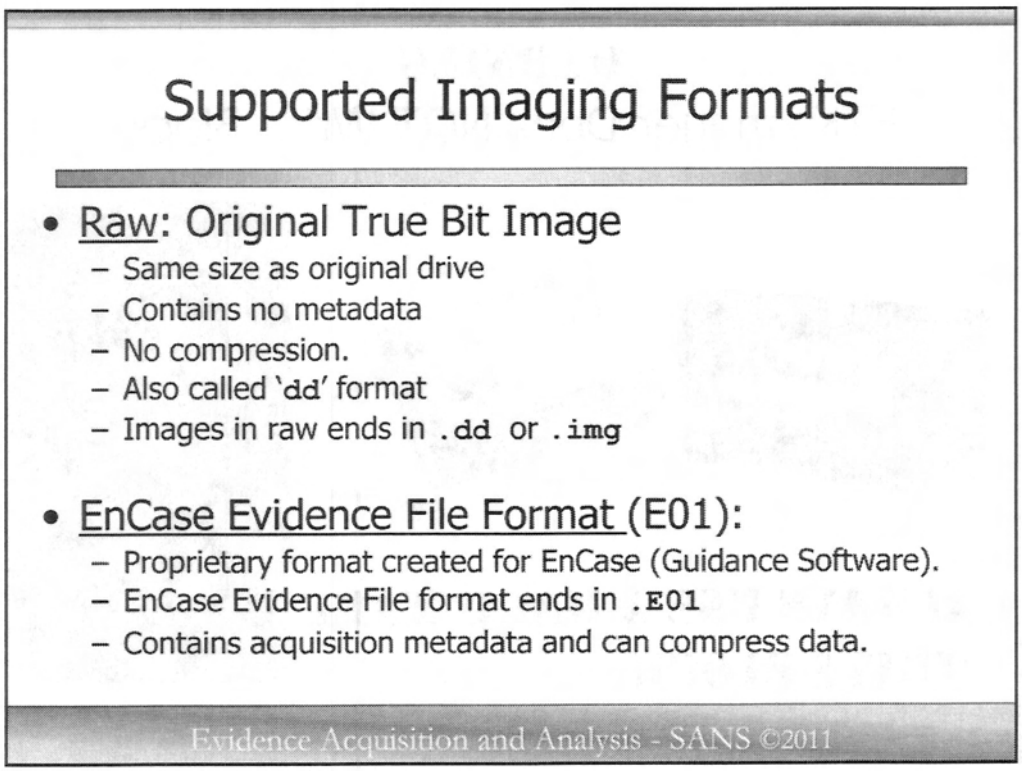
Regardless of how much data you copy from the hard disk, you must store the data somewhere. There are several formats that can be used. The major differences between the formats are based on whether or not you can store metadata, can compress the data, and if the format is open and published.

Examples of metadata that can be stored include the start and finish date and time of the acquisition, the version of FTK Imager used, the source drive serial number and geometry. Some formats allow notes to be recorded as well.

Compression can be used to make the stored data smaller. This helps fit more disk images on a storage disk, but it typically makes the acquisition longer because the computer must compress the data.

Finally, there is a difference between proprietary and open formats. Open formats allow you to use the disk images in different tools, whereas proprietary formats may limit what you can do with the data. The Digital Forensic Research Workshop (DFRWS) has the Common Digital Evidence Storage Format (CDESF) working group to define standards for open digital evidence storage formats:

http://www.dfrws.org/



One of the things that make FTK Imager many investigators imager of choice is that it can create almost any kind of image file format. Additionally, FTK Imager can convert any of these image formats into other formats. This can come in real handy when a defense attorney or expert says they cannot read an EnCase E01 image file. You can either convert it for them into a DD image or provide them instructions on how they can use FTK Imager and convert the image into any forensic format they would like.

The two primary image file formats you will deal with in your forensic career are:

E01 – Encase Evidence File Format – Industry Standard

.001 or .dd or .img – Data dump – DD File Format

FTK Imager also supports imaging in the following formats but you really don't need to worry about them.

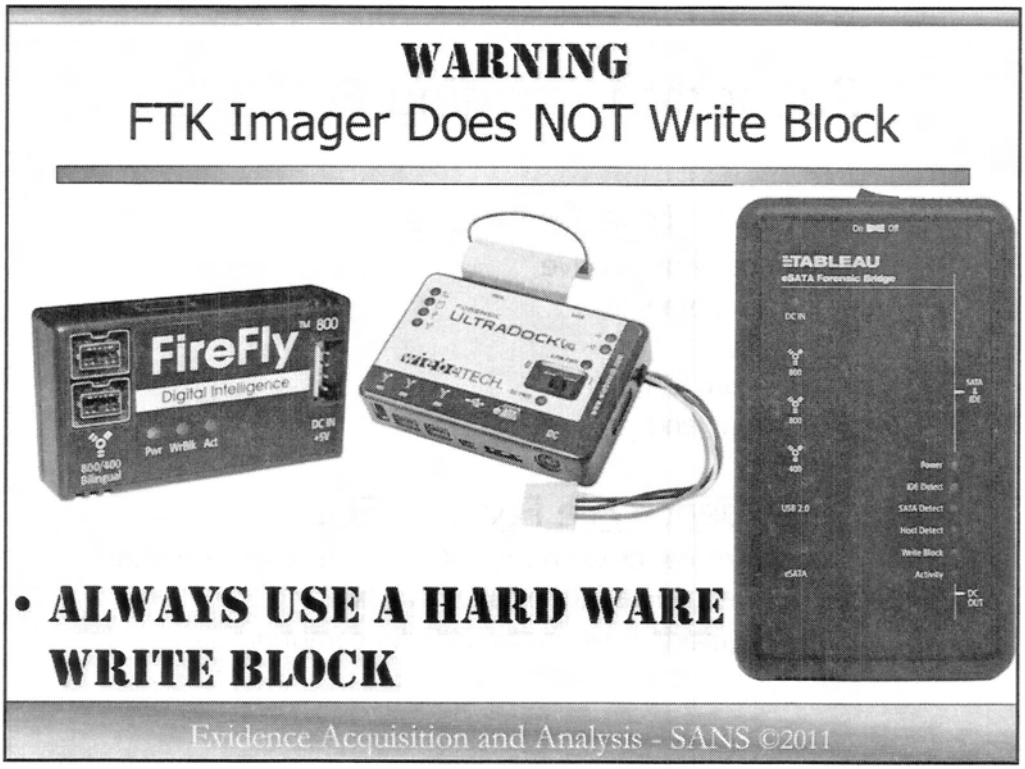
S01 – Smart – Andy Rosen's SMART technology

CUE – ISO buster

ISO – ISO BUSTER

AD1 – Access Data Proprietary Format – Great for targeted imaging rather than full drive imaging

AFF – Advanced File Format is an extensible open format created by Simson Garfinkel and Basis Technology for the storage of disk images and related forensic metadata.



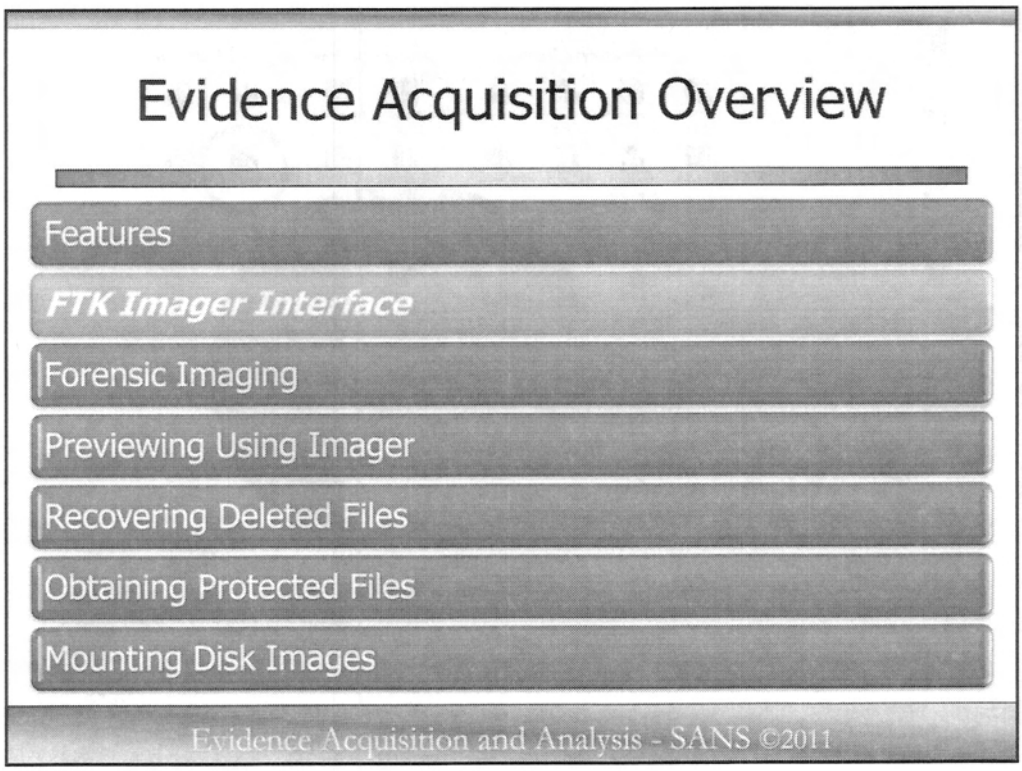
FTK Imager does not write protect.

To show you a few of the most common write blockers found in the field, starting from the left,

Digital Intelligence FireFly – the smallest of the write blocking devices. To be able to image either IDE and SATA drives, you would have to carry two of these devices because each FireFly device supports only one interface type. Additionally, the connectivity to your forensic system is limited to a FireWire 800 connector. You can use an 800-to-400 converter, but you are still limited to FireWire out.

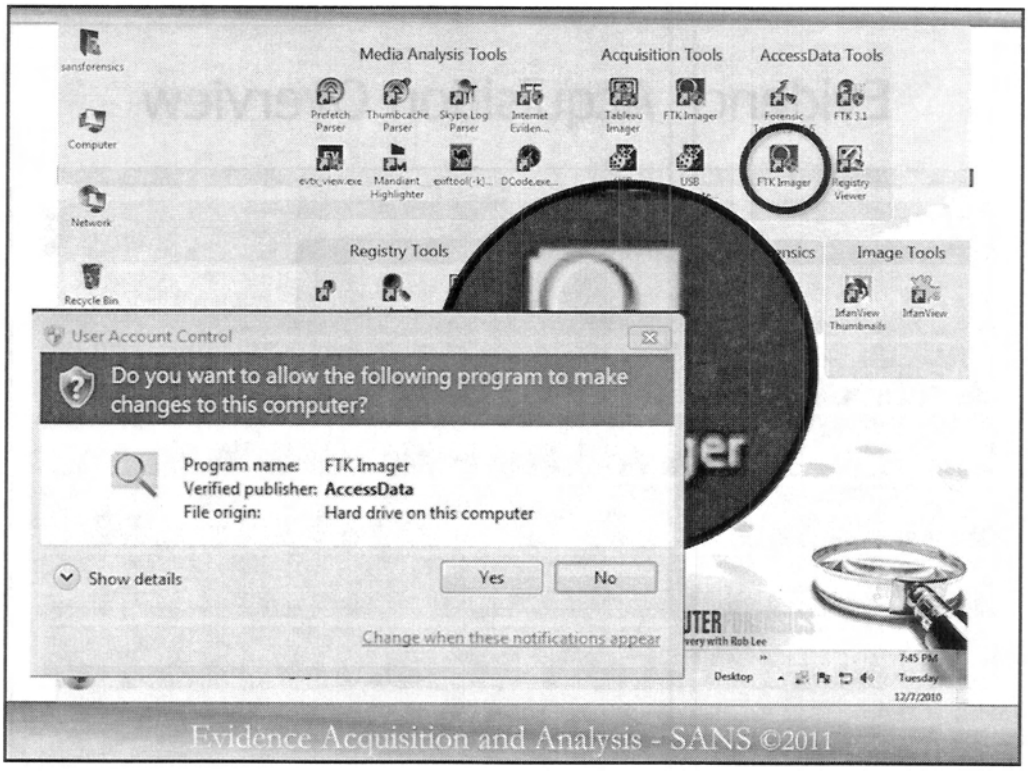
In the middle is the WiebeTech Forensic Ultra Dock. This device offers IDE and SATA connectors to your imaging hard drive as well as FireWire 800, USB 2.0 and eSATA connections to your forensic system. Like the FireFly, if you want FireWire 400 capability, you need to have an 800-to-400 converter attachment. This is a great device and it's aluminum construction makes it rock solid.

The device on the right is the Tableau T35es, which SANS has chosen to issue each of you taking this class.



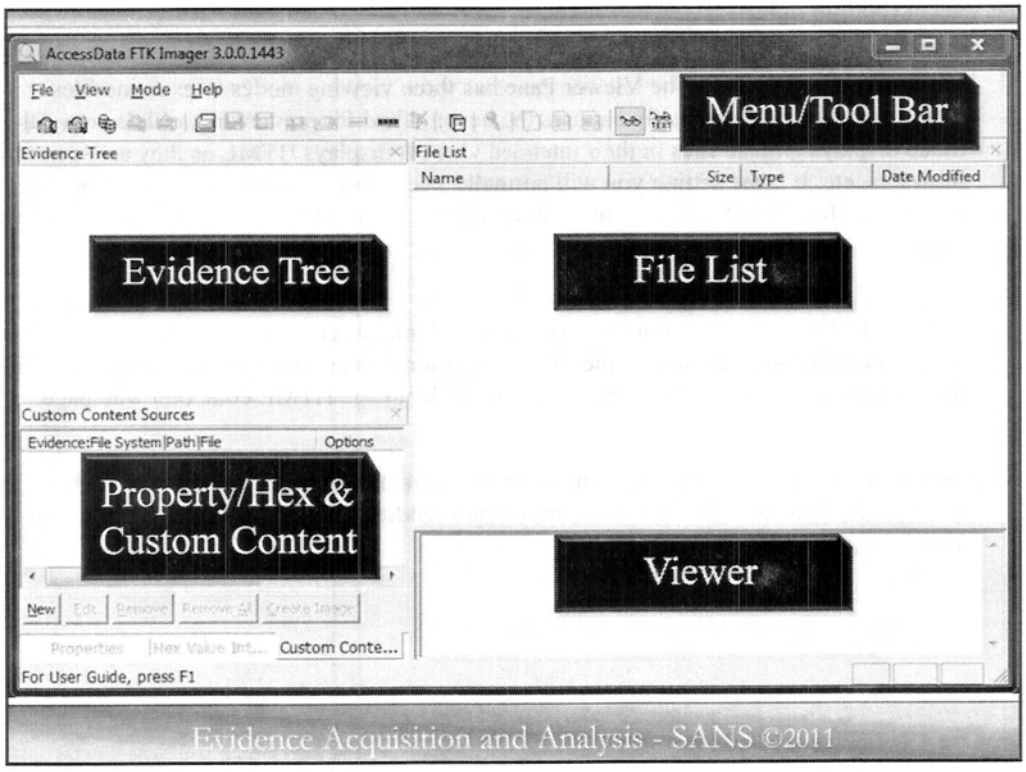
If there are not any questions, what do you say we go through the imaging software/process we use. Let's start our SANS Investigative Forensic Toolkit (SIFT) virtual machine and log on.

The Password on the virtual machines SANS provided you is **forensics**. Once you have your virtual machine running, please launch FTK Imager.



For those that started the virtual machine that SANS provided, you should see something like this on your screen. Now, If you don't already have FTK Imager open, go ahead and launch FTK Imager. You should see an icon on the left side of your screen about halfway down that looks like a magnifying glass over a folder, titled "FTK Imager".

Windows 7 users, you will likely see a User Account Control dialog box verifying that you want to run this program with system administrator privileges. Select "Yes".



The FTK Imager interface is divided into five basic sections:

- The Menu/Tool Bar (across the top)
    - **The Menu/Tool Bar (across the top).** The Menu Bar/Tool Bar gives you access to all the functions of FTK imager. As you know, almost anything you can do from the Toolbar, has a key combination short cut and also a Toolbar icon. FTK Imager is no different. As we go through the lesson today we will cover the most important of the icons and Toolbar options you need to know to get the most use out of the FTK Imager.

- The Evidence Tree (top left)
    - **The Evidence Tree** – The Evidence Tree window is located just below the Toolbar at the top left of the screen. The Evidence tree window pane is where you navigate the directory tree structure of the evidence you are looking at or previewing. Navigation of the evidence tree is done by clicking on the plus symbols to expand the directory tree. The plus will expand the tree one level. When you select an item in the Evidence Tree the contents of that directory are displayed in the File List window pane which is located to the right of the evidence tree window.

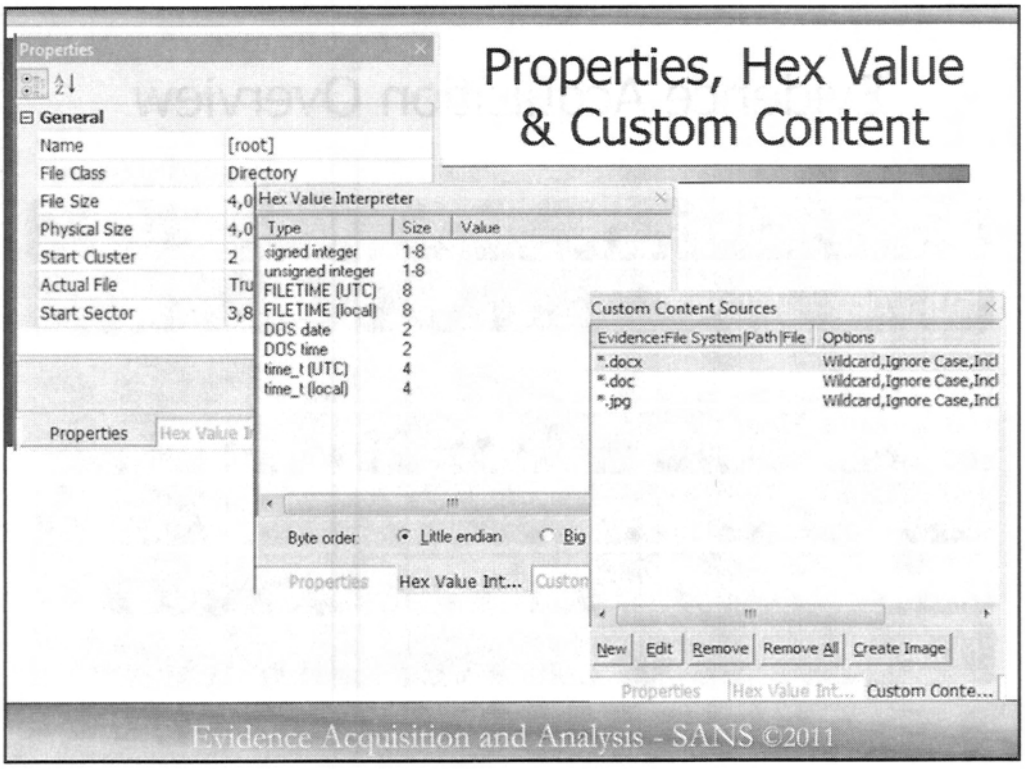
- File List, (top right)
    - **The File List Window –** The File List Window simply displays the contents of the directory you have highlighted in the Evidence Tree Window.

- The Viewer (bottom right)

  The Viewer which is located just below the File List window, located at the bottom right of the FTK Imager application. The Viewer Pane has three viewing modes to examine files. Automatic mode automatically chooses the best method for previewing a file's contents. This mode displays graphic files in their intended view. It displays HTML as they are seen in web browsers, etc. It is the setting you will normally keep your viewer window in. You can change this in the Menu/Toolbar to examine further details of the files such as from the hexadecimal view.

  Text mode displays a file's contents as ASCII or Unicode characters. It displays all the ASCII or human readable characters in the file. This is sometimes handy to see the file in its base format such as looking at the Hyper text markup language HTML code of a web page.

  As you can imagine, Hex mode displays a file's contents as Hexadecimal view. I have found that for files that are difficult to view or will not render in the automatic mode, you can almost always view them in HEX mode.



And the bottom left pane can display

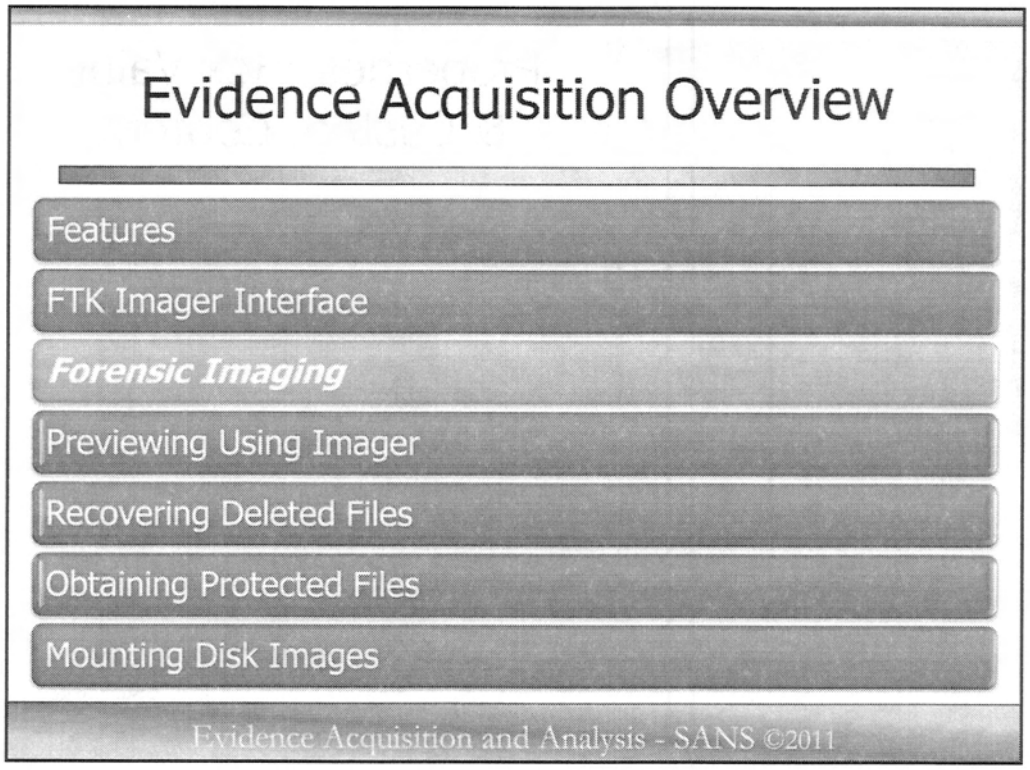
- The Properties pane
- The Hex Value Interpreter
- The Custom Content Sources

Properties Window: Now we come to the last area of the FTK Imager application. This window is located in the bottom left of the FTK Imager application and as you will see, it can be changed to show three different views. So, focusing your attention at the bottom left pane, in its default setting you will see that this window is the Properties window. The Properties window can display all the properties about a file, including the file class, logical and physical size of the file, MAC times and attributes to name a few. Another great capability is that it can identify the file system starting cluster of the file you are looking at.

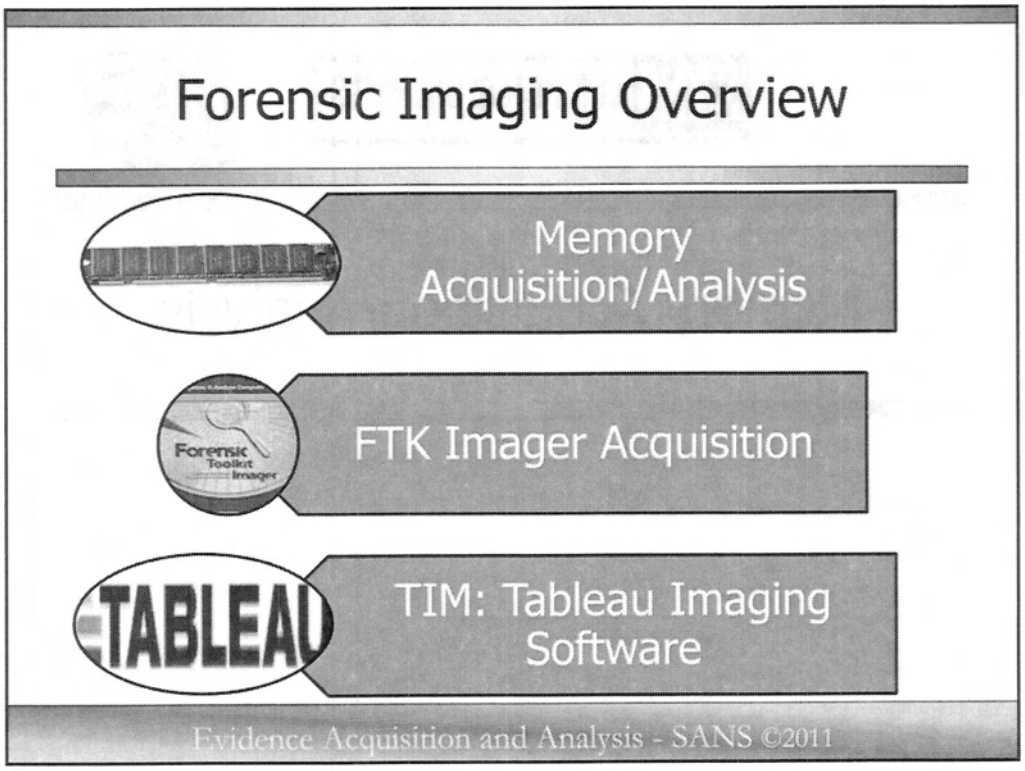
Hex Value Interpreter: As it's name states, this is a HEX value interpreter that will allow you to highlight hex values in the viewer window and this window will interpret date and time values, etc.

Custom Content Sources: This is an extremely valuable feature that will allow you to create custom images containing only the files you need or select. You can individually select files from a live file system to add to a Custom Content image or you can create filters to search for and image only specific items like jpg or doc files. So if you wanted to create a forensic image of just all the Microsoft Word documents and picture files with the jpg file extension, you could create three filters as you see in the slide. This it will create an Custom Content image of just the Microsoft Word document and picture files with the jpg extension and it will maintain their original file path location. So, if you had a document in the c:\windows\system 32\config directory, then your Custom Content image would contain the full directory structure, but only the document file would be inside the directory in your image file. This feature is particularly valuable for investigators who must acquire evidence quickly, or who need only particular items of information.

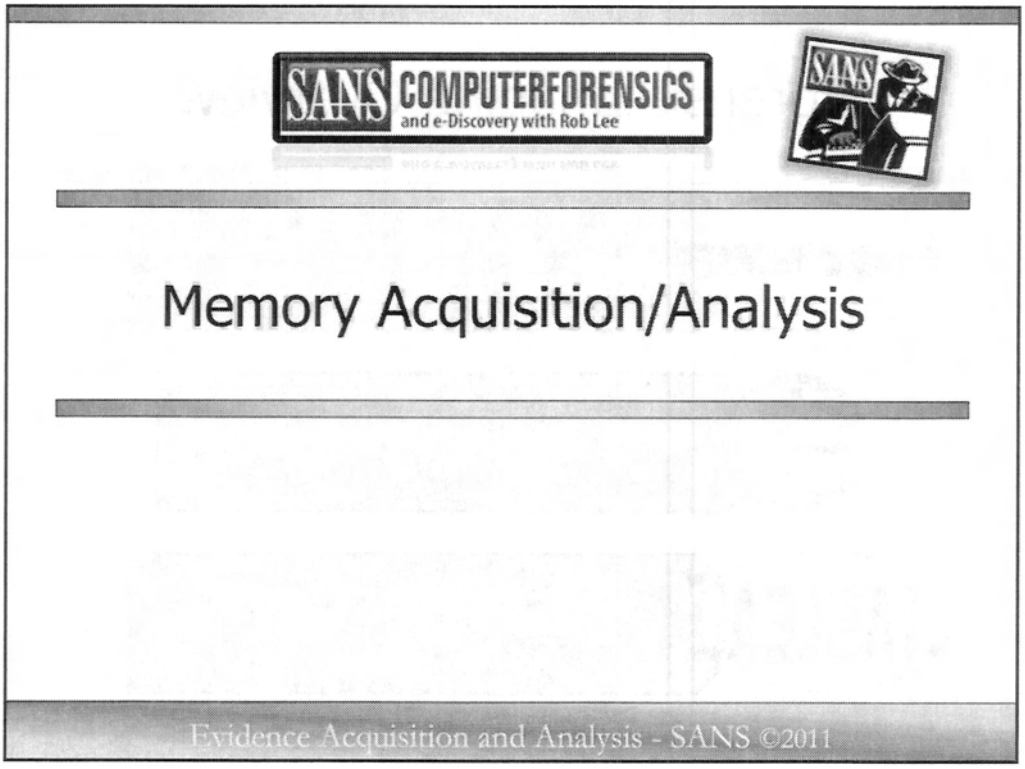
All the panes (except the Viewer) can be undocked from the program window and repositioned on your screen. The Menu and Button Toolbars can also be undocked. To undock a pane or Toolbar, select it and click and drag its title bar to the desired location. To re-dock the pane, move the pane inside the FTK Imager window until an outline shape snaps into place in the desired position, then release the pane. To return all panes to their original positions, select View, and then Reset docked windows.



In this next session we will discuss how FTK Imager can capture and image Random Access Memory (RAM) and create forensic images.



This page intentionally left blank.



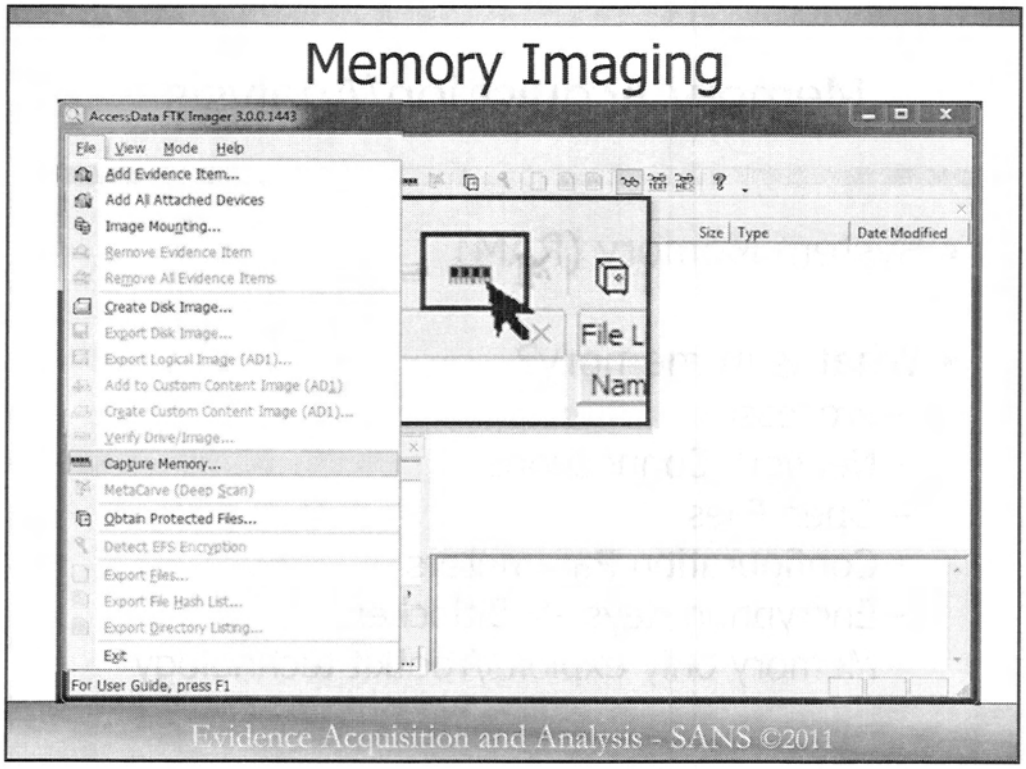
This page intentionally left blank.

Memory Acquisition/Analysis

- System Memory (RAM)
- What is in memory?
  - Processes
  - Network Connections
  - Open Files
  - Configuration Parameters
  - Encryption Keys -> Bitlocker
  - Memory only exploits/rootkit technology

Up until recently, memory analysis was essentially limited to performing string searches and byte searches through what was seemingly random data. The memory image file format has been recently reverse engineered and new tools exist that will allow for a more granular approach to examining the contents of memory.

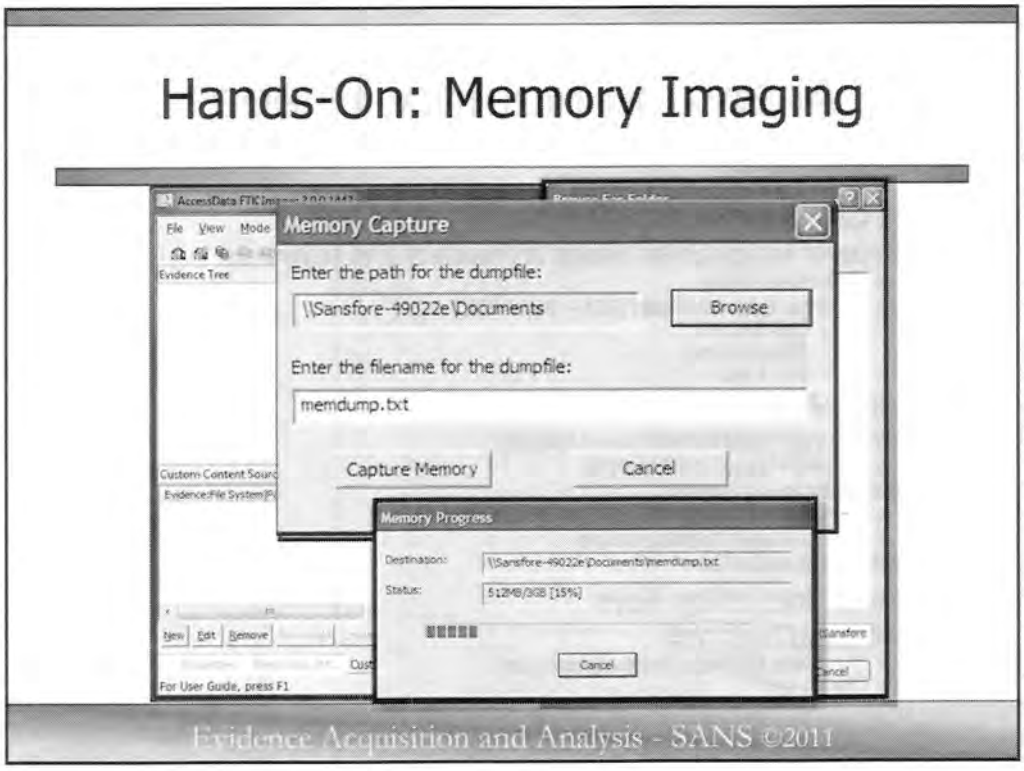
What is sitting in Random Access Memory (RAM)? You have all the processes, files, directories, and any other information that could be sitting in residue in memory. You can use this information to piece together old history and commands that a previous individual may have typed on the system. You might discover old e-mails or website that the user surfed to. You might find residue from exited processes. And probably most importantly, you might have passwords collected in clear text still sitting in memory. While it is the most volatile piece of evidence, it is also one of the most valuable.



FTK Imager now supports Random Access memory (RAM) Acquisition. Capture the contents of the local machine's RAM to a file in a user-specified location. A summary file containing information about what was captured is also created and stored in the same location as the Memory Capture. This feature requires Imager to be run with administrator rights.

Generally it is best to run RAM acquisition through FTK Imager Lite which is found on your Course DVD at D:\FTK Imager Lite\FTK Imager.exe (Win7 and Vista users must right click and "Run-as" Administrator).

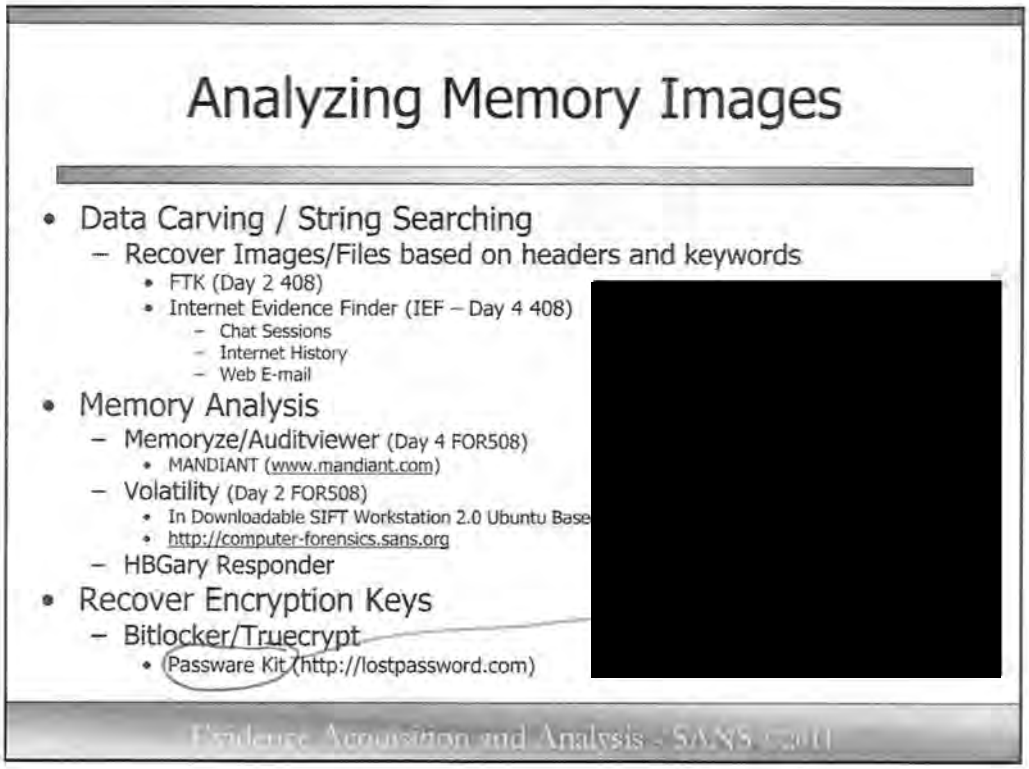
With FTK Imager, the process of capturing RAM is as easy as selecting "**File**" from the Menu Bar, then select "**Capture Memory…**". This can also be accomplished by selecting the icon of RAM in the Toolbar. This will open a dialog box that will allow you to select the location to create the image of RAM.



With the Memory Capture dialog box open, select the "Browse" button to enter a location to create your memory image. When you image memory, it is usually best to export memory to another networked machine rather than to a USB device. Attaching a USB device is not as forensically sound as sending it to another networked machine.

After selecting the location to save the memory image, you can give a unique name to the memory image or accept the default "memorydump.txt" file name. Select "Capture Memory" to start the memory capture.

[redacted]



There are now many tools that will help you analyze and recover artifacts from a memory image.

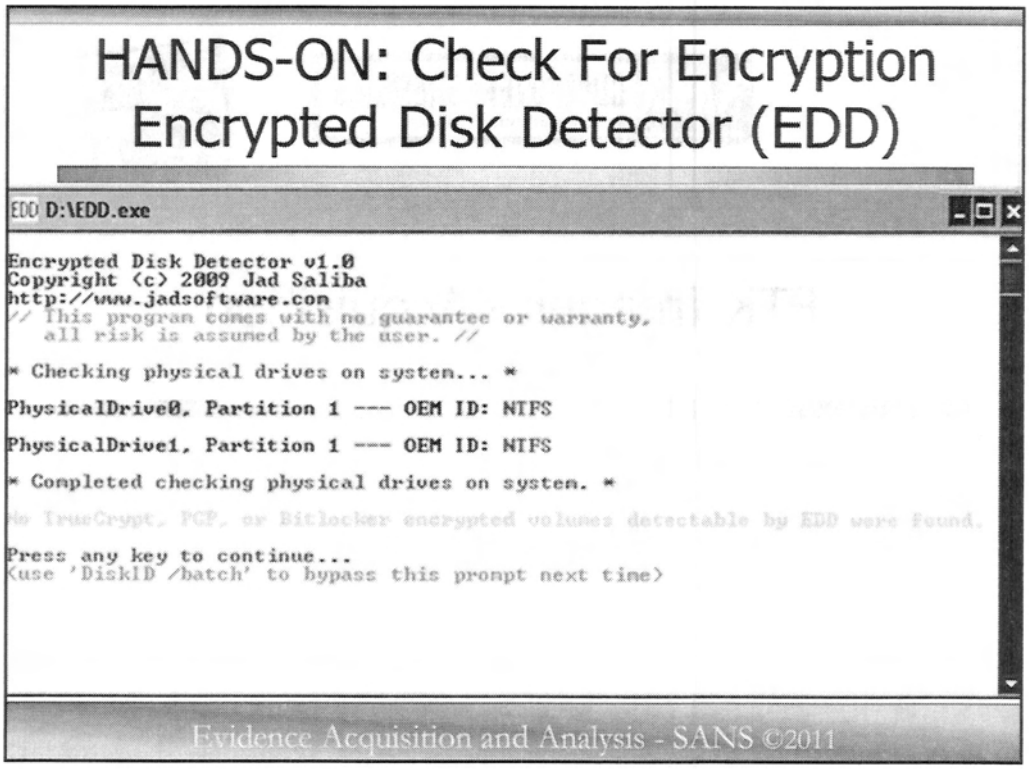
The basic tools examine a memory image similar to a disk image. It will carve out files and artifacts based off of file headers/signatures and keywords that you tell the tool to look for. Several tools in this class can perform basic memory analysis including FTK and Internet Evidence Finder. [redacted]

Using these simple techniques it is possible to recover chat sessions, Internet history, pictures, documents, and web mail from a memory image. As a result, memory analysis becomes even more critical to a case.

More advanced memory analysis will be discussed in the follow-on course 508 – Computer Forensic Investigations and Incident Response. In that course we cover how to analyze memory structures to include process space analysis, network connections, and searching for malware. Several available tools exist currently that are free and can be downloaded. It is recommended to look at MANDIANT's Memoryze and Auditviewer, Volatility, and HBGary's Responder. These tools also come in commercial versions.

Finally, it is possible to recover encryption keys from memory such as bitlocker and truecrypt. Using a tool such as the Passware Kit you can examine a memory image looking for these encryption keys and use them to unlock encrypted passwords. The Passware Kit is a commercial tool and is not free.

This page intentionally left blank.



One of the most important things you should ever do before powering off a system to remove a hard drive is to check to see if the drive is encrypted or not. We will demonstrate this step in an effort to ensure that the attached drives are not currently encrypted.

If they were, it would be advisable to image the drive while it is powered on and live. If you power it off, you likely will not be able to recover the keys.

If you perform a live image of a drive due to encryption, you should always image the logical drive instead of the physical one. The logical drive is seen as unencrypted by the local machine while the physical disk is still encrypted at the disk level.

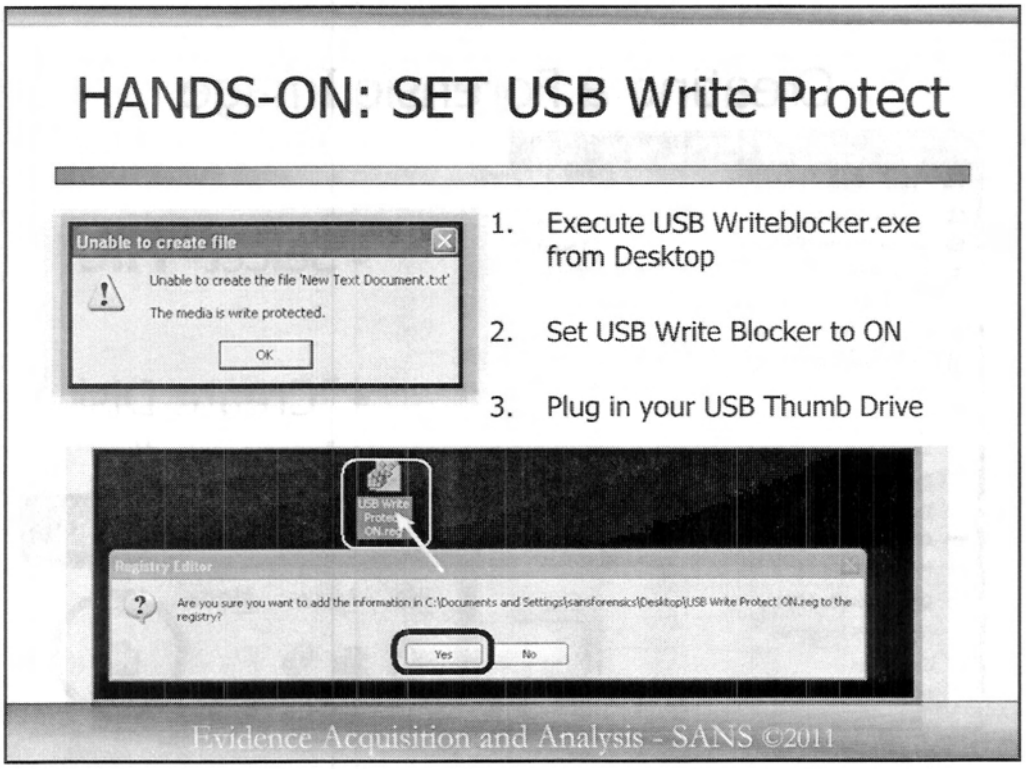
Remember, never make assumptions that a drive might be encrypted… ALWAYS CHECK.
We will check for encryption using a tool called EDD found on your DVD under the D:\Windows Forensic Tool\encryption checker directory. Simply double click on it for the quick scan.

Encrypted Disk Detector (EDD) is a command-line tool that checks the local physical drives on a system for TrueCrypt, PGP®, or Bitlocker® encrypted volumes. If no disk encryption signatures are found in the MBR, EDD displays the OEM ID and, where applicable, the Volume Label for partitions on that drive when checking for Bitlocker® volumes.

EDD does not attempt to locate encrypted volumes that are not mounted; its purpose is to alert the user of *currently accessible* drives/volumes that may be encrypted and therefore may be inaccessible if the system was shut down.

Put in other words, EDD does not scan drives for files that might be encrypted containers. If this is what you're looking for, there are other software packages available elsewhere that attempt to do this.

EDD is useful during incident response to quickly and non-intrusively check for encrypted volumes on a computer system. The decision can then be made to investigate further and determine whether a live acquisition needs to be made in order to secure and preserve the evidence that would otherwise be lost if the plug was pulled.



On the XP SIFT Workstation, USB write blocking is enabled by default, however, just in case, please practice enabling the write blocker prior to plugging in the USB key that you plan on acquiring.

1. Execute USB Writeblocker.exe from Desktop

2. Execute USB Writeblocker from your Host Machine (Found in D:\windows forensic tools\ )

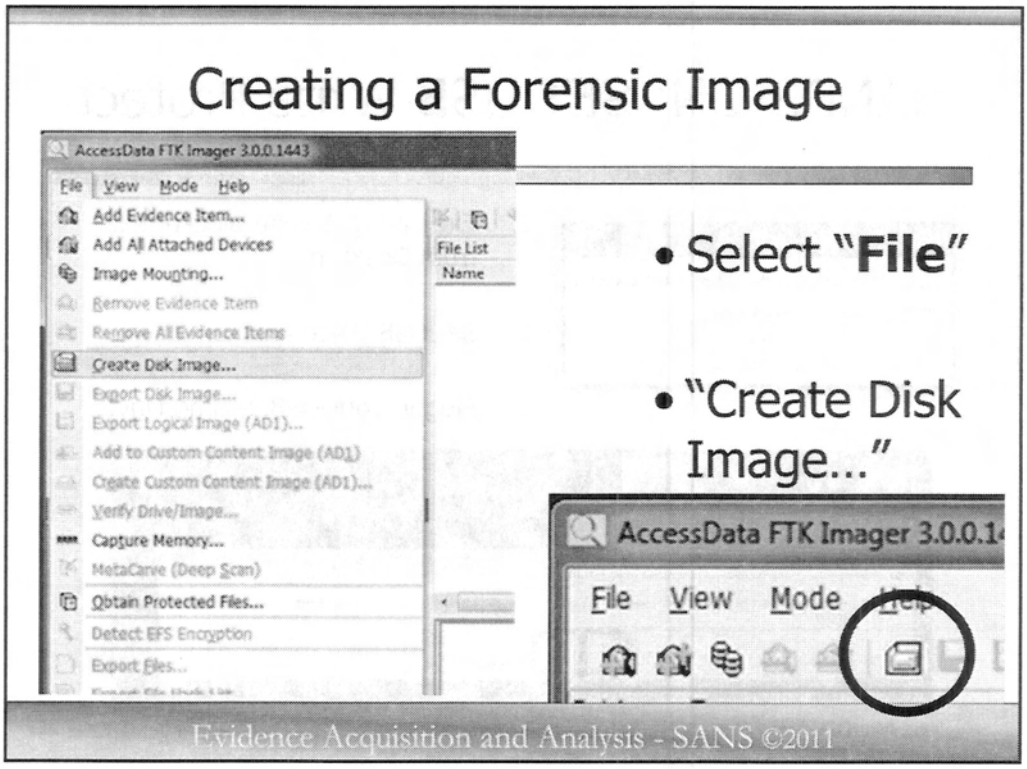
3. Set USB write blocker to ON

4. Plug in your USB Thumb Drive

Now, let's get to the meat of FTK Imager, it's imaging capabilities.

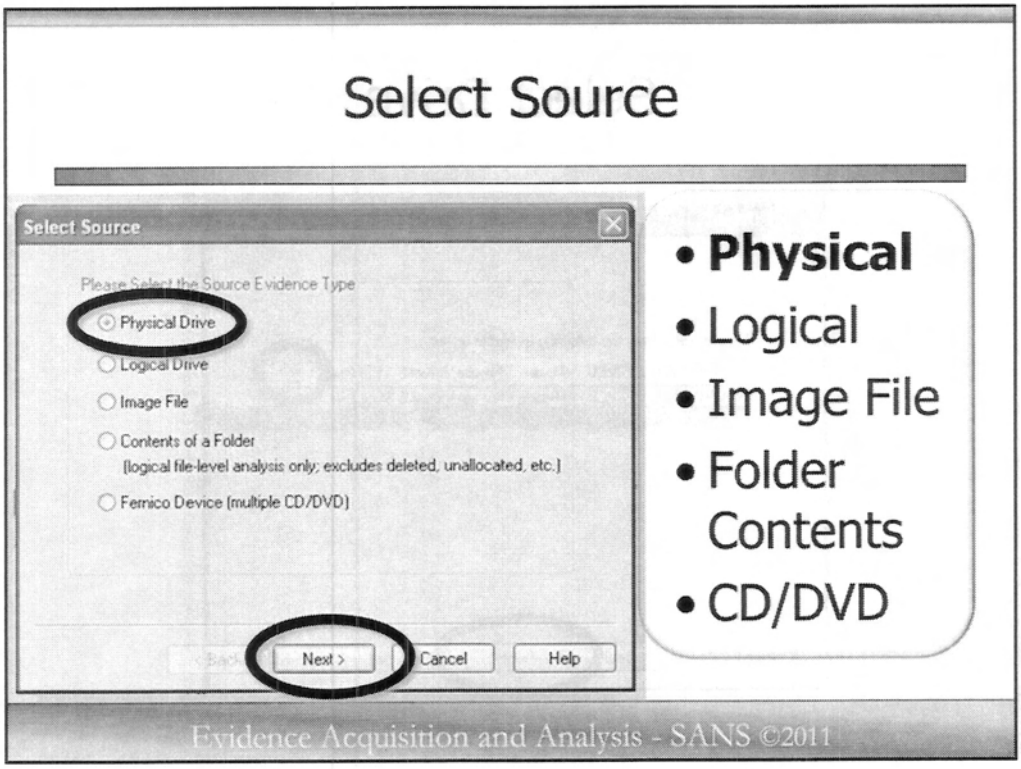
Go ahead and INSERT USB THUMB DRIVE

The preferred method of write protecting a thumb drive would be by using something like the Tableau T8 USB write block. With this device you are absolutely sure no writes will be made to the USB device.



At the top left of FTK Imager, select **File** from the Menu Bar, then go down and select "**Create Disk Image…**"

You can also accomplish the same task by clicking on the 6th image from the left on the Toolbar that looks like a hard drive as shown here in the slide.



You are presented the "Select Source" dialog box where you indicate to FTK imager what type of device you would like to image.

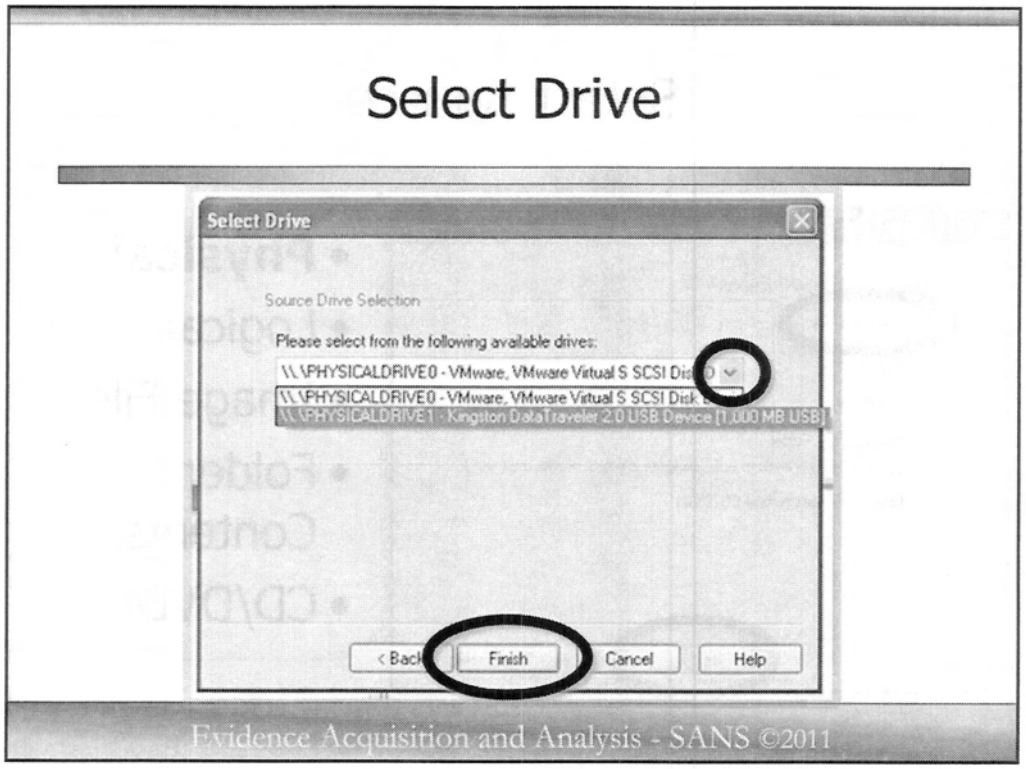
In the forensics world, you almost always want to see everything, so you will usually choose PHYSICAL drive. This will image all the allocated and unallocated space, active and deleted files, etc.

The Logical drive is handy for multi-disk RAID systems where you want to see the logical volume rather than each individual drive. Typically in a RAID system or server, you are not so interested in deleted files as you are active files and log files.

If you had an EnCase E01 image and you needed to convert it to say to a DD image, you could select "**Image File**" and then reimage (e.g. convert it to any other format).

Since we will be creating a new image, you should select "**Physical Drive**".

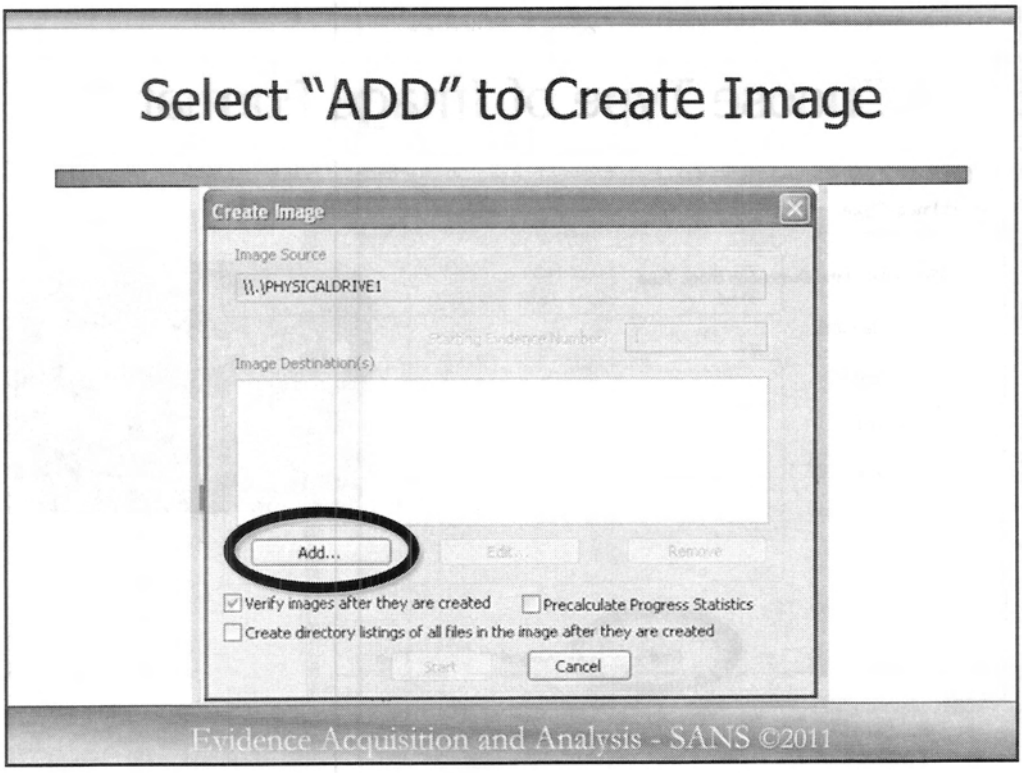
Then select "**Next >**".



The next screen you see will be the Drive Selection screen. Here you will see all the drives connected/recognized by your system. By selecting the down arrow button on the middle right side on the Select Drive dialog window, you can see all the physical drives attached to your forensic system. If you have your thumb drive attached you will see physical Drive Zero which is always your operating system, then physical Drive 1, which in this case is our attached thumb drive.

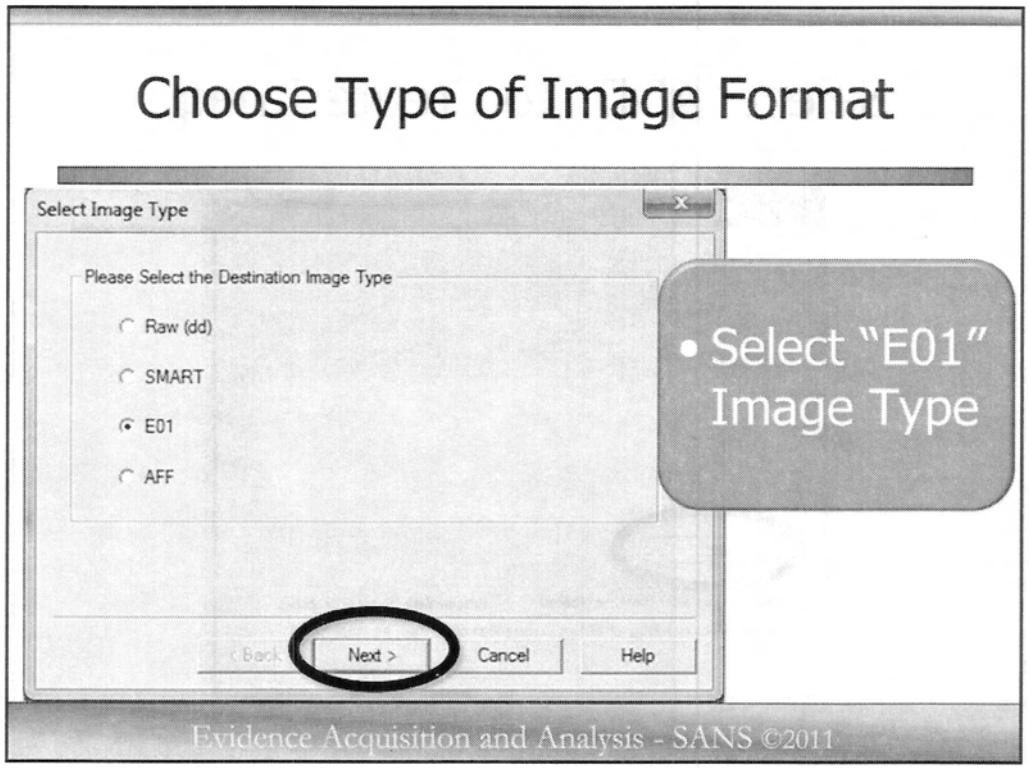
If you have your thumb drive attached and see the Physical Drive 1, go ahead and select it.

Now click "**Finish**".



In this screen, starting at the top, you should see the physical drive you selected to image. In our case it is physical drive #1. Below that you see that the image destination is empty. Now we need to select a destination for our image file to be written to, so click on the "**Add…**" button.

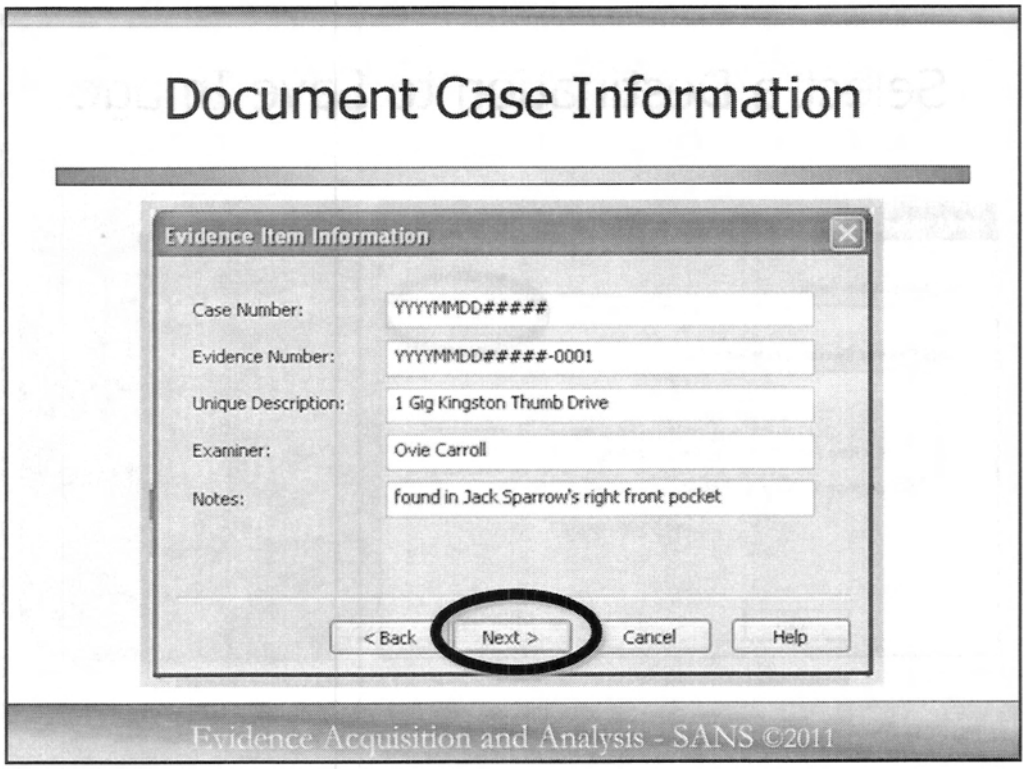
For now, don't worry about the other radio buttons below the add button. We will get to those after selecting a destination.



When you click on the add button, FTK Imager first wants you to select the type of image you want to create. Here in the "**Select Image Type**" dialog box, you can select what type of image file you want to create. It really does not matter what kind of image file you create, although I typically use Raw (dd). One possible advantage to selecting the EnCase E01 image format is that you have the option to use "compression" on your image file. That is to say that the image file is compressed, similar to using WinZip to compress a file so it does not take up as much room on your destination drive.

One possible disadvantage of using compression, particularly when you ratchet up the compression from the default value of "6" to a higher number, is that some forensic programs other than EnCase have difficulty reading the image file. For that reason, when you image using the EnCase E01 image file format, I recommend you just leave the compression at the default value of "6". Another possible disadvantage of using compression is speed. Using compression increases the amount of time it takes to create the image file, so it speed is important, it is recommended to set the compression level to "0" (no compression).

So that we can see the compression option, let's go ahead and select the E01 image file format. Then select "**Next**".



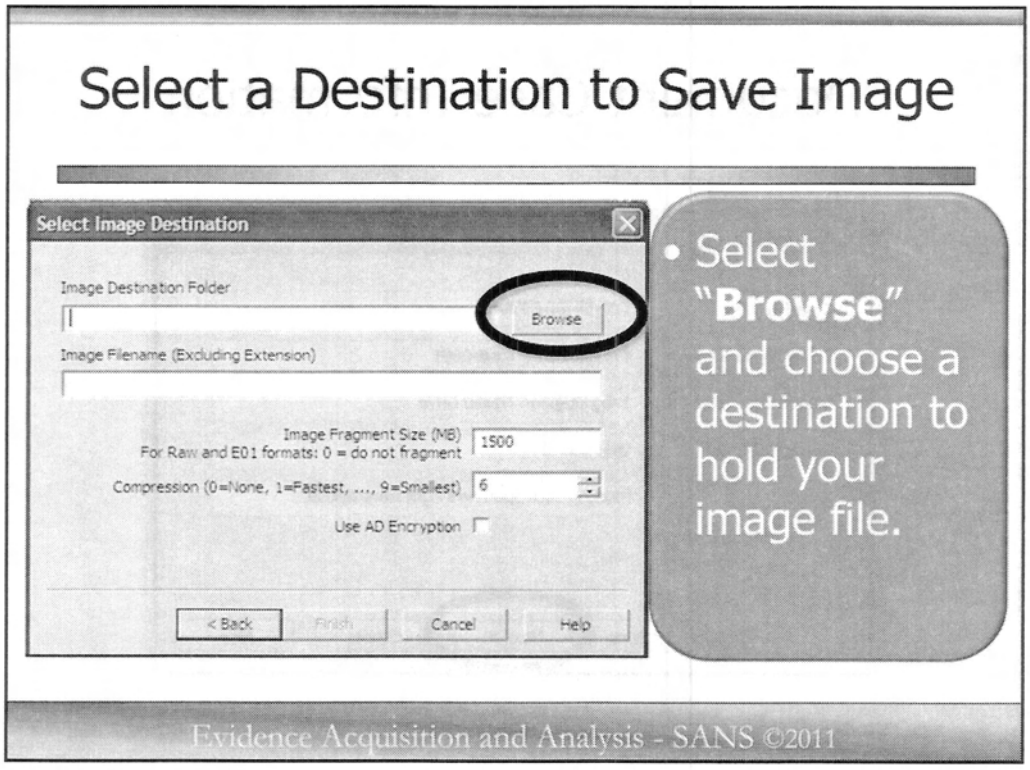
Now you should receive a dialog box allowing you to fill in information about your case or device you are imaging.

The format most commonly used for case and evidence numbers are year-month-day-case sequence number for that calendar or physical year.

Another thing to remember is that you may image many devices while out in the field and when you get back to the lab you do not remember anything about any of the devices. You might not even be the examiner analyzing the images. This is where the notes section can really come in handy. Here you can see we made a note of exactly where we found or recovered the device from. If this was a house or office, you may want to indicate the room and location in the room you took this device or even who it was said to have belonged to.

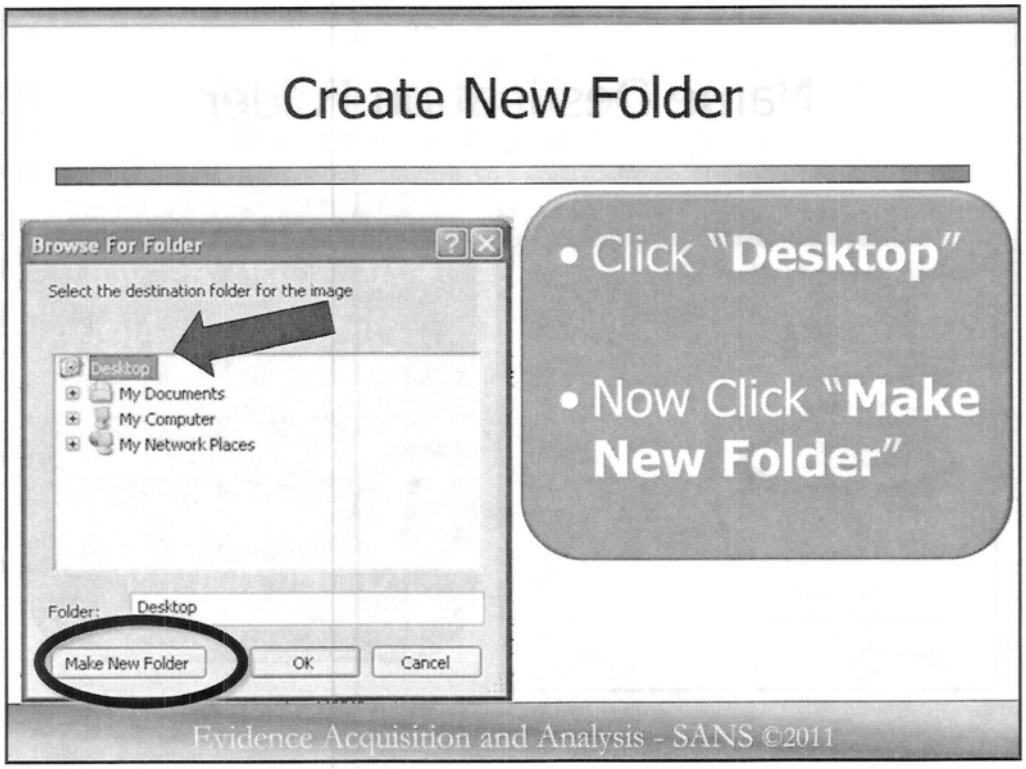
It is also common in large seizures that you create a log file with each image file name and where you found that device (e.g. image file YYYYMMDD####-0001 – thumb drive found in Jack Sparrow's right front pocket). This helps when you look at 20 image files and want to quickly start looking at certain computers found in a particular office or of a particular person.

After completing the Evidence Item Information, select "**Next**".



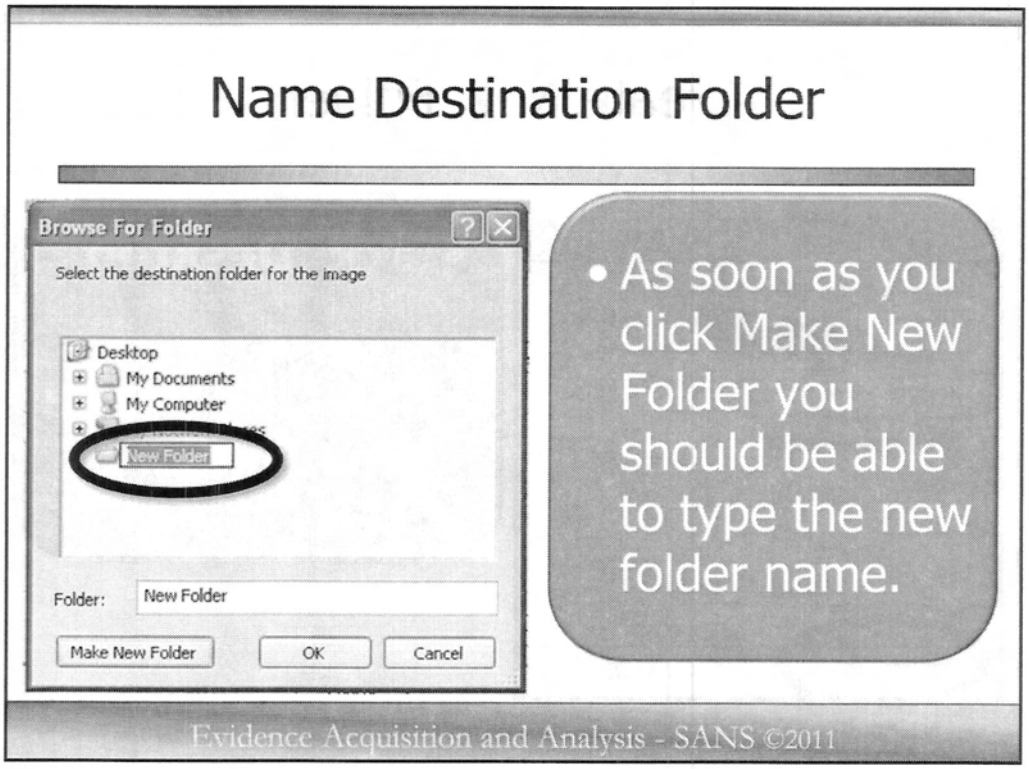
Now that we have the Evidence information filled in, we need to point to the drive or location we want to save our image file. Of course this should be a drive you have prepared to receive evidence.

When we say prepared to receive evidence, what we are talking about is that many forensic shops conduct a forensic wipe, repartition and format on all drives they will copy forensic images to. This is a good practice but some argue that it is overly cautious. Advocates of preparing drive by wiping say that it assures that no viruses or malware infect the forensic image you are creating. Opponents say image files are closed containers, like zip files, that cannot be infected.

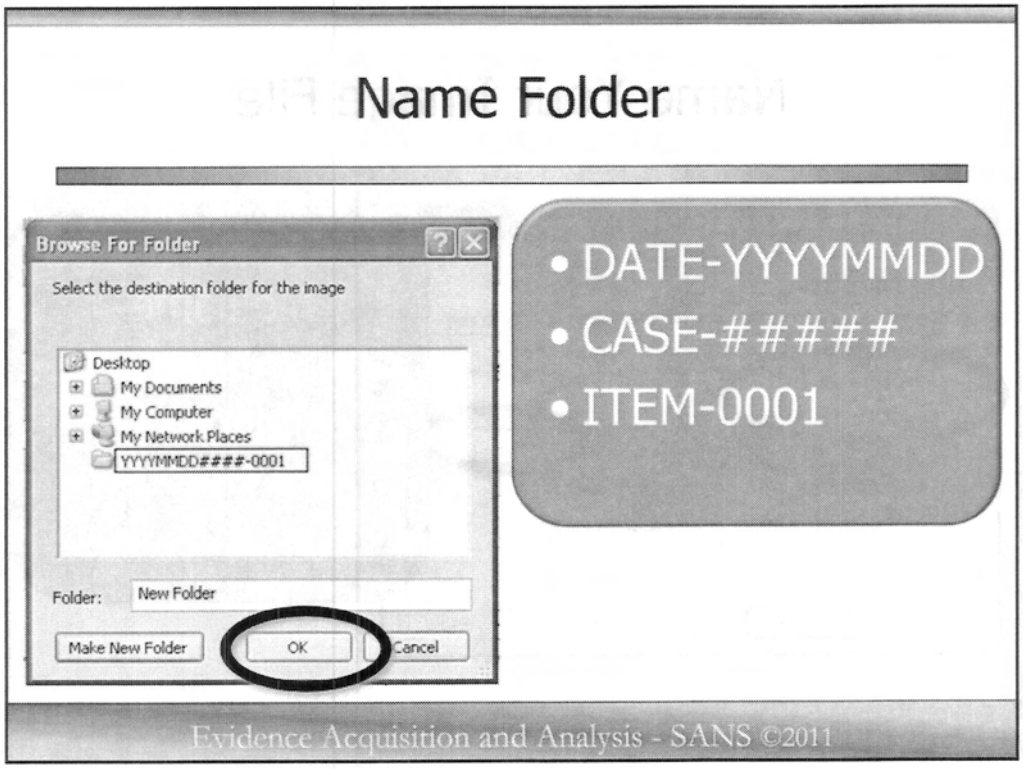


Let us create a folder, and put it on our desktop, so we can easily find it and examine the contents.

Click on "**Desktop**".
Then down at the bottom click on "**Make New Folder**".



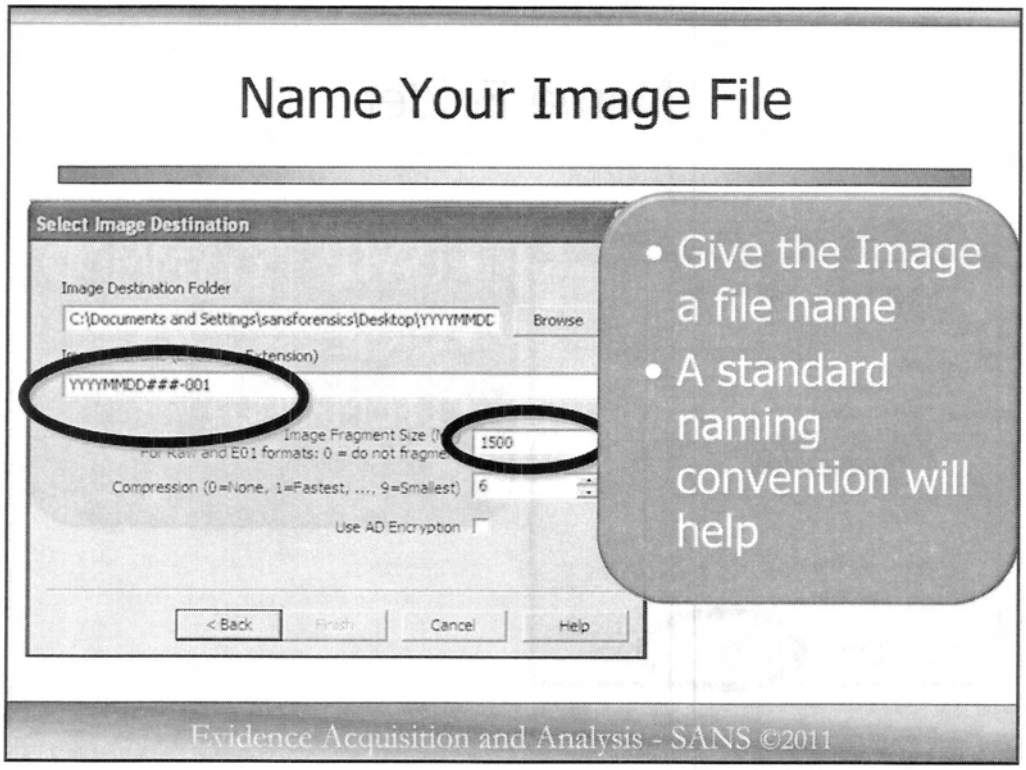
Now, let's name that folder the same name as our case: "YYYMMDD#####-0001".



You will be able to keep track of your images and know what each image is and its basic significance if you use some kind of standardized organizational structure. You will normally find that the naming convention you use at the scene makes perfect sense, but when you get back to the lab, you have no idea what you were thinking.

This is why the naming convention is so important. At this point, we are creating a directory where you want to put the image files. This could be the name of the case, or the subjects name, or even the search locations name, but in our experience, if you use something a little more standard along with an inventory sheet documenting each item, you will have fewer problems.

So for now, let's create a directory where you want to place your image files. We are going to use our case file number indicated here by the YEAR, MONTH, DAY, CASE NUMBER and SEQUENCE NUMBER.



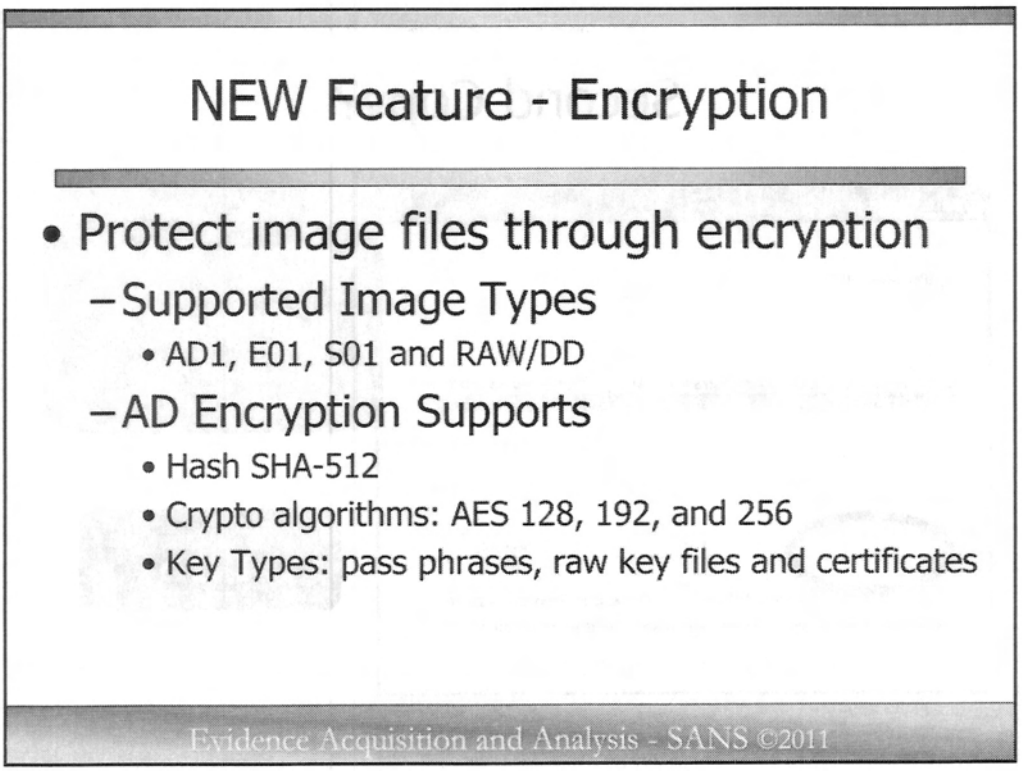
Now it is time to give the image a file name. You can name your image file anything and many people do, but I can tell you from experience that having a standard naming convention will help you later when you try to identify what each file is and where it came from.

If you are imaging a lot of media or at a search scene, you should employ a **log file** to identify where you found all the digital media you are imaging and what the corresponding image file name is.

Change the Image Fragment Size from 1500 to 0. In most cases, your evidence drive should be formatted NTFS and can handle large files. Splitting a file image into chunks may cause problems in the long run and should be completely avoided if possible.

You should give some consideration to what your agency's naming convention will be. Some have chosen to leave out month and day altogether, but the reason I like it is so I have another signal as to when I created this image file. Now as for the SEQUENCE NUMBER, I typically increment this number for the number of digital evidence items I image. You may also want to include the examiner's initials if you frequently have multiple people creating images.

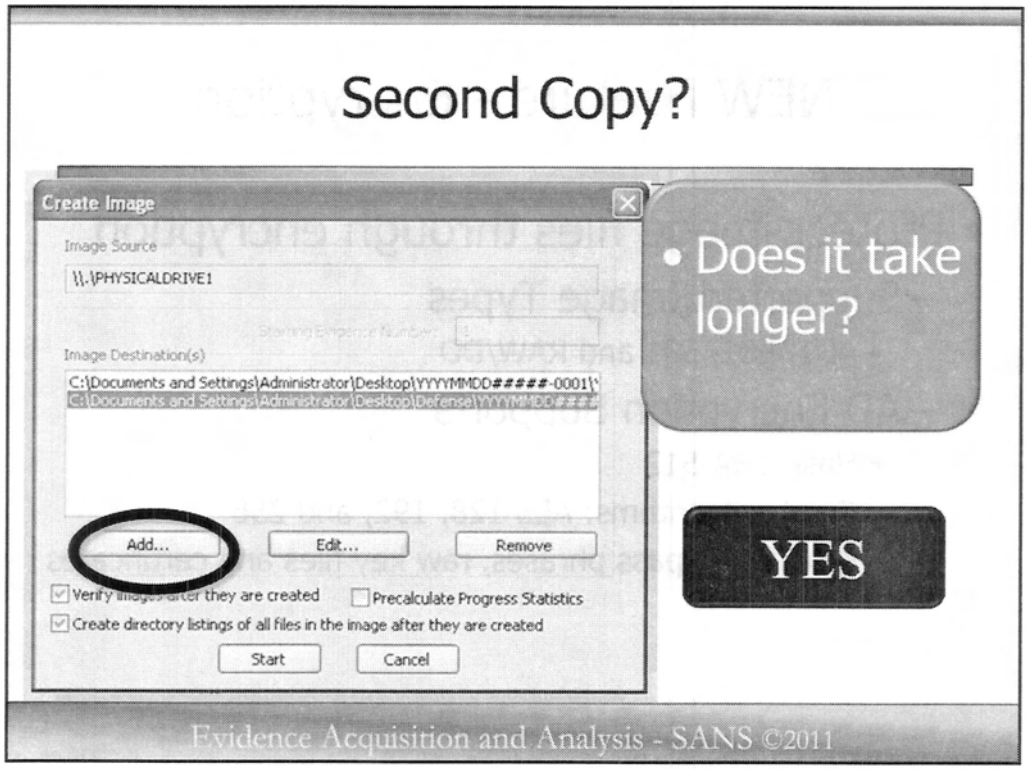
Now if you selected to create a DD or RAW image file format, then you will not be able to access the compression dialog box, but if you select EnCase E01 image file format, then you can adjust the compression level. I do not recommend changing this. While it is forensically sound, sometimes adjusting compression causes some compatibility issues with FTK or other non-EnCase forensic software.



No matter if you are supporting a criminal investigation or doing civil discovery work, seized data often contains extremely sensitive information and in the case of child pornography, could also be contraband. Forensicators are responsible for properly collecting digital evidence and for safeguarding the contents until it is placed into a secure evidence holding location. With child contraband, new legislation in the form of the Adam Walsh Act, requires law enforcement to take measures to safeguard the contraband.

With the new encryption feature of FTK imager 3.0,, forensicators can encrypt forensic images to further ensure that unauthorized persons are not able to view or extract the contraband or sensitive data.

FTK Imager can encrypt AD1, EnCase E01, SMART S01 and RAW DD Image types through the use of AES 128, 192 and 256 cryptographic algorithms. Images can be encrypted using a pass phrase, raw key files and certificates. Starting with FTK Imager 3.0, AFF image file format is supported. If you selected AFF as your image file format, you will see a "Use AFF Encryption" option. Selecting this option will automatically change the image fragment size to 0, resulting in a single image file.



Another feature of FTK imager is the ability to create multiple copies of the source drive at the same time.

To do this simply select the "Add…" button again and give it another file location and name.

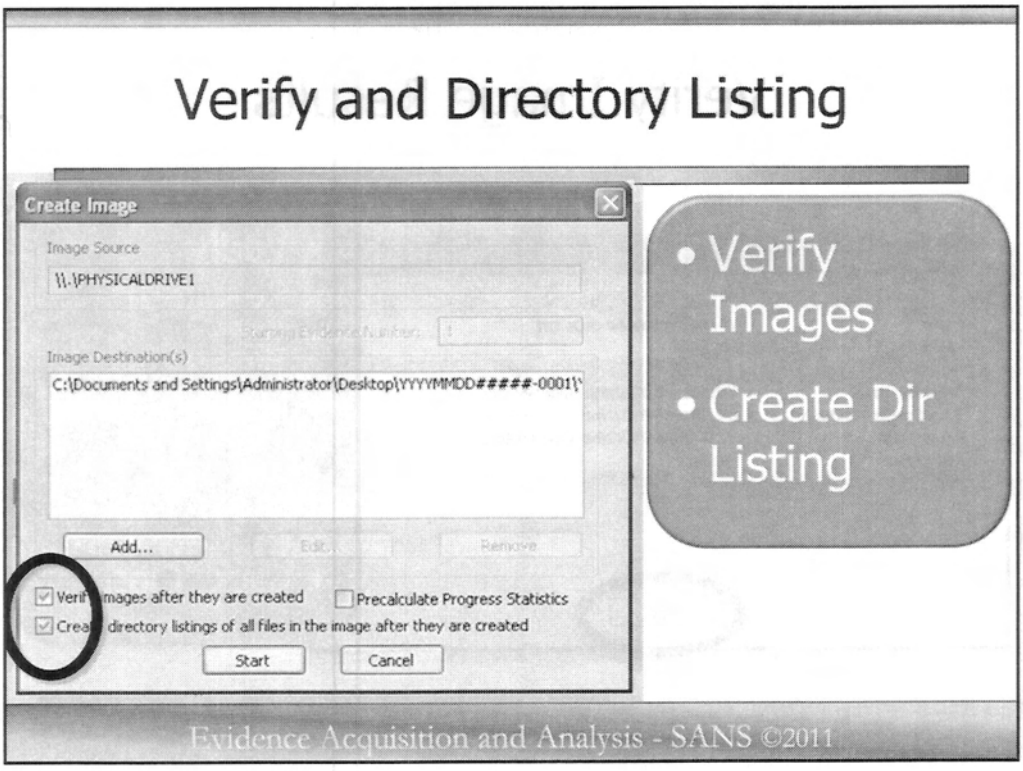
This is particularly useful if you need to produce one forensic image copy for you and one for another party such as the defense attorney or another agency. I have heard a lot about some law enforcement agencies that will create the forensic image but when it comes time to share a copy of that image with another law enforcement agency conducting a joint or parallel investigation, they will refuse to provide a copy. If you have experienced this situation, you can suggest or instruct the individual creating the forensic image to make two copies of the forensic image at the same time.

QUESTION: Does this slow down the imaging process, creating 2 images rather than 1?

ANSWER: Yes, it is not multi-threaded. It does take longer. Not quite double, but in our tests of a 1 gig thumb drive, it took approximately 48% longer doing two images rather than one image:

One 1 gig Thumb drive - 5:18 = 318 seconds

Two 1 gig thumb drives - 7:51 = 471 seconds



Now there are two buttons you want to make sure you select. The first is obvious … "Verify images after they are created".

The second is not so obvious as many in the community do not do this.

This second option allows you to "Create a directory listing of all files in the image file after they are created".

This option creates a tab-separated value (TSV) file listing file names with full path, MAC times, and if the file is active or deleted.

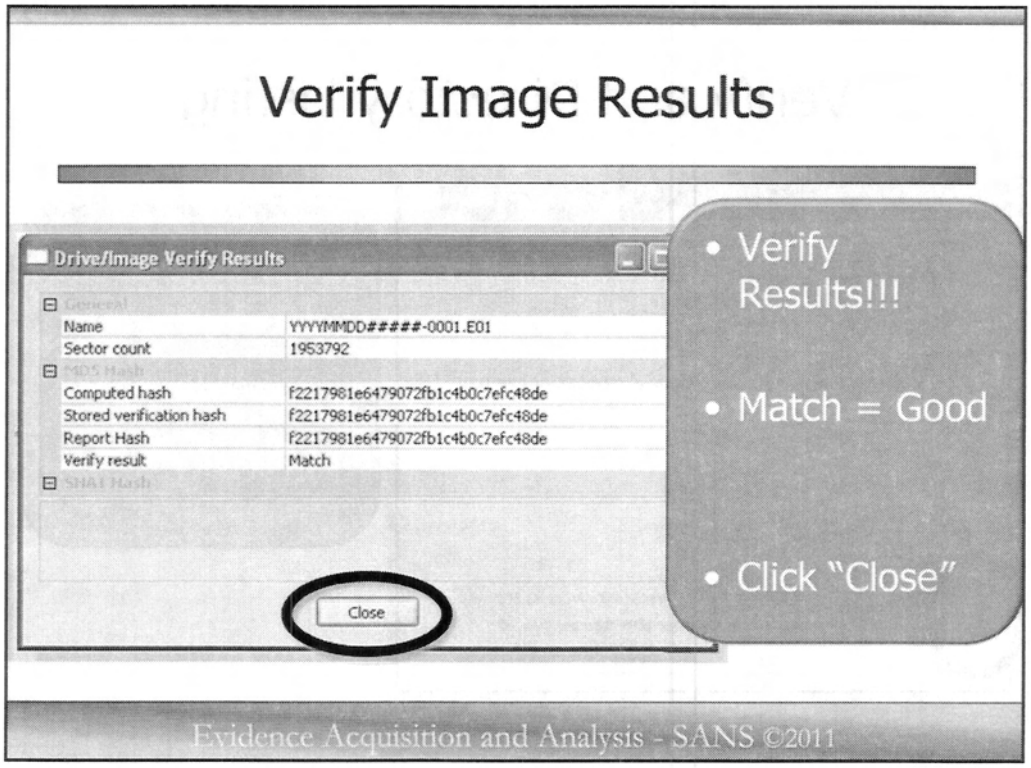
Be careful not to misrepresent what this TSV file is. Some might want to consider it a complete list of everything that is on the drive…

QUESTION: Why would this be wrong? What is missing from the file listing?

ANSWER: UNALLOCATED SPACE, FILE SLACK, ENUMERATION OF REGISTRY KEYS AND CONTENTS OF COMPRESSED FILES.

This is important if you recover information or a file from unallocated space that was not identified as a deleted file and somewhere earlier you told the prosecutor or judge that this was everything on the drive. They might ask you to tell them where on that list the recovered file is.

That's it. Click **START**.

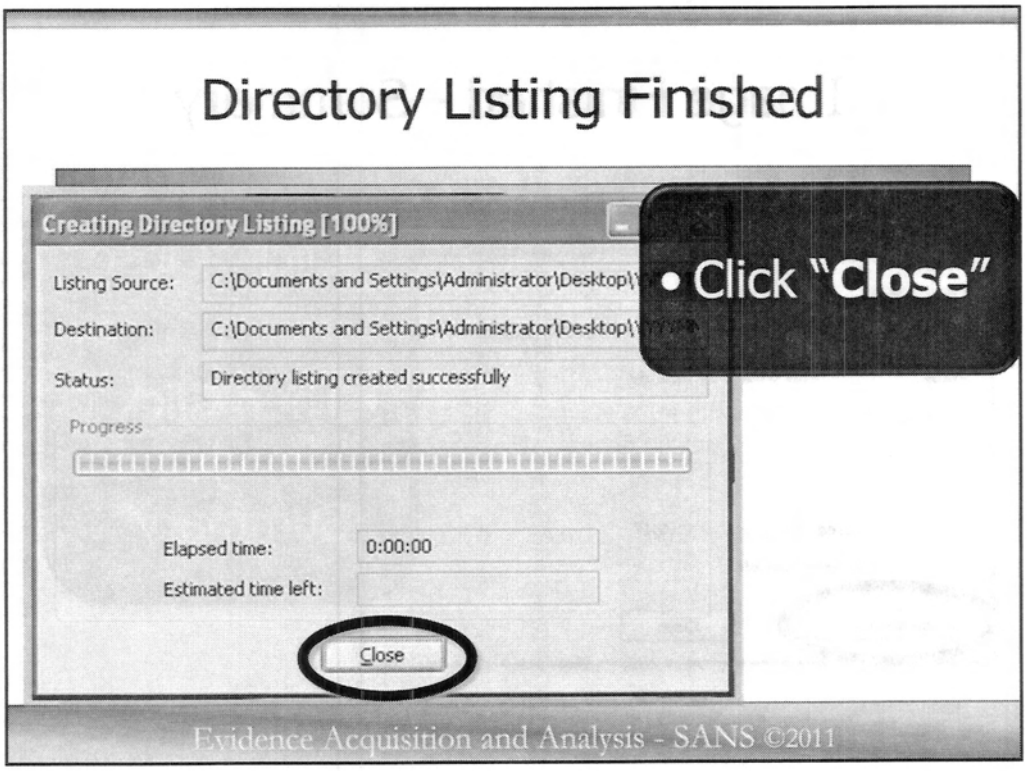


When FTK Imager is finished creating all the images and verifying that the hashes match, FTK Imager will display the Drive/Image Verify Results. This does not take much effort but it is the most critical part of the imaging process. If FTK reports that the image hashes do NOT match and you just blow by it, you are going to have a real problem back at the lab, particularly if you did not seize or maintain control of the original equipment because there will be no way to recreate the image. Check it and THEN close it. You may even way to make a note in your investigator or analyst notes that the image hashes matched.

One thing to be careful of here is that when you make your notes, you DO NOT need to write out the hash in your notes. You can actually cause yourself some problems later in court if you accidently write the number down wrong in your notes or transpose a number. Even though the image matched, a defense attorney could try to make out like it did not or the image has changed from when you created it and annotated it in your own notes.

This shows you that the computed HASH and the Image HASH match.

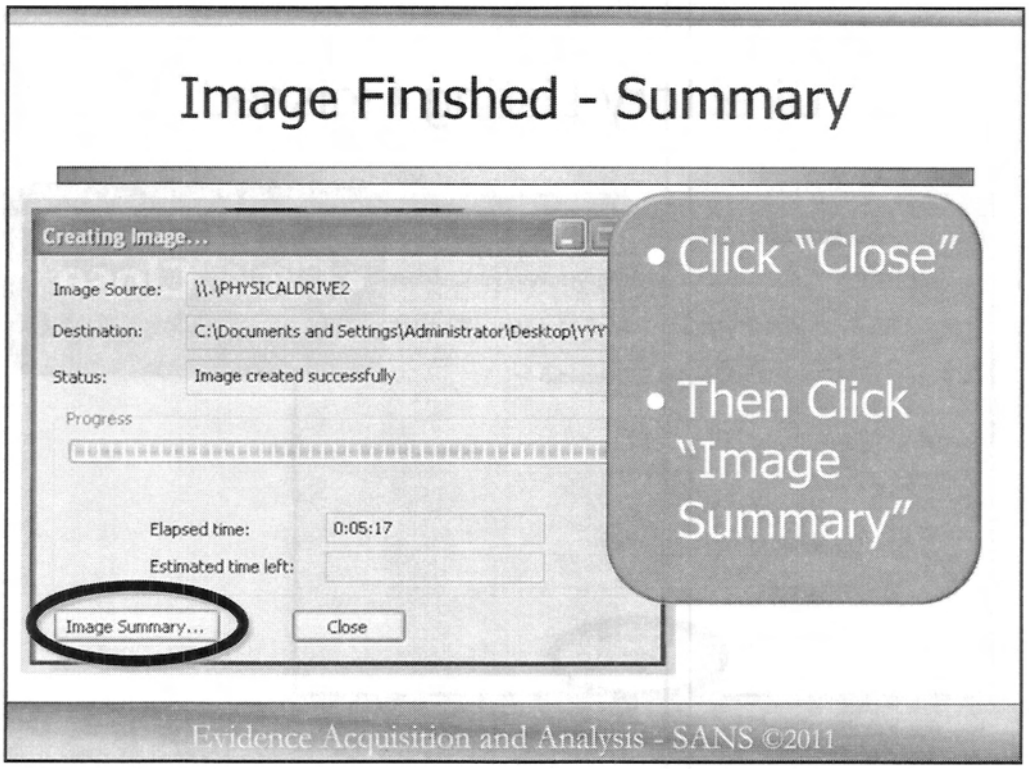
Select Close.



If you choose to create the directory listing, the first dialog box you will see is one stating that the **directory listing has been completed**. You can select the **CLOSE** button.

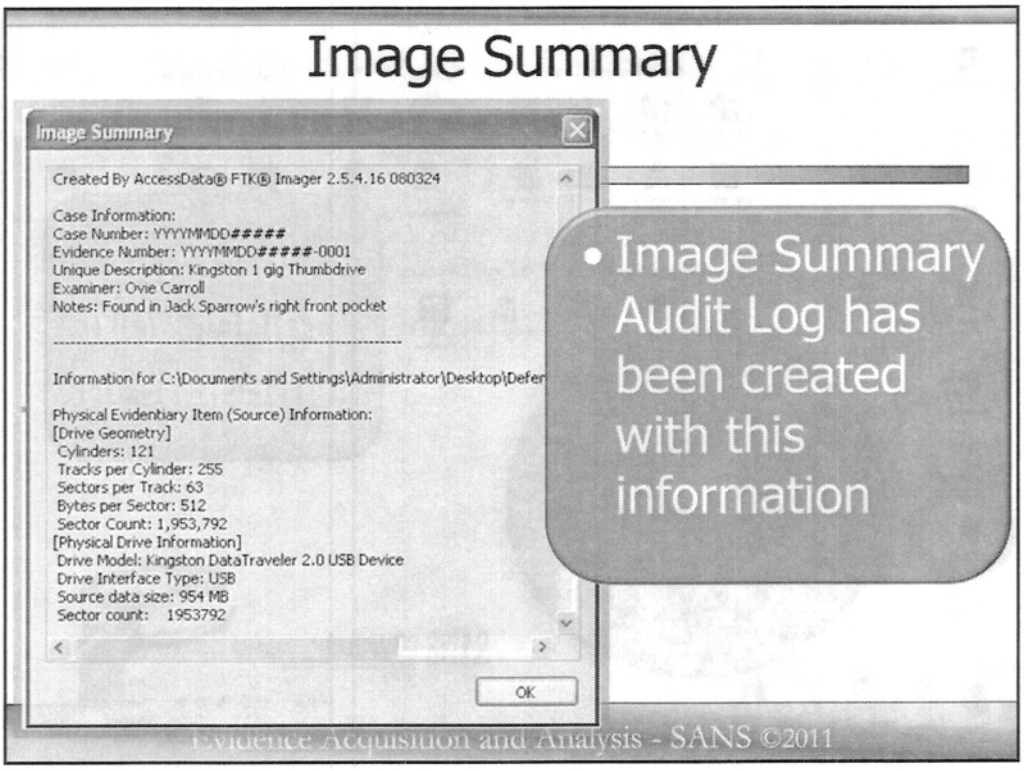
More and more, I am finding that a directory listing is a good thing to go ahead and create. It can be used in a number of ways. First, if the judge wants to require a "Return" on the search warrant, you would typically only provide a list of what items you seized from the scene, which would state: one HP computer system, make, model and serial number etc. But, it might even be as detailed as the make, model and serial number of the drives imaged.

In some districts, the Magistrate Judges are asking for more detail as to what was seized, and if they insisted on more detail, you could provide this list to the courts, saying that this is a list of all files. This obviously does not include unallocated space or file slack information, but it may be enough to satisfy the courts.



Now that you closed the Directory Listing Dialog box, you now see what appears to be the exact same box, but this time it is telling you the image is finished and gives you the option to view the Image Summary. A quick review of this Image Summary is never a bad idea. Everything that you will see inside this image summary will also be included in the audit log text file that FTK Imager creates in the same directory as your image files.

Let's select "**Image Summary...**" to review the complete audit log.



Review contents of the audit log.

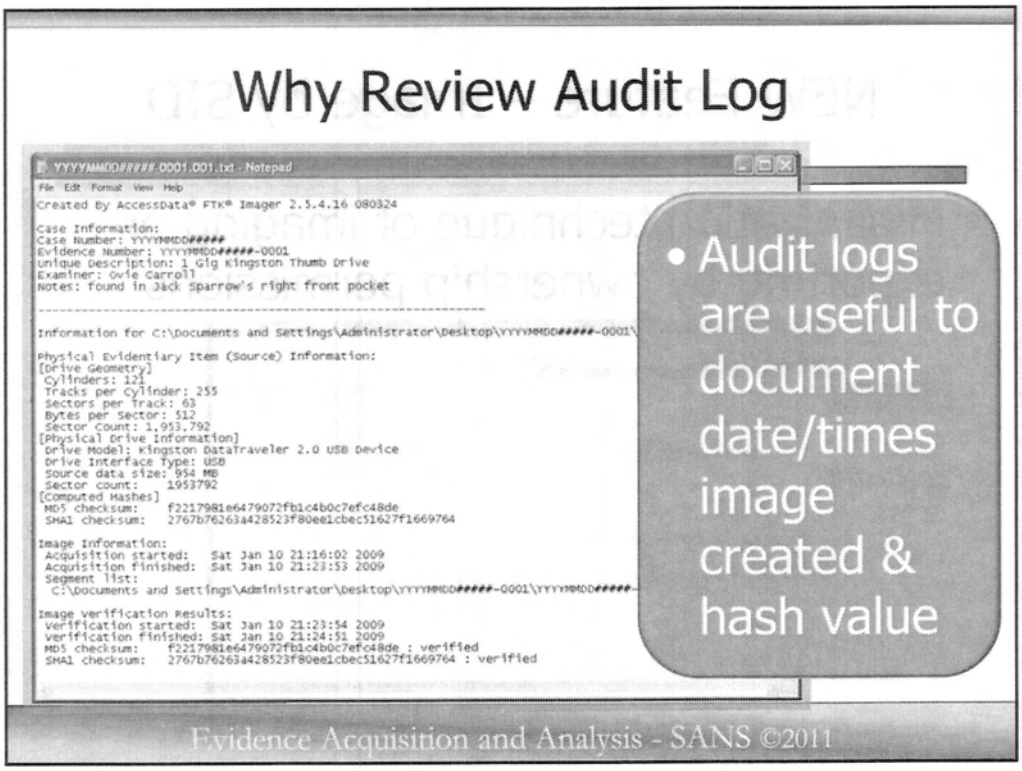
As you can see, the Audit Log or Image Summary includes the version of FTK Imager used to create the image file. This may become important later when writing your report to document that you used an approved version of FTK Imager and it is the same version as your lab has tested and validated, or has documentation that it has been tested and validated. A good place to go for this is the **National Institute of Standards and Technology** (NIST). They have tested several imagers and write blocks and you can get their test results papers for your lab at http://www.cftt.nist.gov/disk_imaging.htm.

The audit log also includes the case information you entered during the imaging process as well as the drive information/geometry.

Again, everything you see here in the Image Summary will also be in the audit log text file in the same directory where you created your evidence image.

Now that you have reviewed the Image Summary, you can close it and also close FTK imager. If you followed our instructions, on your desktop you should see a folder/directory containing the forensic image you just created. Go ahead and open that folder and verify what we were just talking about, you should be able to locate and open the audit log.

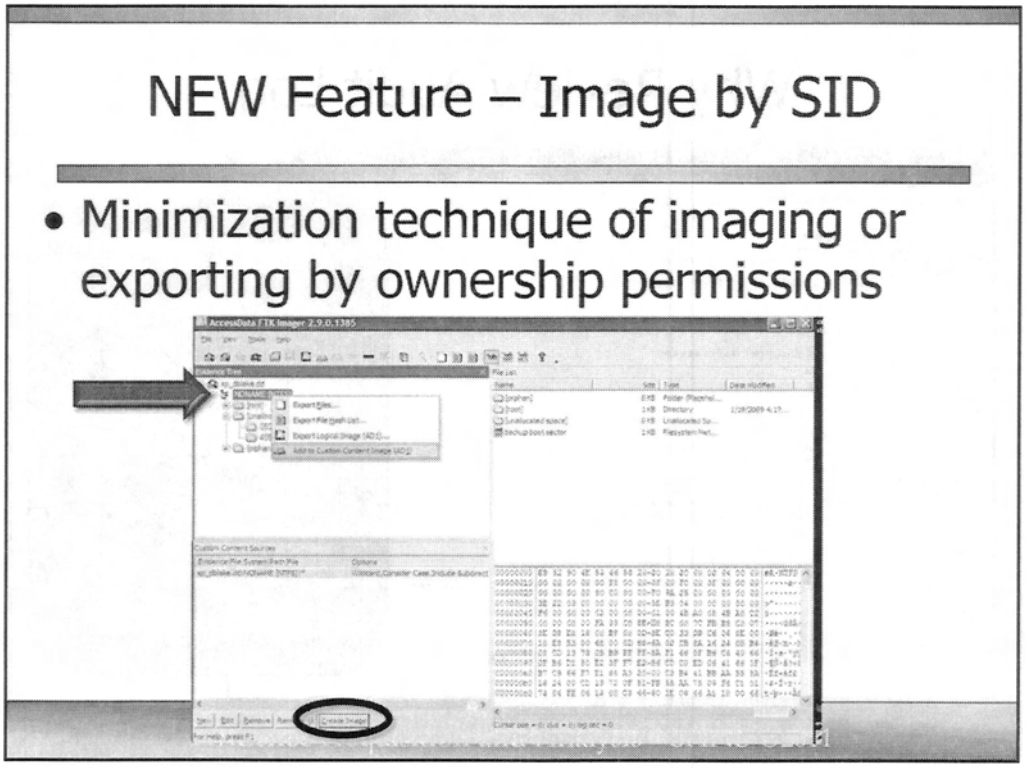
The audit log will be the only text file in the directory with the file name of your image file. Again, this is another reason to think about the naming convention of your image files. If your naming convention does not create a unique name for each image and at some point someone combines image files from different cases into the same directory on your forensic server, you could overwrite an image file or audit log.



The audit log contains all the information about your image such as:

- Case Information you entered at time of creation
- Drive and directory you saved the original image file to
- Physical geometry of the drive you imaged
- Pre-Image MD5 Hash
- Pre-Image SHA1 Hash
- Date Time Created
- Date Time Image Finished
- Post-Image MD5 Hash
- Post-Image SHA1 Hash
- Verification

You should always keep this file with your image file.



New with FTK Imager 3.0, you can create custom AD1 images of all files with ownership permissions by user SID.

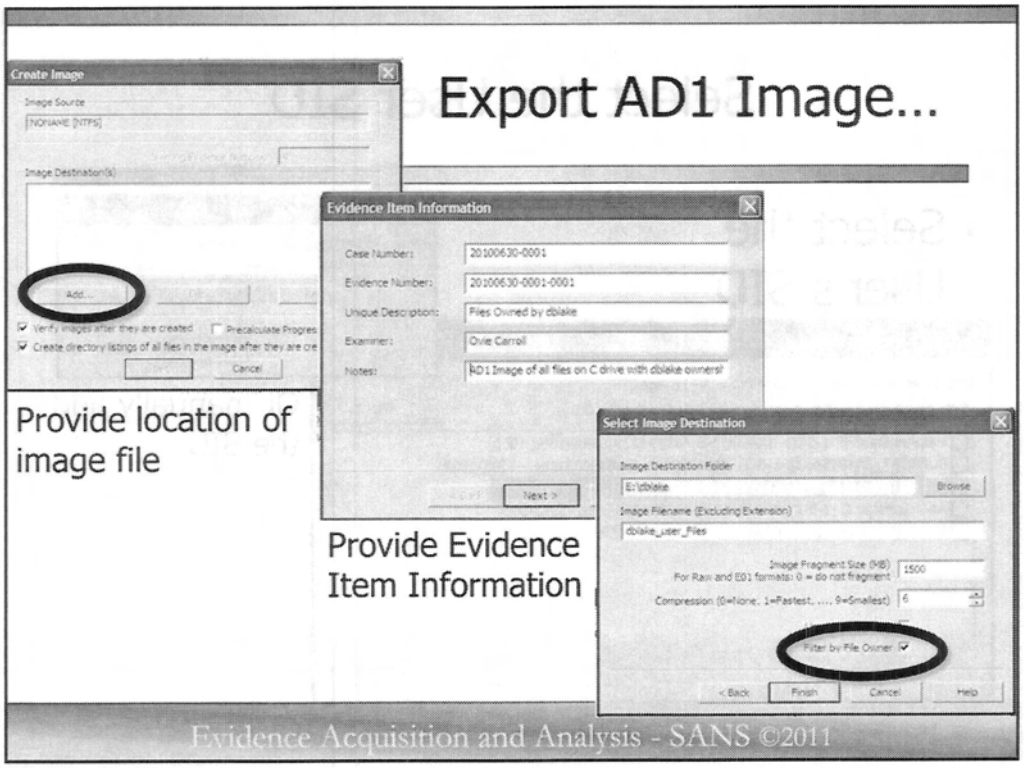
Recognizing that hard drive capacity is getting larger each year and more of our personal information is on our computers, the United States Courts have expressed concern recently about potential invasion of privacy. Where possible, this may be an excellent way to minimize collected data.

You can also use this techniques to **extract** all files owned by particular users from a forensic image previously created.

To create a custom AD1 image of all files owned by a particular user SID, you would first preview the drive to be imaged, then, in the Evidence Tree Window, right click on the file system entry directly above the "Root" of the drive and select "**Export Logical Image (AD1)…**" or "**Add to Custom Content Image (AD1)**".

If you selected "**Add to Custom Content Image (AD1)**" then click the "Create Image" button at the bottom right of the Custom Content Sources section of FTK Imager.

If you selected "**Export Logical Image (AD1)…**" you will then be prompted for the location of your image file.

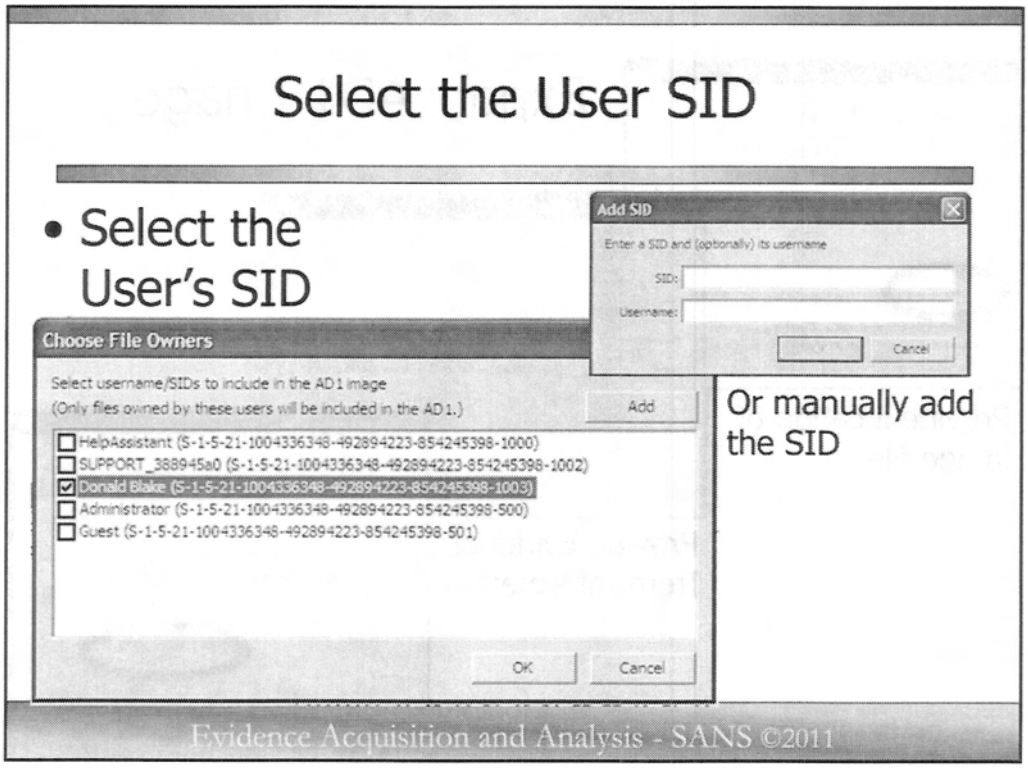


Next, select "**Add…**" to add a location for your evidence item/image file.

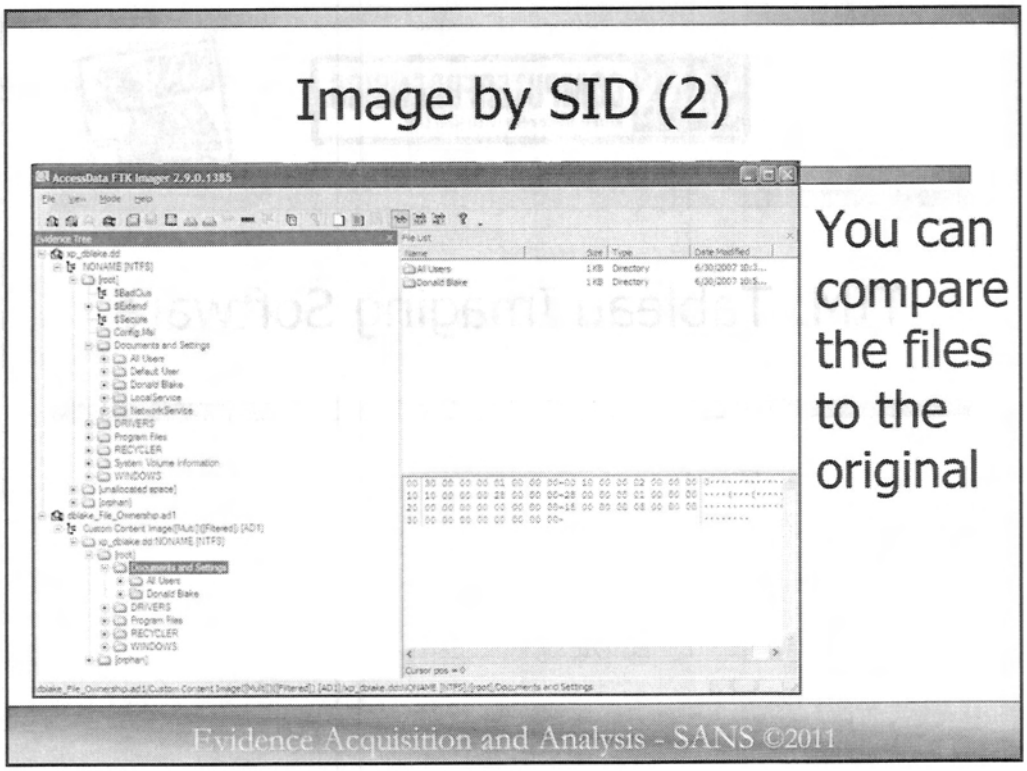
You will then provide the Evidence Item Information, making sure you add notes that this is an image file of files owned by a specific user.

Then, just like when creating a regular image, provide the location and name of your image file.

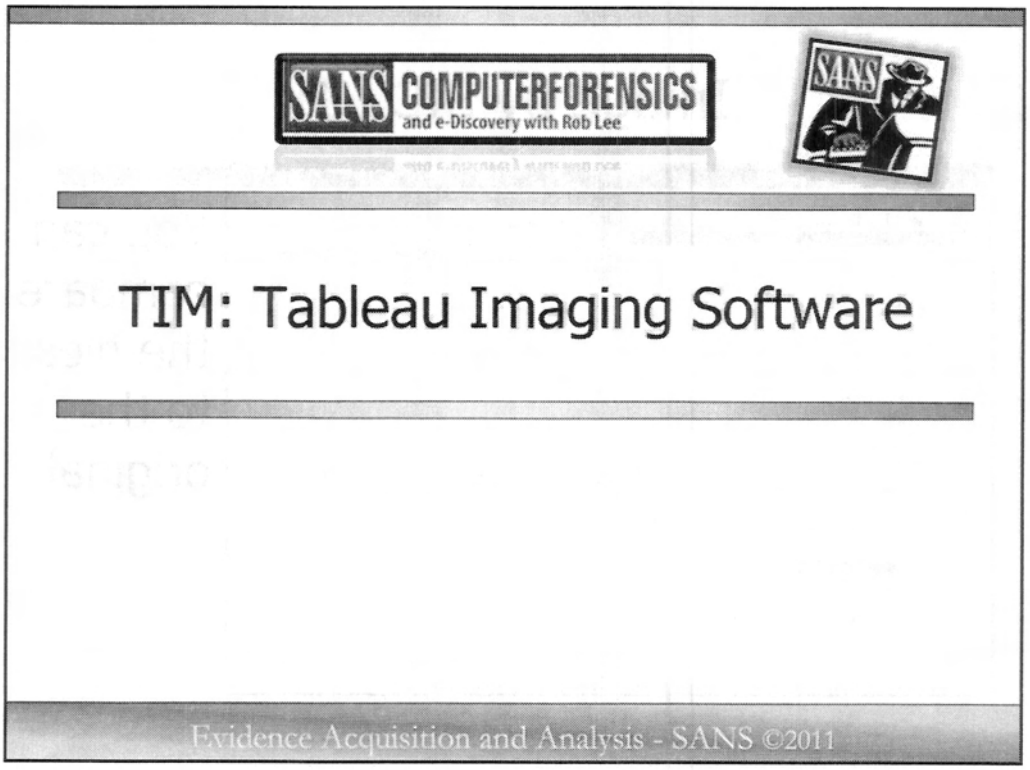
Select the "**Filter by File Ownership**" box.



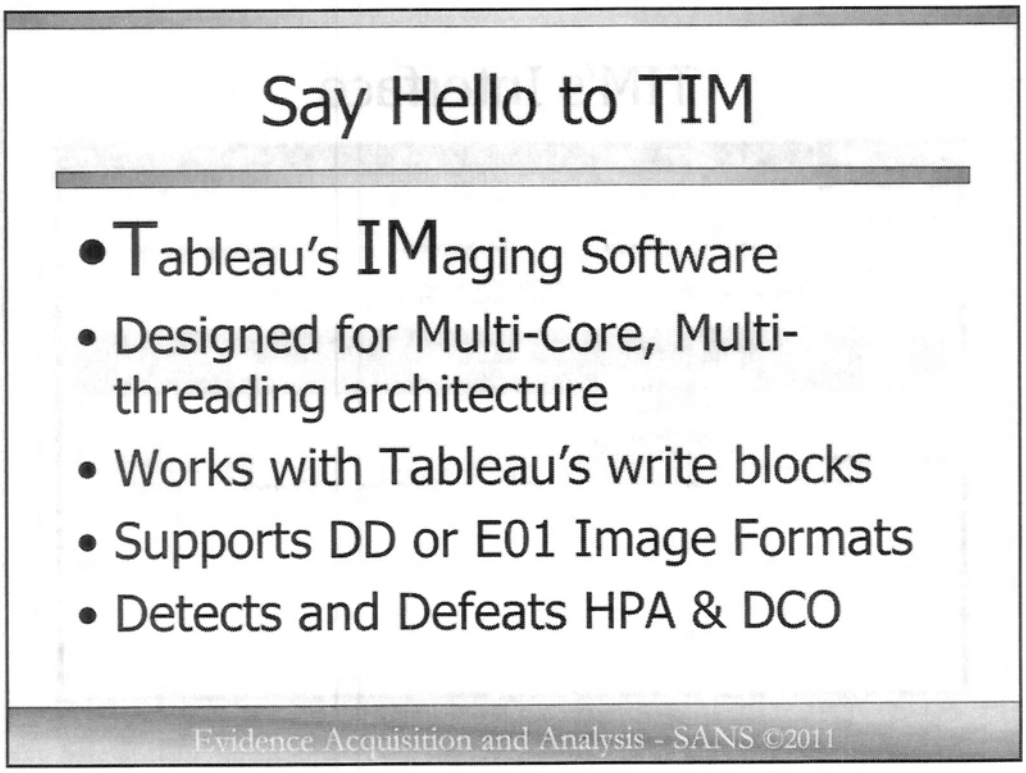
When using the "Filter by File Ownership" feature, you will be presented with a new dialog box that list all the users on the system. Simply select the user who's files you want to image/export and click OK. If the user's account does not show up, you can click the "Add" button and manually add the user's SID. You can also optionally include the user name but the SID is required.



Using this feature can be of great help identifying only those files owned by a particular user. This is also an excellent way of complying with minimization demands of the courts in many civil cases. Lastly, by exporting just the files owned by a particular user, you may more quickly be able to identify activity conducted by that user. Imagine if only the web browsing files, documents, etc., are imaged or exported, how much easier would it will be to zoom in on the user activity without the noise of hundreds or thousands of other users or system files.



This page intentionally left blank.

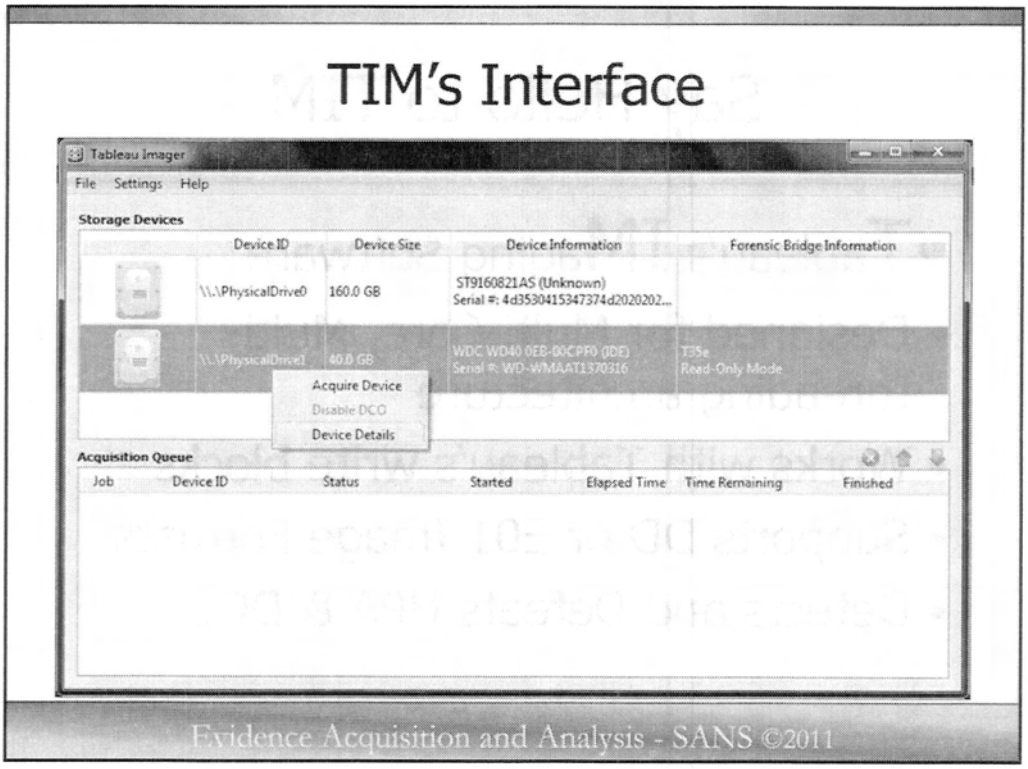


Say Hello to TIM….No not Tim the tool man Taylor, TIM is the new Tableau Imaging software. TIM works seamlessly with the Tableau hardware write blocks like the T35es you received in this class.

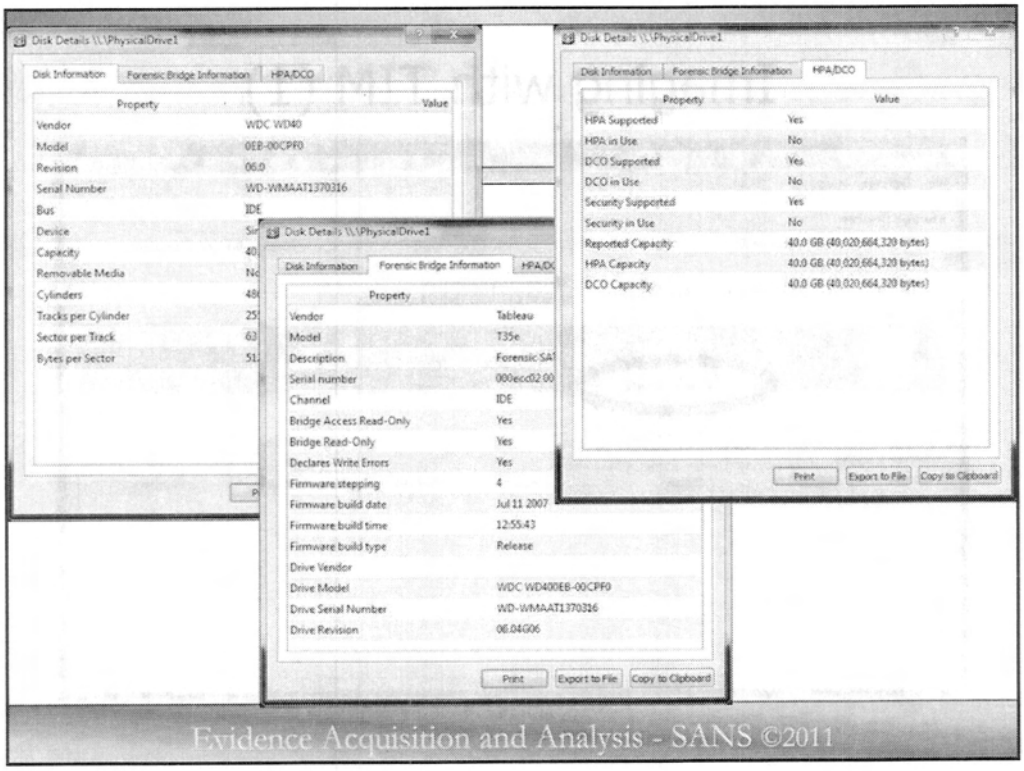
With TIM, you can see and record all features of the Tableau write blocks such as the model, serial number and firmware build.

TIM supports the most popular forensic imaging formats; both DD and EnCase E01s. Tableau reports that because TIM can take full advantage of seamlessly accessing the Tableau hardware write block, it is the fastest imaging software available.

TIM works on Windows XP, Vista and Windows 7 operating systems in both 32 and 64 bit versions.



TIM's user in interface is clean and simple. It has two windows, the top showing the drives connected and the bottom window showing your acquisition queue. You can right click on the attached drives in the top window and select "**Device Details**" to see all the details about each device.



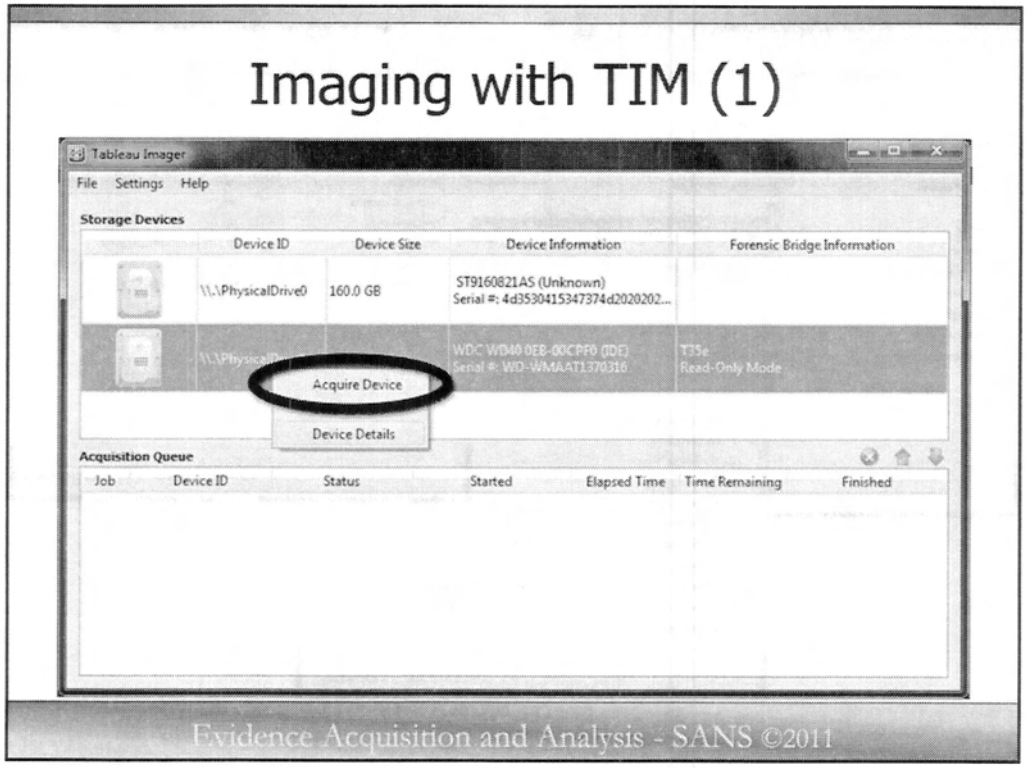
To access all the details about a selected drive, simply click on any of the three tabs across the top. The first tab shown by default is the **Disk Information** tab, which include detailed **Disk Information** about the drive vendor, model, serial number, capacity as well as geometry information like the cylinders, tracks and sectors.

The middle tab is the **Forensic Bridge Information** tab, which provides all the information about the attached Tableau forensic write block. This information includes the model write block you are using, the serial number, connection method (if you are connected to the drive via IDE, SATA, etc.), and all the attributes about the write block.

The last tab is the **HPA/DCO** tab, and it reports the results of any Host Protected Areas (HPA) or Device Configuration Overlay (DCO).

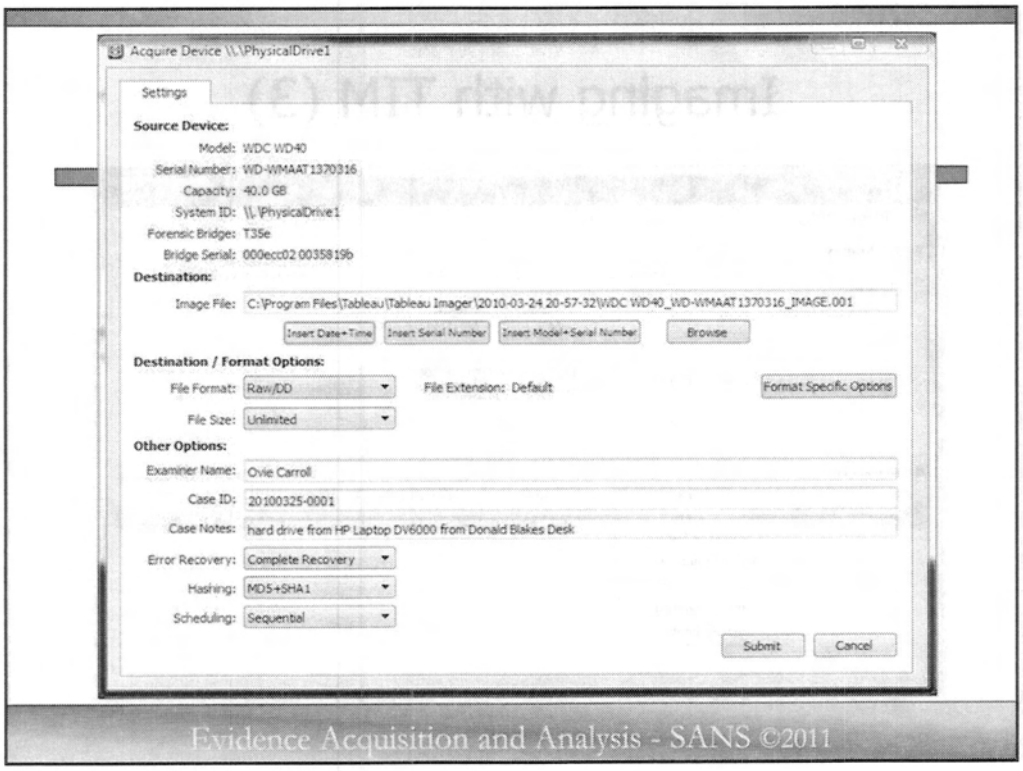
HPA's are essentially reserved area on a hard disk originally designed to store diagnostic tools and boot sector code or other information in such a way that it cannot be easily accessed, modified or changed by the user, BIOS or the operating system. The Disk Configuration Overlays were a way vendors could purchase disks of varying sized and make them all appear to be the same size. So an 80 gig hard drive could have a disk configuration overlay to look like a 60 gig drive. With all these hidden areas it is possible for criminals to hide data from inquiring eyes. TIM, reports any HPA or DCO and gives the true capacity of the drive.

Once an examiner is aware of a drive with an HPA or DCO, appropriate steps can be taken to recover data within the HPA or DCO.



You can schedule or initiate multiple acquisitions to start sequentially or concurrently by right clicking on the device in the top window and selecting "**Acquire Device**".

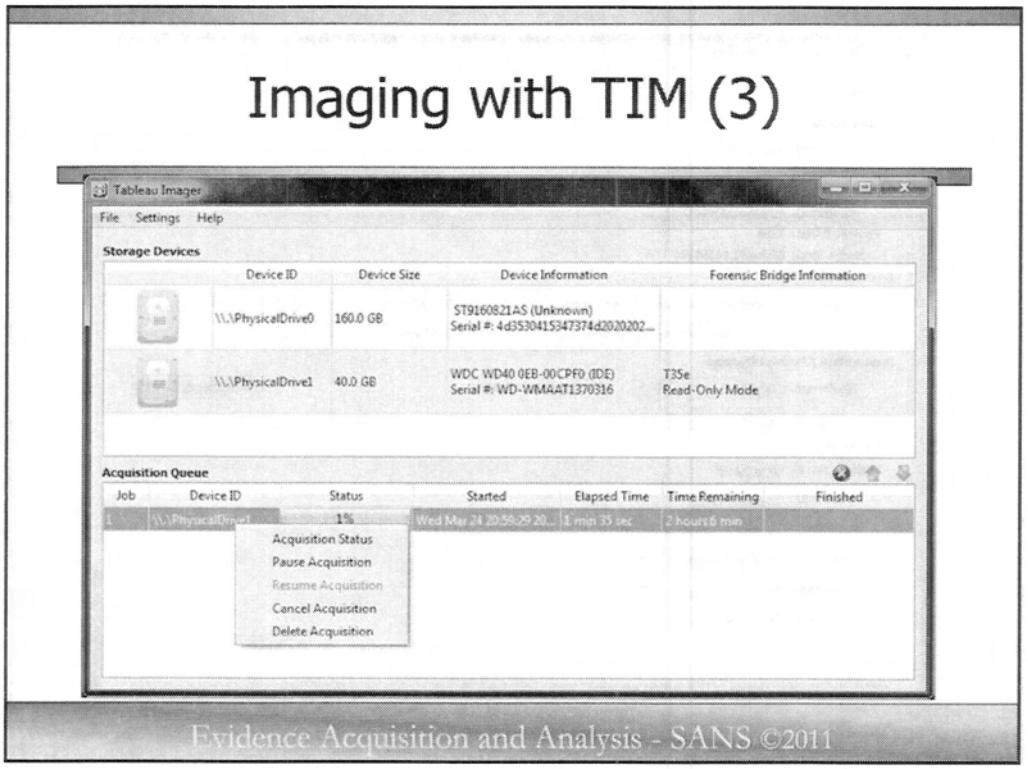
Once you select Acquire Device, a dialog box will appear…



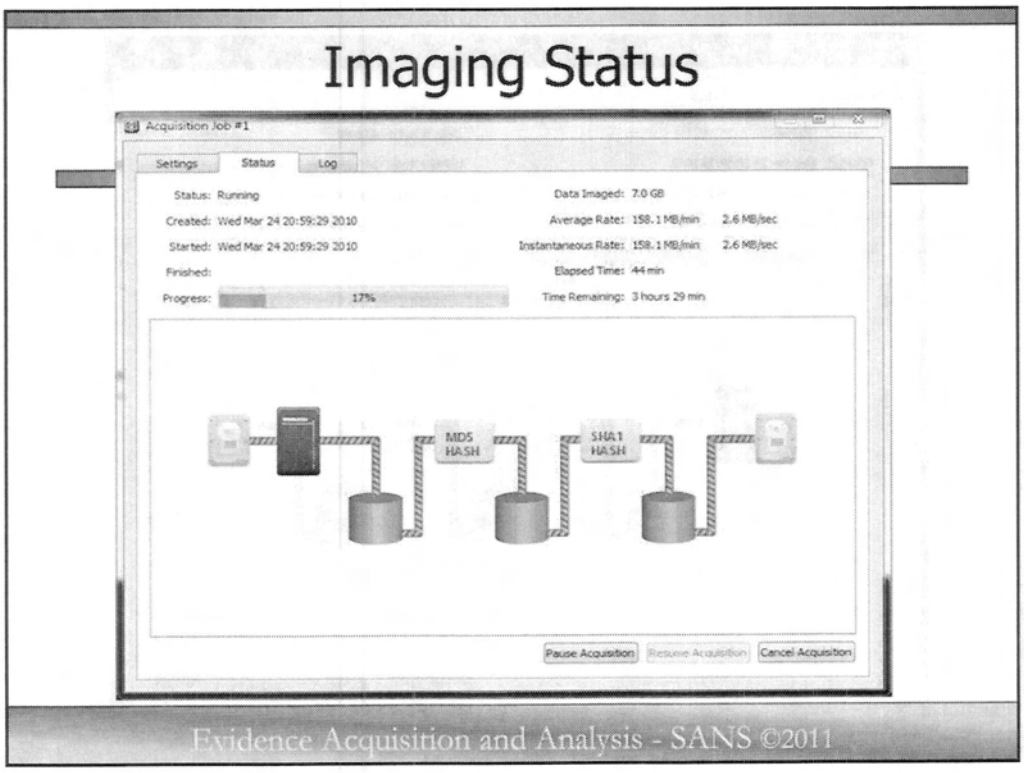
Here you will be able to modify the default location for the forensic image to be created at as well as select the forensic image type of either Raw/DD or EnCase E01 image file format. You can also specify if you want the image file split into 700 MB, 1, 2, or 4 gig chunks or if you don't want the image file split/fragmented, you can select "unlimited".

Again, like most forensic imaging software, you also have the option to document case specific information such as the examiners name, case information and notes. You can choose to have MD5, SHA1, MD5 and SHA1 or no hashing. I can't imagine a reason not to hash an image file.

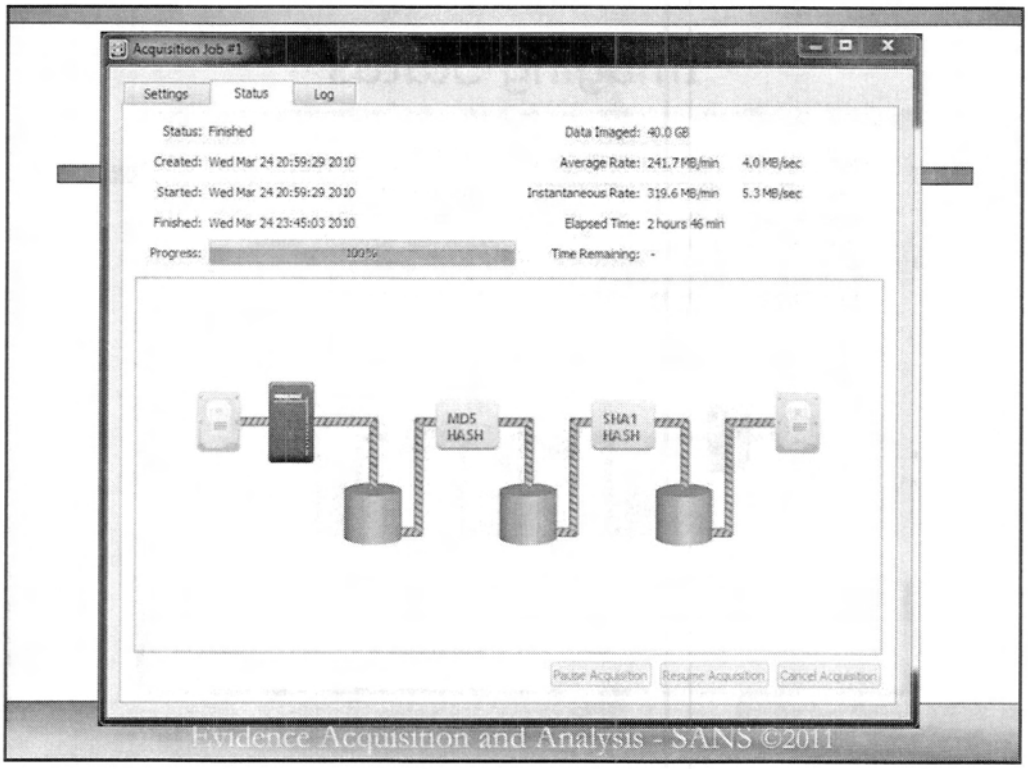
Lastly, if you are acquiring multiple devices, you can choose to launch the imaging jobs sequentially (one after the other) or concurrently/immediately.



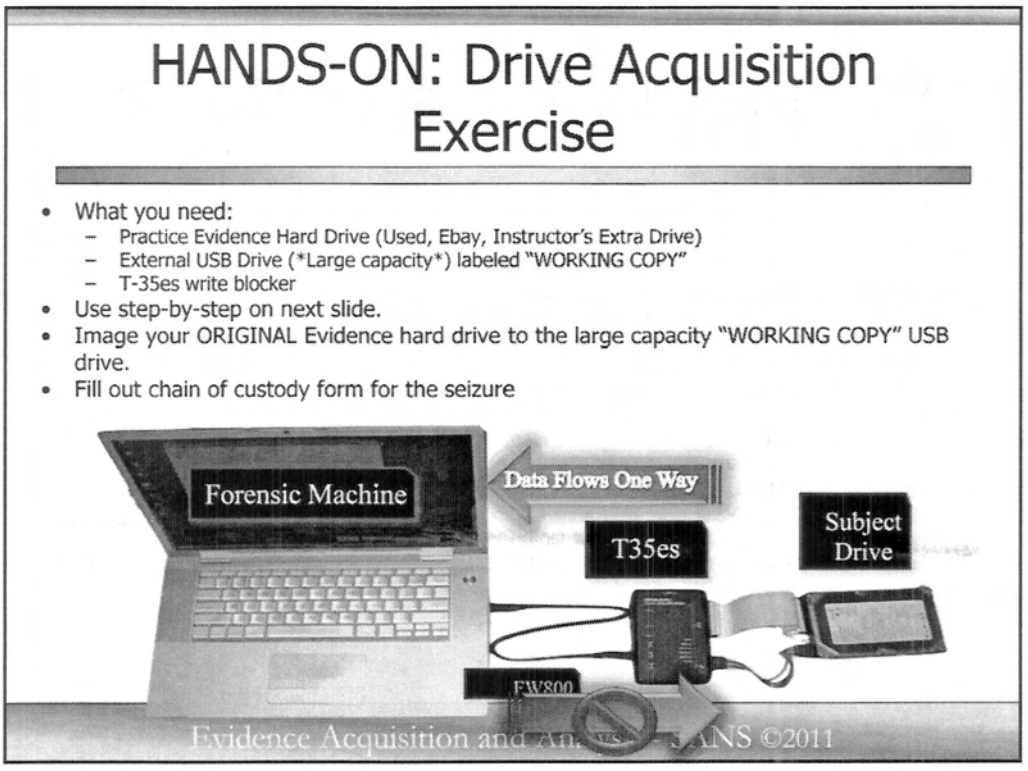
Once you start an imaging job or process, the status is displayed in the bottom window. You can obtain additional information on the status of any imaging job by right clicking on the job in the bottom window and selecting "**Acquisition Status**".



Here you will see a graphical representation of the imaging status. You can click on any icon and receive additional information such as the size of the target and destination drive, Tableau write block device info, etc. You can also click on the "**Log**" tab at the top and see the audit log information.



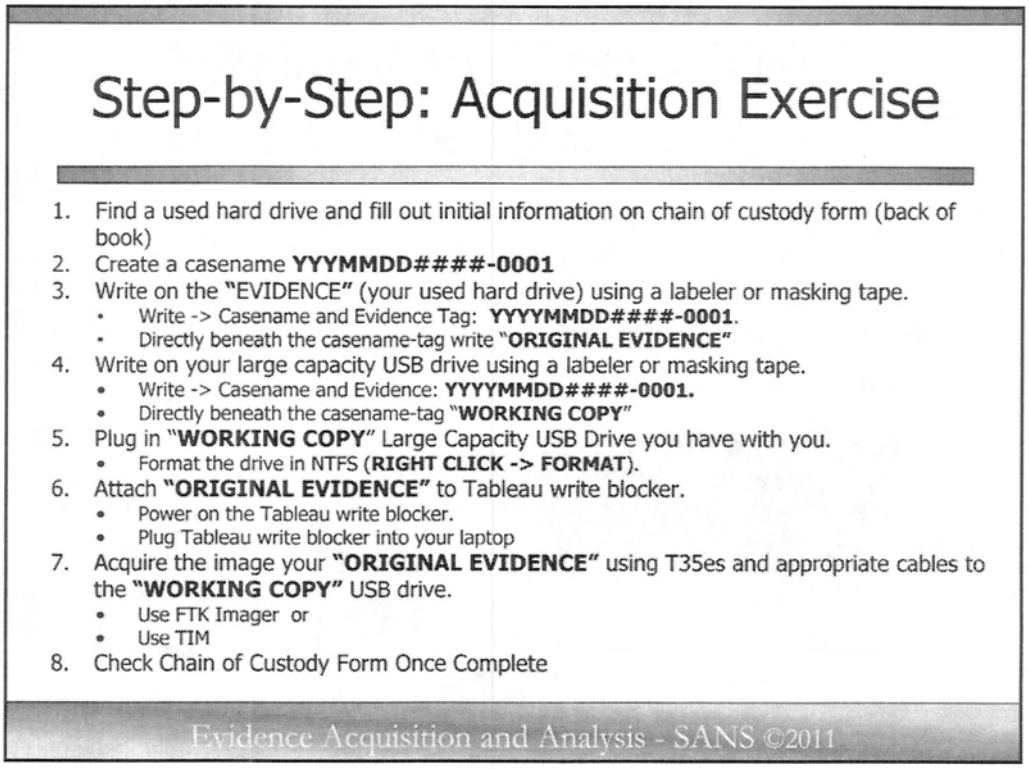
Once finished, the status window will report finished and hovering over any of the hash icons will display the hash values as they are reported and recorded in the audit log.



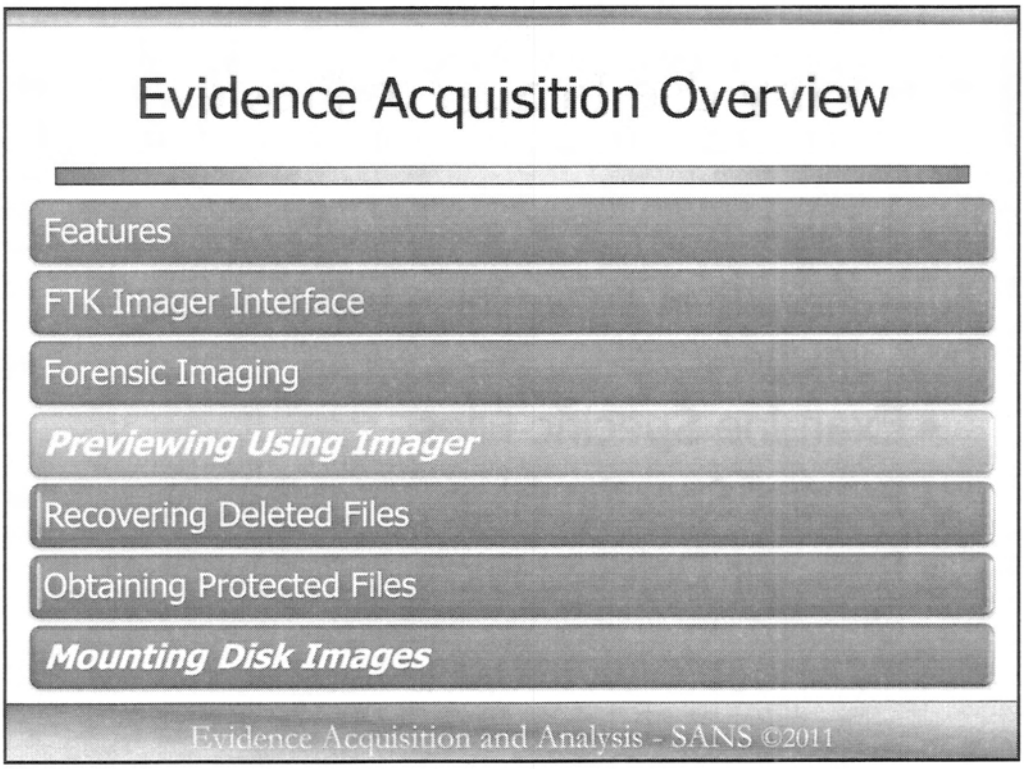
HANDS-ON: IMAGING A HARD DRIVE HANDS-ON

Utilizing your knowledge from the first part of the class, follow the instructions of the Step-by-Step Acquisition Exercise to fill out an evidence tag and image the used hard drive you brought to class.

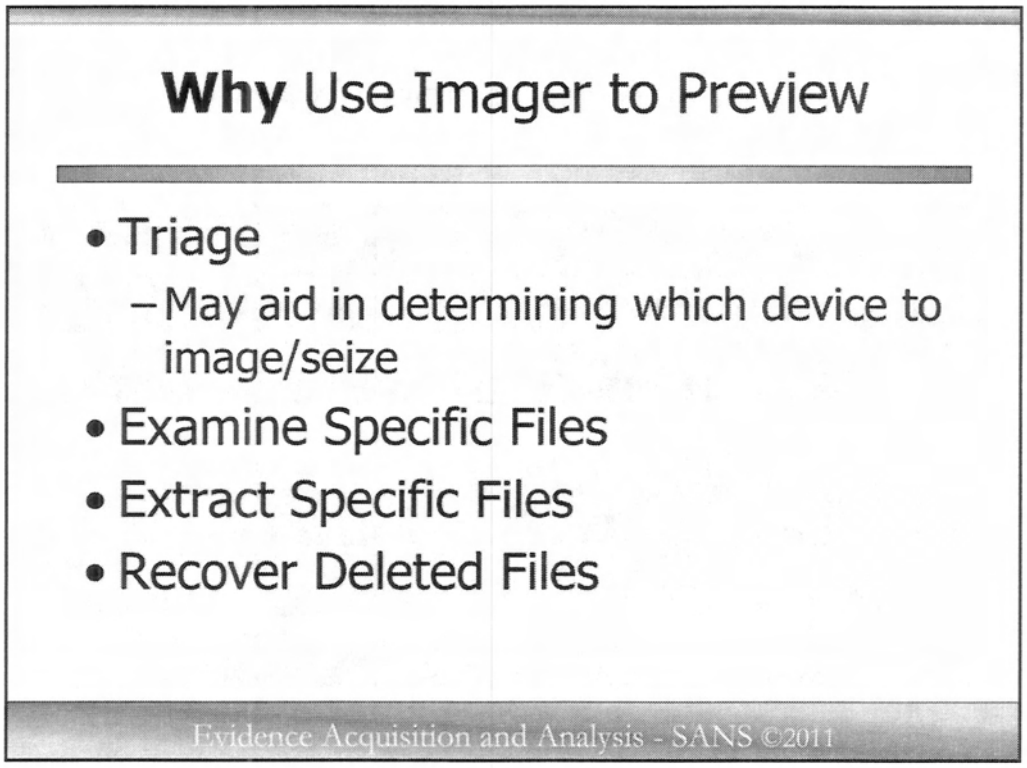
Note: This exercise will take some time to complete. It might not finish during class. If not I recommend you practice this again in your room tonight.



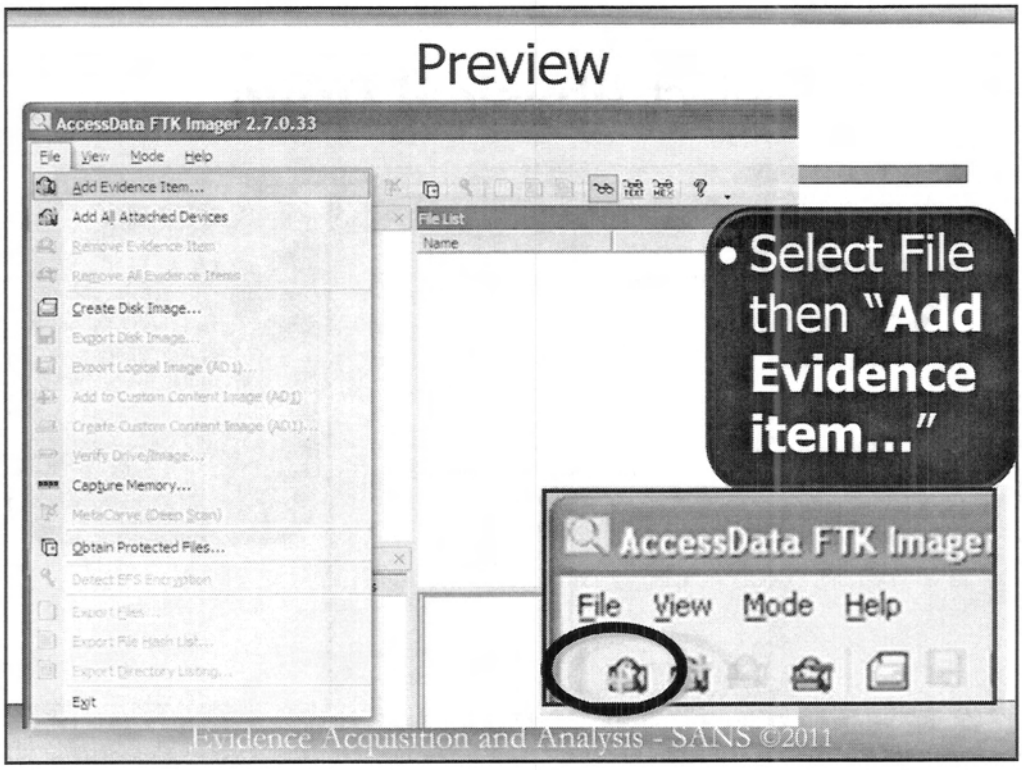
1. Find a used hard drive.
2. Create a casename **YYYMMDD####-0001**
3. Write on the **"**EVIDENCE**"** (your used hard drive) using a labeler or masking tape.
   Write -> Casename and Evidence Tag: **YYYYMMDD####-0001**
   Directly beneath the casename-tag write "**ORIGINAL EVIDENCE"**
4. Write on your large capacity USB drive using a labeler or masking tape.
   Write -> Casename and Evidence: **YYYYMMDD####-0001**
   Directly beneath the casename-tag "**WORKING COPY**"
5. Plug in "**WORKING COPY**" large capacity USB drive you have with you.
   Format the drive in NTFS (**RIGHT CLICK -> FORMAT**)
6. Attach **"ORIGINAL EVIDENCE"** to Tableau write blocker.
   Power on the Tableau write blocker.
   Plug Tableau write blocker into your laptop
7. Acquire the image your **"ORIGINAL EVIDENCE"** using the T35es and appropriate cables to the **"WORKING COPY"** USB drive.
8. Fill out chain of custody form for the seizure. Have your neighbor check your documentation.



Next, we will be discussing how you can use FTK Imager as a previewing tool, while both on scene or back at the lab. Sometimes, before you start imaging, particularly when you have multiple systems to image, you want to preview the drive to see which system may be most critical to start imaging first. FTK Imager provides a very easy-to-use feature that allows you to do that.

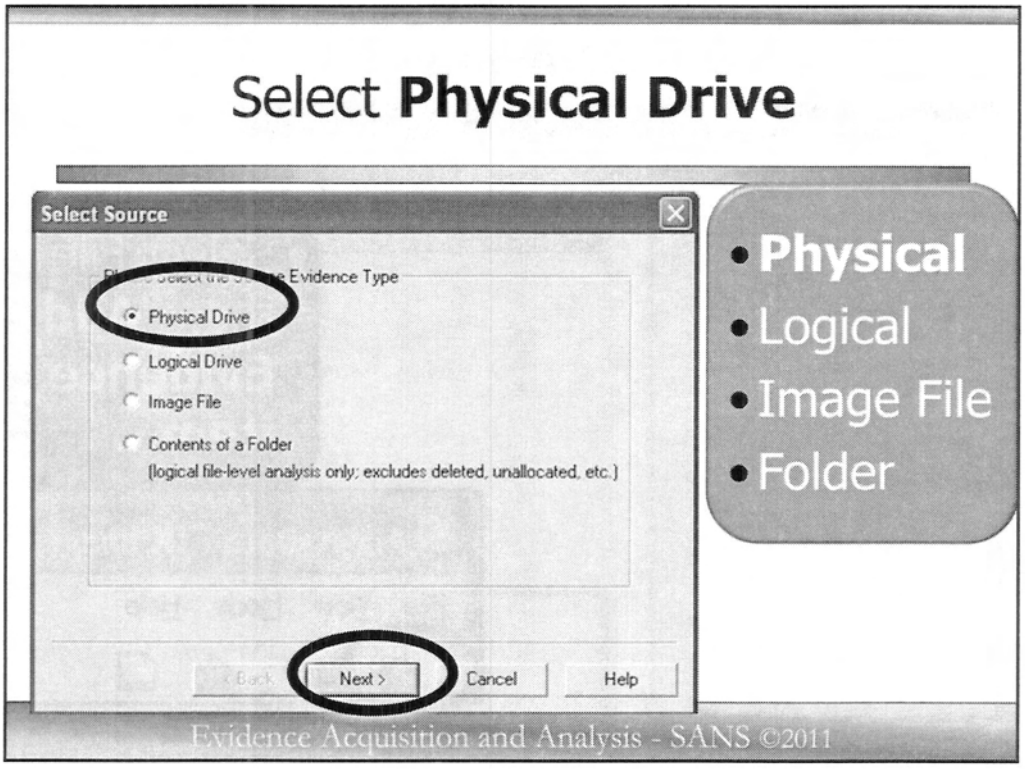


As I mentioned in the overview, one of the power features of FTK Imager is the ability to preview evidence before imaging it. Preview can be used to conduct a triage, look for and or export specific files before, or in lieu of, conducting a time consuming forensic image.



Now, once you have inserted your thumb drive and it has been recognized by your system, and you start FTK Imager, from the File Menu Bar, select "**File**", then select "**Add Evidence item…**"

Now, as many of you know, there is always more than one way to do anything on a computer. So just to touch on another way you can do this, you could also simply click on the 1st icon on the Toolbar. The icon looks like a magnifying glass with one green plus symbol. Be careful not to click on the second icon from the left with two green plus symbols, because that will add every drive connected to your system into FTK Imager's preview.



You are now presented the Source screen where you indicate what type of device you would like to preview.

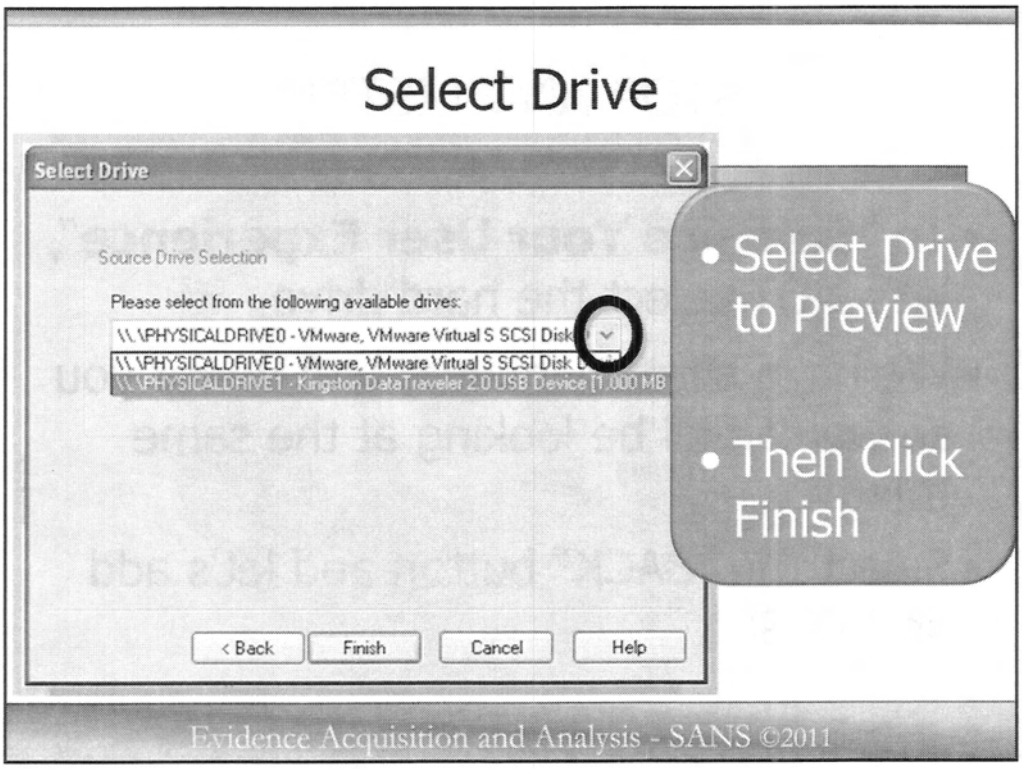
In the forensics world, since you typically want to see everything including the deleted files and unallocated space, you will almost always choose **PHYSICAL** drive. This will show you all the allocated and unallocated space, active and deleted files, etc.

The Logical drive is handy for multi-disk RAID systems where you want to see the logical volume rather than each individual drive.

Image File will allow you to open and preview a previously imaged drive that has been created in any of the supported formats. This comes in real handy back at the lab or if you need to look inside a DD file or Encase image file.

We also suggest using this technique for defense attorneys or other reviewing officials (not on our team) that may not have $5,000 for forensic software licenses.

Select "**Next >**".

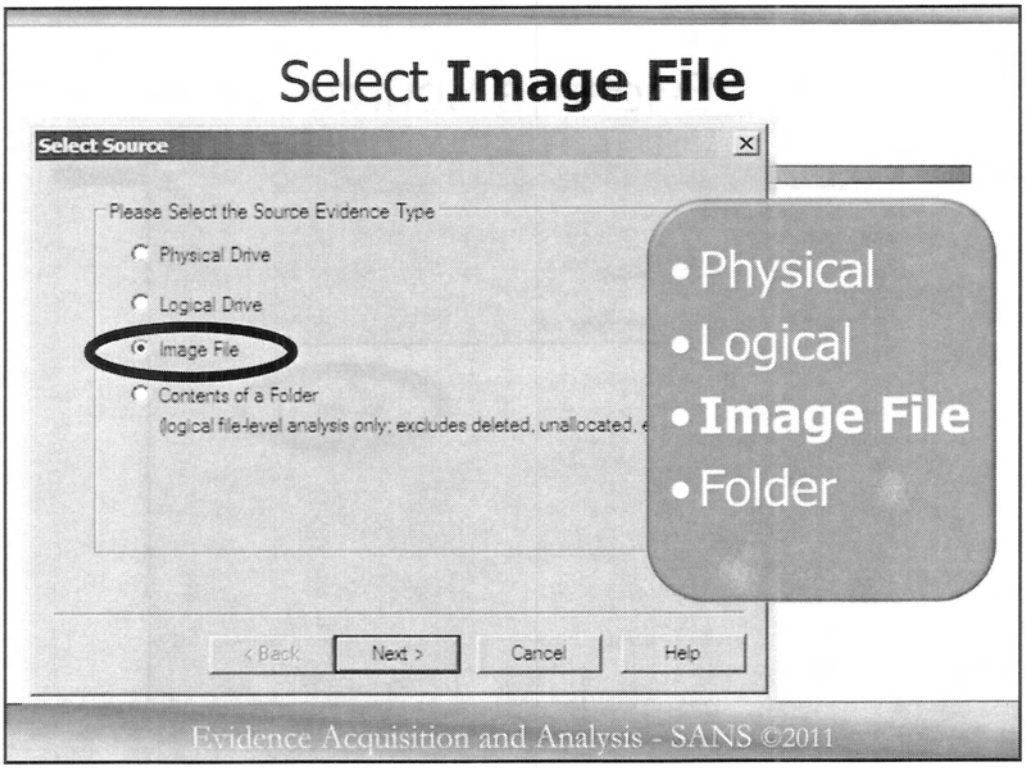


By selecting the down arrow button on the middle right side on the Select Drive dialog window, you can see all the physical drives attached to your forensic system. If you have your thumb drive attached, you will see Physical Drive Zero, which is typically your operating system, then Physical Drive One, which would be the second drive (this would typically be your suspect's hard drive you want to preview). If you have your thumb drive in your computer, you will likely see that it is listed as Physical Drive One.

BUT WAIT - DO NOT CLICK FINISH!

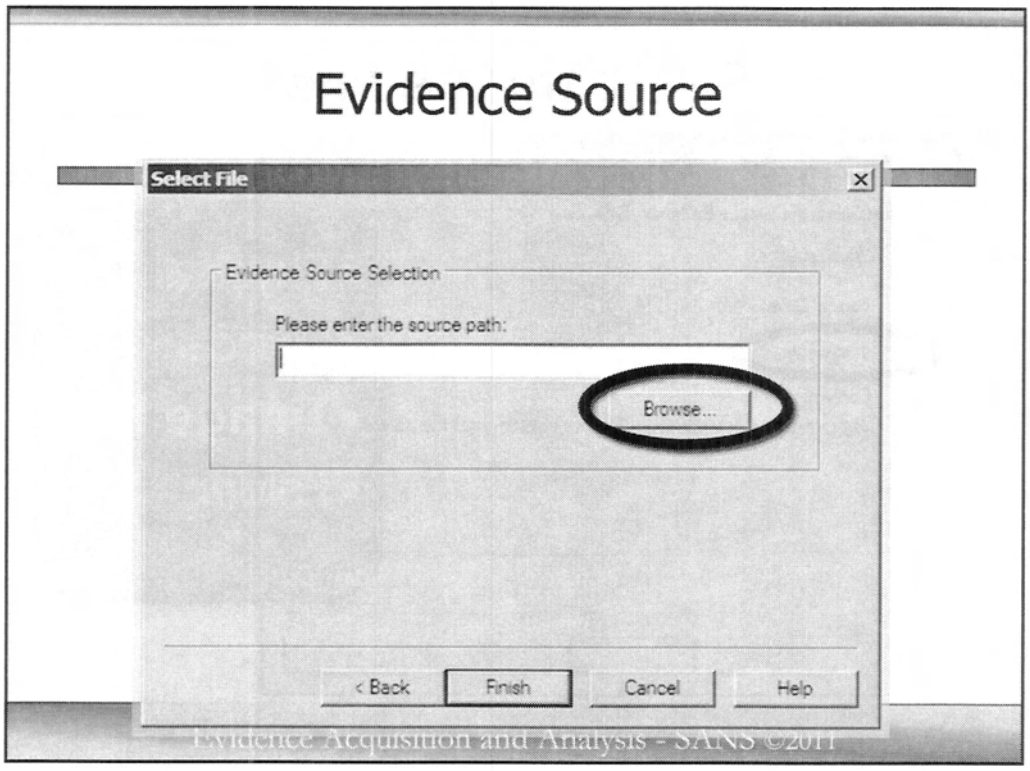
In order to better show you the Preview features as well as how you can use FTK Imager as a lightweight recovery tool, we have created an image file for you to use in this exercise. Do not click the Finish. Instead, click the **BACK** button and let's go to the previous screen where it asked you what device do you want to add.

Using the image file we have created will allow you to see exactly what everyone else is seeing. After we go through this part of the lesson, we will give you time to do this with your own thumb drive, but for now, we ask that you follow along with me.



So you should have selected the "**BACK**" button. As we said, in order to preview a hard drive or any device, you would select physical image. For this exercise, so we can all be looking at the same thing, let's select "**IMAGE FILE**", then select "**NEXT**".

If you were looking at your drive, you would follow all the same procedures as you did when imaging. The only difference is that you chose to preview, rather than create, an image.

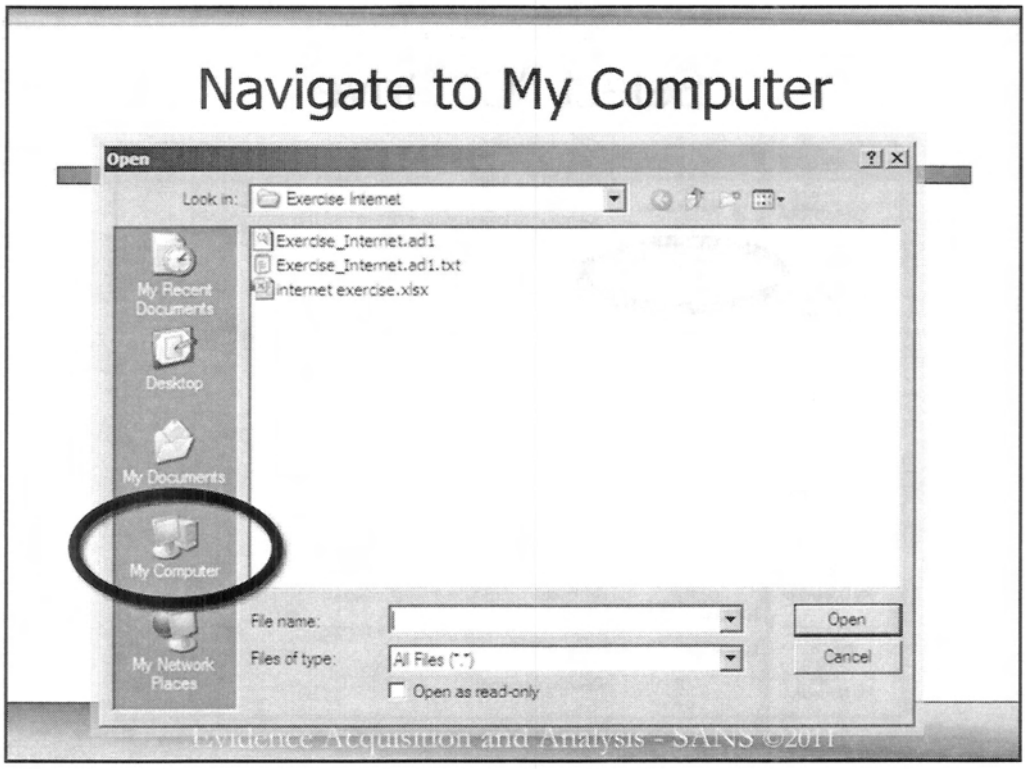


Because you said you wanted to load an image file, FTK Imager should now prompt you for the location of the image file you would like to preview.

Go ahead and select the "**BROWSE**" button and let's navigate to our image file.

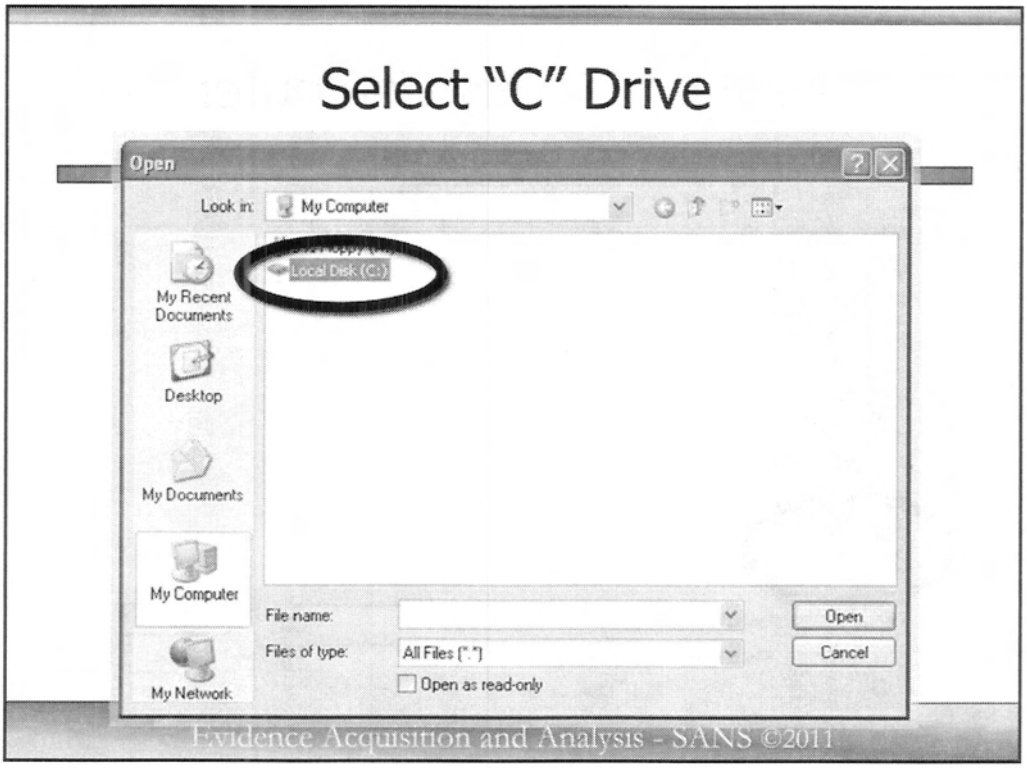
Navigate to the C:\cases\thumb_drive_caseYYYYMMDD###-001\YYYYMMDD####-0001.E01 and select it.

This is the same technique you would use back at the lab or even on-scene after you imaged a system and perhaps you need to quickly preview the device but don't want to have FTK go through the indexing and creation of a case file. I have used this technique to both preview as well as locate and extract specific files quickly for use in interviews, interrogations and even to extract a file and give it to a prosecutor so it can be used in a detention hearing to keep a subject in jail.

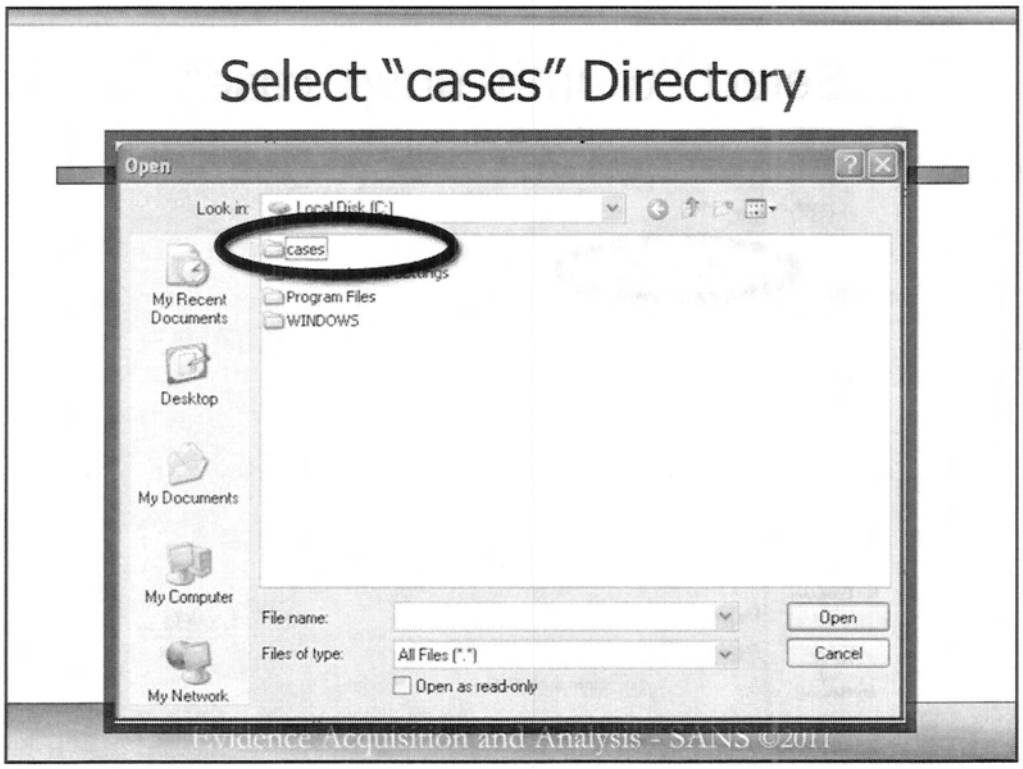


Again, to keep us all on the same page, first, let's start by clicking on the My Computer icon on the left side of the screen. This will take you to the display that will show you all your logical drives connected and recognized by your system. You can also use this if you have a forensic server or the image file is on a networked drive in the lab and you wanted to quickly look at something or extract data. In that case, you would simply click on the My Network Places, navigate to the location where the drive image file is, then select the image file.

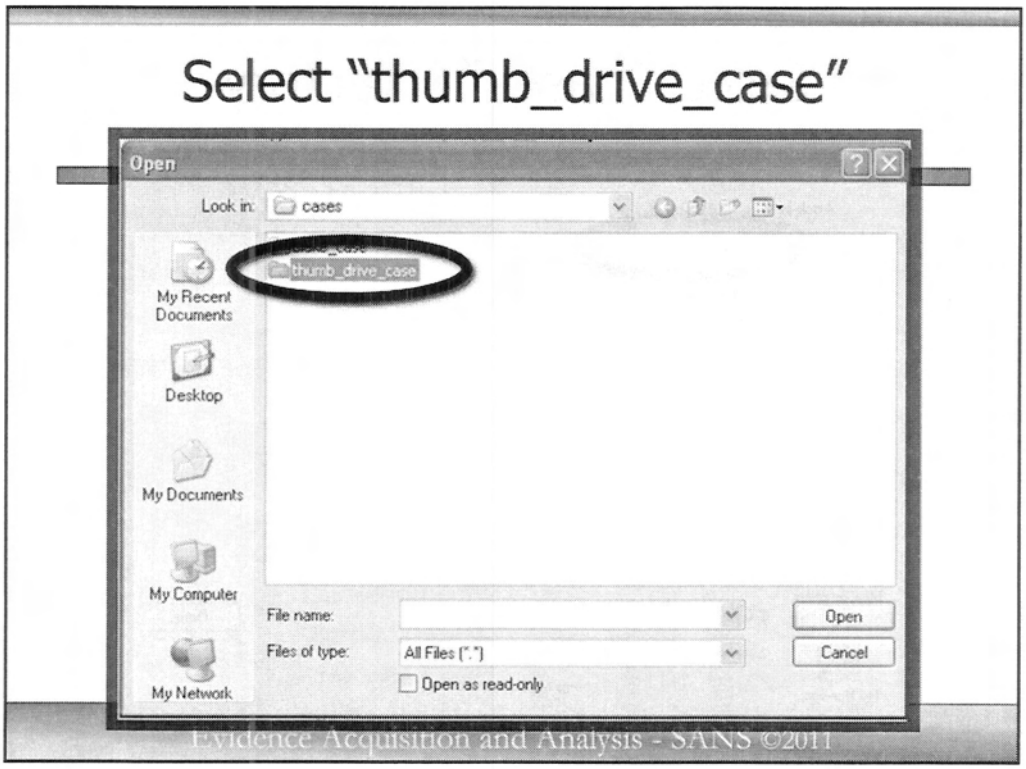
Again, to stay on track with us, let's select the computer icon by clicking on it once.



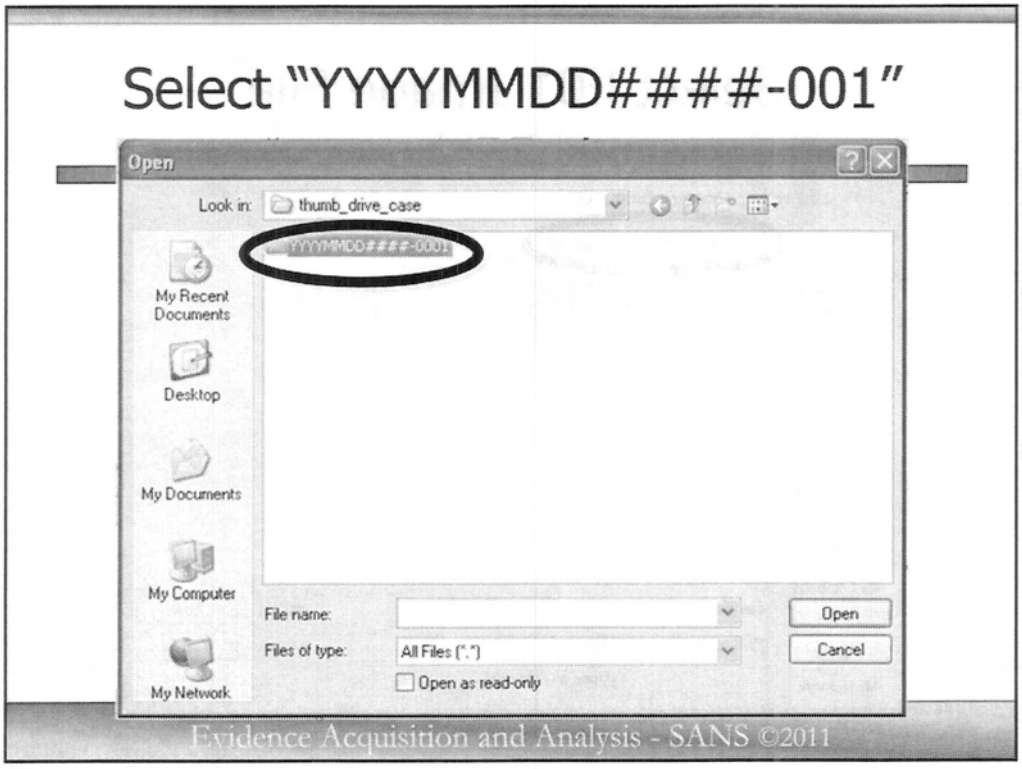
Now you should see all the drives connected to and recognized by your forensic system. At this point, simply select the "C" drive by double clicking on the icon next to the "C" drive, or for those who are opposed to double clicks, you can click once on the "C" drive, then click "Open" This will now take you inside the "C" drive where we can navigate to the location of our image file.



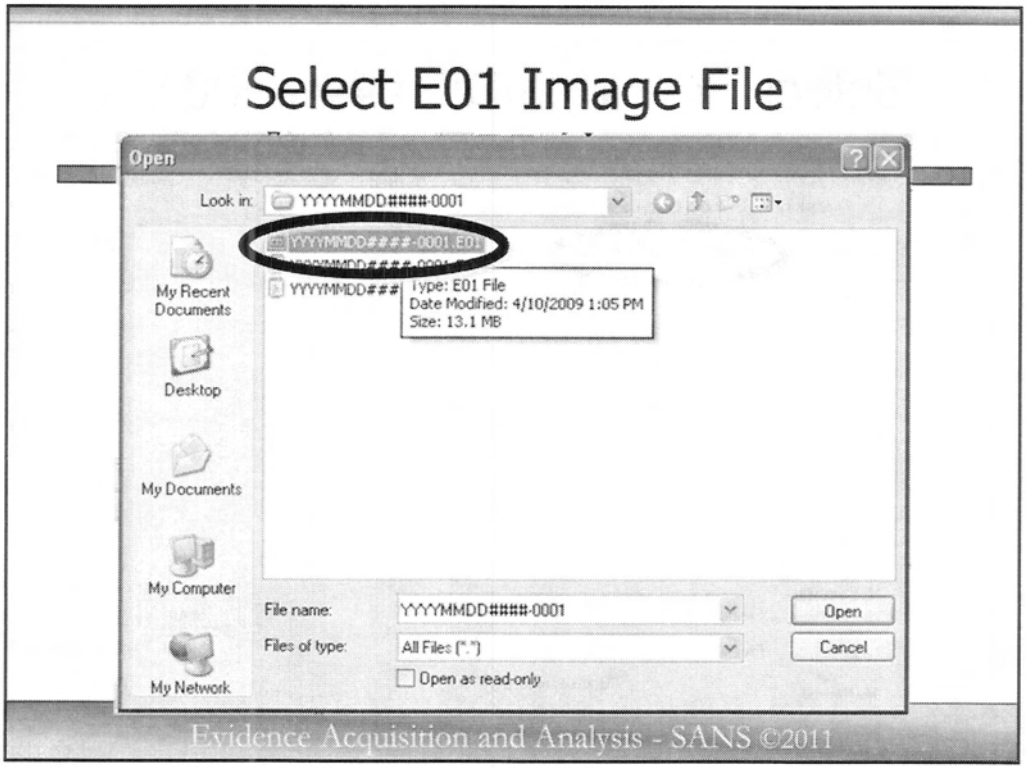
You should now see all the directories in the root of your "C" drive. At the very top of that list you should find a directory folder named "cases" (all lower case). Double click on the directory folder labeled "**cases**" to navigate inside that directory. Again, all we are doing at this point is navigating to the location that contains our image file.



Inside the cases directory folder, you should find at least two additional directory folders. Find and double click on the directory folder labeled "**thumb_drive_case**".



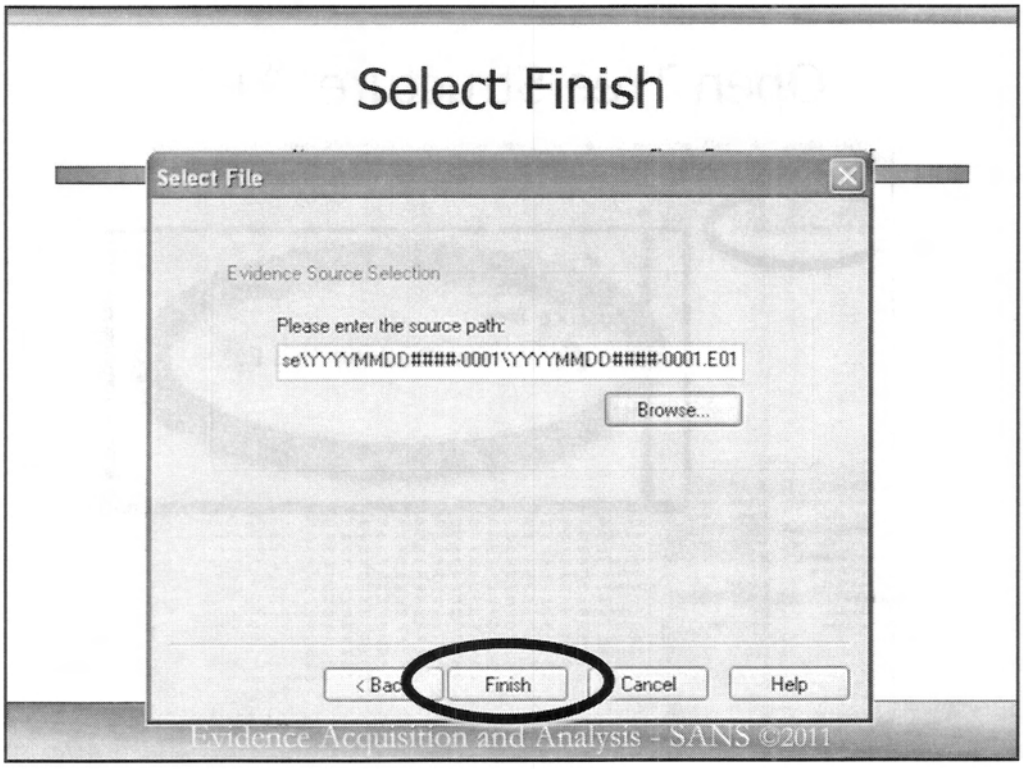
You can see how we have organized everything into a case folder. Because you will often have more than one piece of electronic evidence per case, we have also created sub-directories for each individual item. Find and double click on the directory folder labeled "YYYYMMDD####-001".



Inside this folder you should see three files. An EnCase E01 image file, a CSV or Comma Separated Value file and a text file, which is the audit file.

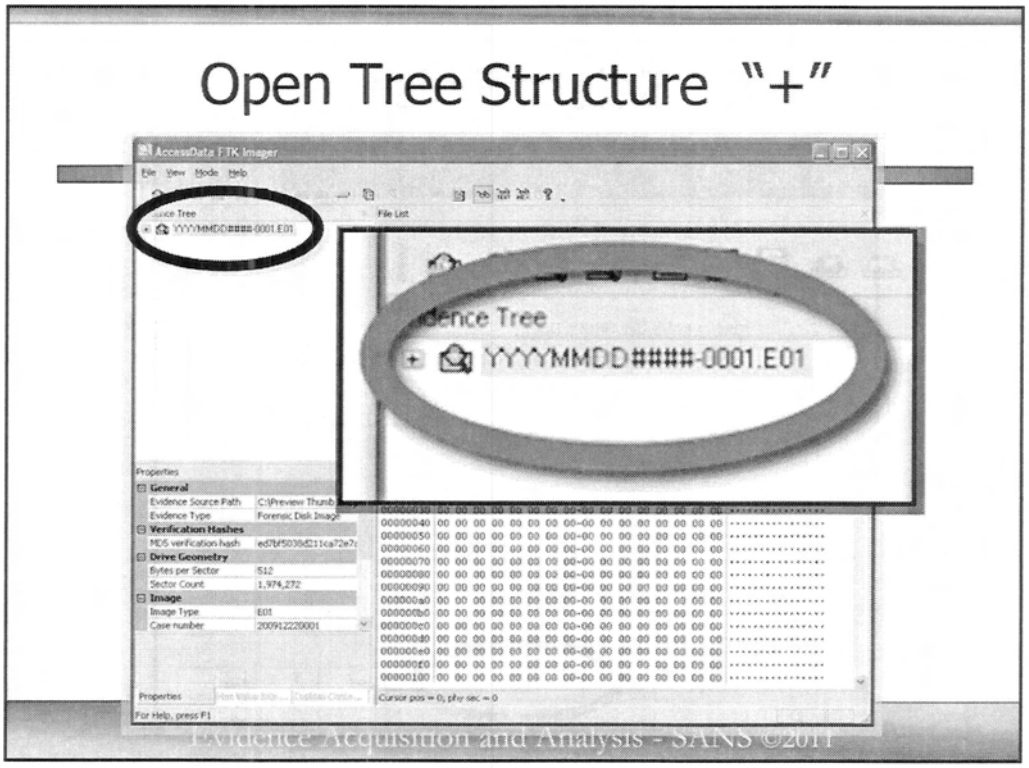
Find and double click on the top file labeled "YYYYMMDD####-0001.E01.

If you want to get a little more information about this file, if you place your mouse over the file, you should see the file type is E01, the date the file was last modified, and the file size. We are looking for the file that is 13 MB. You could also change the file view preferences in this dialog box to the detailed view and it would show you all of the files sizes.



You should now be back at the "**Select File**" dialog box.

Here you should verify the image file you just selected is listed correctly in the dialog box. After verifying, select "**Finish**" This will complete the process and add the device to your preview window.

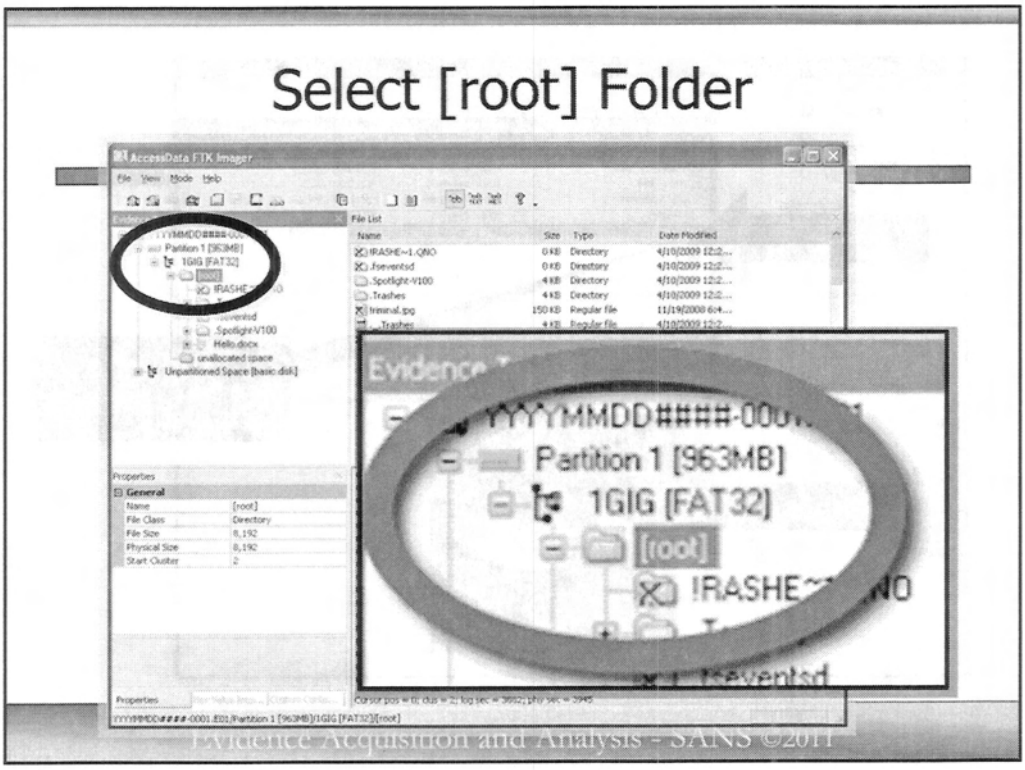


At the top left corner of the FTK Imager application, in the Evidence Tree window, you will see the image file/evidence you just added.

To the left of the evidence file name you will see a plus symbol.

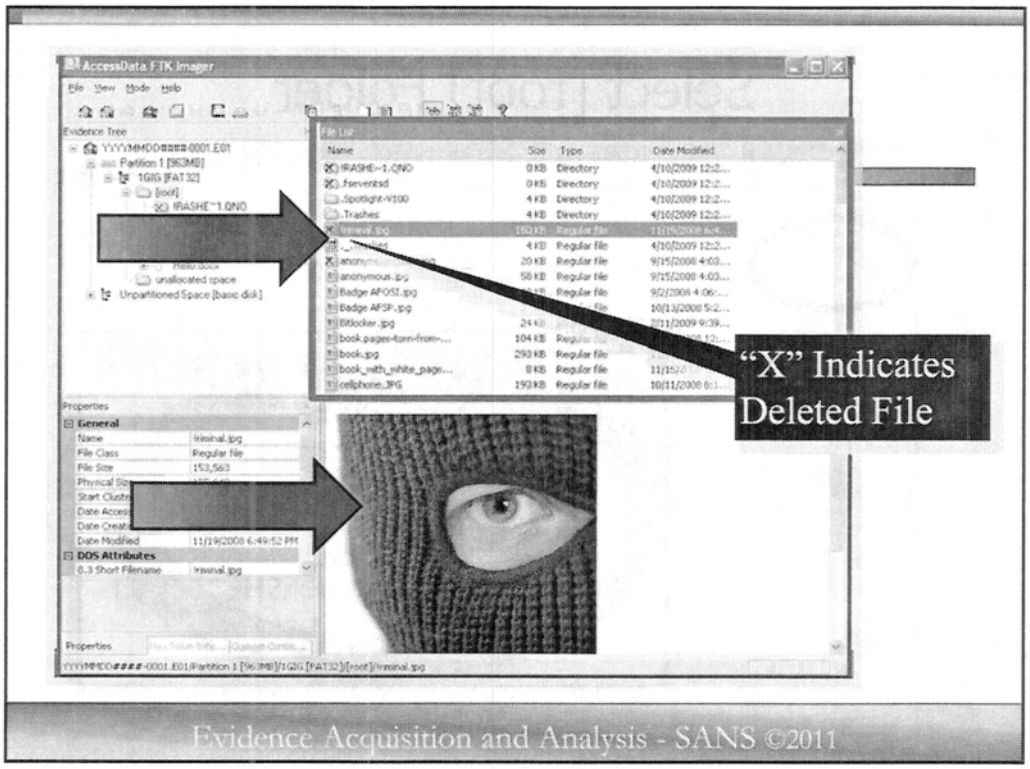
Just like in the Windows operating system, if you click on the plus symbol, you will open one level of the directory tree structure.

You should start to see the partition and directory structure. Go ahead and start clicking on the plus symbols to start expanding the directory tree.



As you expand the directory tree, once you reach to the directory labeled [root], you are now at the root of the partition.

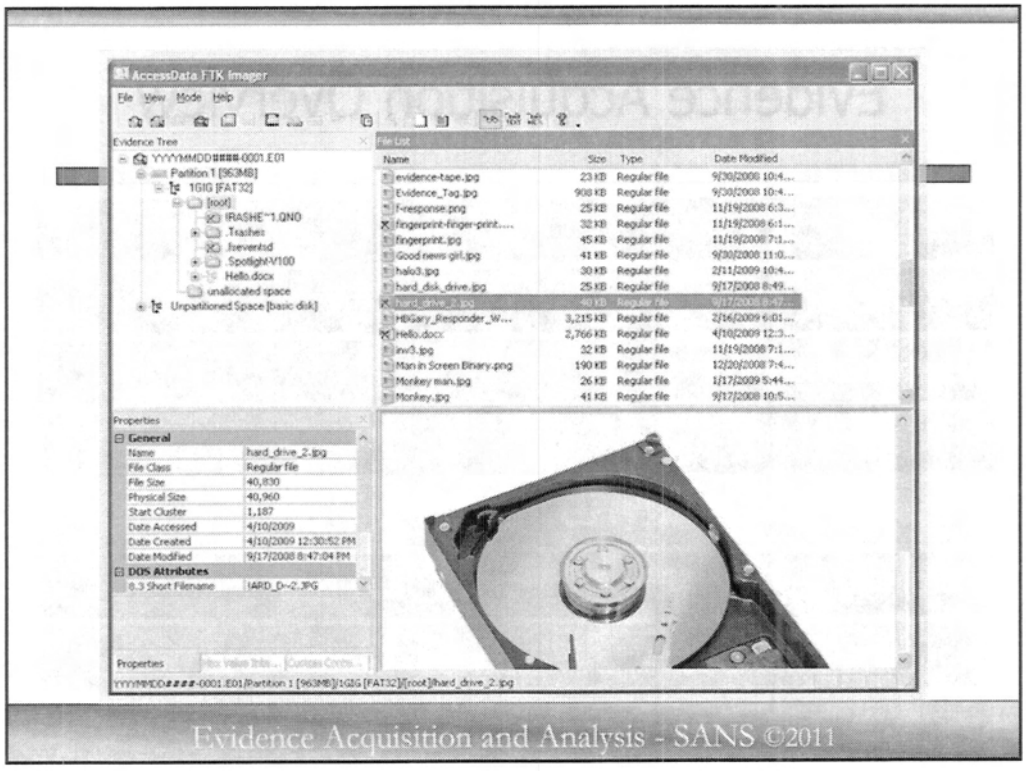
Once there, go ahead and expand at least one more directory, then click once on the directory labeled [root].



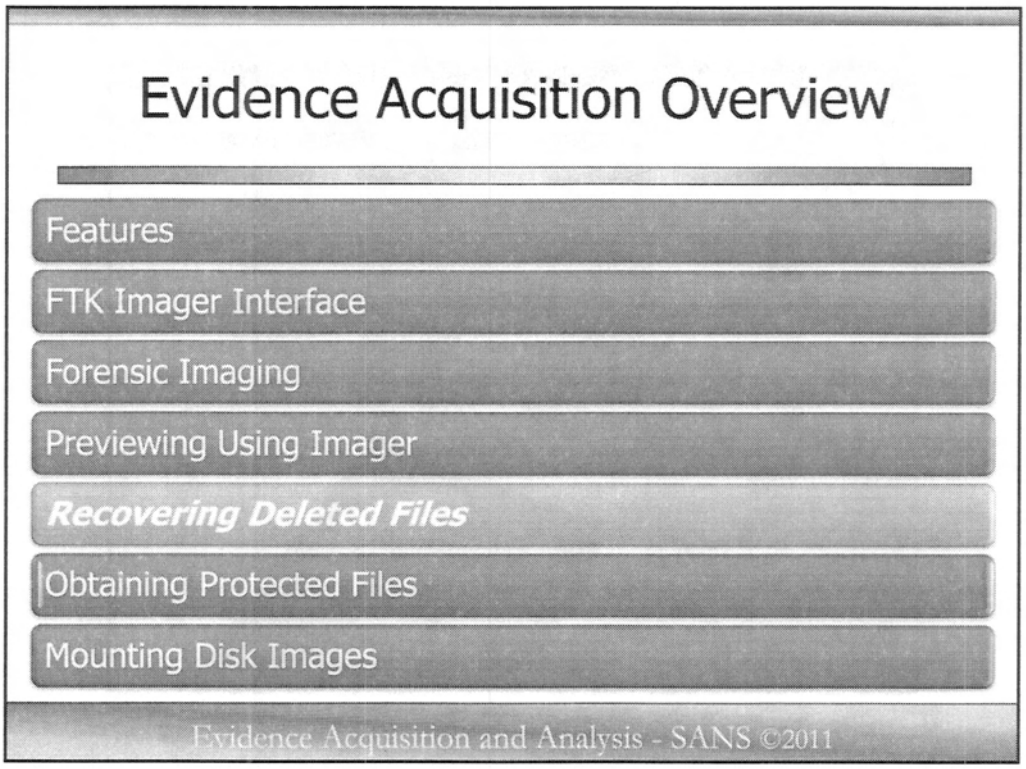
Now that you have selected the [root] directory in the Evidence Tree window, look to the window directly to the right of the Evidence Tree window we earlier identified as the File List window.

You will see that some of the files have a red "X" on top of their icon. This red "X" indicates the file is deleted and FTK Imager is able to recover the file for you.

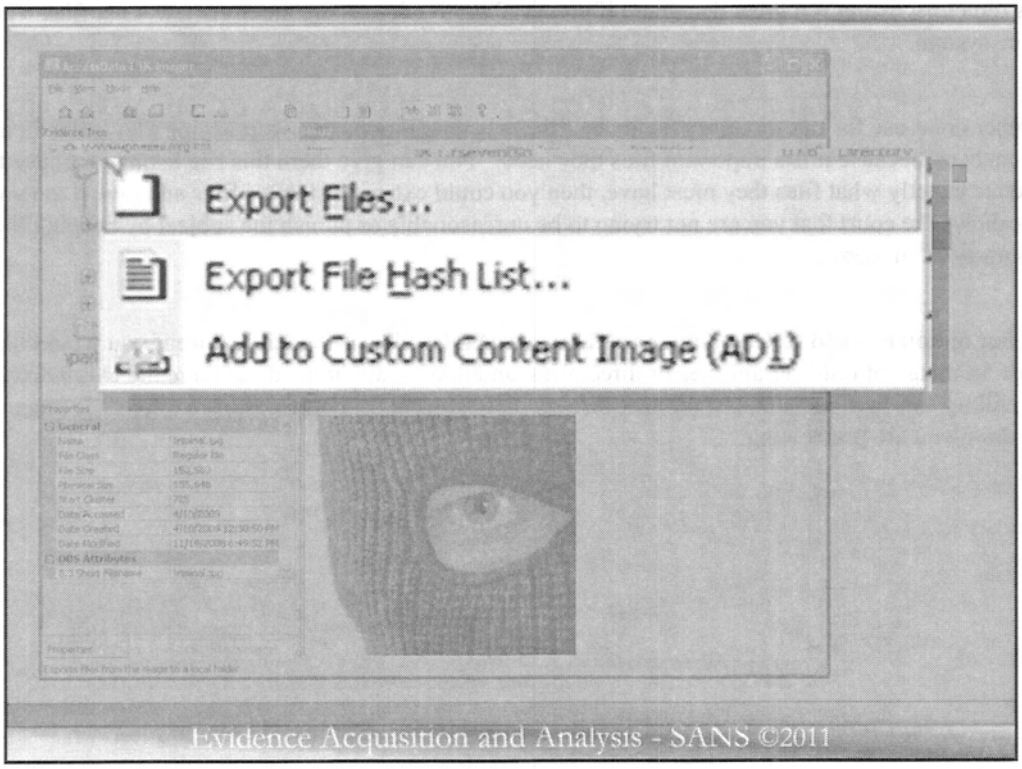
Find one of the deleted files and click on it. When you click on any of the files, the file or its contents are displayed in the viewer pane located directly below the File Viewer window.



I would like you to go ahead and take a look at a couple of files and see how they are displayed in the viewer window. You can even look at the files with the "X" on them indicating they are deleted. You can navigate through any piece of electronic evidence this way and preview what kind of evidence or files are on the system, assuming the evidence has a file system recognized by FTK Imager. Just by doing this you can sometimes identify exactly the files or information you need in your investigation and either confront the subject, identify additional time critical evidence that require additional investigative leads, etc. Imagine having this ability on-scene to give files to the investigators, all before they even leaves the scene. I have also found sometimes that is is useful to bring the case agent over to my computer and we quickly poke through the system together.



Now that you have seen how FTK Imager can be used as a preview tool, let's go ahead and see how you can use FTK Imager to RECOVER deleted files or quickly export files from a hard drive.



Go ahead and find the file called "**!riminal.jpg**" or any file that has the red "X" on it indicating it is a deleted file.

If you RIGHT CLICK on that file in the File List window, you will see three options:

Export Files…

Export File Hash List…

Add to Custom Content Image (AD1)

Export Files allows you to export the file, files, or directory to a location of your choice. We will be doing this in just a moment, but let's first talk about the other two options.

Export File Hash List creates a (CSV) Comma Separated Value file of the file or files you have selected. This file includes the MD5 and SHA1 hash as well as the full path and file name of the file. You can also select a directory in the File List window pane and it will create a CSV file containing all files and subdirectories below the selected directory.

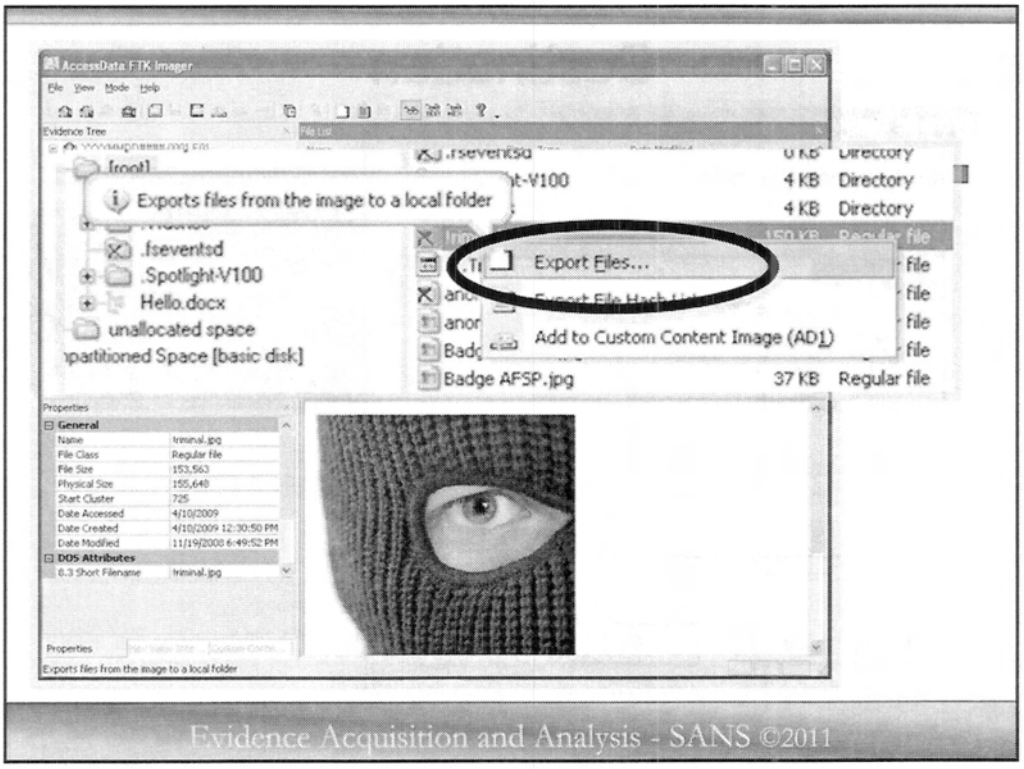
If you want to create a hash file list of everything on the device, you can click at the very top of the tree structure in the Evidence tree window pane (on the left side), then choose "Export Directory Listing". This will give you a nice list of every partition:

- File name & Full path
- File Size
- Created, Modified and Accessed Time
- And a YES or NO as to if the file was deleted or not
- **It DOES NOT give a Hash list for each file**

This directory listing is a great document if you need to give it to someone to review what files were on the system.

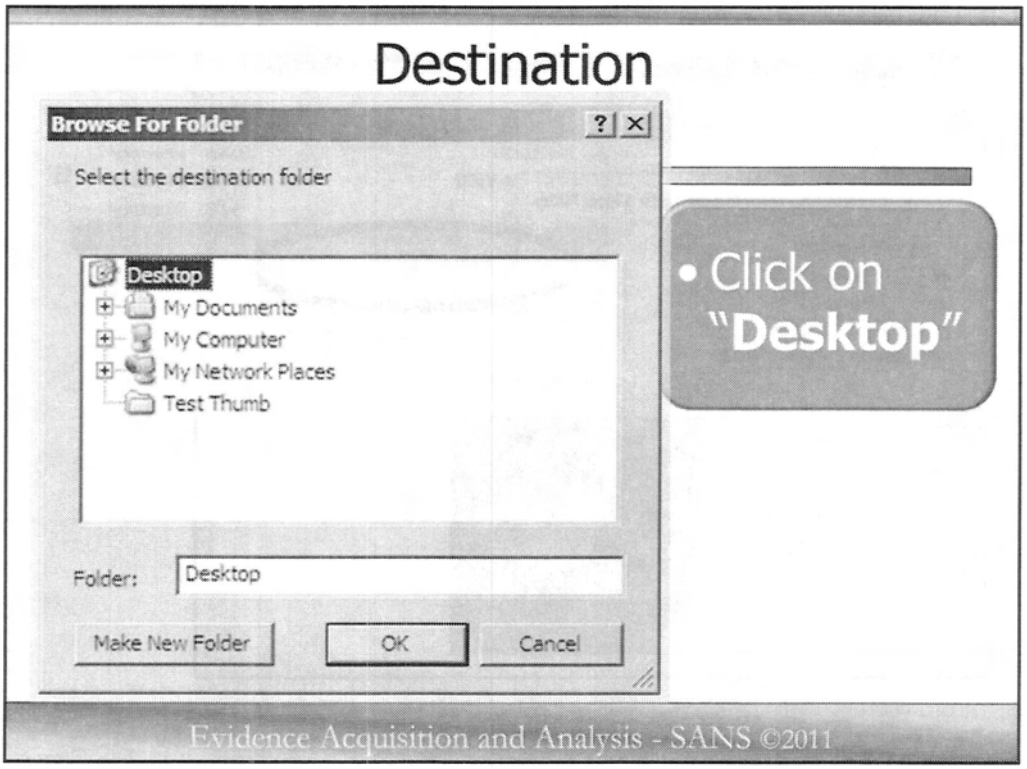
Another great use for this directory listing is if the subject petitions the court saying they need their system back because it has important files they need. You can give them this file listing and have them annotate exactly what files they must have, then you could extract just those files and give it to them. This shows the court that you are not trying to be unreasonable or punish the subject by keeping their files away from them.

The last option is "**Add to Custom Content Image (AD1)**. This is a great feature if you would like to create an image of only certain files or directories, and don't want or need to image the entire drive. We will try this in a moment, but for now let's see how you can Export Files from a forensic image file or a drive you are previewing.



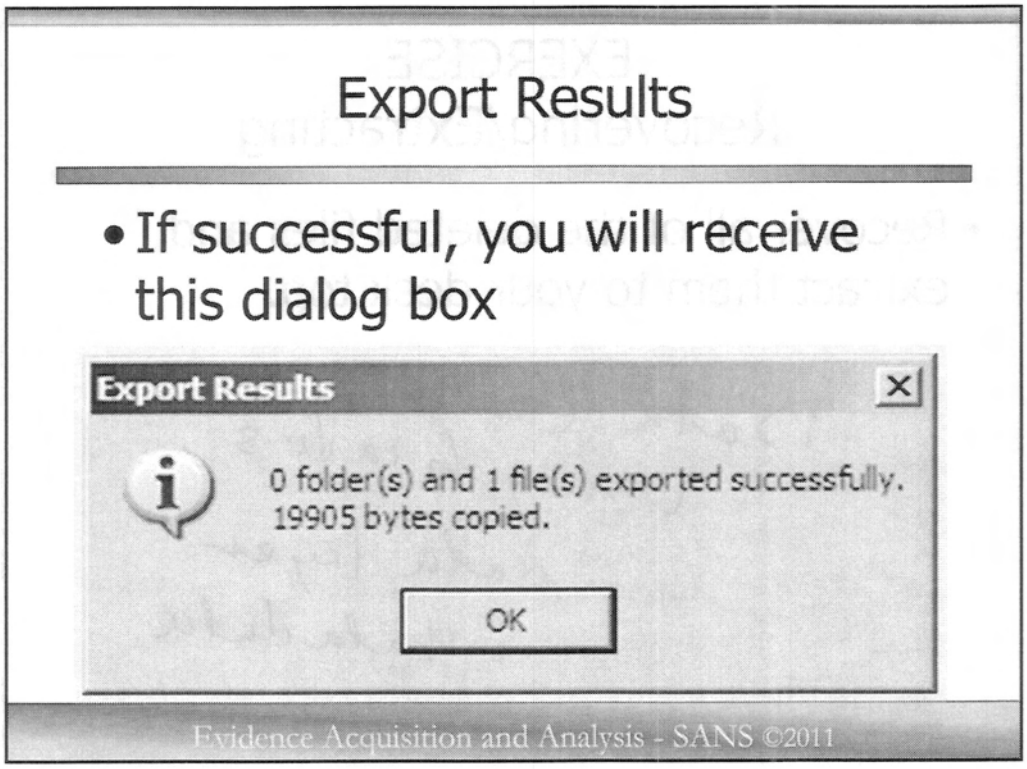
To review, you should have right clicked on the file called "**!riminal.jpg**" or any file that has the red "X" on it, now go ahead and select "**Export Files…**"

As I mentioned before about sitting down with a case agent or investigator and quickly going through the system, the investigator may say "Hey, can you give me a copy of that file right now?". Using this technique, you can do just that. Another possibility is that you may want to extract specific data like a PST file, index.dat, or the registry files. so you can start analyzing them immediately.



After selecting "**Export File…**", you see a dialog box to select where you want to export your file(s) to. Remember, you will never export anything to the subject's drive, and since you have a write block attached to the device, you would not be able to anyway. But again, perhaps you just want to extract some files to lead investigator's thumb drive.

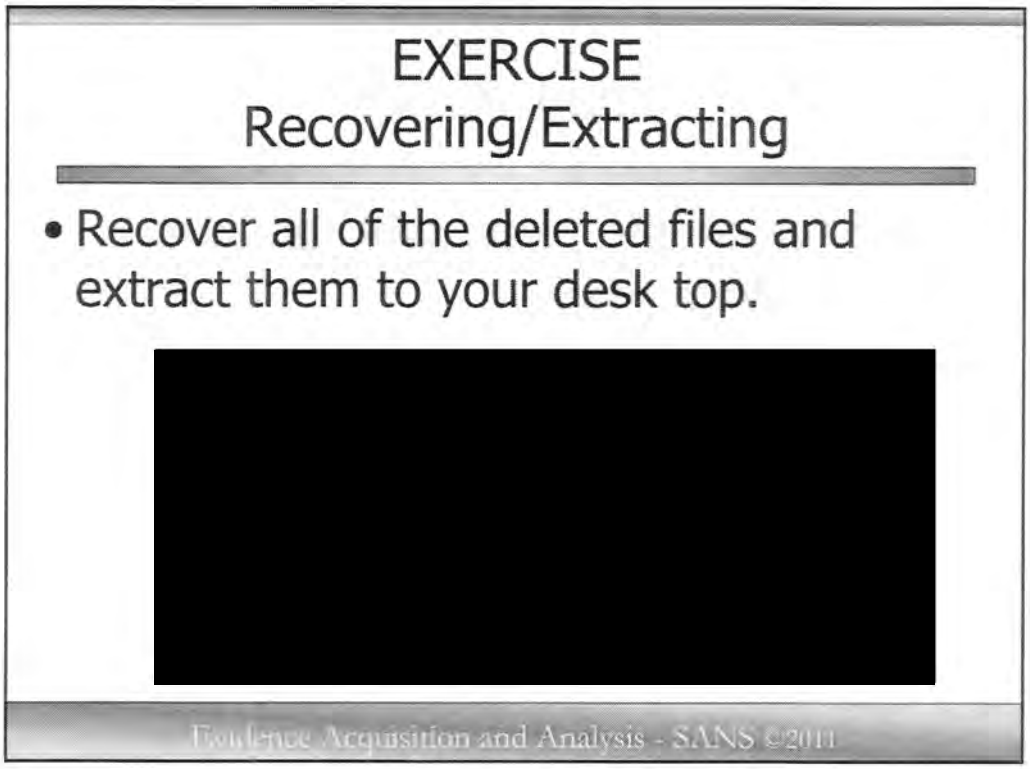
So we can easily find it, let's select the Desktop folder then click "**OK**".



You should have heard an audible alert letting you know you were successful and also received an Export Results dialog box letting you know your file was successfully exported.

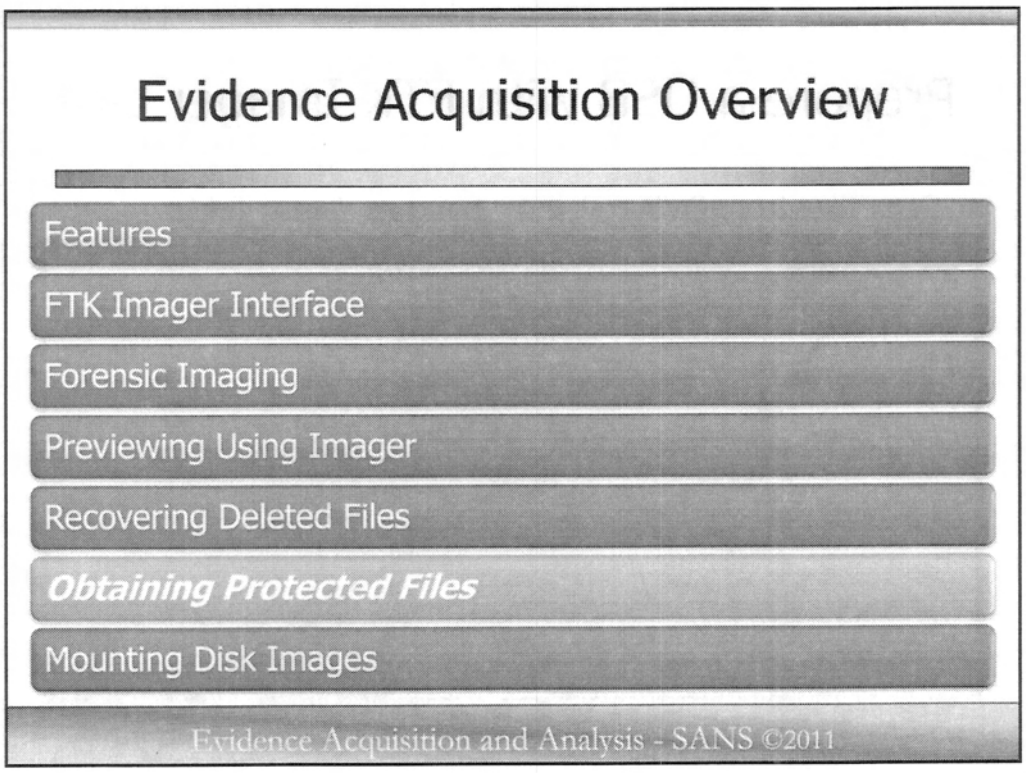
You can click "**OK**" to close the dialog box.

You can now look on your desktop and examine/open the file you just exported.



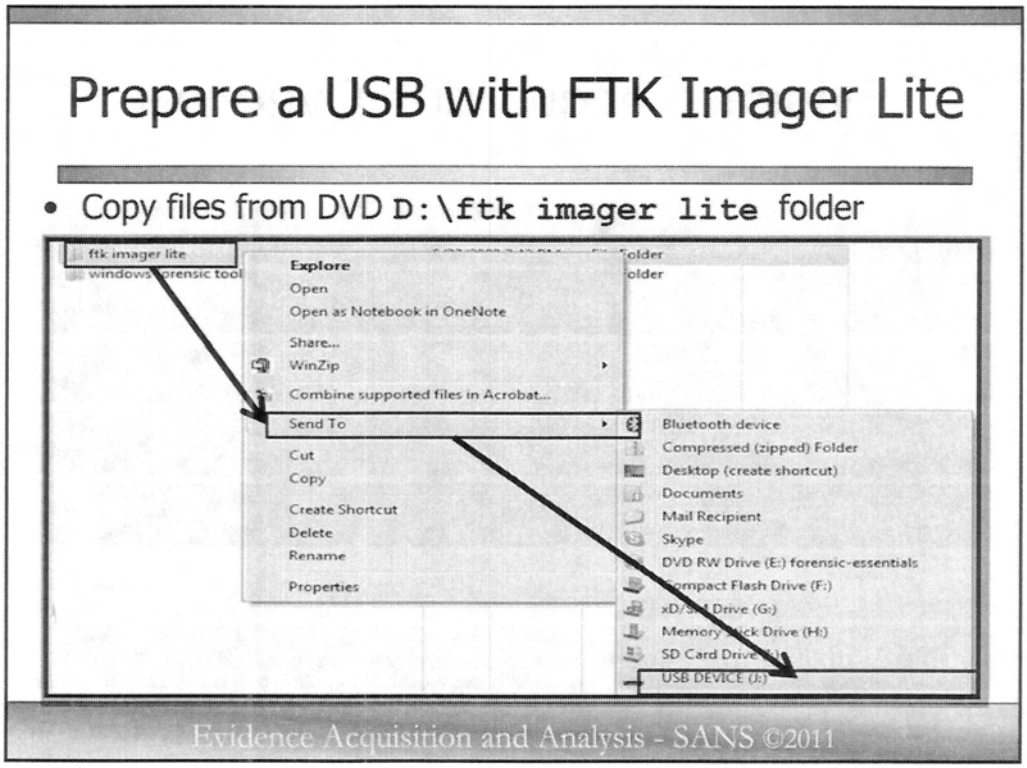
EXERCISE

Let's take a couple of minutes now and let you practice reviewing, recovering, and extracting several items from this image file.



Next we are going to discuss the FTK Imager Lite to demonstrate how to obtain protected registry files.

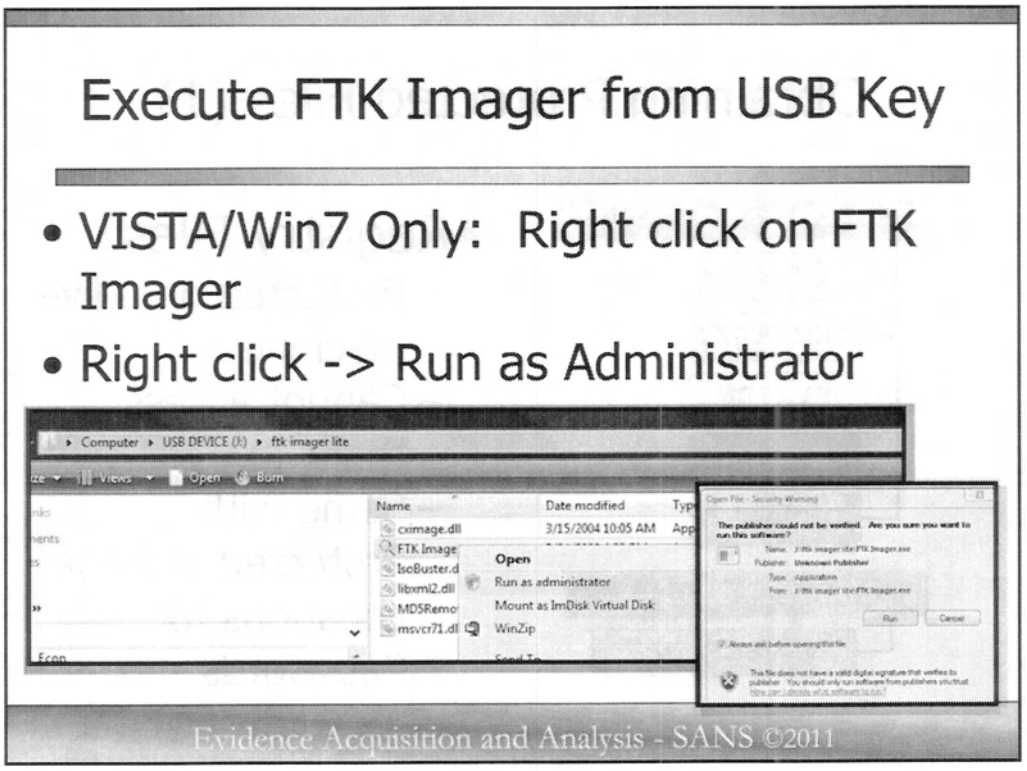
We will be preparing and using FTK Imager Lite because you would obviously never install FTK Imager or any program on the suspects system.



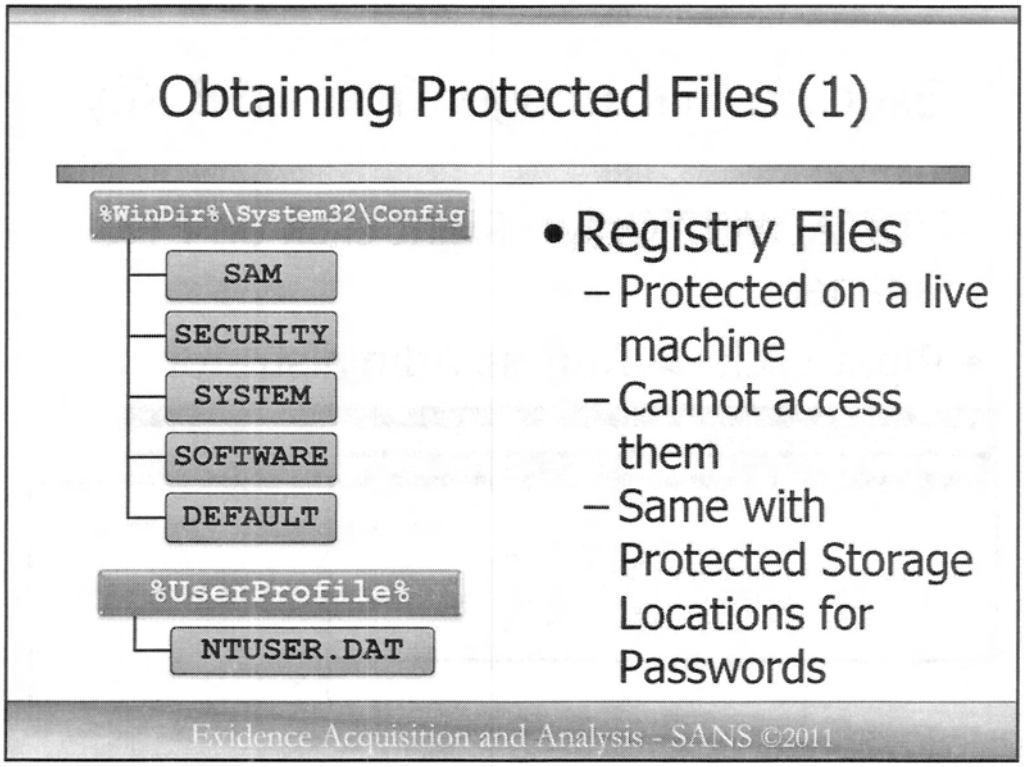
To prepare a thumb drive for FTK Imager Lite, simply insert whatever thumb drive you would like to have FTK Imager Lite on, then with your SANS DVD in your system, you should see a directory off the root of the DVD named "FTK Imager Lite".

Right click on **`D:\ftk imager lite`** folder then select

Send To -> USB Device



If you have a VISTA or Windows 7 machine as your host, please execute FTK Imager Lite from your USB drive with **Administrator** permissions by right clicking on FTK Imager and selecting "Run As Administrator".



FTK Imager also provides you the ability to easily extract Windows registry hives from a live system.

It bypasses the Windows operating system and allows you to copy registry files underneath the Windows file lock.

Using FTK Imager's Preview feature we just demonstrated, you could go to each registry file individually in the C:\Windows \ System 32 \ Config directory and each user's Profile Directory, but that takes time. You could miss something and, well, FTK Imager will do it very easy for you.

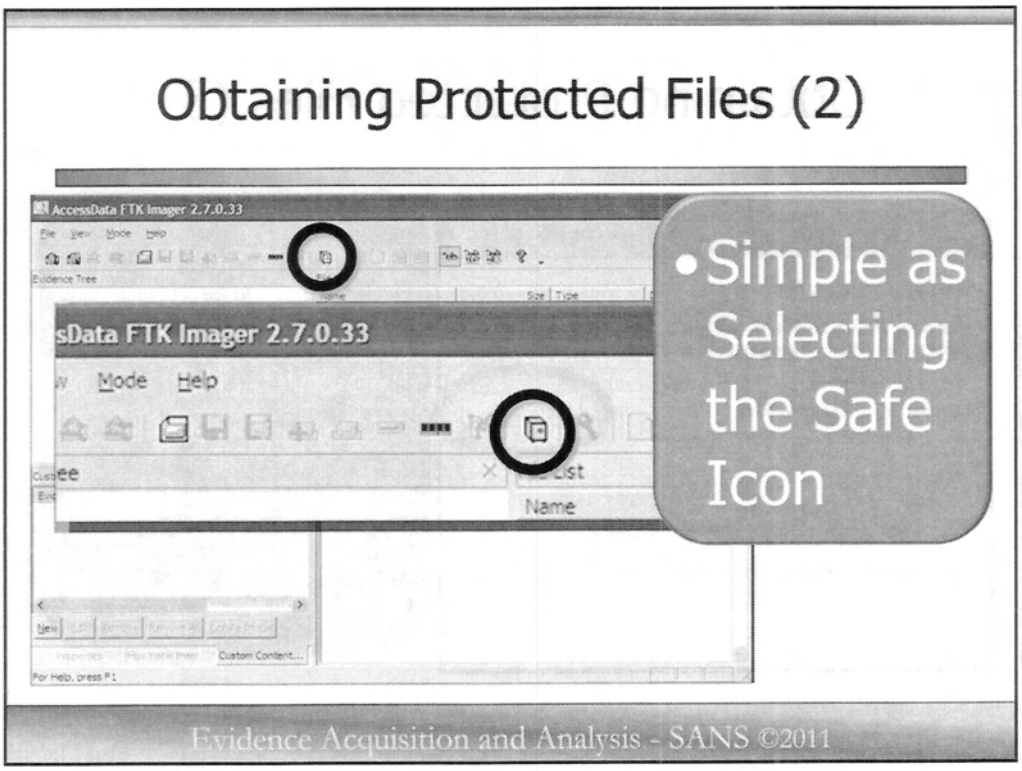
Why would you even need to worry about getting registry hives?

Answer: What if you want to boot the system and see what it looked like to the user?
You could use Mount Image Pro's Virtual Forensic Computing (http://www.virtualforensiccomputing.com) or Live View (http://liveview.sourceforge.net) to boot the forensic image as a virtual machine, but if they have their system setup to require a password, then you have a problem. By extracting the appropriate registry hive, you could use a password cracking utility to crack the password. Additionally, you could use the law enforcement version of Live View or a password injection tool to blank the user's password, but you still may have a problem.

What if the subject has Windows Encrypted File System (EFS) enabled? If you use a password injection attack, will you be able to see their files?

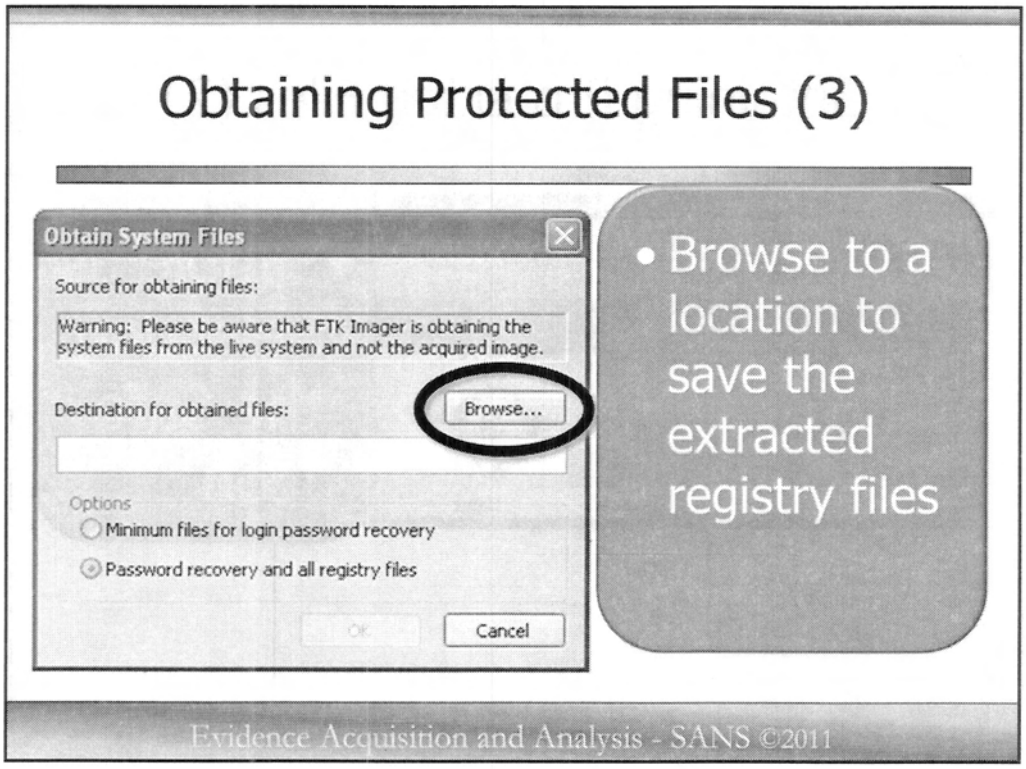
Answer: No. They are encrypted to their password.

Great, so we now know a couple of reasons why we might want to collect the registry. So let's use FTK Imager to see how easy it is to extract registry hives.



To obtain the protected registry files using FTK Imager, you would insert your thumb drive containing FTK Imager Lite on a running Windows system. From the thumb drive you would launch FTK Imager Lite.

Either click "**File**" from the Menu Bar, and then "**Obtain Protected Files"**, or you can click the yellow icon on the toolbar that looks like a safe.



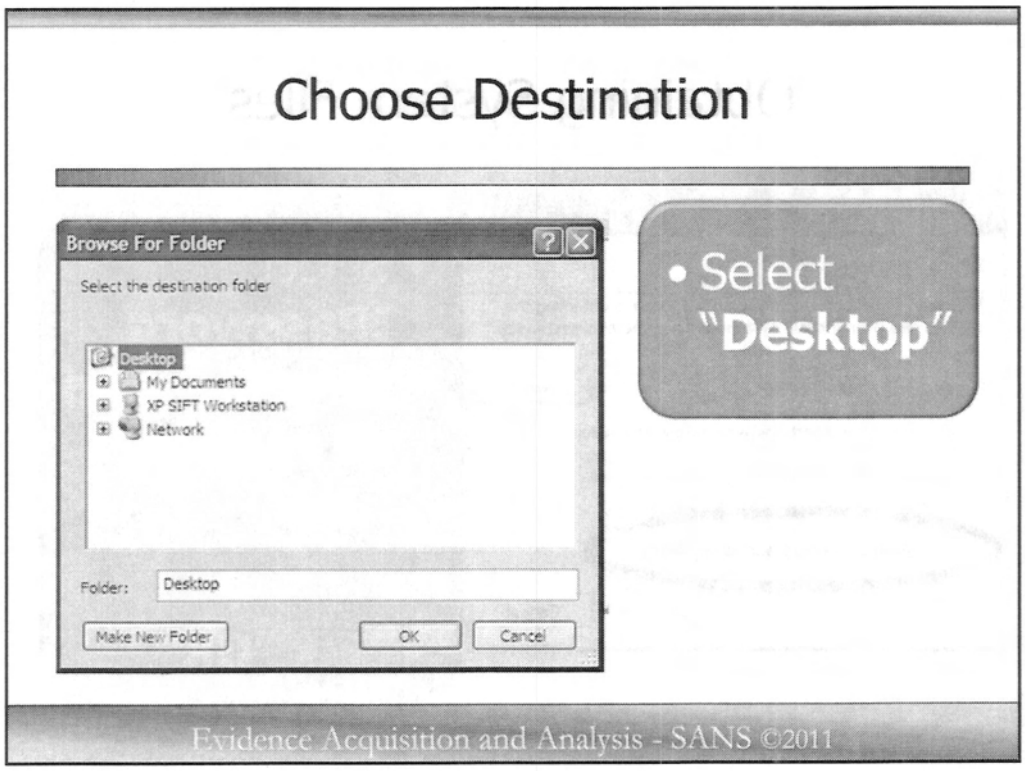
Browse to the destination directory you want to save the registry files (a network drive or USB thumb drive, etc.), then click **OK**.

You have two options now. By default, the minimum files needed for login recovery is selected. This option retrieves **Users**, **System**, and **SAM** files.

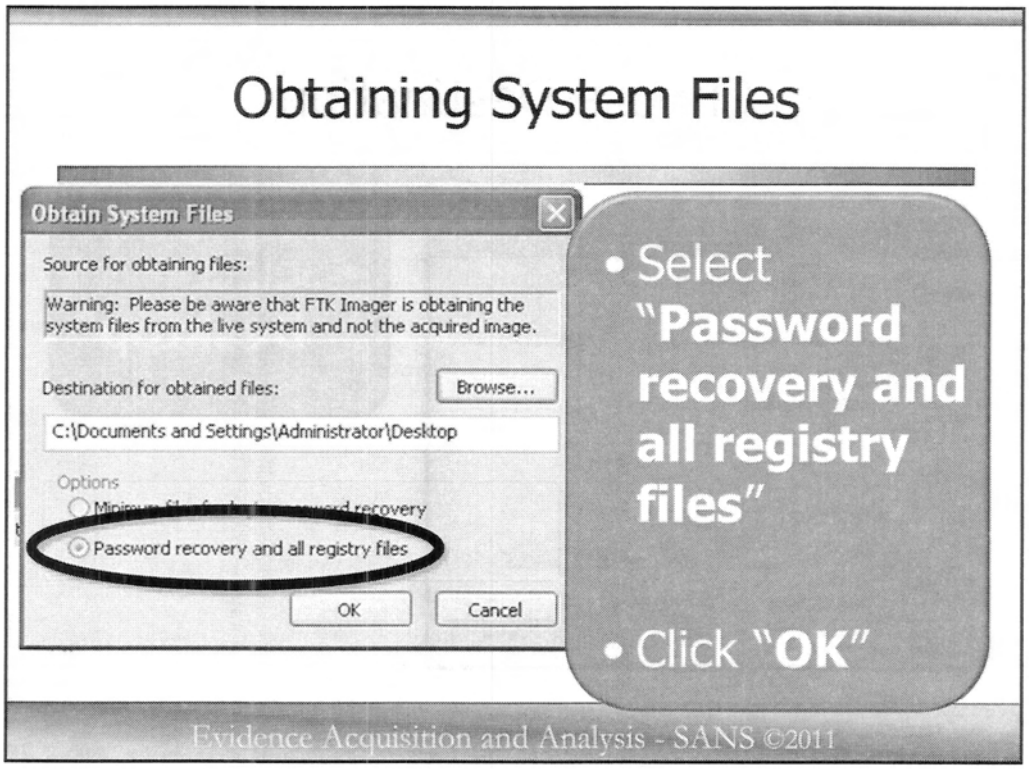
Or you can select "**Password recovery and all registry files**" which will extract Users, System, SAM, NTUSER.DAT, Default, Security, Software, and Userdiff files from which you can recover account information and possible passwords to other files.

This list can also be imported to the AccessData password recovery tools, such as PRTK, and DNA.

Select "**OK**" and FTK Imager exports the selected files to the designated location.

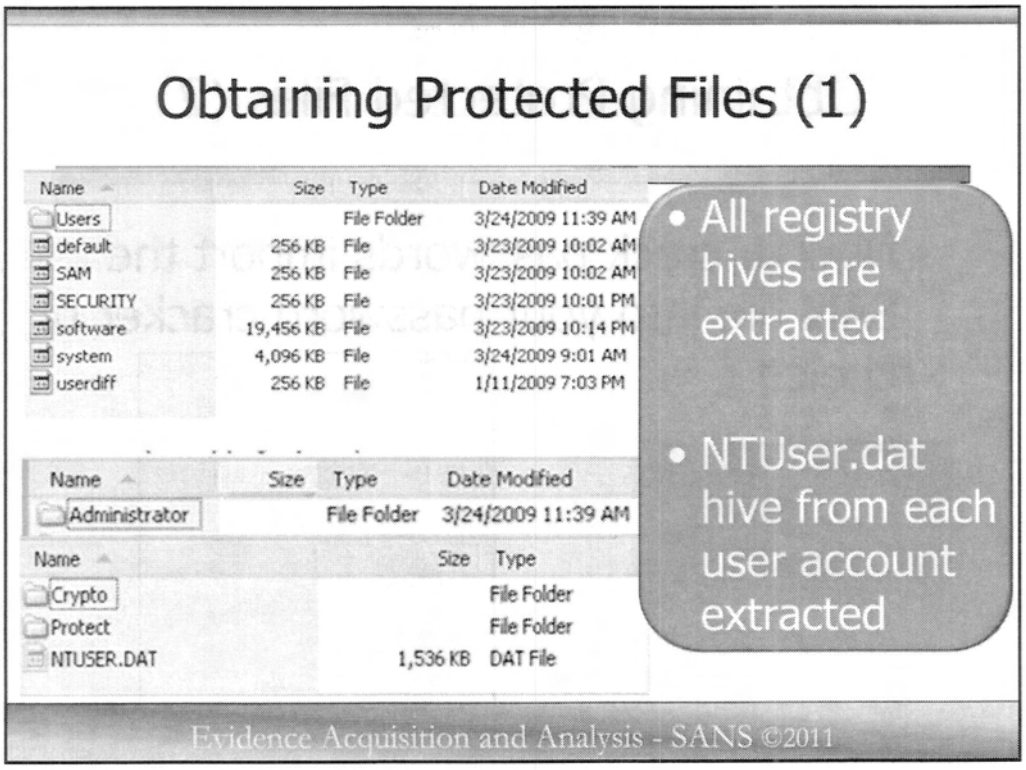


The next screen you will be looking at is the "Browse For Folder" screen. It is here that you will select the destination for the file or files you want to export. For our purposes here today, please go ahead and select the Desktop. Again, remember that the only rule on this is that you would never save or export a file anywhere on the subjects drive. For this process it is also helpful that you have FTK Imager Lite that can fit and be used on a thumb drive. This gives you the ability to, if necessary, stick your thumb drive into the running computer system, extract the registry files, then shut the system down.



If you only want to crack the password file, all you have to do is select the Minimum files for password recovery; but in most cases, you will likely want to extract all registry files, so select "**Password recovery and all registry files**", then click "**OK**".

This process does not take long at all, so there is no real benefit to selecting the minimum files necessary to recover passwords.



On your desktop you will now find a Users folder and 4 registry files: SAM, SECURITY, SOFTWARE and SYSTEM. We will be discussing in detail later in this course the incredibly valuable amount of information that can be harvested from the different registry keys. Just by accomplishing this task of extracting the registry haves, you have the ability to identify every USB thumb drive/storage device ever plugged into the system, the most recent files opened or saved by almost every application on the system, what applications are or were installed, when they were first executed/launched and the last time they were executed as well as how many times they have been executed, IP addresses assigned to the computer, wireless routers associated with, etc.

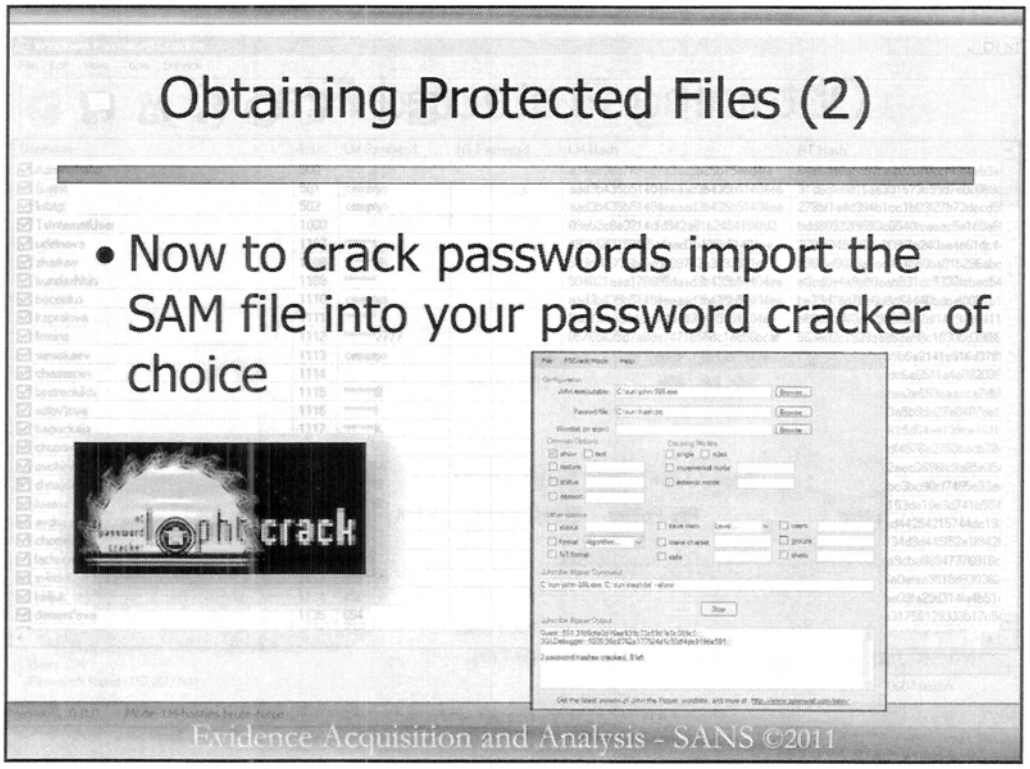
Inside each of the user directories you will find the NTUSER.DAT registry key along with other files that may contain passwords for the Windows protected files.

FTK Imager Lite is a very useful program for a number of reasons:

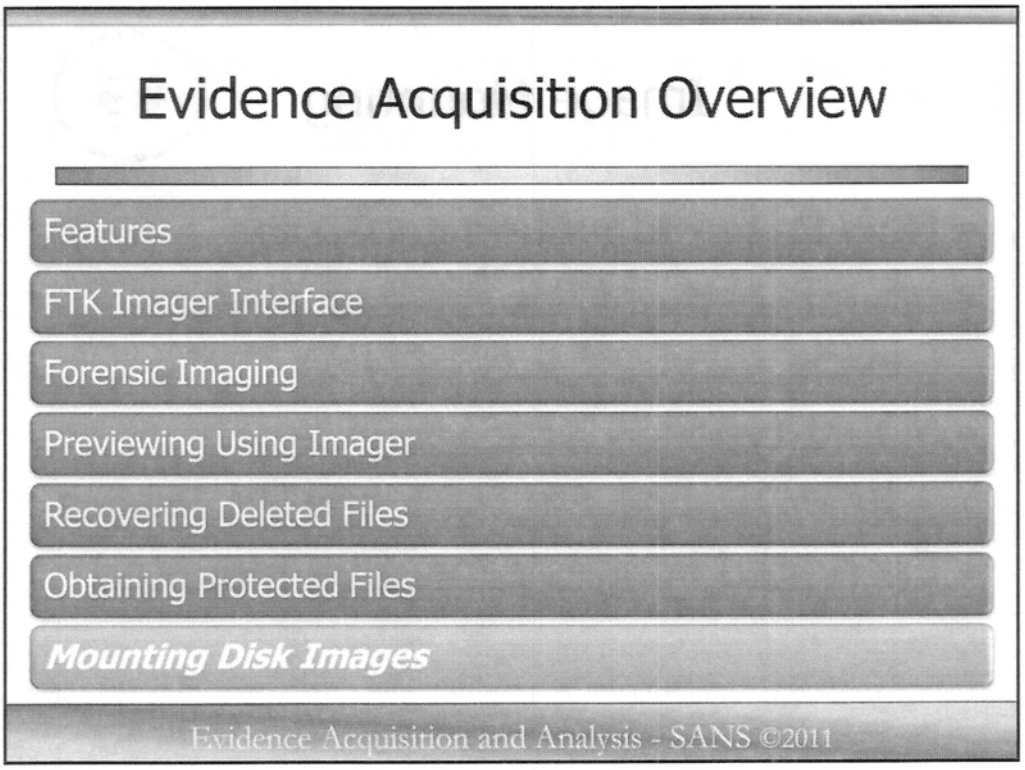
1st, the fact that you can carry FTK Imager Lite around on a thumb drive so you always have it with you is great.

2nd – using a write block of course, you can preview systems onsite at a search scene and determine what systems really need to be imaged or at least imaged first. Sometimes, you might even be able to extract certain files and resolve the situation immediately (confession, investigative lead, etc.).

3rd – You can recover lost/deleted files for friends quickly without having to image the drive.

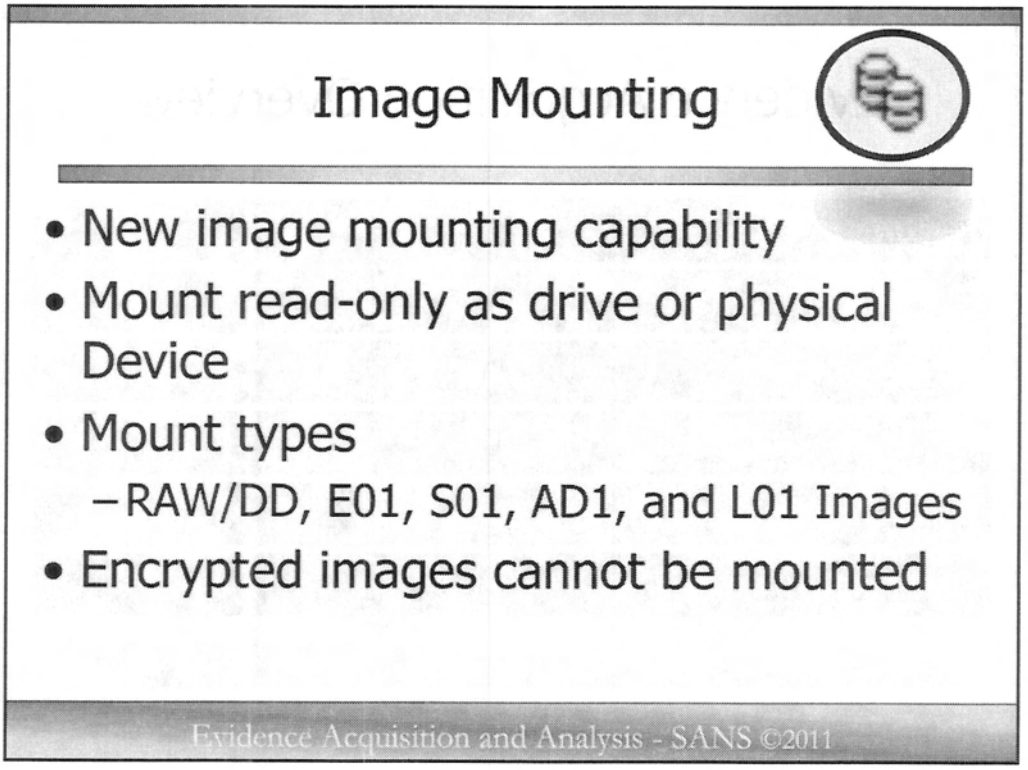


Of all the files obtained, the SAM file contains all the encrypted passwords for every user account on the system. This is the file you will use in your password cracking software to decrypt the passwords.



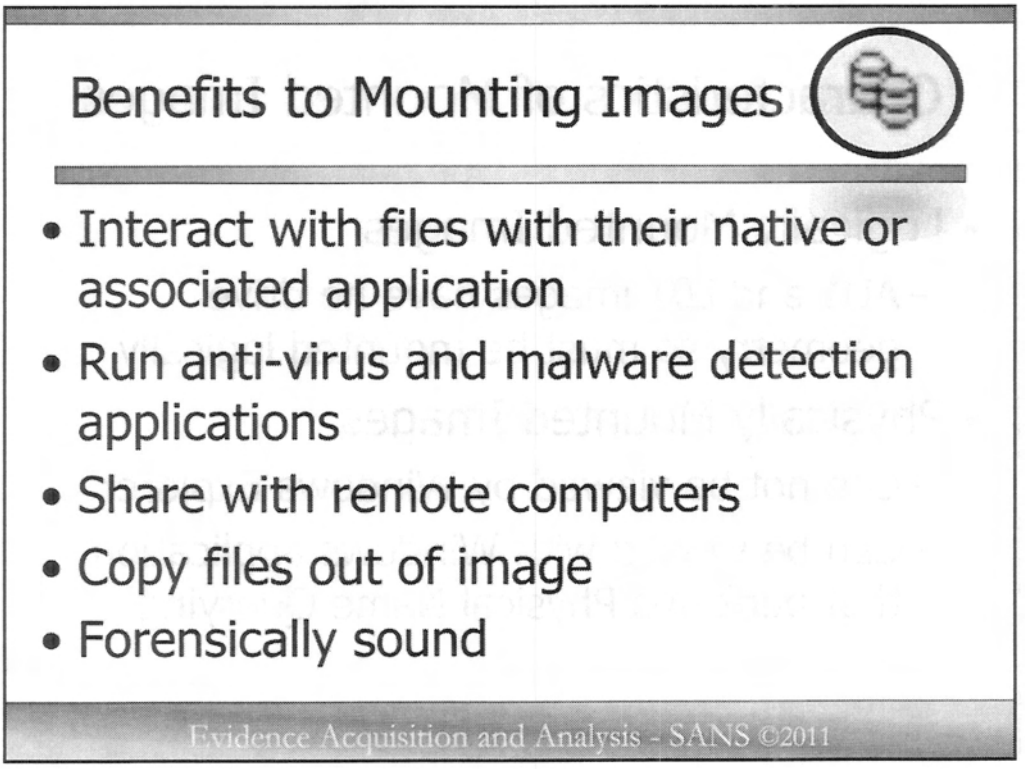
Next we are going to discuss the FTK Imager Lite to demonstrate how to obtain protected registry files.

We will be preparing and using FTK Imager Lite because you would obviously never install FTK Imager or any program on the suspects system.



One of the great new features of FTK Imager 3 is the ability to mount forensic images as a drive or physical device for read-only viewing inside a Windows operating system. This allows the reviewer to read the mounted device with any Windows application that performs Physical Name Querying.

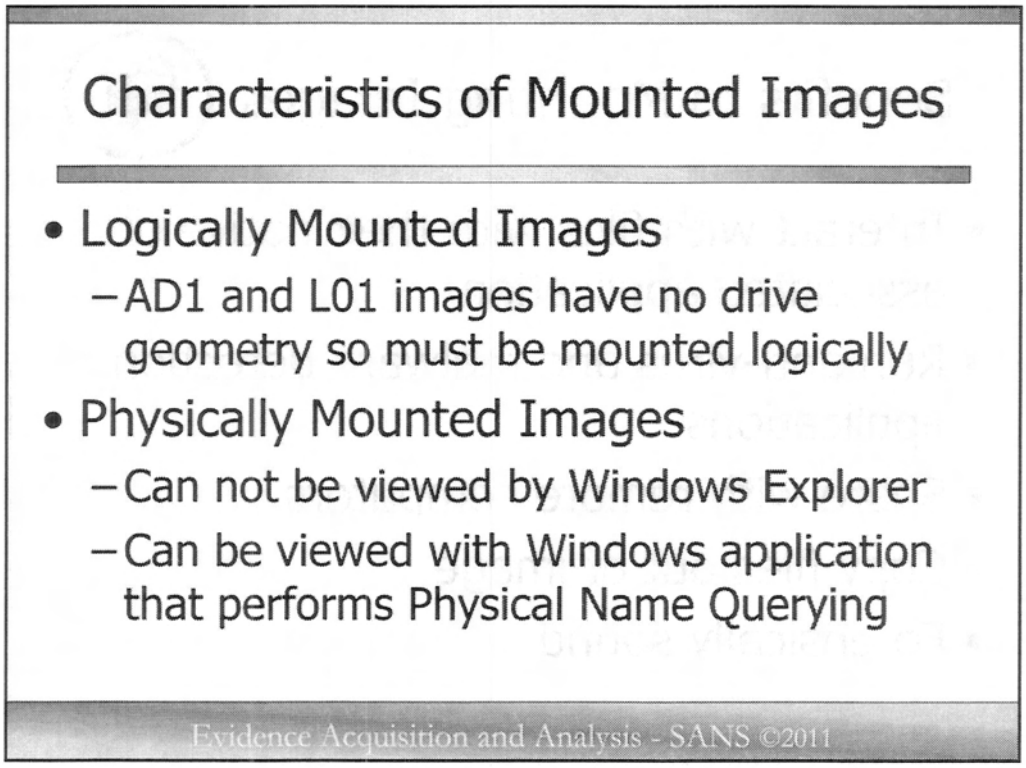
You can mount a full disk forensic image with all its partitions all at once with either the first available drive letter or any available drive letter of your choice.



Some of the many benefits to mounting forensic images are that examiners, or even investigators with no forensic training, can view and interact with the mounted files in their native or associated application installed locally on the reviews machine. This allows the reviewer to copy files out of the mounted file system. Because the image is mounted read-only, there are no worries that files can be copied into the mounted image or that the mounted image will be changed in any way.

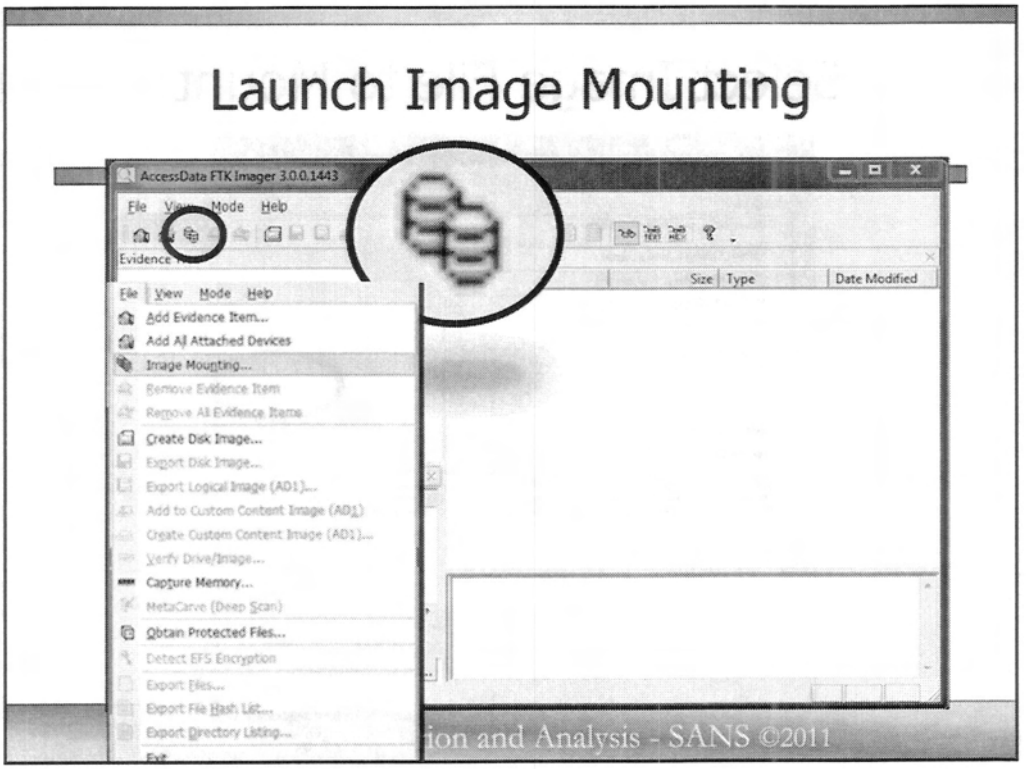
A forensic image that is mounted is seen as another drive attached to the host system and it can subsequently be shared out or viewed from remote computers systems using remote access applications.

Anti-virus and malware detection applications can run against the mounted file system. This could be a great first step to determining if a virus or malware was infecting the system.

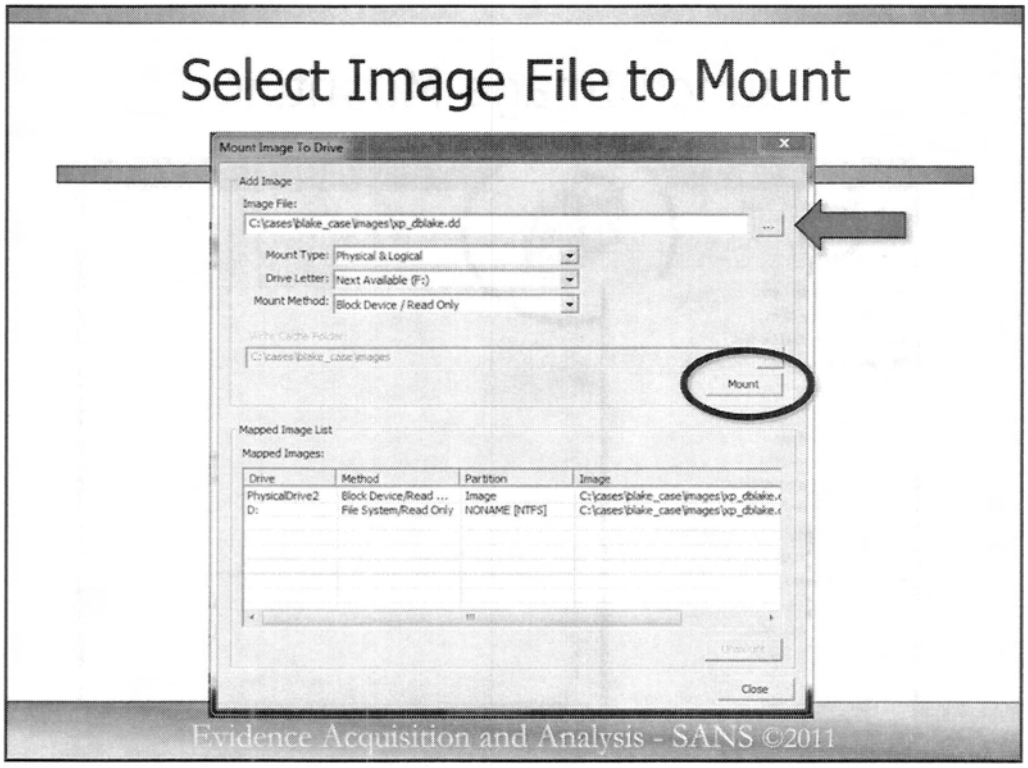


When you create AD1 or L01 custom content images, they contain full file structures but do not have any drive geometry or any other physical drive data. This will prevent them from being mounted physically. Additionally, when you mount them logically, the drive or partition size will not be displayed correctly (since it does not have that information).

When you mount a forensic image physically, it cannot be viewed by Windows Explorer, however, it can be viewed by any Windows application that performs Physical Name Querying. When you create an E01, S01, or RAW/dd image of a properly working drive, the images contain all the appropriate drive data, disk, partition, and full file structure. The disk image can be mounted physically and the disk image partition(s) can be mounted logically.



With FTK Imager open, either select the third icon from the left on the Tool Bar, or from the Menu Bar, select "**File**" then "**Image Mounting…**". If you are already have a forensic image added as evidence, you can simply right click on the image in the Evidence Tree window and select "**Image Mounting…**".

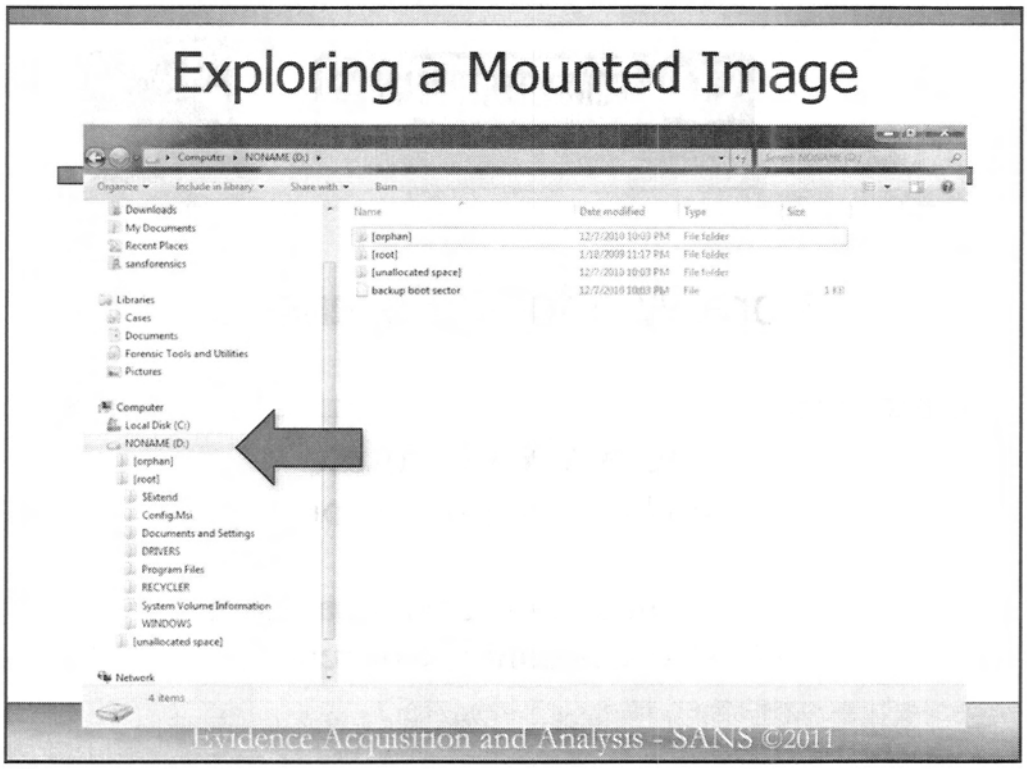


Click the "…" adjacent the "Image File" field. Brows to the location you image file is located. Let browse to the **C:\cases\blake_case\images** directory and select the "**xp_dblake.dd**" image file.

Click "**Open**".

Now that you have selected the image file, the "Map Type" will default to the supported mapping based on the type of image that is selected. There are three different map types, Physical & Logical, Physical Only, and Logical Only. If the map type includes one of the "Logical" choices, the "Drive Letter" automatically defaults to the next available drive letter. You can optionally select the drive letter to assign the mount point manually.

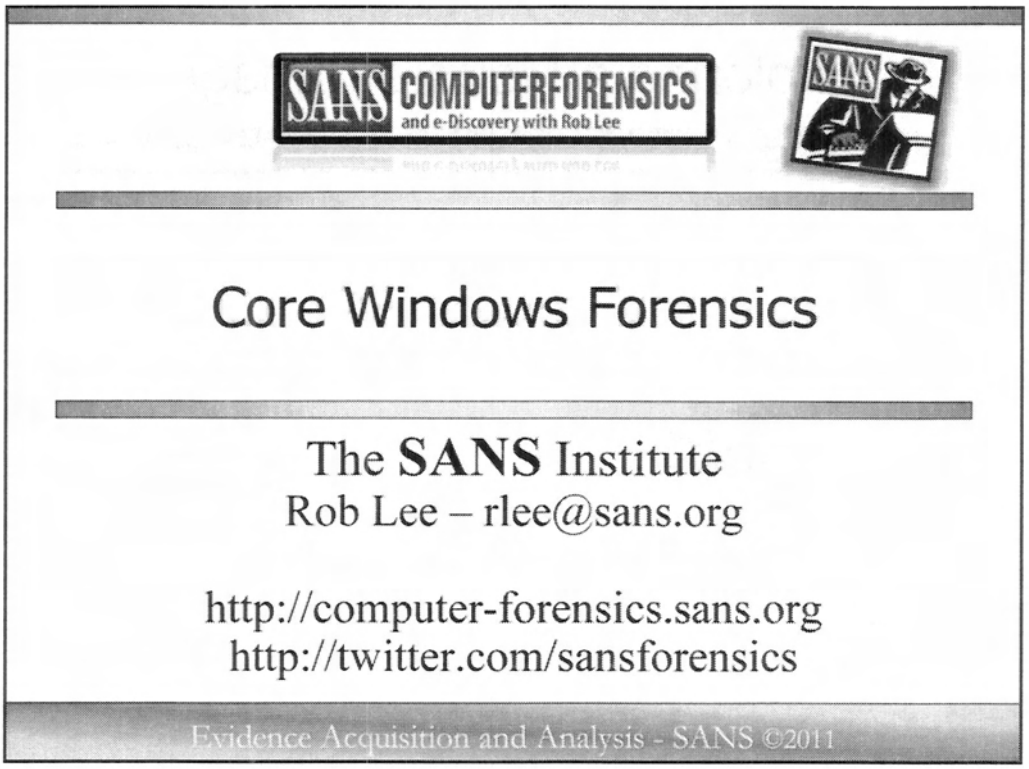
Click "**Mount**" and the selected image file will be mounted. You can see in the bottom half of the "Mount Image to Drive" area the details of the mounted images in the "**Mounted Image List**".



Now that the image is mounted, you can open Windows Explorer and interact with the mounted file system. You can also run applications and and point to the file mounted system as input.

To unmount images, highlight the "**Mapped Images**" in the "**Mapped Image List**", then select "**Unmount**".

Caution: Mapped images will also be unmounted automatically if FTK Imager is closed.



Welcome to Core Windows forensics.

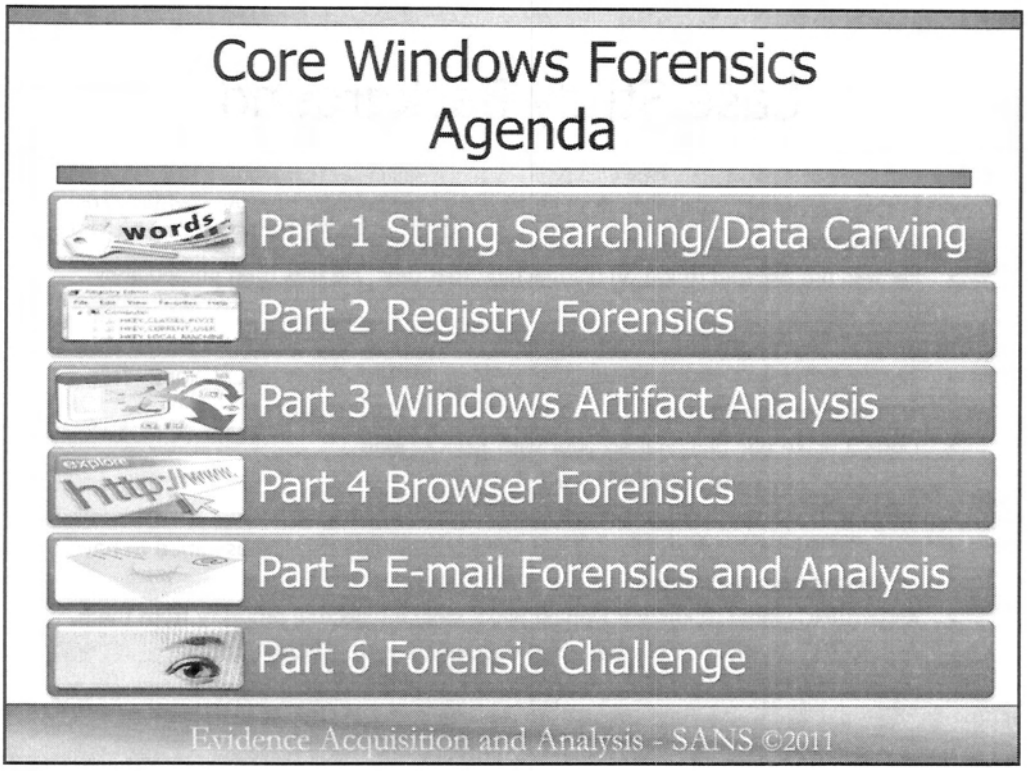
Rob Lee

rlee@sans.org

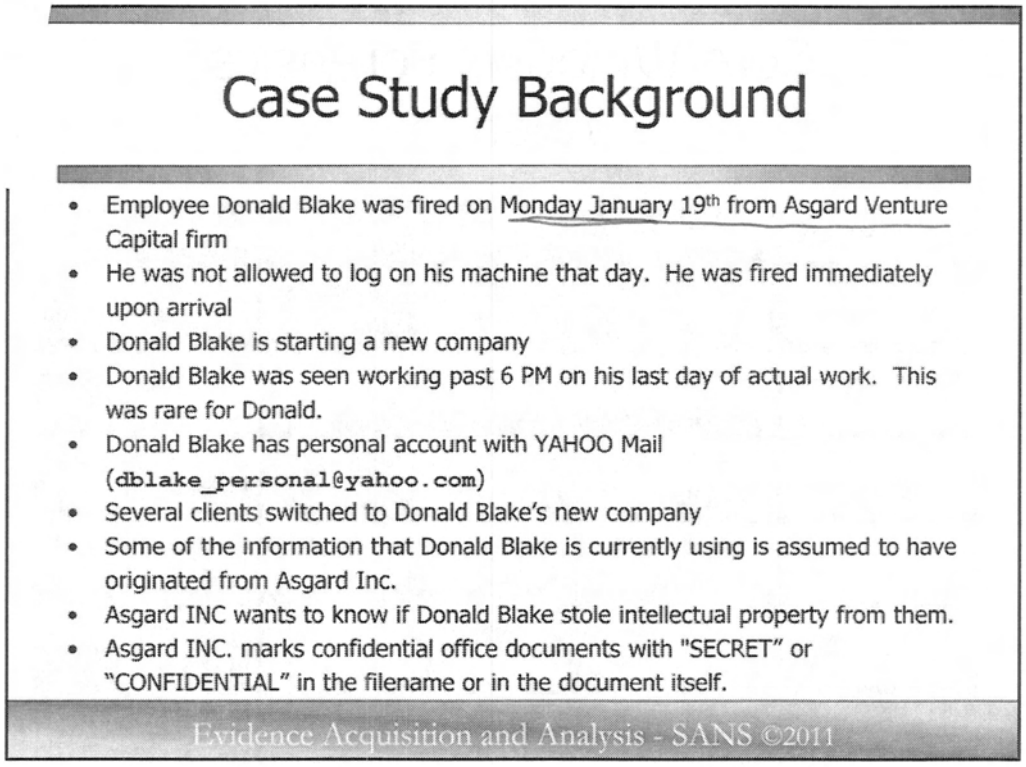
http://twitter.com/robtlee

http://twitter.com/sansforensics

Special thanks to Chad Tilbury for his work on this day in helping create SEC408 Computer Forensics and E-Discovery Essentials. I could not have done it without you.



This page intentionally left blank.

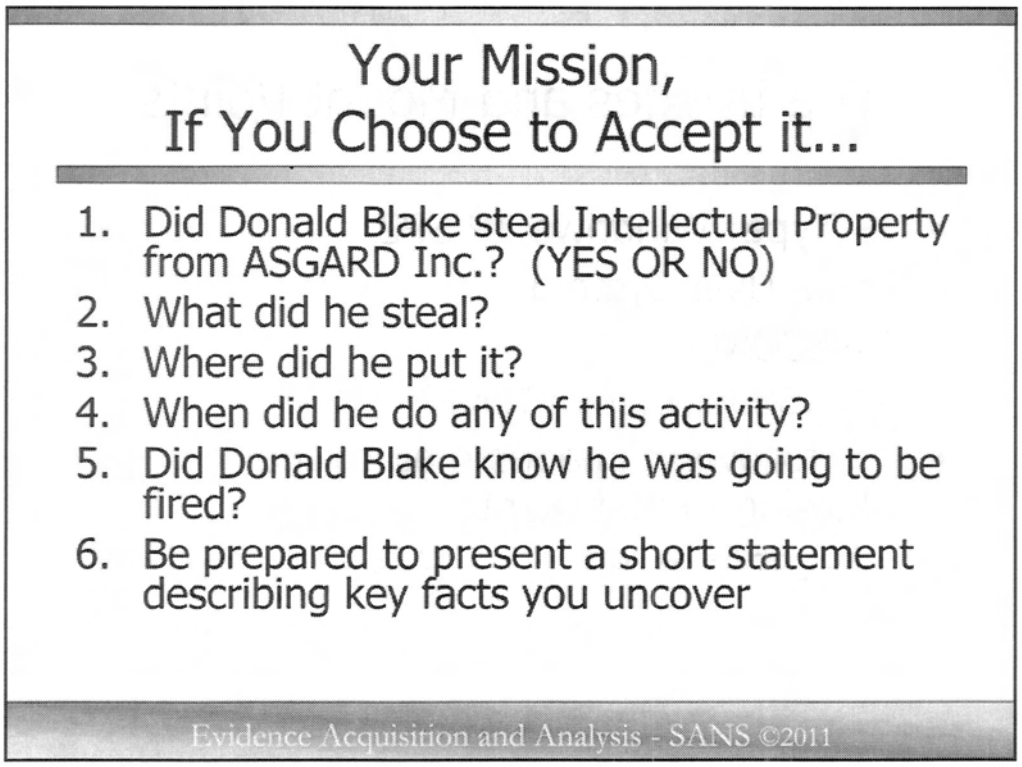


Above is the background to the case that you opened in FTK in the previous book.

Employee Donald Blake was fired on Monday January 19th from Asgard Venture Capital firm. He was not allowed to log on his machine that day. He was fired immediately upon arrival. Donald Blake is starting a new company.

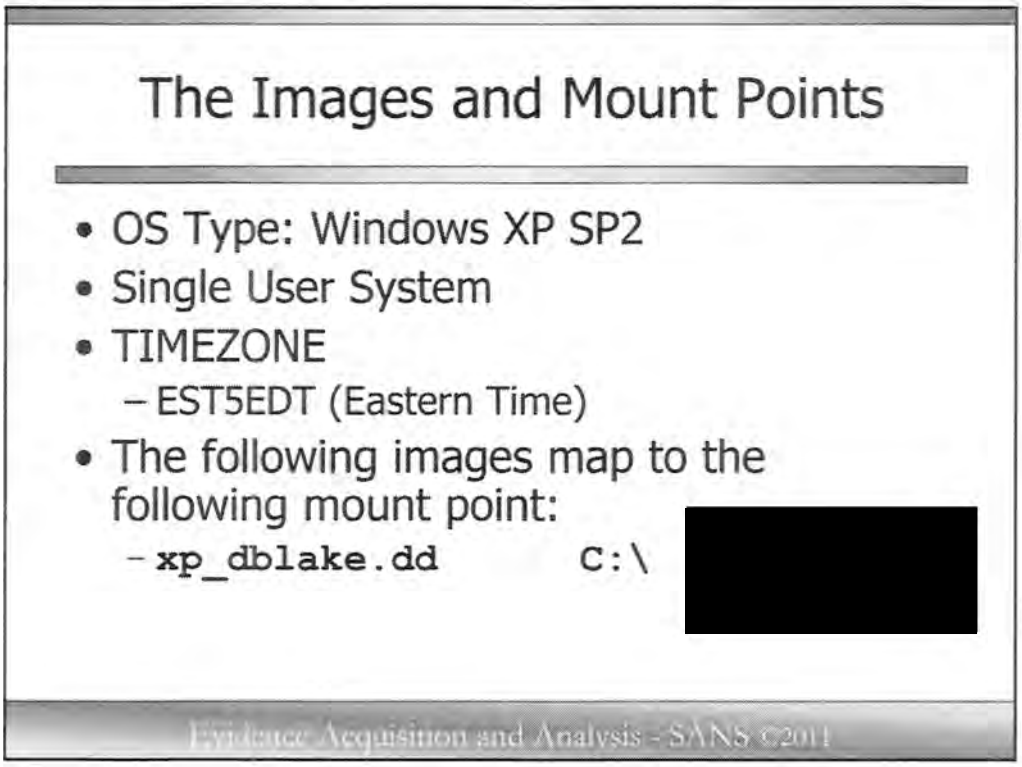
Donald Blake was seen working past 6 PM on his last day of actual work. This was rare for Donald.

Donald Blake has personal e-mail account with YAHOO Mail (**dblake_personal@yahoo.com**). Several clients switched to Donald Blake's new company. Some of the information that Donald Blake is currently using is assumed to have originated from Asgard Inc. Asgard INC wants to know if Donald Blake stole intellectual property from them. Asgard INC. marks confidential office documents with "SECRET" or "CONFIDENTIAL" in the filename or in the document itself.



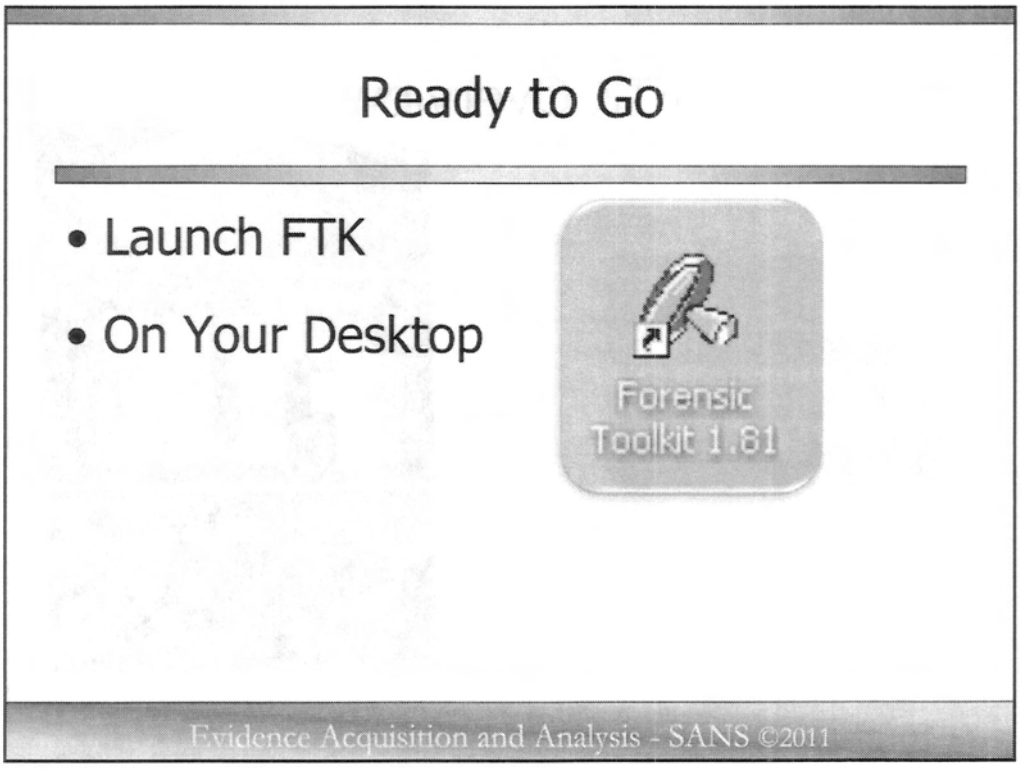
Your goal will be to answer the following questions over the next few days while learning about forensic artifacts that exist:

1. Did Donald Blake steal Intellectual Property from ASGARD Inc.? (YES OR NO)
2. What did he steal?
3. Where did he put it?
4. When did he do any of this activity?
5. Did Donald Blake know he was going to be fired?
6. Be prepared to present a short statement describing key facts you uncover.

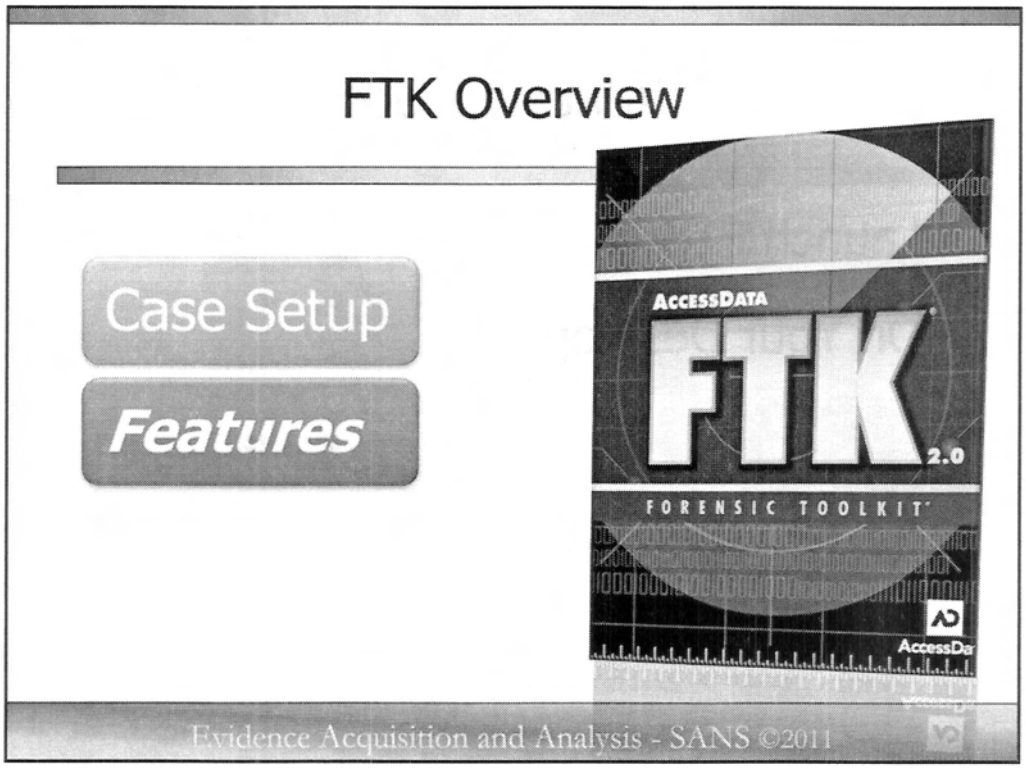


Additional information that is useful to your case. Note that the Time Zone is essential information to know. You will need to convert between UTC (Universal Time) a.k.a. GMT and the local Time Zone of the actual machine. In this case, you know the machine will be UTC minus 5.

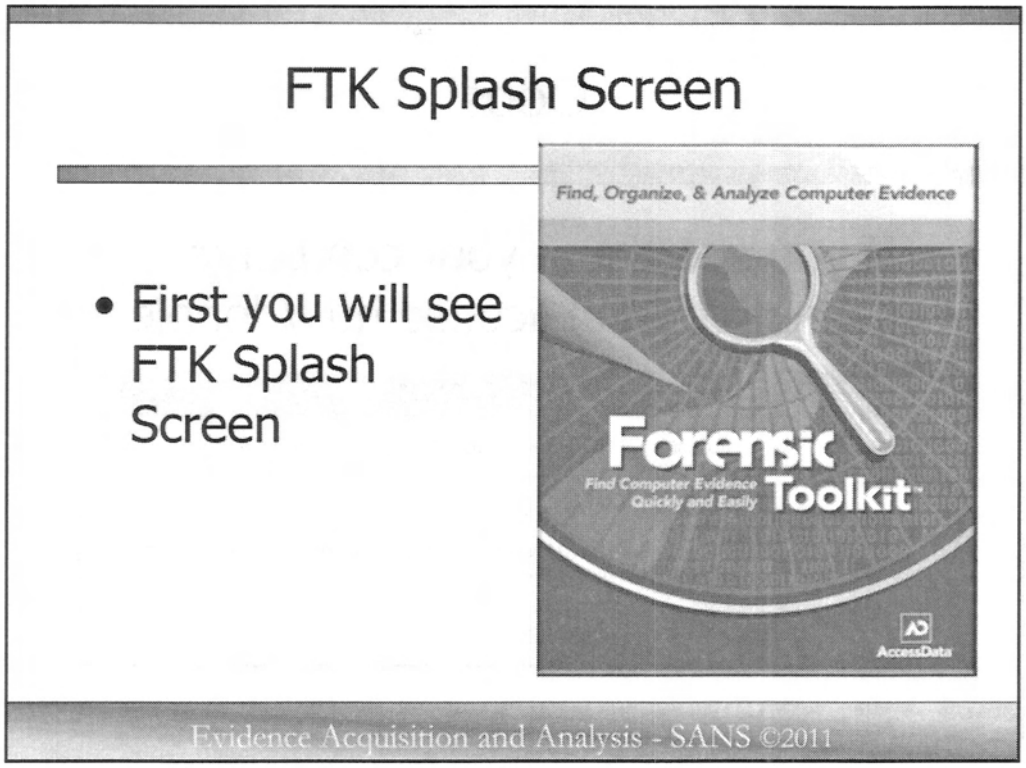
The operating system of the machine is Windows XP SP2 and it a single user system. This simplifies the forensics to an extent. Any human activity on the machine will be limited to a single user.



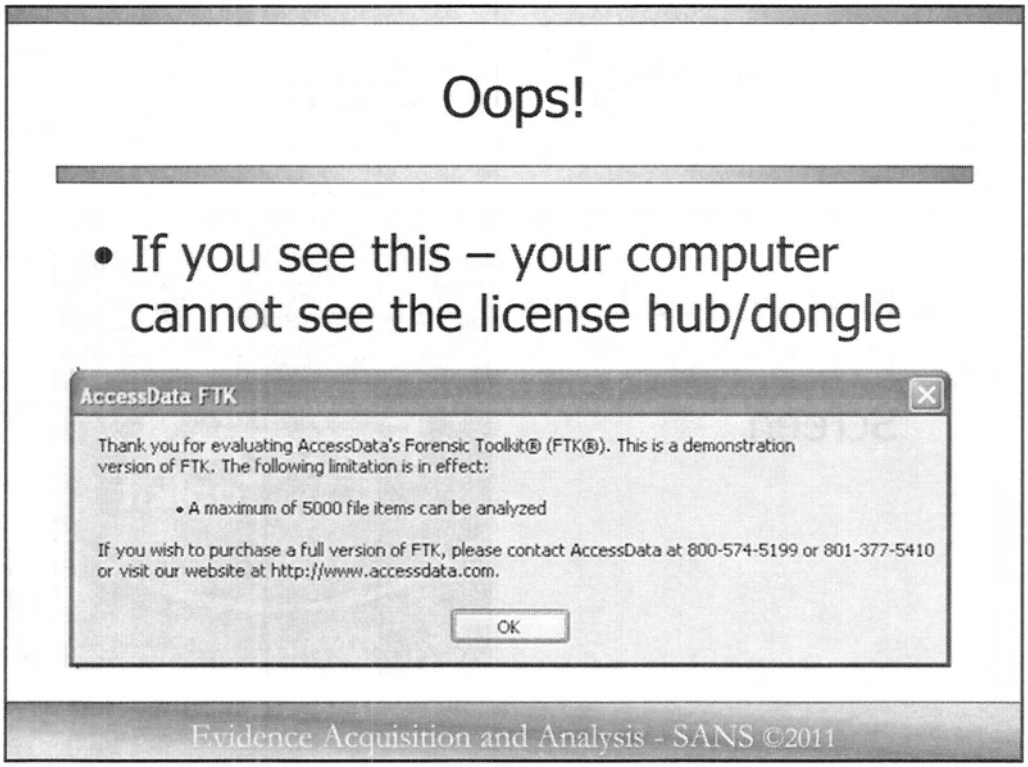
We have your SANS virtual machine set up so if you are connected to our Virtual Private Network (VPN), you will obtain your FTK license from our server, and everything should work just as if you had plugged in your own FTK license.



This page intentionally left blank.



After launching FTK, you should get the FTK Splash screen – hang on … depending on the speed of your machine, this will go away in seconds after FTK initializes. The version we are using in class is FTK version 1.8X. This version is still being sold by FTK at a reduced price because with the upgrade of the of FTK to version 3, FTK had become too powerful to run effectively on a typical laptop.



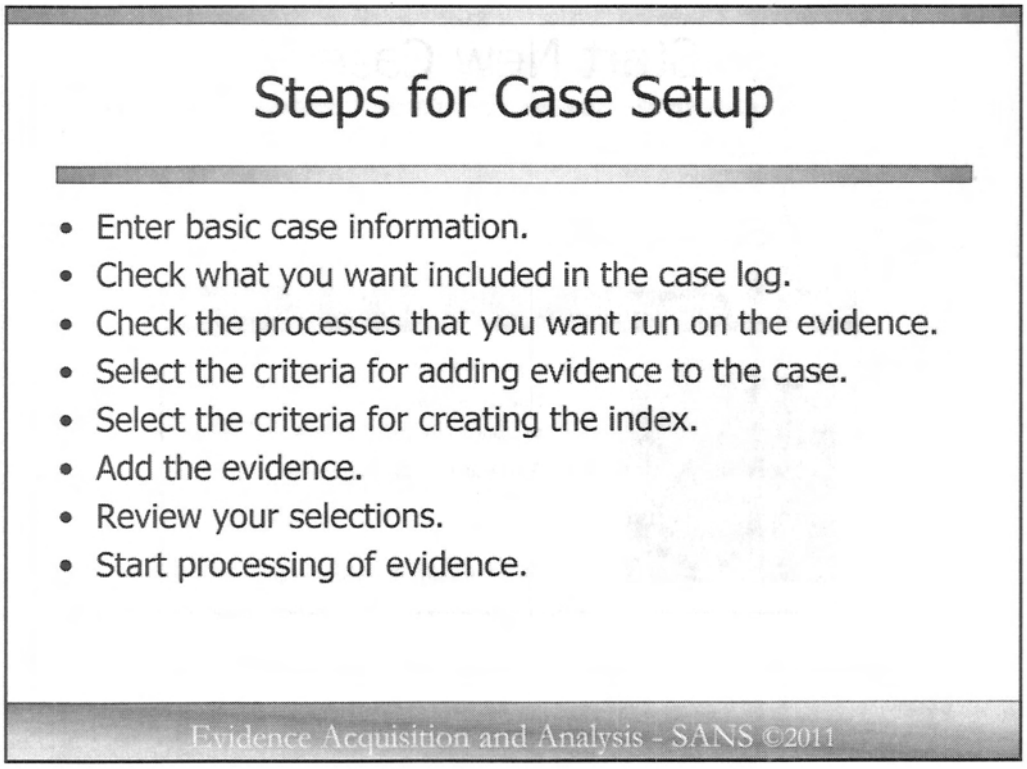
Now did anyone receive this warning dialog box?

If you did, one of four things happened:

1. you forgot to insert your license dongle
2. you did not install the dongle drivers
3. something happened during the install of your dongle drivers that caused the driver installation not to successfully complete
4. you are not connected to the SANS VPN

If your dongle is inserted into your machine, first try inserting it into a different USB port. If that does not work, try uninstalling the dongle driver from the control panel "**add and remove programs**" and then reinstall the dongle drivers, making sure you **DO NOT** have your dongle inserted.

If you are using the SANS VPN to obtain your license and are seeing this, then raise your hand and let me or one of the class assistants know so we can try to help get you connected.



Next we are going to go through the steps necessary to set up your own case file. In some organizations, you may have lab technicians do this for the examiners so when the examiner gets ready to start an analysis, the case file has been already created and indexed. We will be covering:

How to enter basic case information.

How to check what you want included in the case log.

How to check the processes that you want run on the evidence.

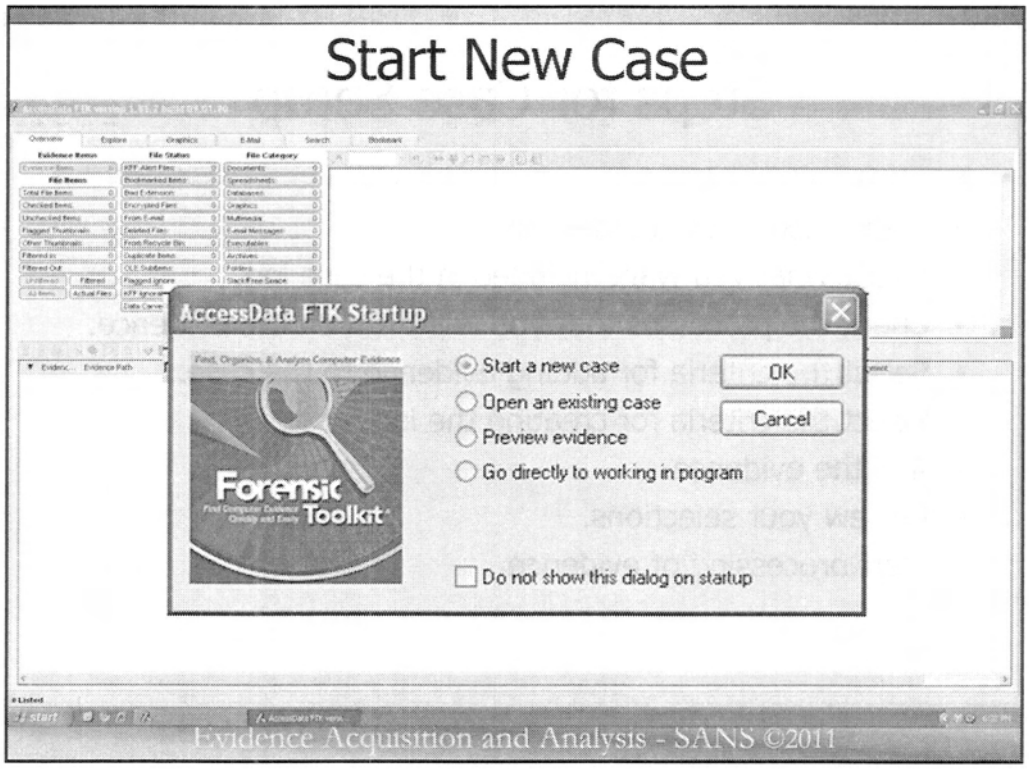
How to select the criteria for adding evidence to the case.

How to select the criteria for creating the index.

How to add the evidence.

How to review your selections.

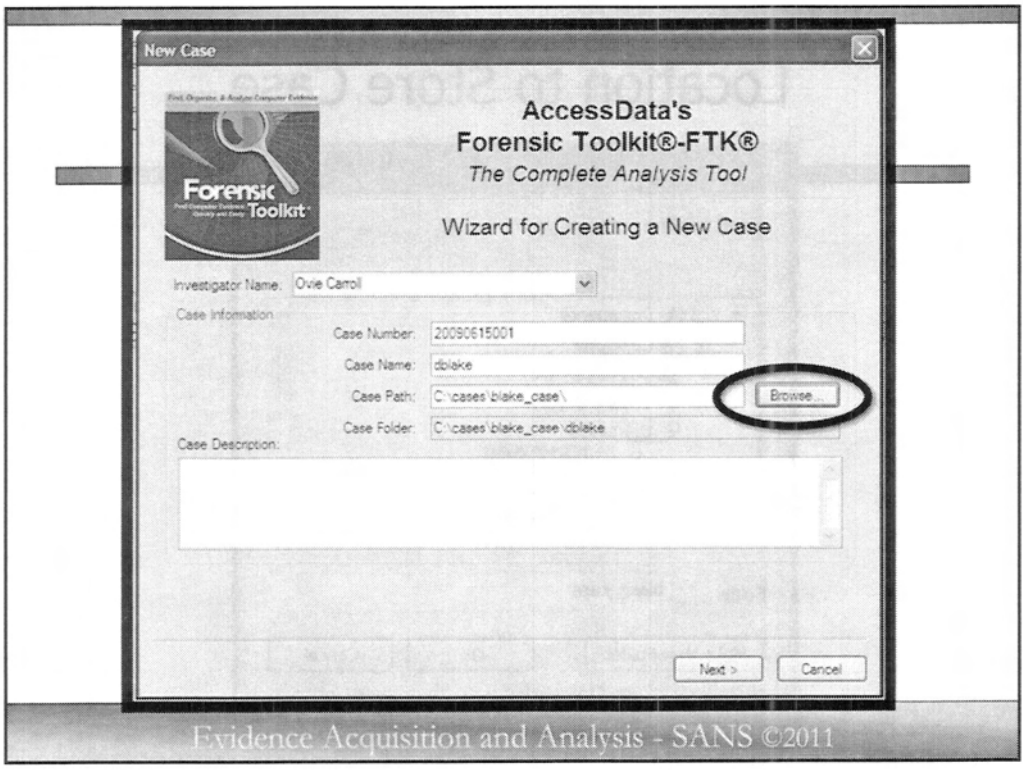
And how to start the processing of evidence.



When you launch FTK, the first thing you should see by default is the AccessData FTK Startup wizard.

This allows you to start a new case, open an existing case, preview evidence or go to working directly in FTK.

For our purposes today, let's select START A NEW CASE.



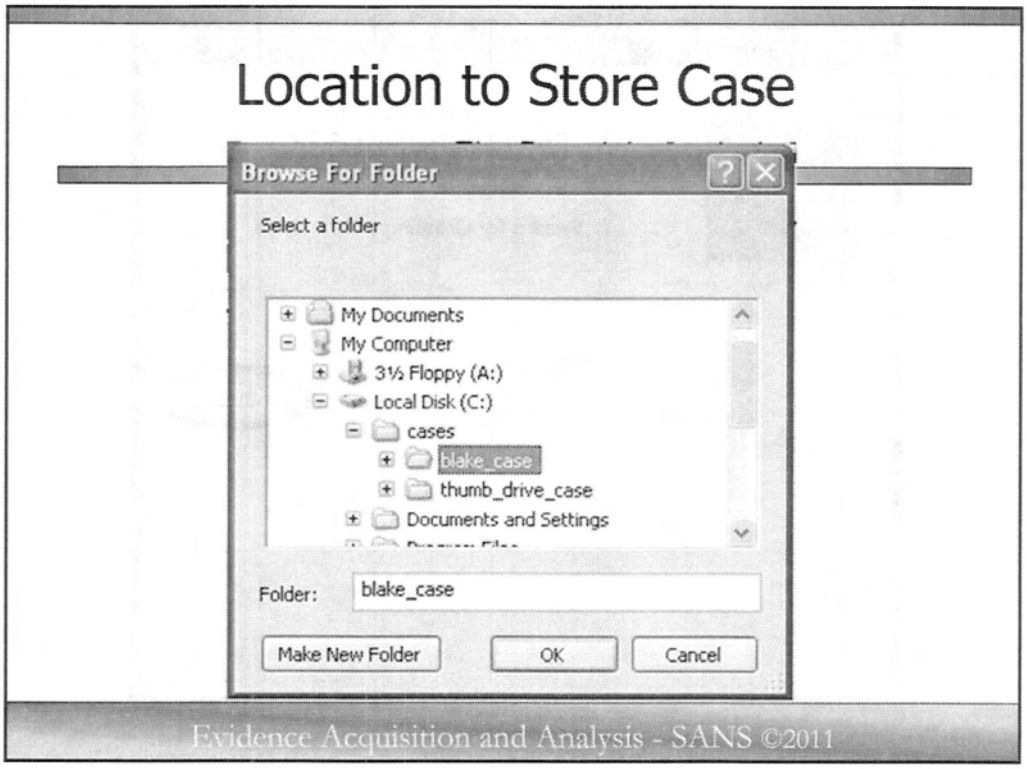
The next dialog box requires that you fill out the INVESTIGATOR name. The investigator may be different than the forensic examiner, or could be the same.

Next is your **Case Number** and **Case Name.**

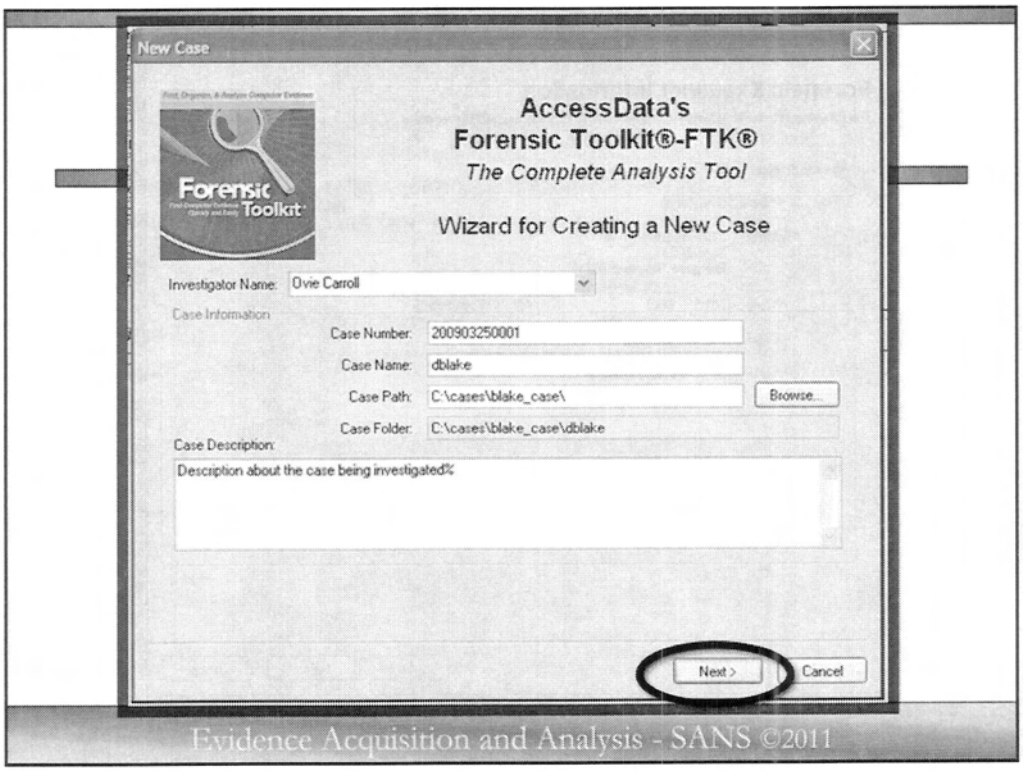
These two fields must be filled in.

Next, you should click **"Browse..."** and select a directory where you want to process the evidence. This location will be where the index is created so it should be of sufficient size to support a large index of information. Additionally, if possible, for absolute optimal conditions, it should be a separate drive than your operating system and should have as fast read/write times as possible. You would not want this to be an old poky 40 gig, 4200 RPM drive with a ton of bad sectors.

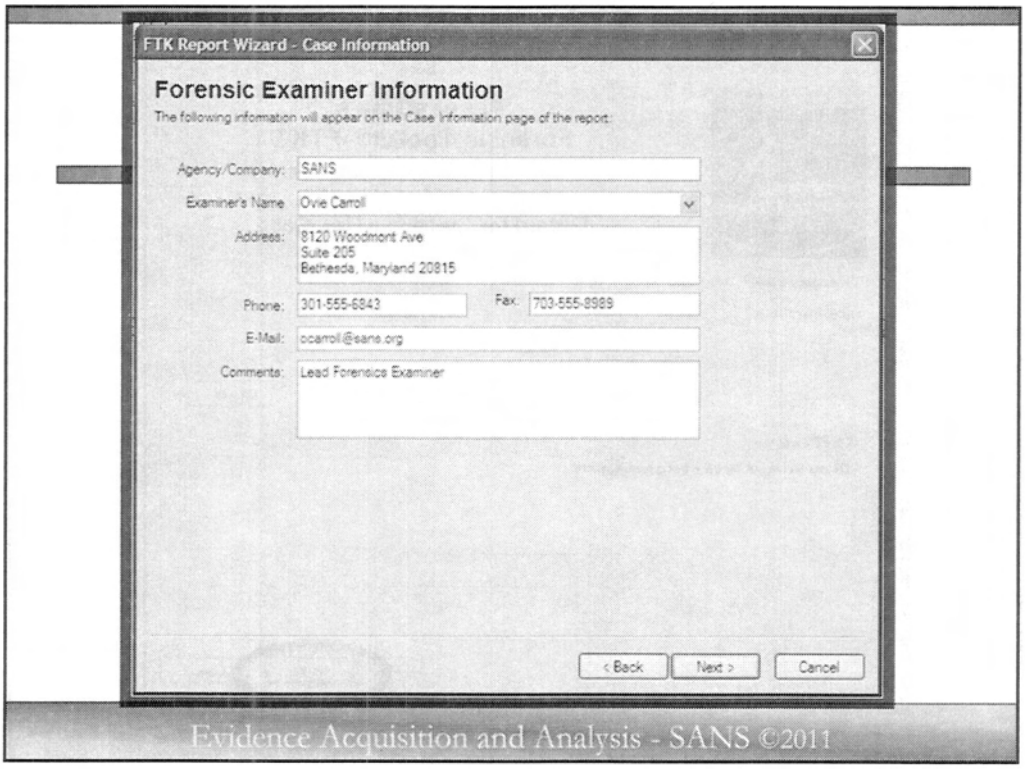
Lastly, you have an opportunity to give a description about the case.



You should now see the Browse For Folder dialog box. Here, you should navigate to the directory that will contain your case file. For today that will be on the root of the "C" drive, then the subdirectory "**cases**" and the subdirectory under that named "**blake_case**".

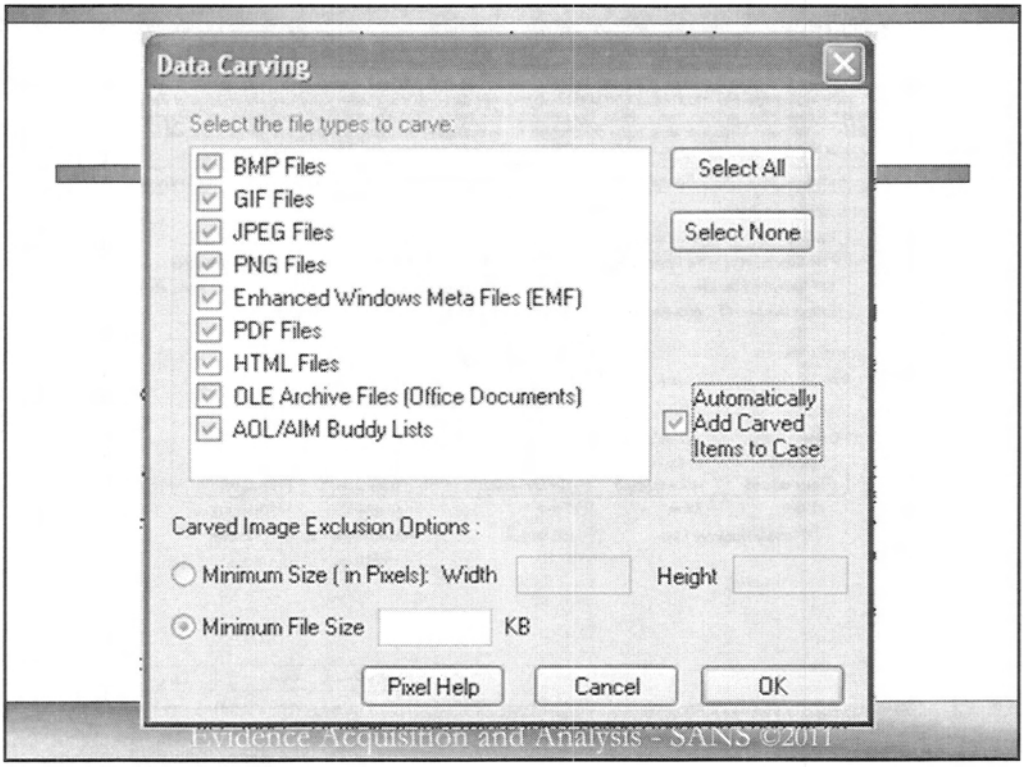


Next, you should fill out a short case description in the case description freeform input area. Remember that what you put here, and everywhere in your case file, is discoverable in court, so you would not want to put anything here that suggests you have already come to a conclusion in your case, or anything derogatory about the defendant/subject.



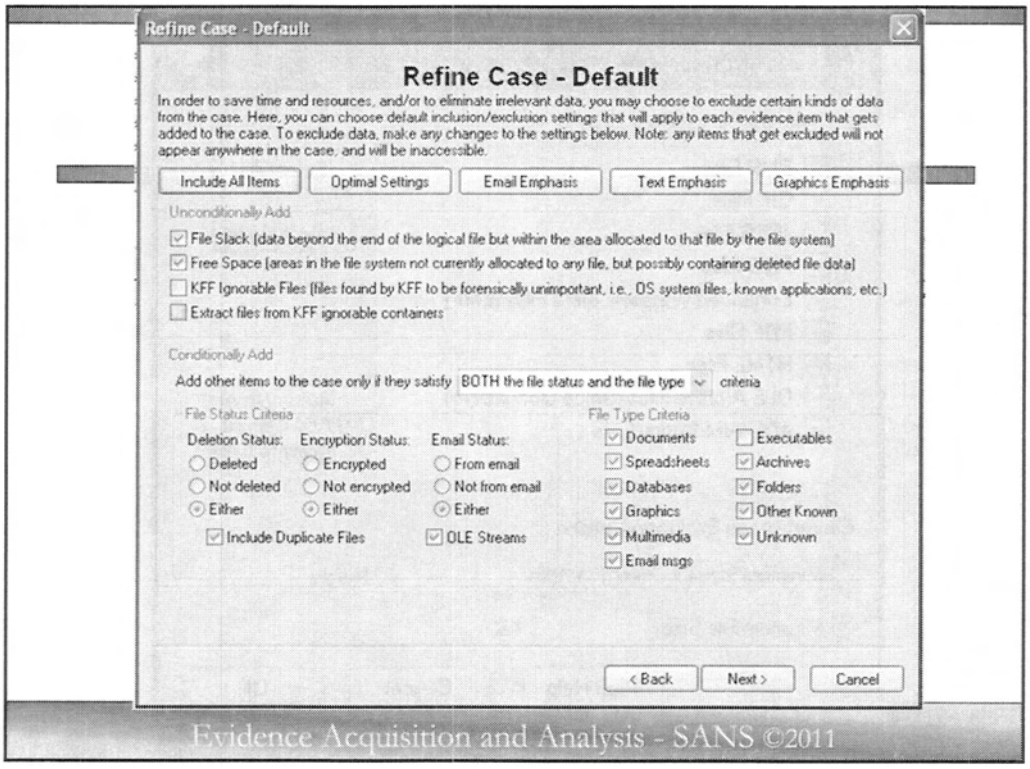
Next you fill out the appropriate examiner information which should include your agency's name, the examiner's name, the examiner's address, phone number and fax, an e-mail address and any comments about your case that is examiner specific.

Special Note – This information can be auto-populated by editing the FTKExaminer.dat file located in the "C:\Program Files\Access Data\Access Data Forensic Toolkit 1.81.3\Program" directory.



Make sure everything is selected, then select **Automatically Add Carved Items to Case**.

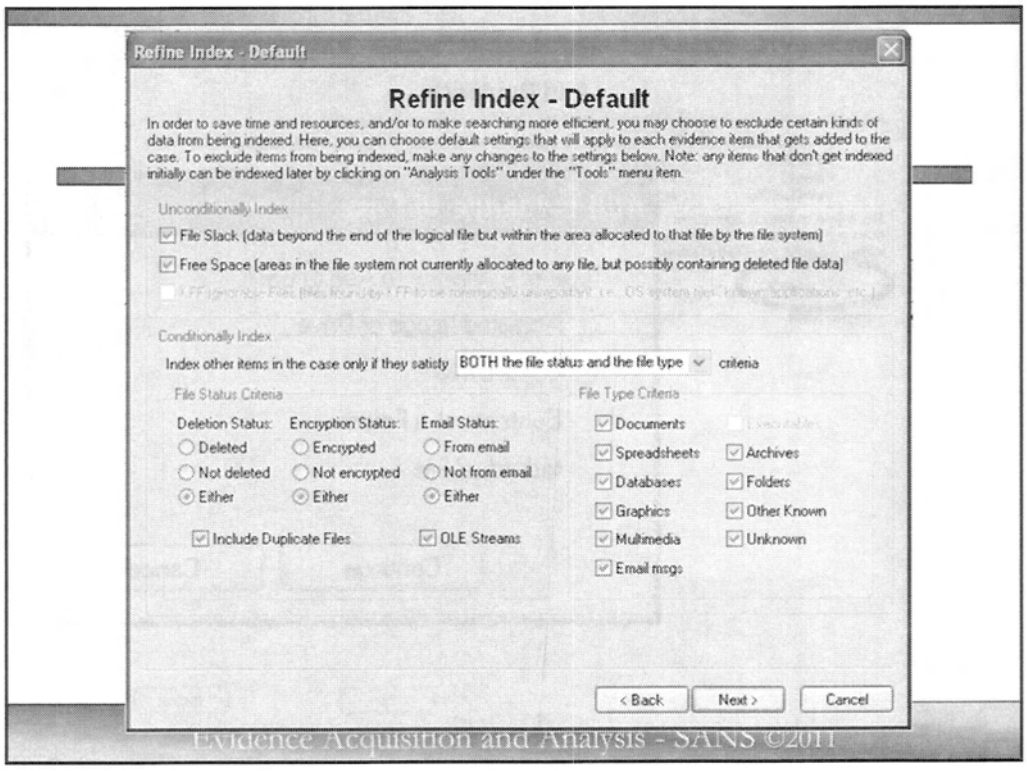
You can experiment yourself about finding the minimum size graphic to add to the case. With this setting, you can avoid a lot of the tiny application icons from being added to your case.



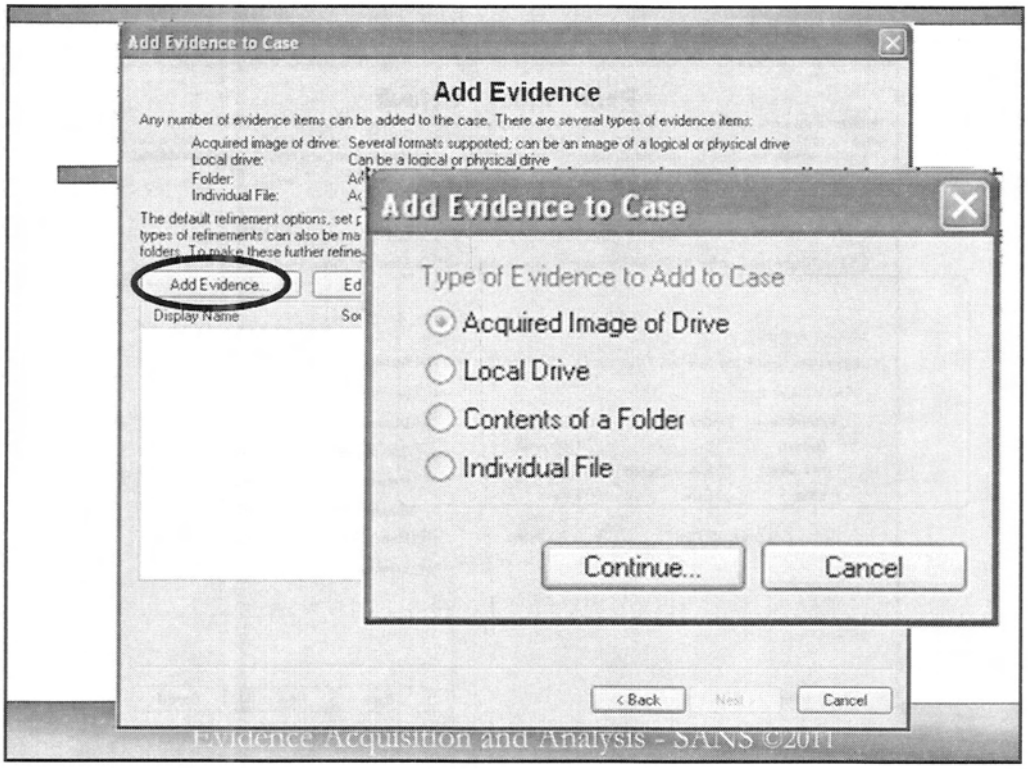
In this dialog box you have the opportunity to further refine how your case is processed. As you can see, you have some preset processing options across the top, such as if your case is primarily e-mail or graphic based, you could choose E-mail Emphasis or Graphic Emphasis, etc.

My recommendations for the standard cases is to use the "**Include All Items**" button, then under the "Unconditionally Add" area, REMOVE the check box from KFF Ignorable Files.

KFF's are Known File Filters which can be used to filter out files that are a standard part of an operating system, or what is sometimes known as Gold Tape files. These would be files that are part of a base load on every system in your organization. If these files have not been modified, why look at them or add them to your case?



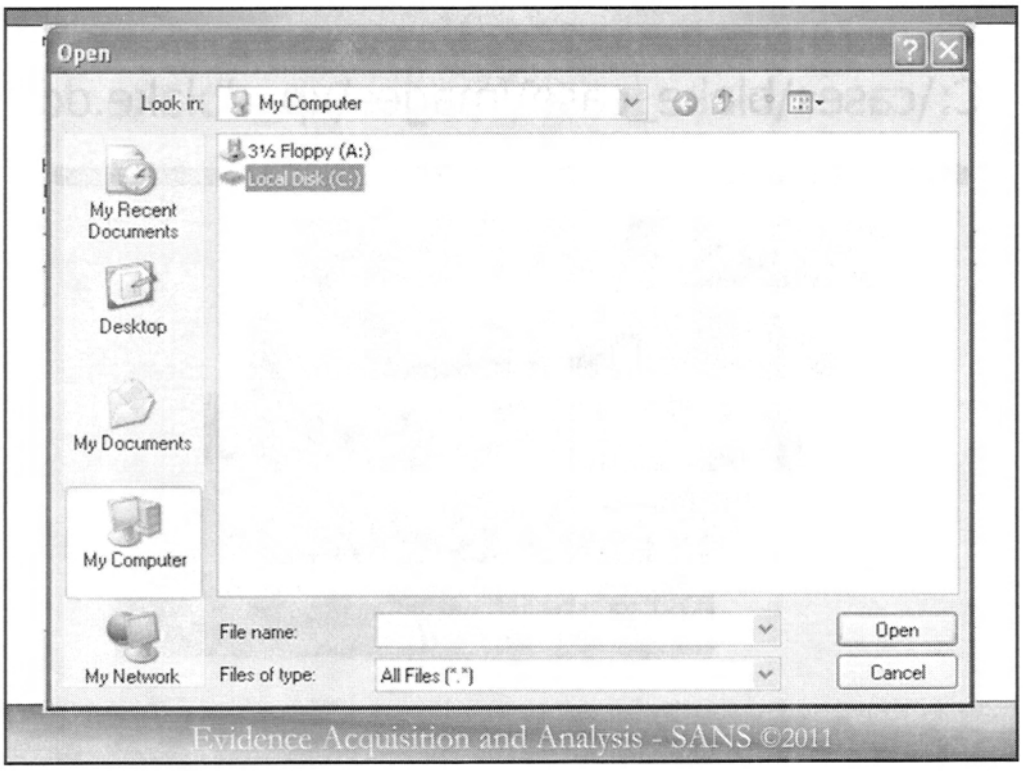
This next screen looks very similar to the last screen, but the difference is that these are things you want added to your case but NOT INDEXED. You can always index later but in 99.9% of all your cases, you will just accept the defaults.



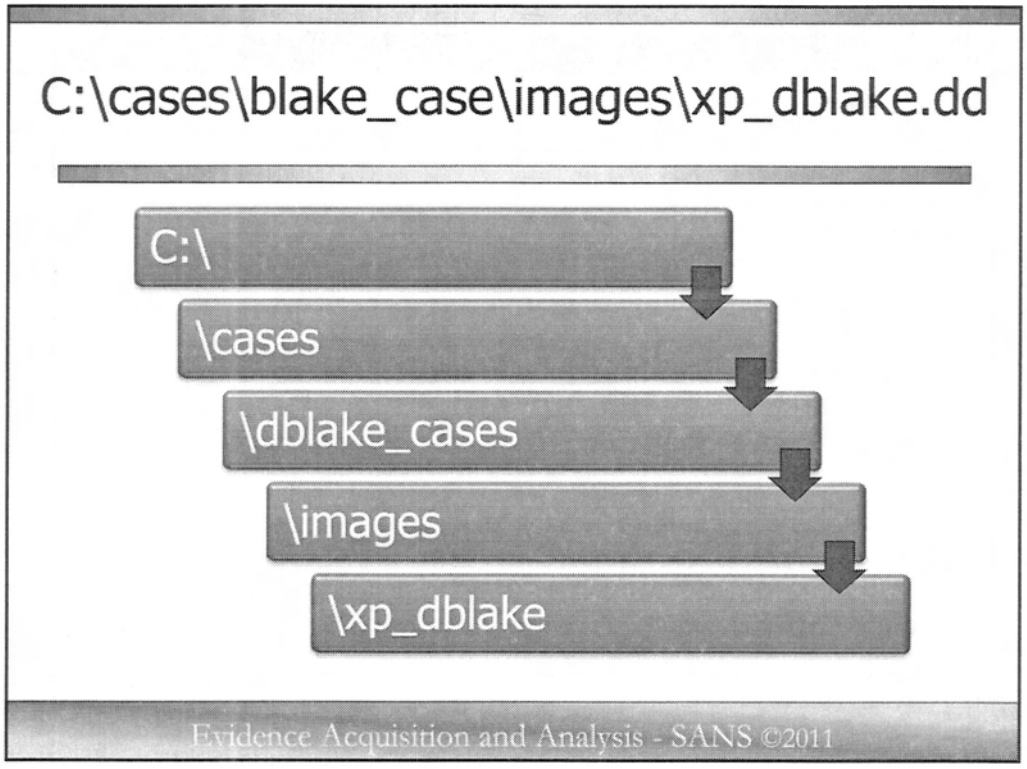
Now it is time to Add Evidence to your case. To do this, simply click on the "**Add Evidence…**" button.

Next, you choose what type of evidence you are adding to your case. Typically it is going to be an "**Acquired Image of Drive**". You could, however, connect the actual drive with a write block to your forensic computer and then select Local Drive.

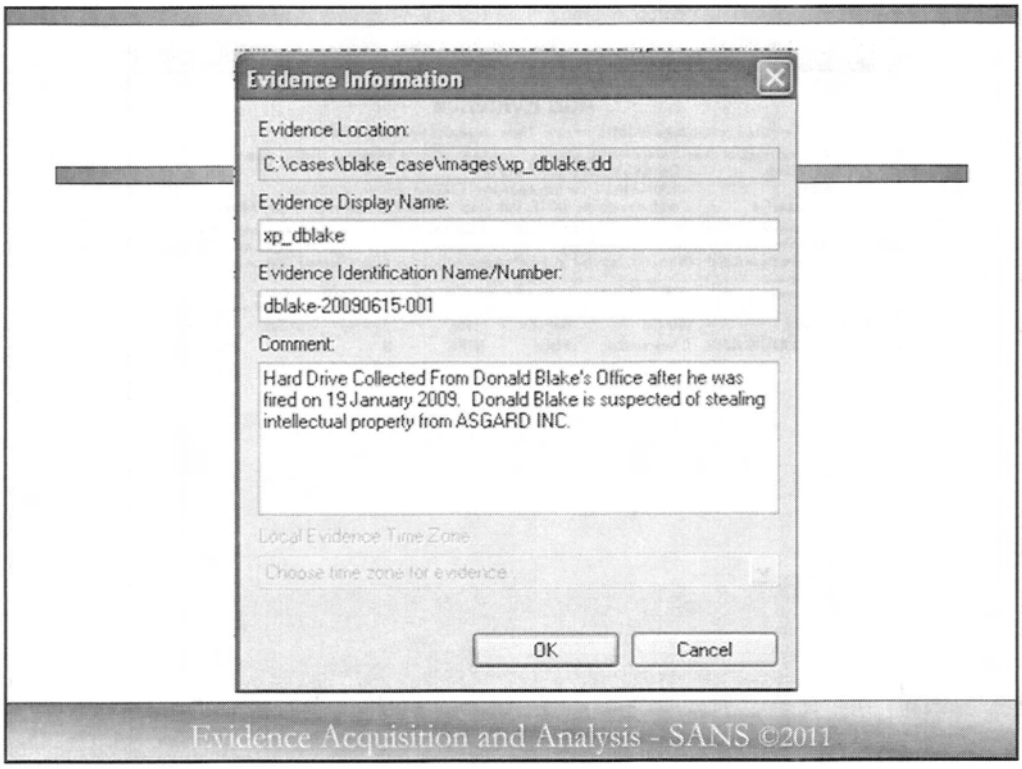
Click "Continue", then navigate to to the location where your image file is located.



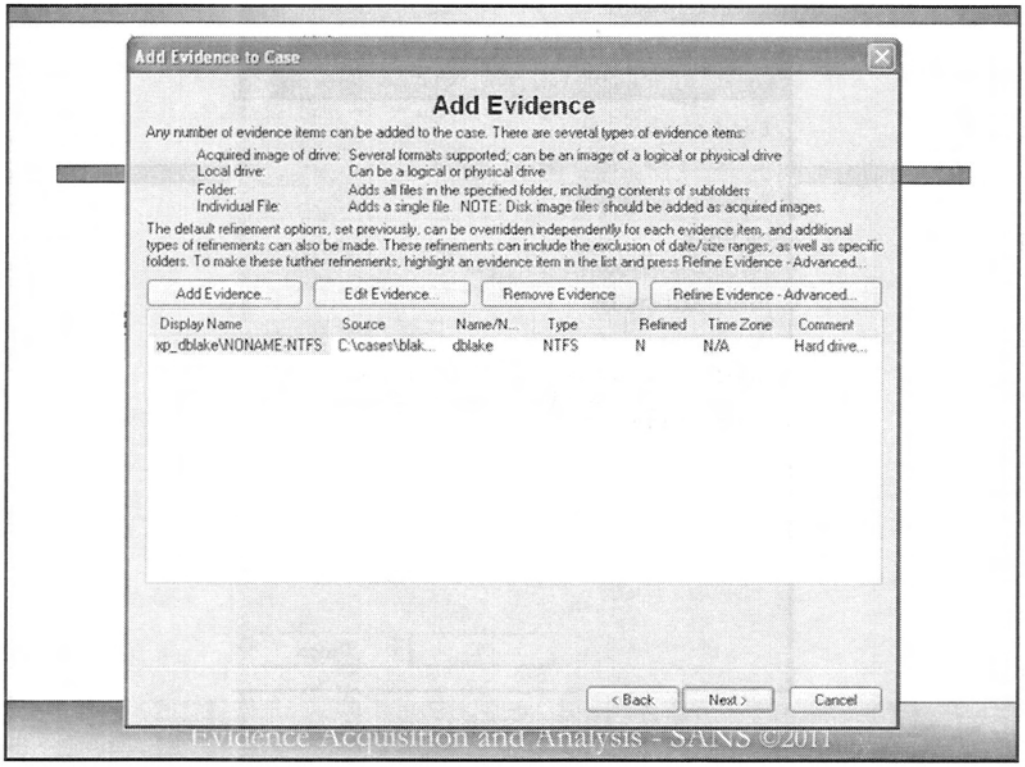
Next, in this dialog box, you should navigate to the "C" drive. Click on you're my Computer icon, then go to the "C" Drive.



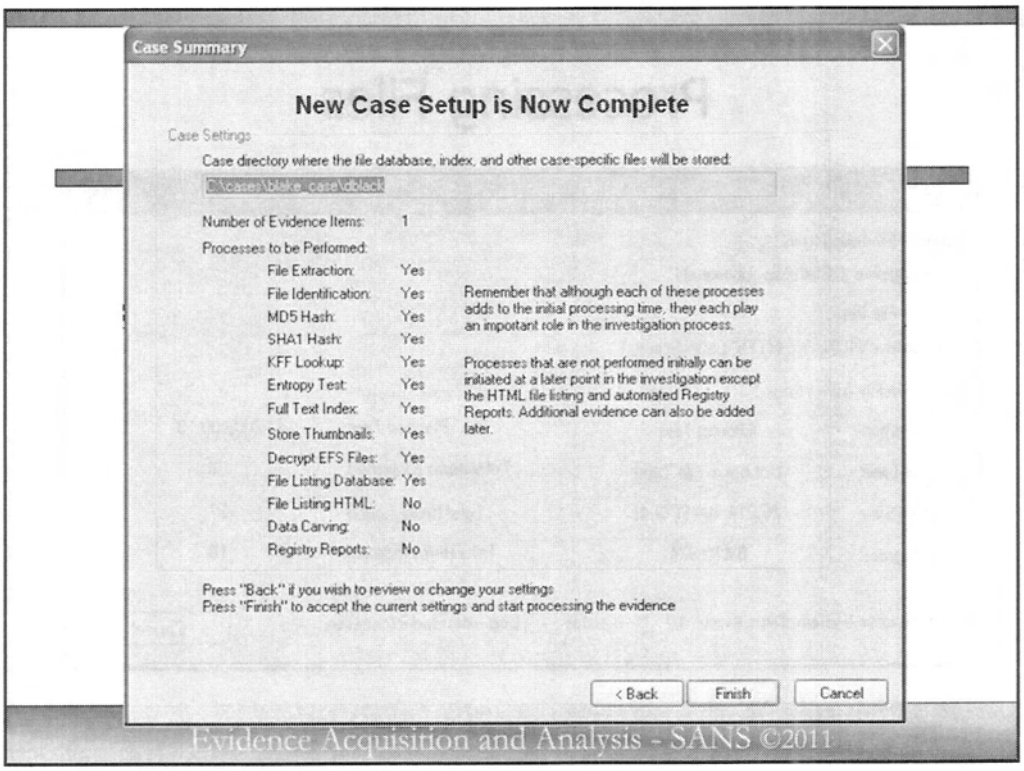
Next, you should navigate to the C:\cases\blake_case\images\ and select the file labeled **"xp_dblake.dd"**, then click Open.



Because you may often be examining multiple drives or pieces of evidence, FTK gives you an opportunity to give each piece of evidence a specific or unique name and description. This is very helpful when you are examining several hard drives, thumb drives, and other media, all for one case, at one time. A descriptive name will help you more quickly identify which piece of electronic evidence you are looking at.

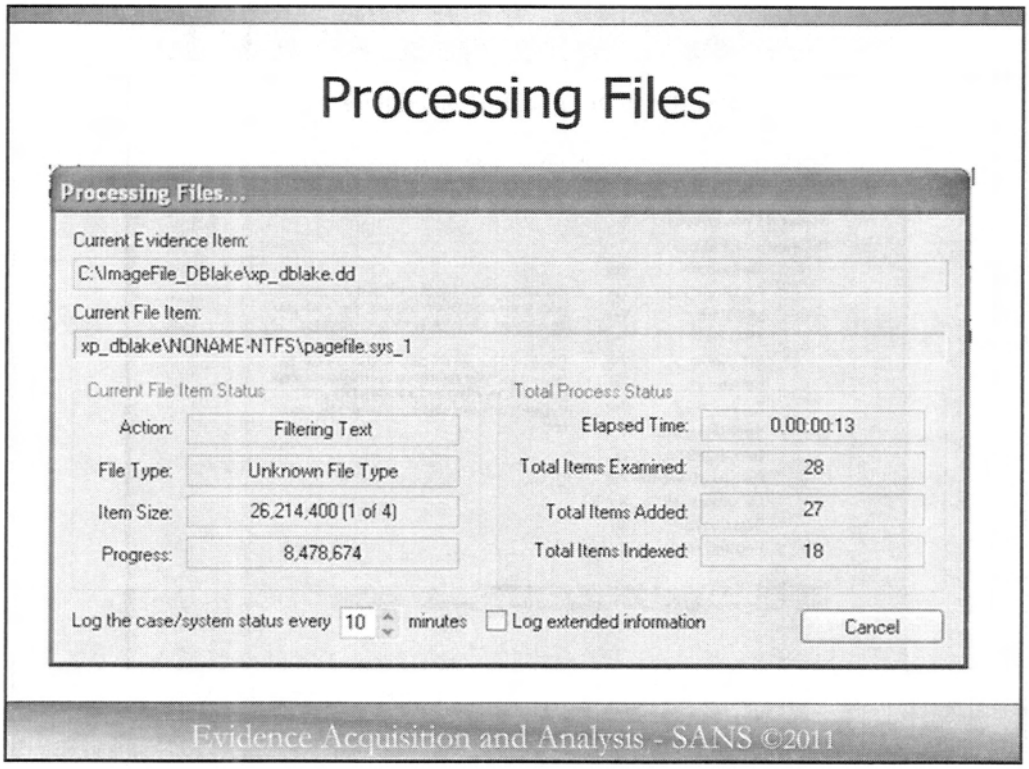


You can continue to add more evidence, or remove evidence, if you accidentally added something in error. Once you start your case indexing, you cannot remove evidence, so review what you add before moving on.



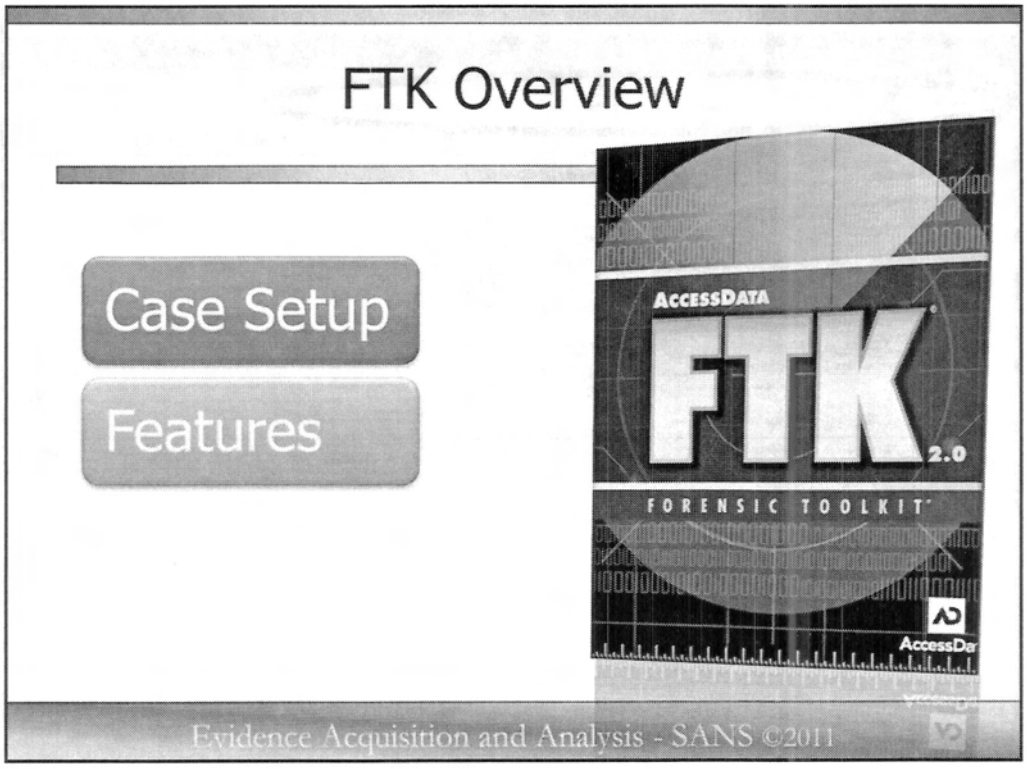
Finally, we get to the "Are you sure" screen. Review what your choices are and what you are about to do, then click Finish and go home.

I say go home because when you get back to the office, you will find only junior examiners start a case indexing during the day, because it ties up your system completely until it is finished indexing. Most examiners start the indexing process just before they go home for the evening.

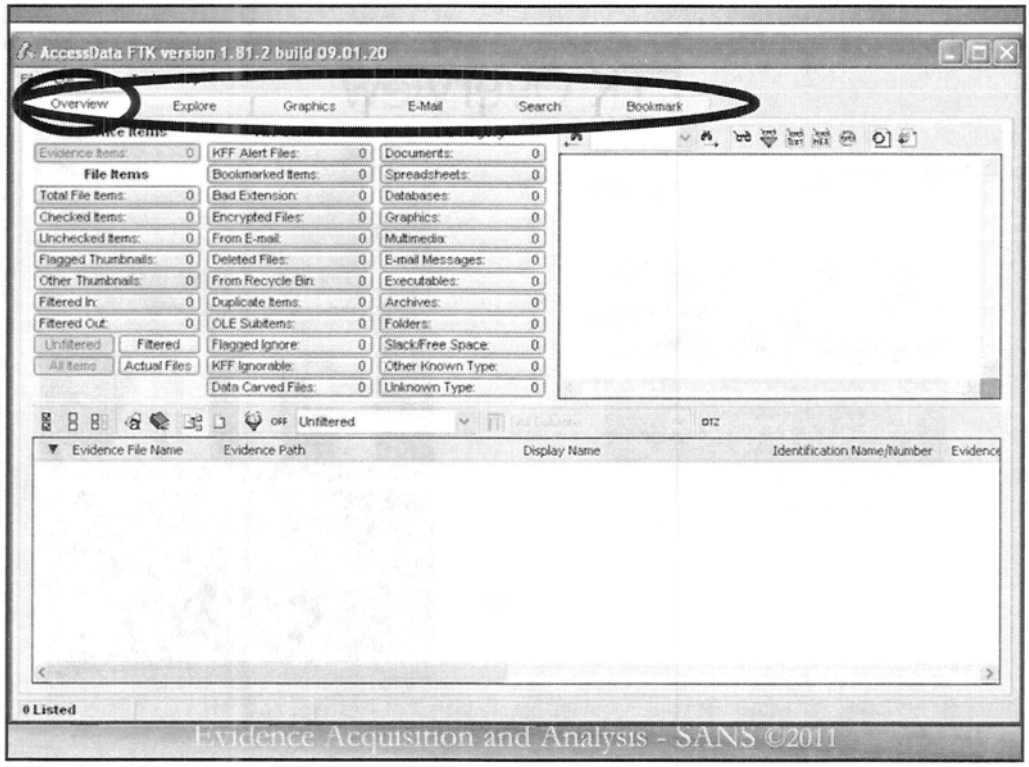


Get used to looking at this screen since it will be there for hours, or even days.

While FTK is getting better and better, I still have experienced great difficulty if something bad happens while a case is indexing. Typically, you will have to start this whole indexing process over again. FTK does not seem to gracefully pick up where it left off if you have a crash or power failure, even though it is saving its progress in a log every 10 minutes.



This page intentionally left blank.

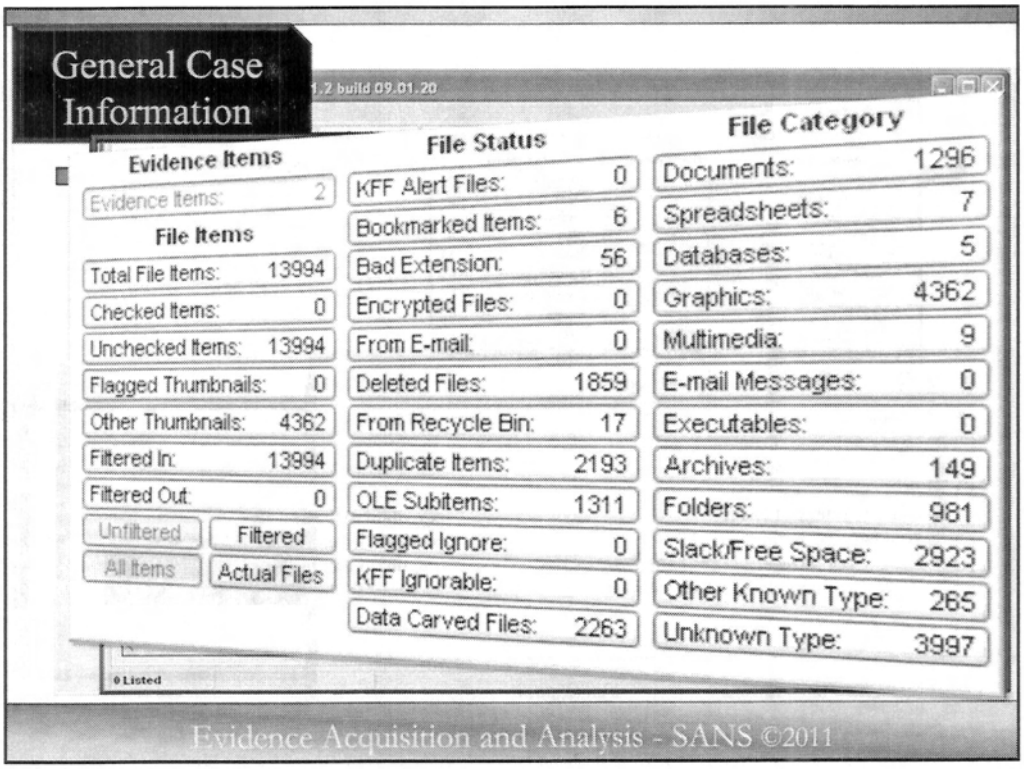


One of the great features of FTK is the way it presents information to the investigator/analyst.

The first thing you may notice is that across the top of FTK are (6) SIX tabs. We will be discussing each of these tabs briefly because you will be navigating your analysis through using these tabs.

Here we are at the OVERVIEW tab, which is the first thing you see when you start FTK. At a glance, the overview tabs tells you all the basic information about your case, as well as, provides you the ability to immediately review specific groups of files.

The Overview Tab can be broken down into (3) Three basic areas.



In the top left of your screen, the General Case Information section that tells you all the basic information about your case. To name a few, it shows you:

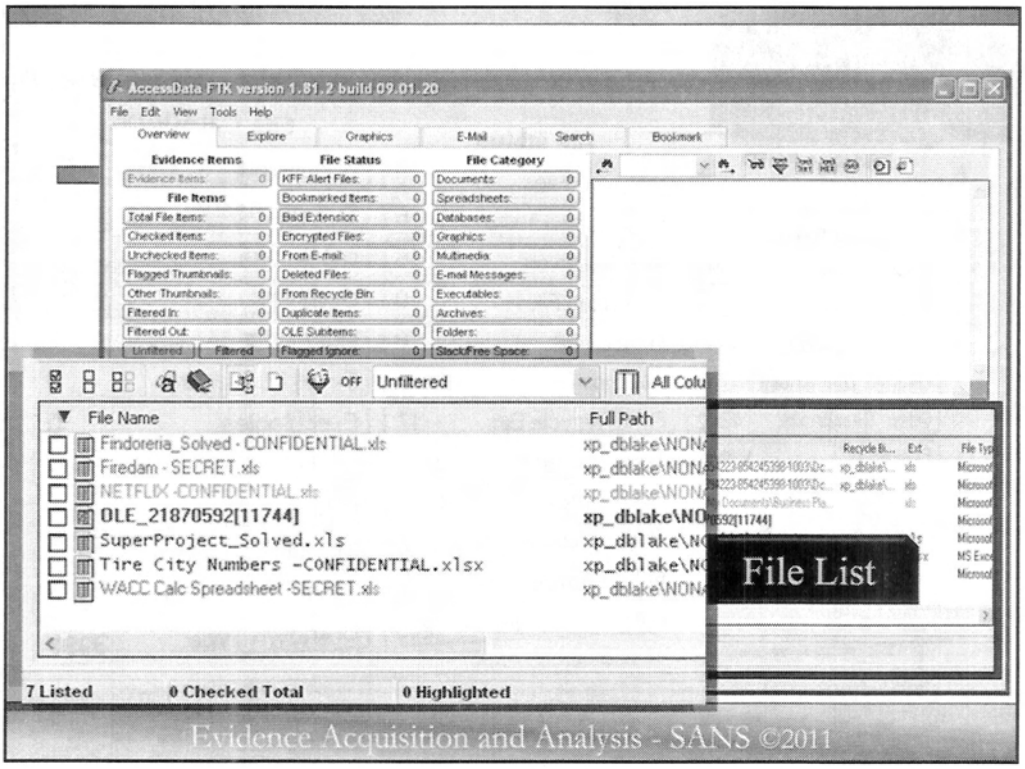
The number of **evidence items** – this is so if you bring into one case multiple hard drives, imaged thumb drives, CDs or DVD, etc, you can see them all here.

The **total number of files** across all media.

The number of **graphics**, **e-mails**, **documents**, **spreadsheets**, **databases**, etc.

This provides you a really easy and quick way to go right to the files you may need to review.

If this were a case involving child pornography, with one click you could go directly to review all graphics in the case. You could quickly pull up all the spreadsheets or deleted files on the system, etc.

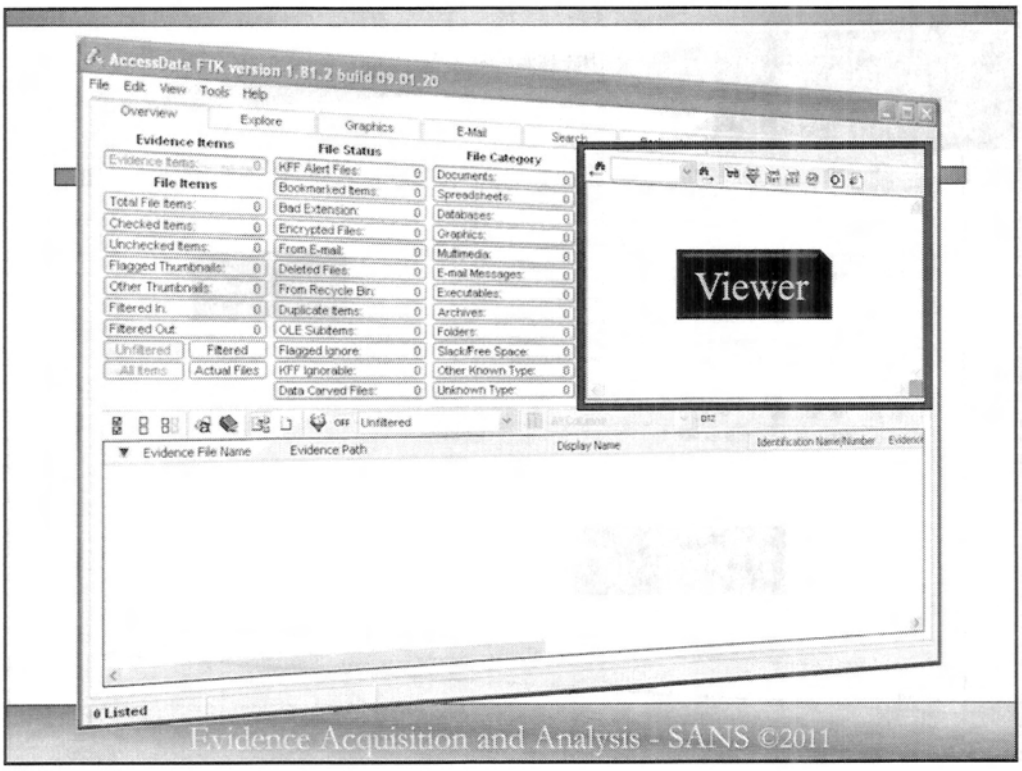


Directly below the General Case Information section you will find the File List area.

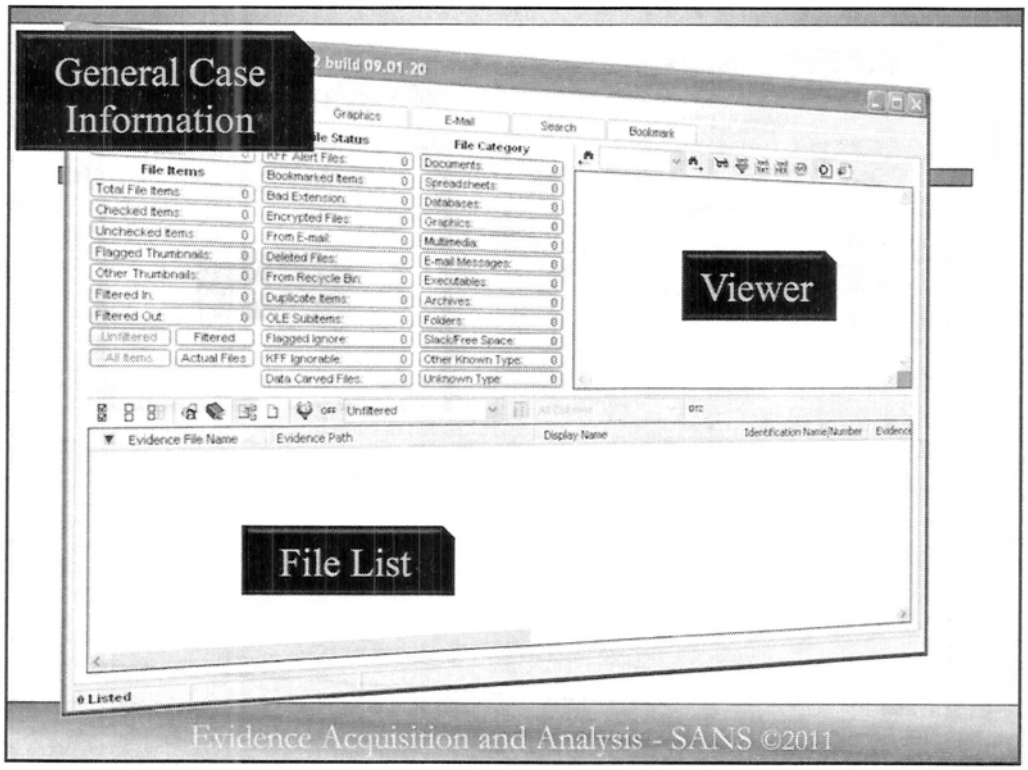
If you click on any of the buttons in the above General Case information Section, all files of that particular button will be listed here. You can scroll through and review, bookmark, or export these items quickly and easily.

By clicking on the spreadsheet button, a file listing of all spreadsheets would be displayed in the File List section.

As you select any of the files in the File List area, the contents of that file will be displayed in the top right windows, which is called the View Window.

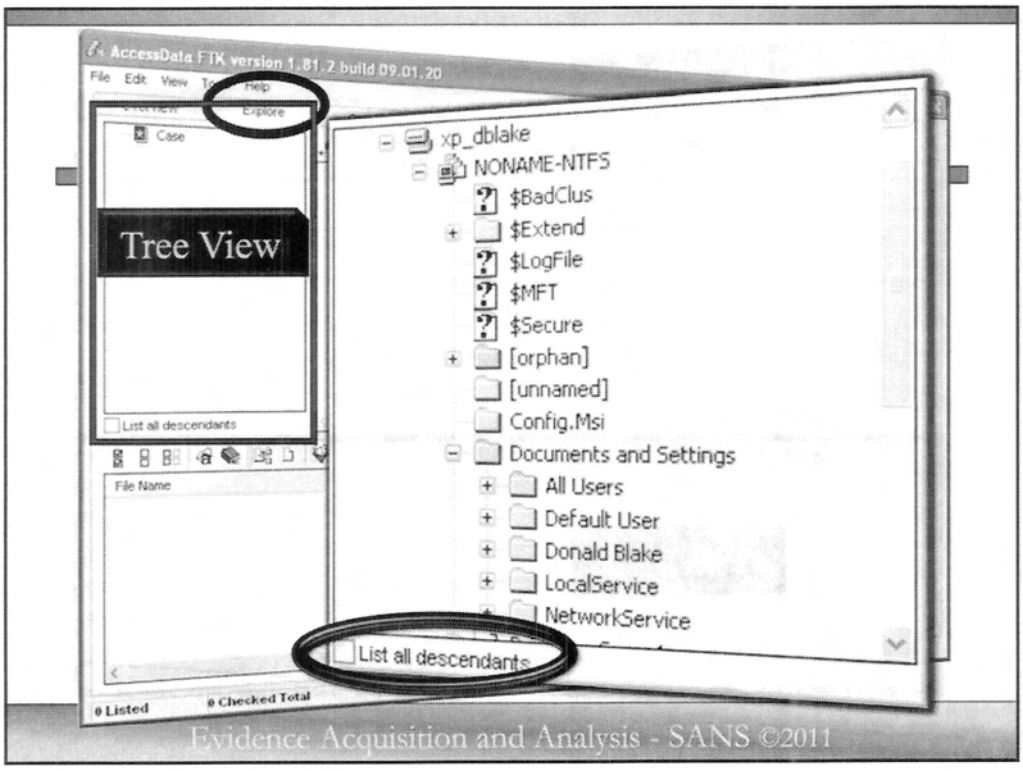


At the top right of your screen you will find the Viewer Window. FTK uses "Quick View" like technology to display almost any file in the view window. This gives the reviewer great ability to view a wide range of file types without having to launch all the associated viewers. Imagine having to open each application for each associated file type. The file is displayed almost as quickly as the reviewer can select each subsequent file.



So that was your FTK overview tab. This is such a valuable tab because from here, you can quickly get information about what is on the drive you are examining, as well as quickly access specific files sets like all graphics, documents, spreadsheets, etc.

Next, let's click on the Explorer Tab found across the top of FTK to the right of the Overview tab.



The Explorer tab provides a directory tree display of the evidence items that can be navigated much like in the standard Windows Explorer.

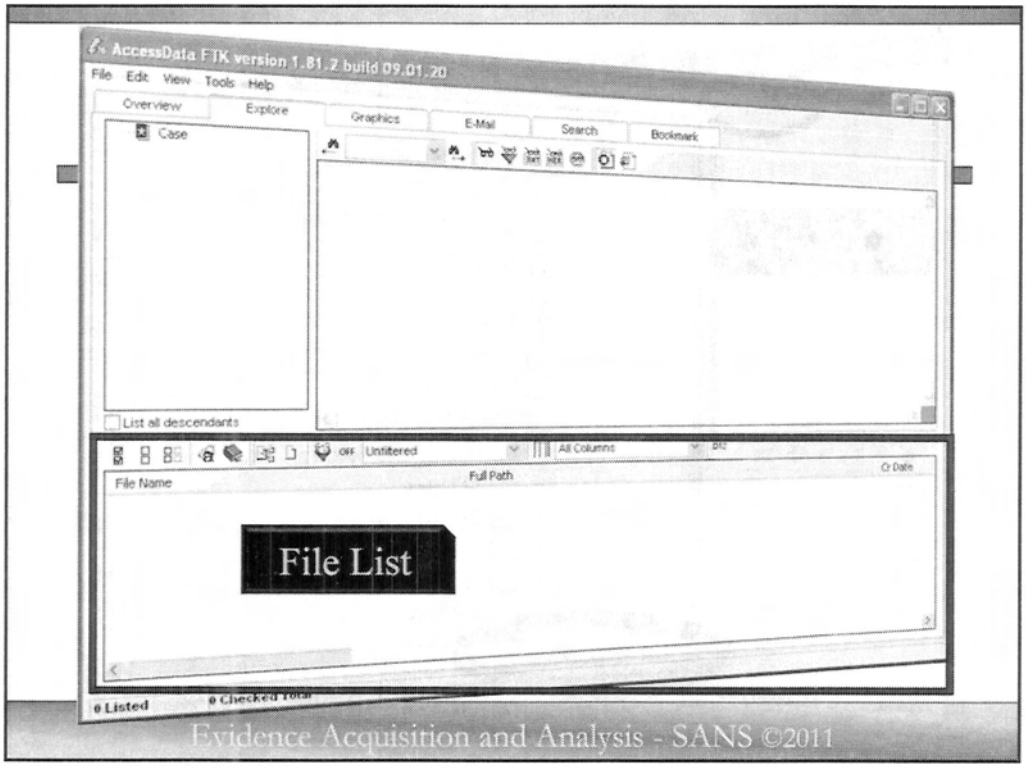
Starting at the Top Left, you will find the "**Tree View**".

You can see in this window the directory tree structure and you can expand and contract the directory structures by clicking on the "+" PLUS or "-" MINUS symbols, just like in your standard Windows programs.

You can view the file within each of the folders by clicking on each directory. As you click on each directory, ONLY the files in that directory will be displayed. You can view ALL files in that directory and all subdirectories or DESCENDANTS by clicking on the **LIST ALL DESCENDANTS** box.

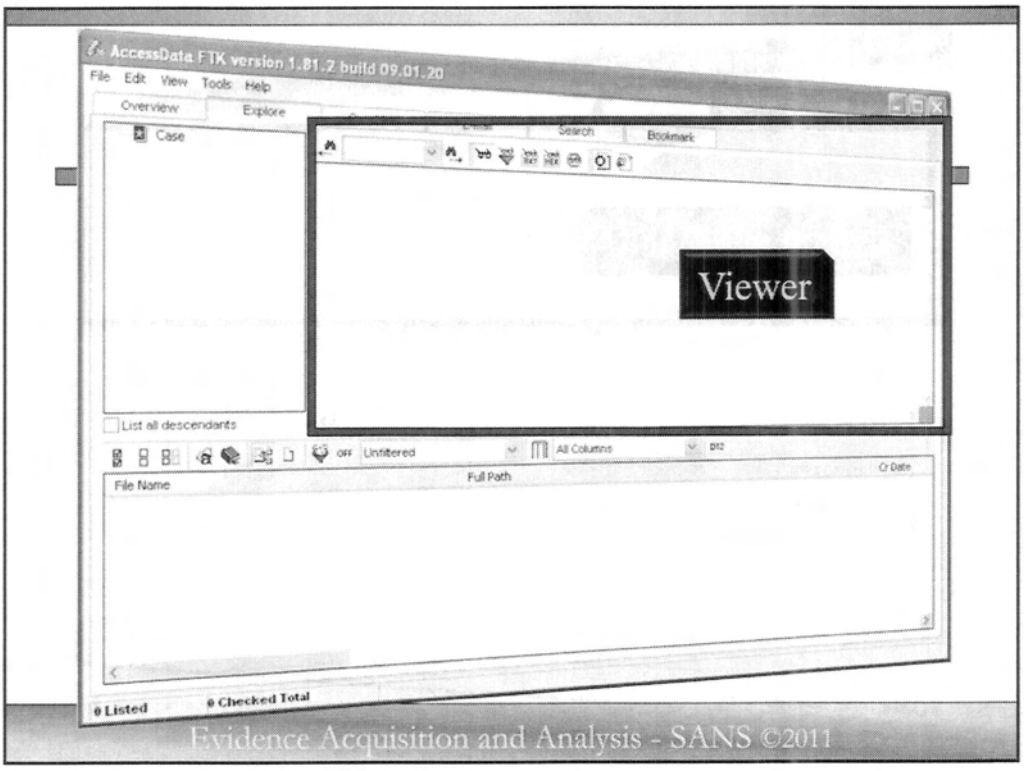
You may find that many times while reviewing your case, you are not seeing all the files you think you should see. The first thing you want to check is if you have the **LIST ALL DESCENDANTS** box checked or not.

From a performance aspect, your forensic machine must work a lot harder to display or sort all files and descendants from the root directory, so just make a note about if you want the checked. I must confess that because at my office we have dual quad-core Zeon processors, I don't really worry about this much, but depending on the system you are doing forensics on, you may want to be judicious with its use.

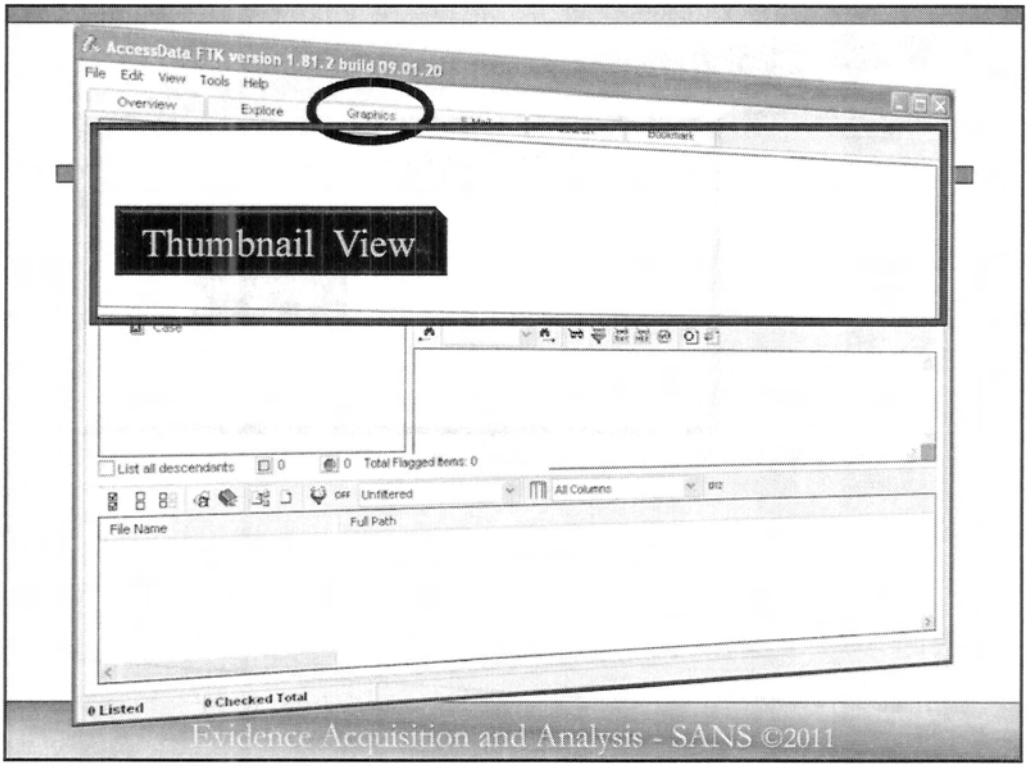


Directly below the Tree View window, you will find the File List window. As you click on any directory in the Tree View window, the contents of that directory, and it's subdirectories, if the "list all descendants" button is selected, will be displayed here.

As you select any of the files in the File List Window, the contents of the file will be displayed in the Top Right Viewer Window.



At the top right of your screen you will find the Viewer window. Just like we saw from the overview tab, this and all the viewer windows in FTK use the same "Quick View" technology to display almost any file in the viewer window. This is a very convenient feature to quickly look at virtually any file on the drive.

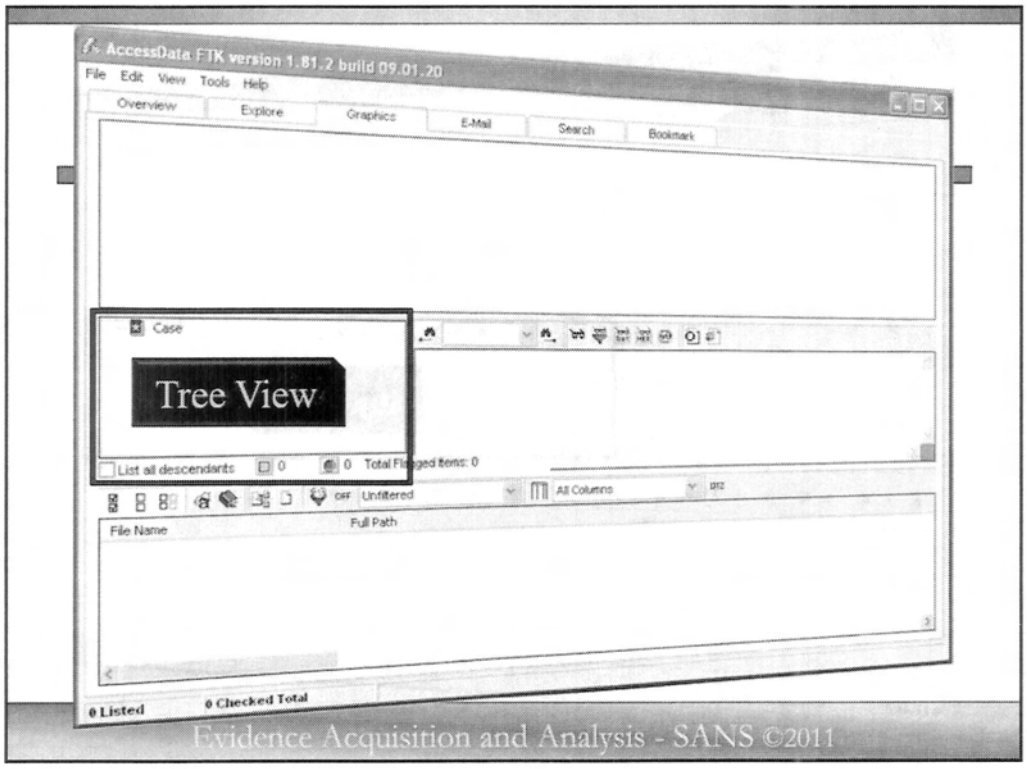


Almost no matter what kind of case you are working, you will be spending a lot of time in the **Graphics Tab.** The Graphics Tab displays all graphic files in a photo-album or contact sheet style display. Depending on the size or number of monitors you have, this allows you to review 20, 40, or more images at one time. This allows you to quickly scan and triage graphics.

You can adjust the size of the Thumbnail View window by clicking and dragging the bar below the Thumbnail View windows. If you are like me, when you have to review a lot of graphics, you can spread FTK across multiple large monitors so you can quickly triage or review them.

Under each thumbnail image you will notice a button that can be clicked red or green. This is called **Flagging** and it is mainly used when you bookmark a lot of graphic files but perhaps you do not want the graphic PRINTED in your report. You can create your reports so that ONLY graphics flagged GREEN will be displayed in your final report. This might come in handy with child pornography cases where you don't want to be producing reports with child pornography images in the report. This will also help you comply with the Adam Walsh Act.

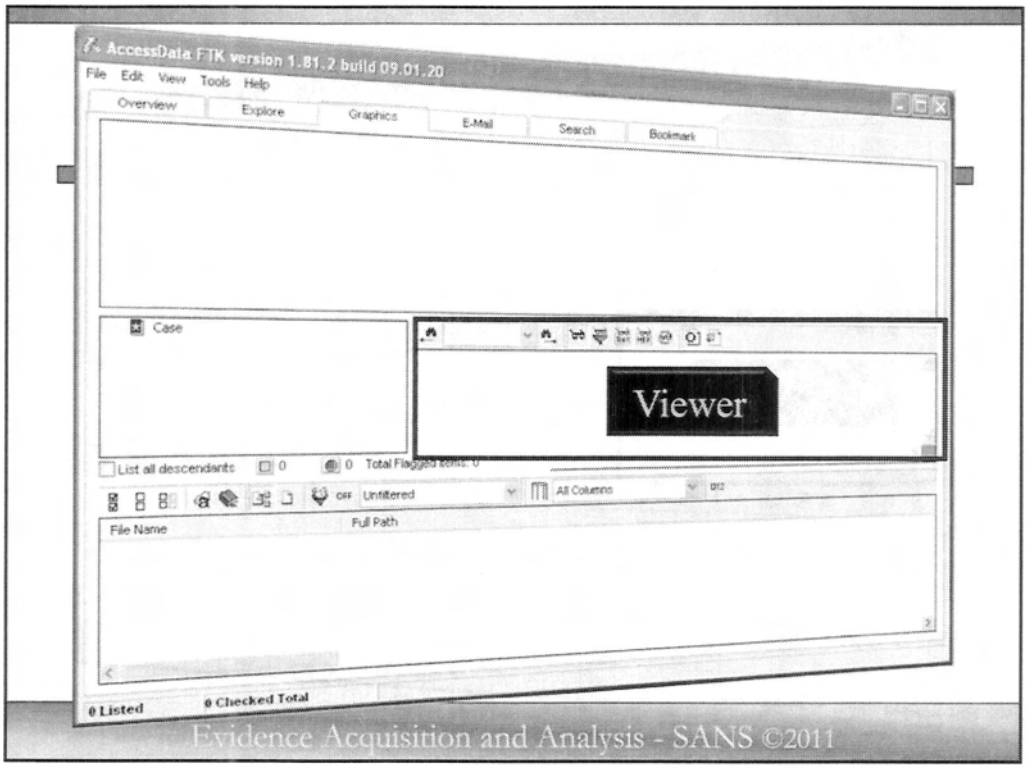
Discuss Adam Walsh Act that prohibits LE from releasing copies of child pornography and thereby possibly re-victimizing the victim every time that image is seen.



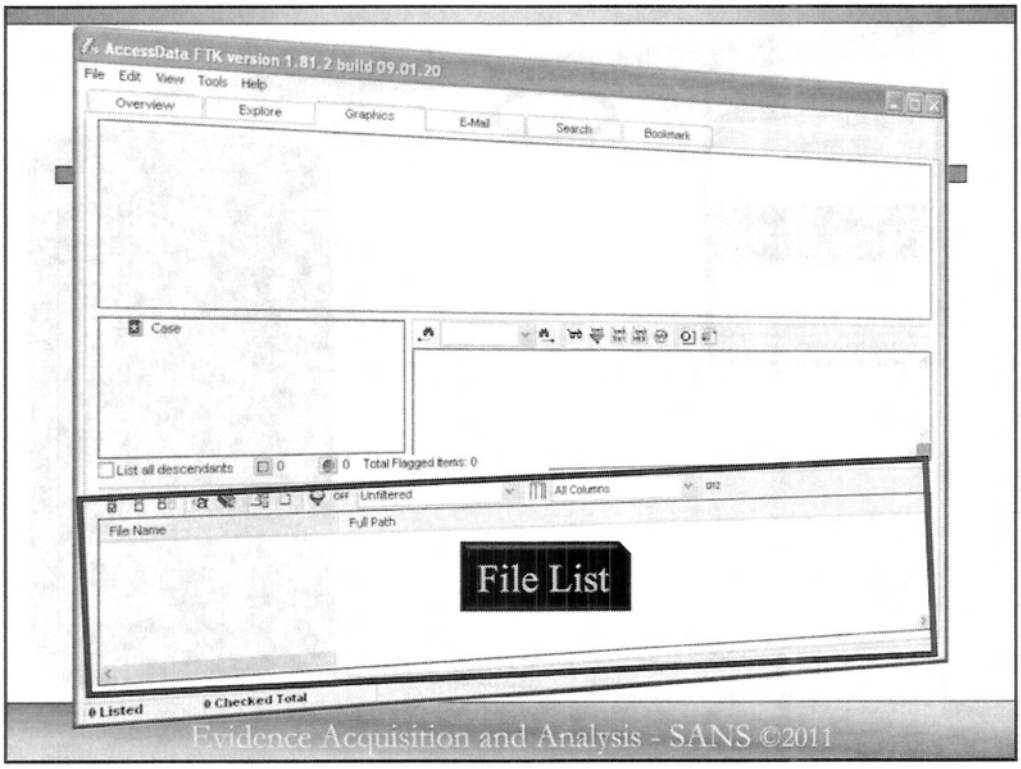
In the middle of the screen on the left side you will find the "**Tree View**". You can see in this window the directory tree structure. You can expand and contract the directory structure by clicking on the "+" PLUS or "-" MINUS symbols, just like in your standard Windows programs.

You can view the file within each of the folders by clicking on the directory. Like with the Explorer Tab, as you click on each directory, ONLY the files in that directory will be displayed, however, you can view ALL files in that directory and all subdirectories by clicking on the LIST ALL DESCENDANTS box.

So remember, if you want to review ALL graphic files on the system, you would go to the root directory in the tree view window, then select the List All Descendants button.

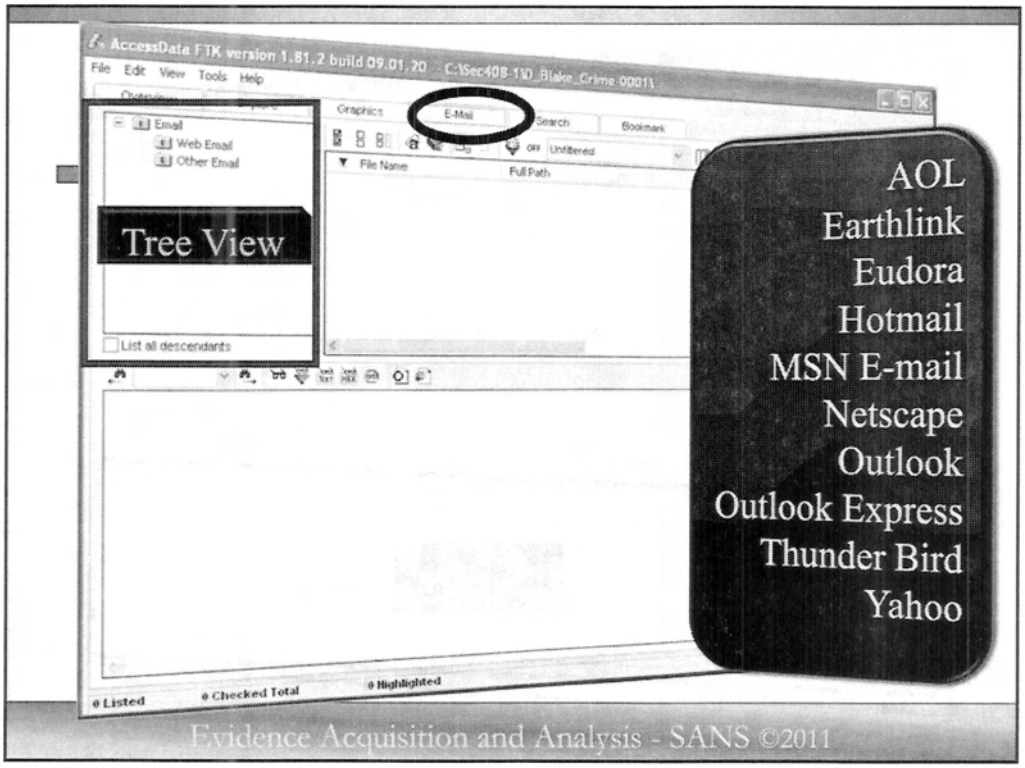


In the middle of the screen to the RIGHT of the Tree View windows, is the Viewer window. In this window, the graphic will be displayed in its full size for a more detailed inspection. In many cases, you will find you do not need to display each and every thumbnail image in the viewer windows.



At the very bottom you will find the **File List** window.

As you click on any of the graphics in the Thumbnail View window, the file will also be highlighted in the **File List** window. It is here that you will find where the file is located on the drive, what directory it is in, etc. You will also be able to look here in the **File List** window to see the MAC times and other interesting details about the selected file, such as if it is a match to one of the hash sets you have loaded, if it has a file extension mismatch (if someone changed the extension of a picture file from a JPG to a word document file such as DOC.



If you go to the top again and click on the next tab to the right of the Graphics tab, you will see the **E-MAIL** tab.

When you talk to people that do a lot of computer forensics, almost everyone will agree that FTK processes and displays e-mail better than the other forensic programs.

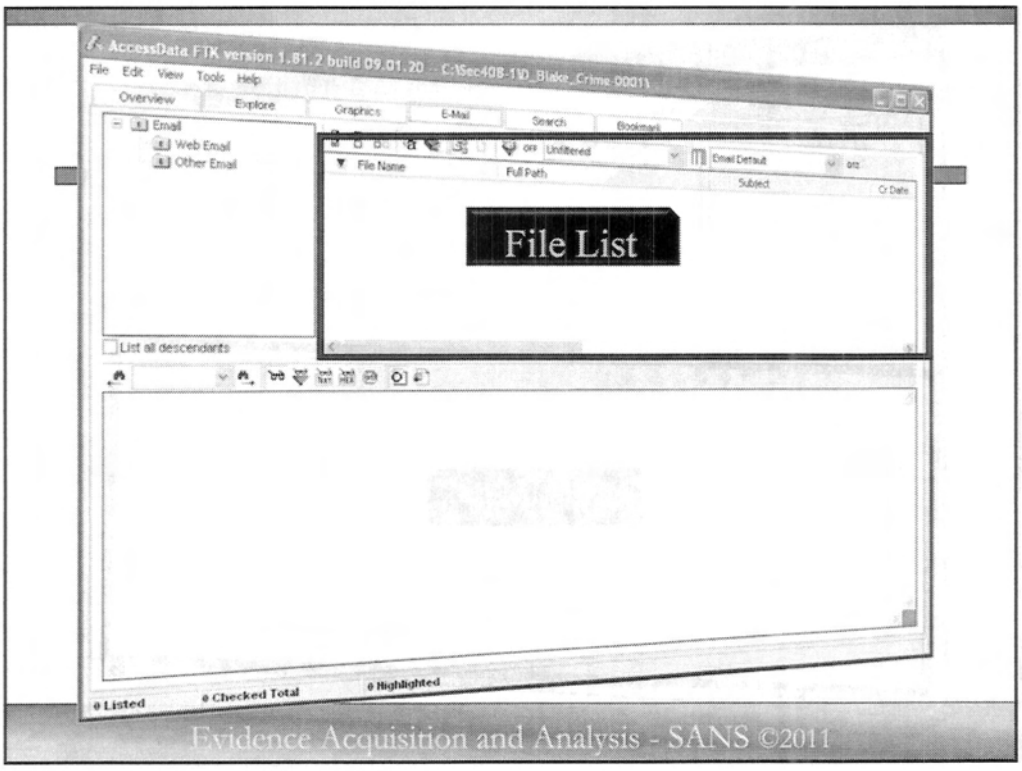
Starting at the top left, you will find the Tree View.

During preprocessing, FTK attempts to locate all e-mail based on e-mail archives and special headers, and will categorize them here.

FTK currently recognizes:

- AOL
- Earthlink
- Eudora
- Hotmail
- MSN e-mail
- Netscape
- Outlook
- Outlook Express
- Thunder Bird
- Yahoo e-mail

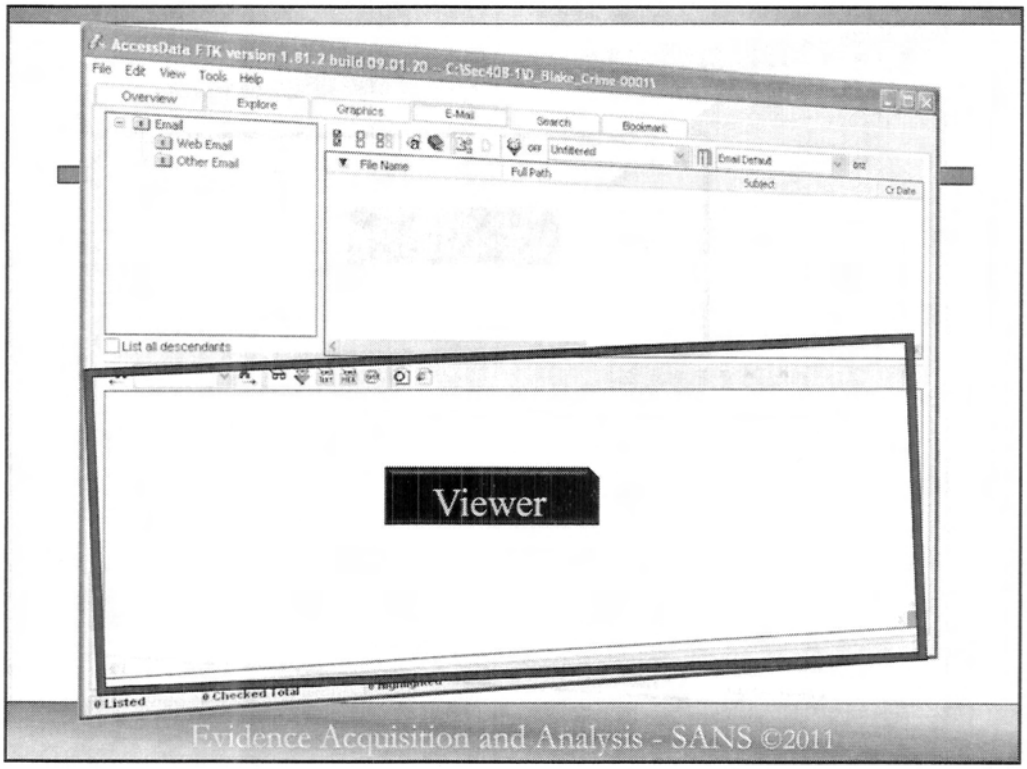
FTK will also attempt to recover deleted e-mail messages, even if the waste basket has been deleted from Outlook, Outlook Express and Thunderbird.



To the right of the Tree View, is where you will find all the messages. Remember, like in the other tabs, you will see only messages in the directory or mail folder you have selected in the Tree View window unless you have LIST ALL DESCENDANTS checked.

Now, the one thing you should be aware of is that FTK numbers all e-mail messages numerically in ascending order for EACH FOLDER. What this means is that you will have a Message 00001 in the INBOX, another Message 00001 in the SENT BOX, another in the DELETED folder, etc. This can sometimes get confusing, but FTK will tell you exactly what folder they came from.

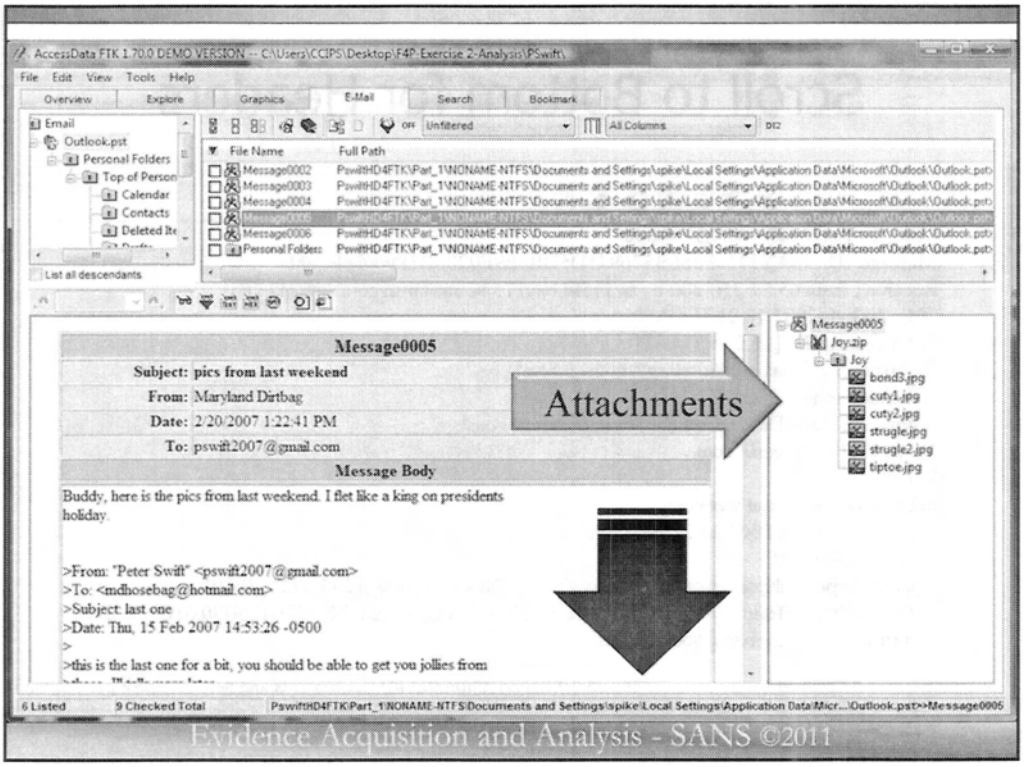
When you click on any of the messages in the File List window, the message will be displayed in the Viewer window directly below.



At the bottom of the screen you will find the **Viewer** window for e-mail.

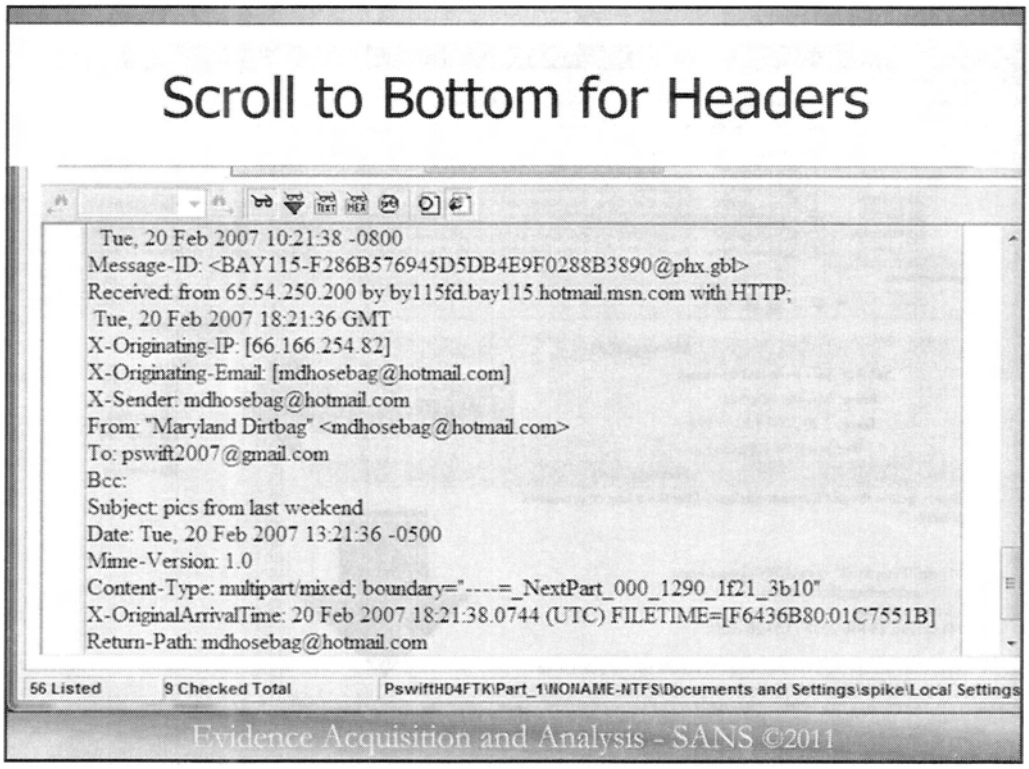
FTK displays all e-mail in HyperText Markup Language (HTML). You may recognize this as the language web pages are made of. The reason FTK displays all e-mail in HTML is so when you export all this out for your report, it will all be self-contained and displayed neatly.

Two additional things you should know about the e-mail tab...

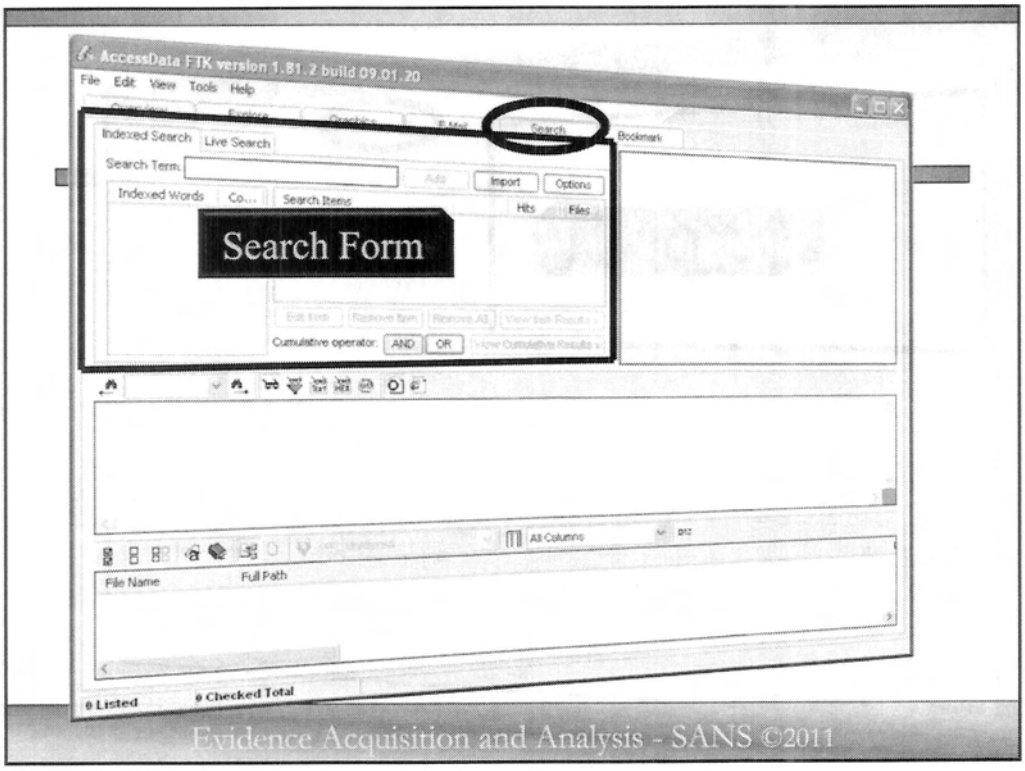


When an e-mail is displayed in the Viewer window, any attachments will be displayed in a window to the RIGHT of the displayed e-mail. This allows you to see what, if anything, was attached to any e-mail.

Additionally, FTK organizes the e-mail to display the contents of the e-mail at the top where you can see it, and places ALL e-mail headers at the bottom of the e-mail. So if you want to examine the mail headers, scroll down to the bottom of the e-mail.



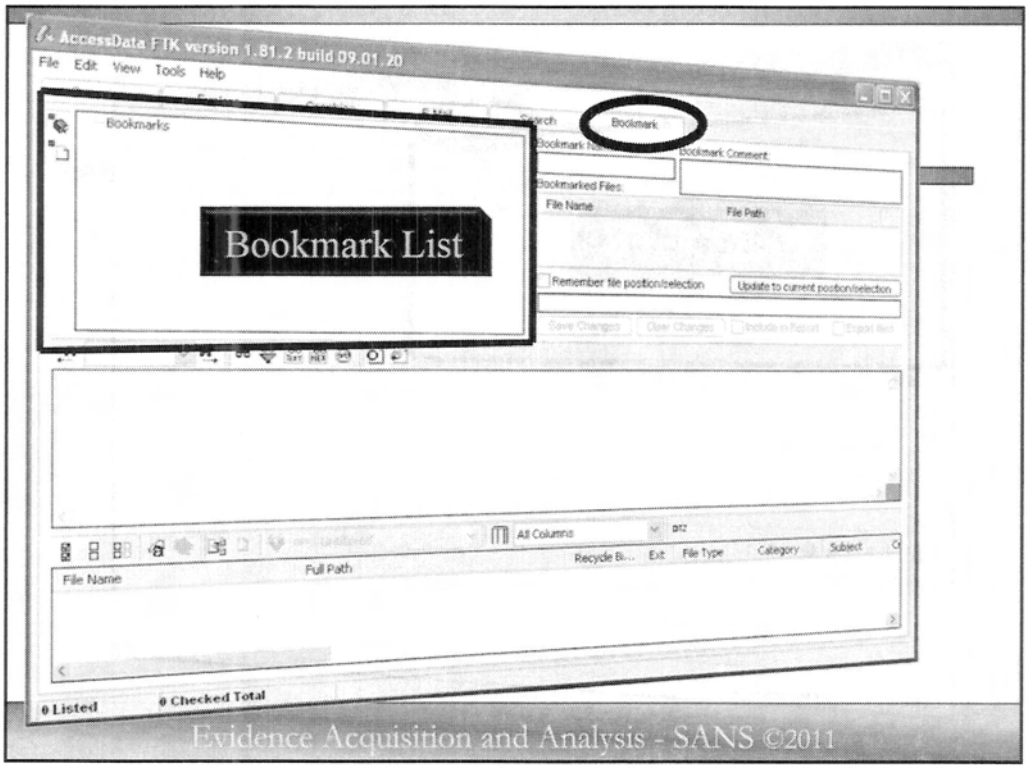
So if you want to examine the mail headers, scroll down to the bottom of the e-mail and here are all the mail headers. From here you can attempt to determine where the e-mail came from, the originating IP address, if possibly it was spoofed, etc. If you print this file, you will get the HTML version of the e-mail, and below the e-mail it will print the full mail headers.



The Search tab.

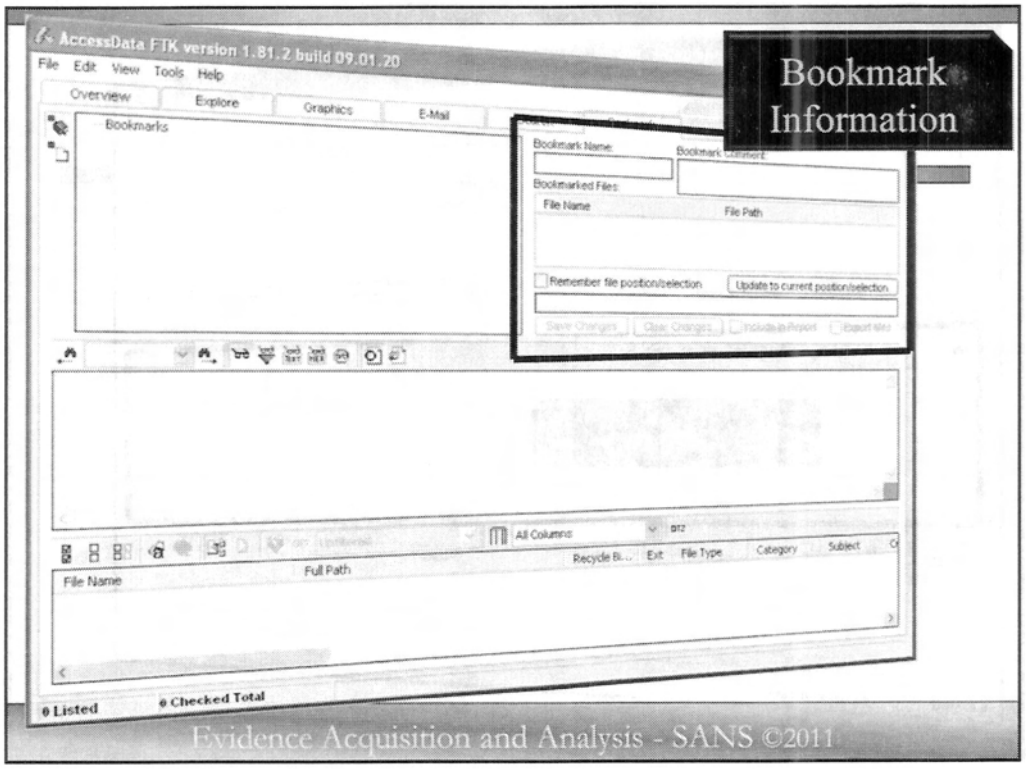
The Search tab is where the real magic happens in FTK. FTK uses the dtSearch technology to index everything up front and subsequently all indexed searches are virtually instant.

You should note that FTK does not index EVERYTHING – It cannot index binary, so essentially what it does is go through the media and finds all the ASCII strings and indexes them.



Now let's take a look at the Bookmark tab. As you might imagine, this is where you can store and manage all your bookmarks.

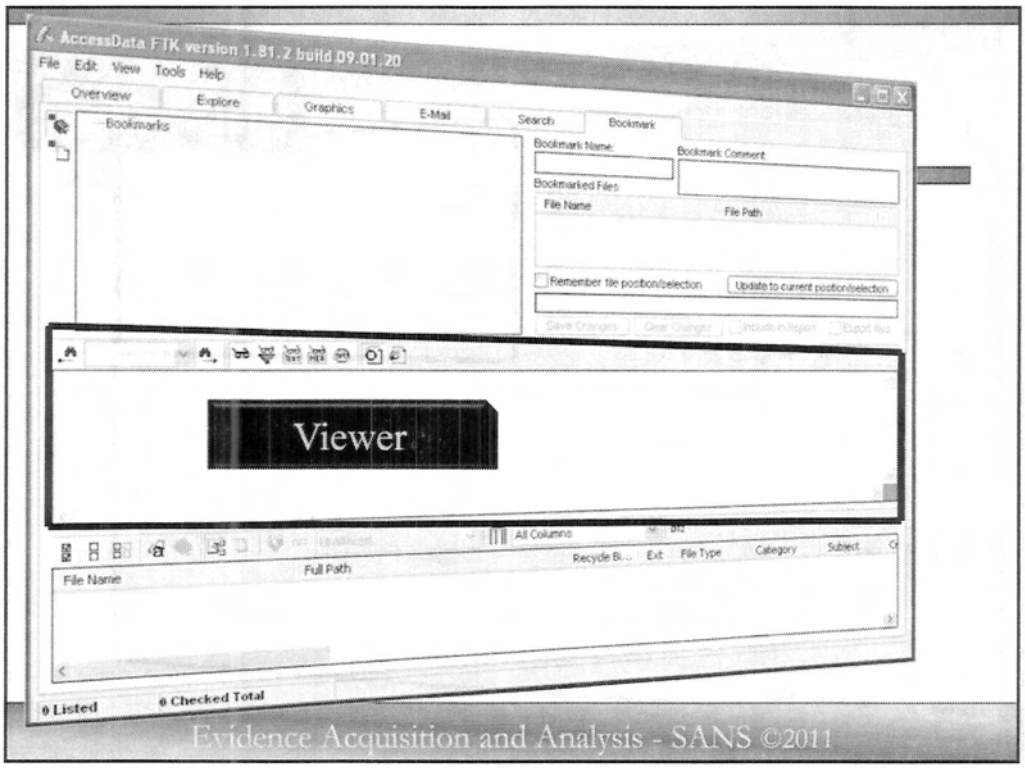
In the top left corner you will see the "**Bookmark List**". By clicking on any of the bookmarks in this list you will see the associated files for that bookmark. To get a better look at each of the files inside a bookmark, click on the plus (+) symbol next to the bookmark. By clicking on any of the files inside the bookmark you will see all the information in the adjacent windows. We will now look to the right and look at the Bookmark information window.



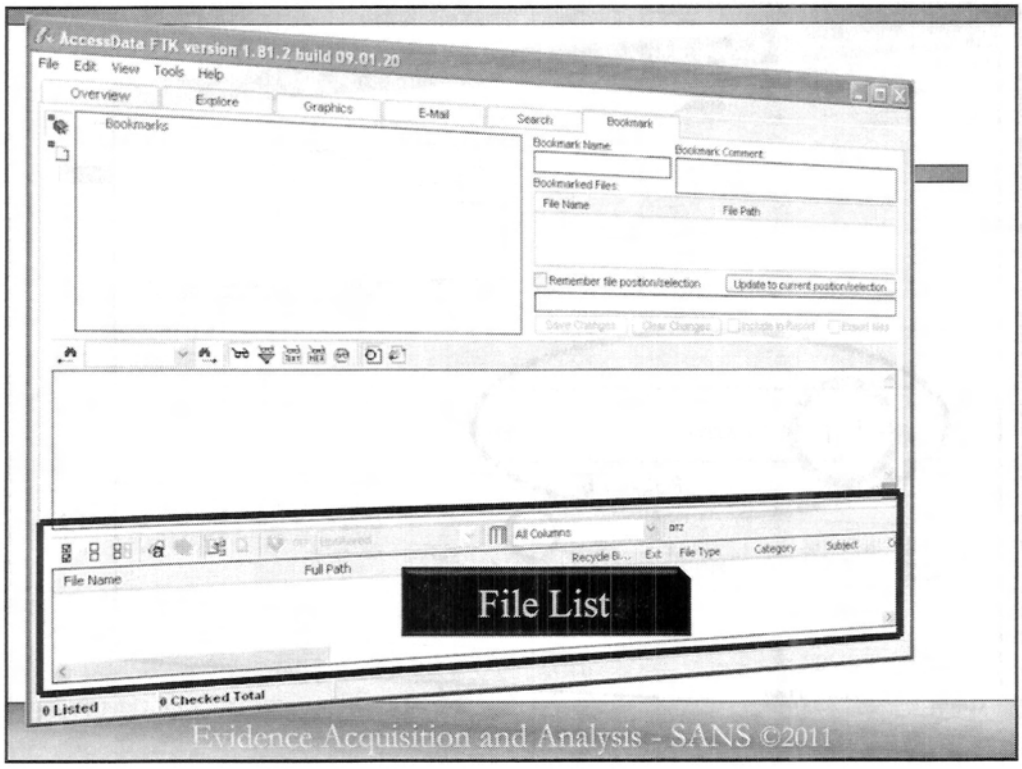
At the top right, is the "**Bookmark Information**" window. When you click on a bookmark in the Bookmark list window, the associated information for that bookmark is displayed here. You can also edit your bookmarks here, once created.

One tip I have found to be useful is that after you have finished your examination, before generating a report, rename your bookmarks in the order you want them to appear in your report by preceding the bookmark name with a number (e.g., 01-Secret Documents, 02-Confidential Files Copied, etc.).

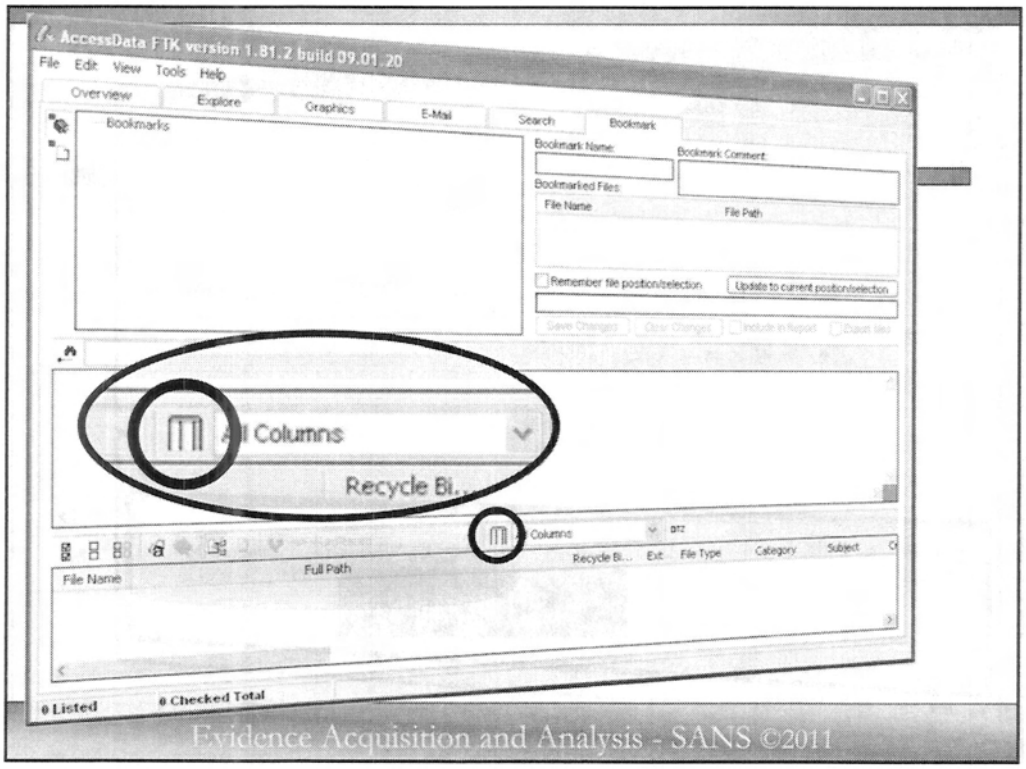
You can also organize your bookmarks according to the elements of the offense you are investigating. For instance, 01-Items stolen, 02-Conspiracy to commit crime, 03-Communication with co-conspirators.



In the middle, you will find the **View** window. This will display the contents of the file you select in the Bookmark List window. This window may help in the event you need to review items inside the already created bookmarks. Just click on each of the files inside the bookmarks and the contents will be displayed here in the Viewer window.



As you click on any of the graphics in the Bookmark List window, the file will also be highlighted in the File List window. As we discussed in previous tabs, it is here that you will look to find where the file is located on the drive, what directory, etc. You will also be able to look here in the File List window to see the MAC times and other interesting details about the selected file.



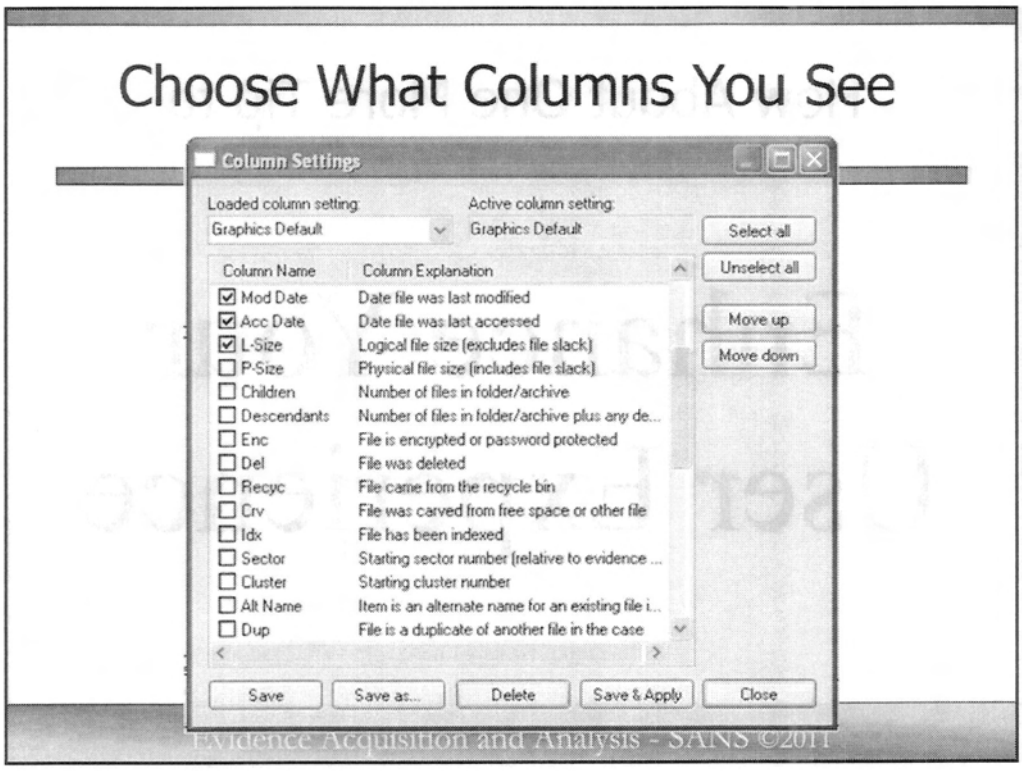
Now because computers have so much data, one of the great challenges of any forensic analyst is being able to display it in a humanly digestible manner, not only to their customer but to THEMSELVES.

Another helpful hint in organizing your data is to minimize the columns that are displayed in the File List windows of each of the tabs we have just talked about.

If you scroll across from left to right you will see that by default, FTK is displaying 41 columns with different aspects to every file. It shows everything from file extension, MD5, and SHA1 Hash, all MAC times, logical file size, physical file size, and the list goes on.

Do you really need to see all these columns or could you minimize the amount of information you see.

At the top middle of the File List window, you will see a white icon that appears to be paper with columns on it. Click that icon.



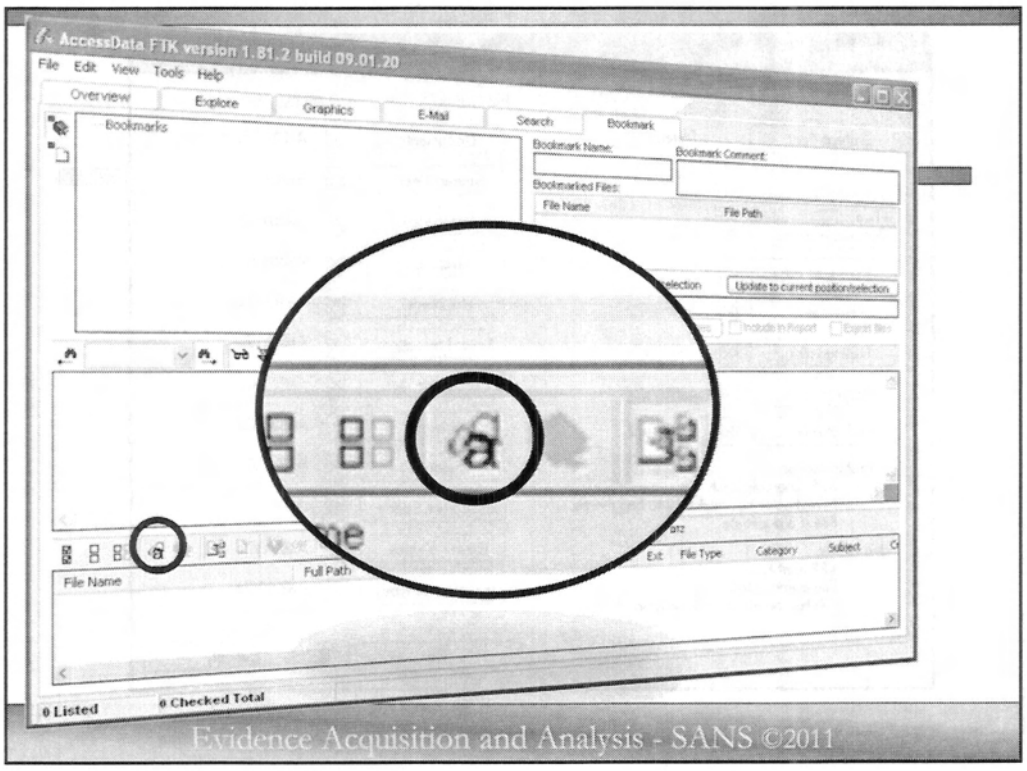
Now you can select what columns you see for that tab. This way, you can see just the information you want without suffering from information overload.

After selecting the columns, select "Save as..." and give your special column setting your own unique name.

You can do this for each of the tabs and each tab can be set to show only the information you want to see in that tabbed view.

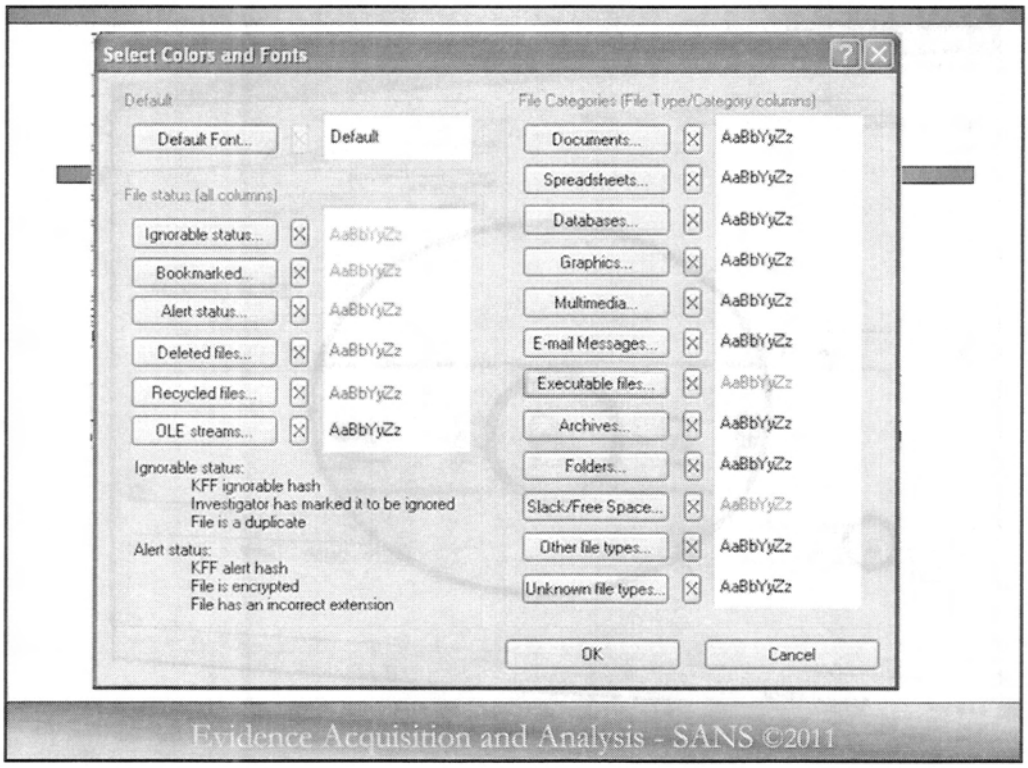
After all, you probably don't want to see To, From, and CC fields in the graphics tab, right?

How about one additional tip to further enhance your Forensic Experience.



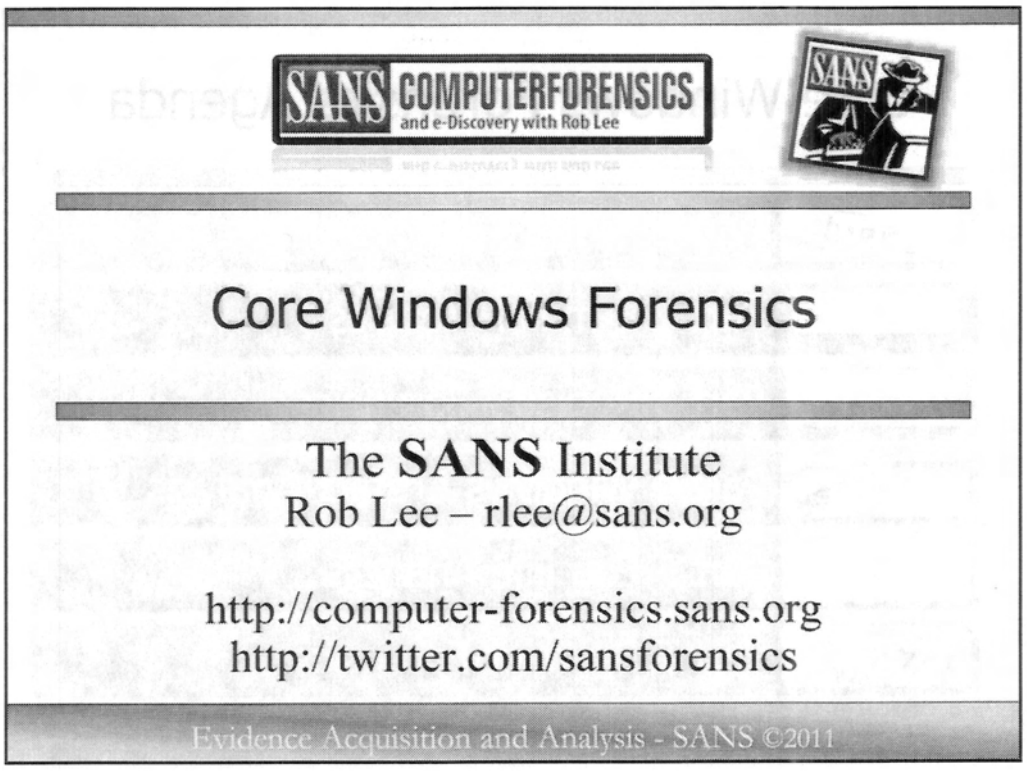
If you look again at the top of any of the File List windows, on the left side you will see three letter "a"'s in red, black and blue.

If you click on those letters, you will bring up a configuration window which will allow you to tailor how FTK displays specific file types.



Here you can color code almost everything in FTK. You can set FTK to display any executable file in GREEN, all deleted files in RED, and all bookmarked items in FUCHSIA.

You can even change the font style. You should consider experimenting with this so you can setup your forensic environment in a way that will allow you to more easily and quickly recognize specific file types. Also, some people have found that certain fonts register in their mind better than others and this is where you can change the display font in FTK. When you finish class today, you might want to tinker around with these settings to see what works best for you.



Welcome to Core Windows forensics.

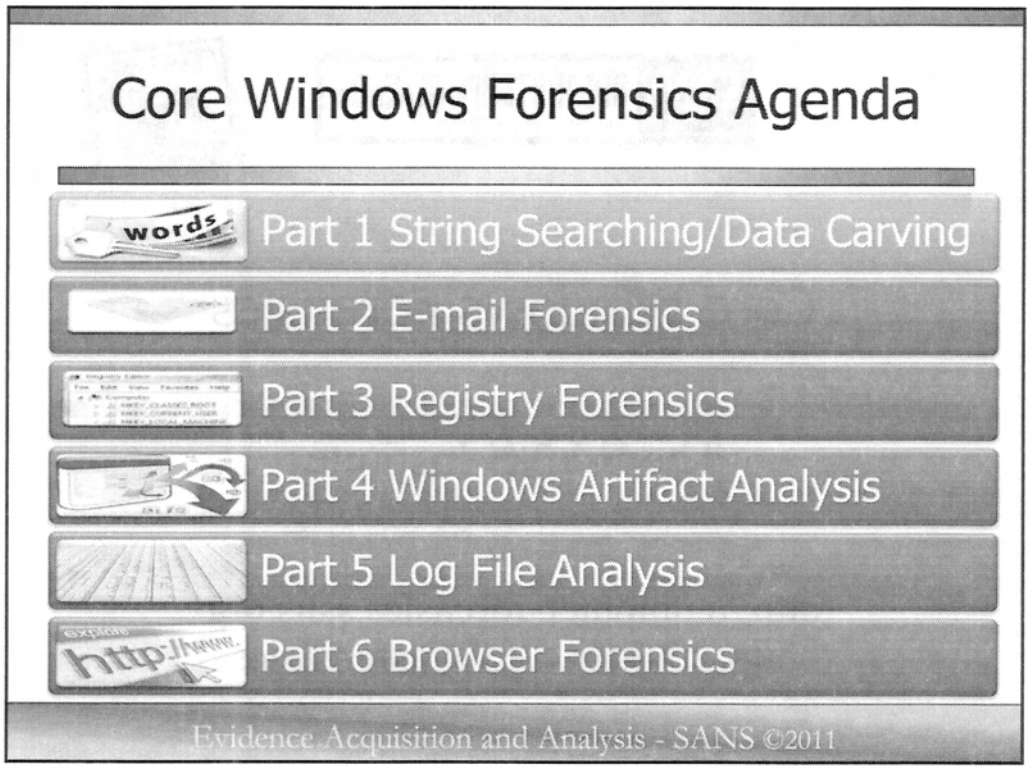
Rob Lee

rlee@sans.org

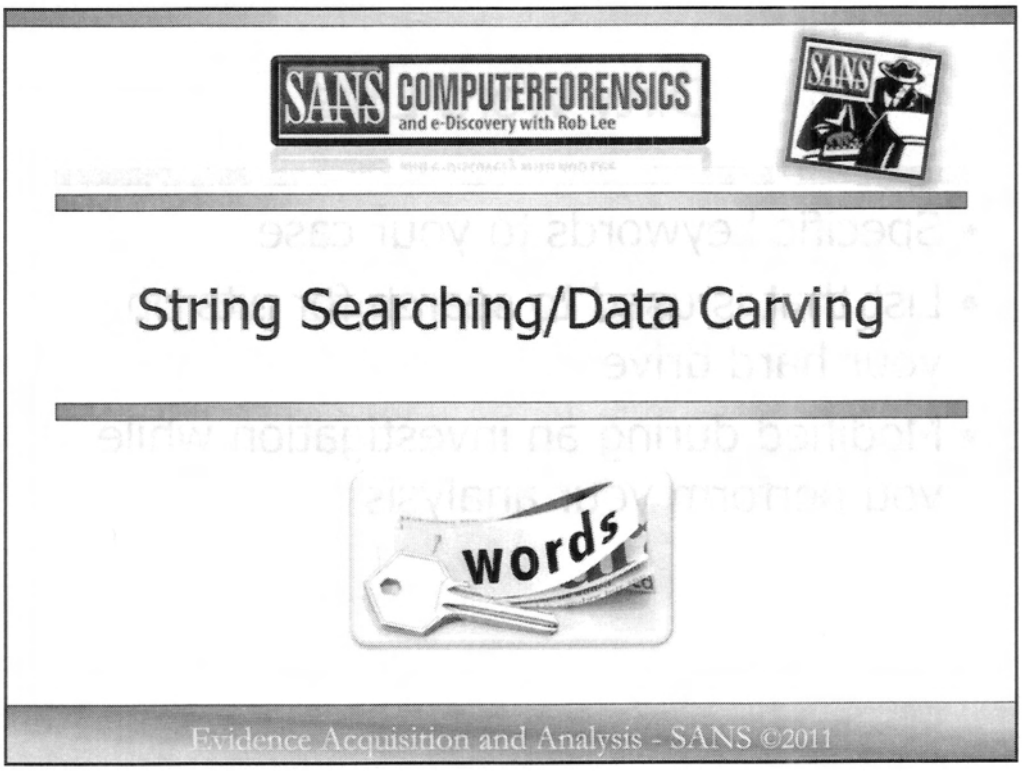
http://twitter.com/robtlee

http://twitter.com/sansforensics

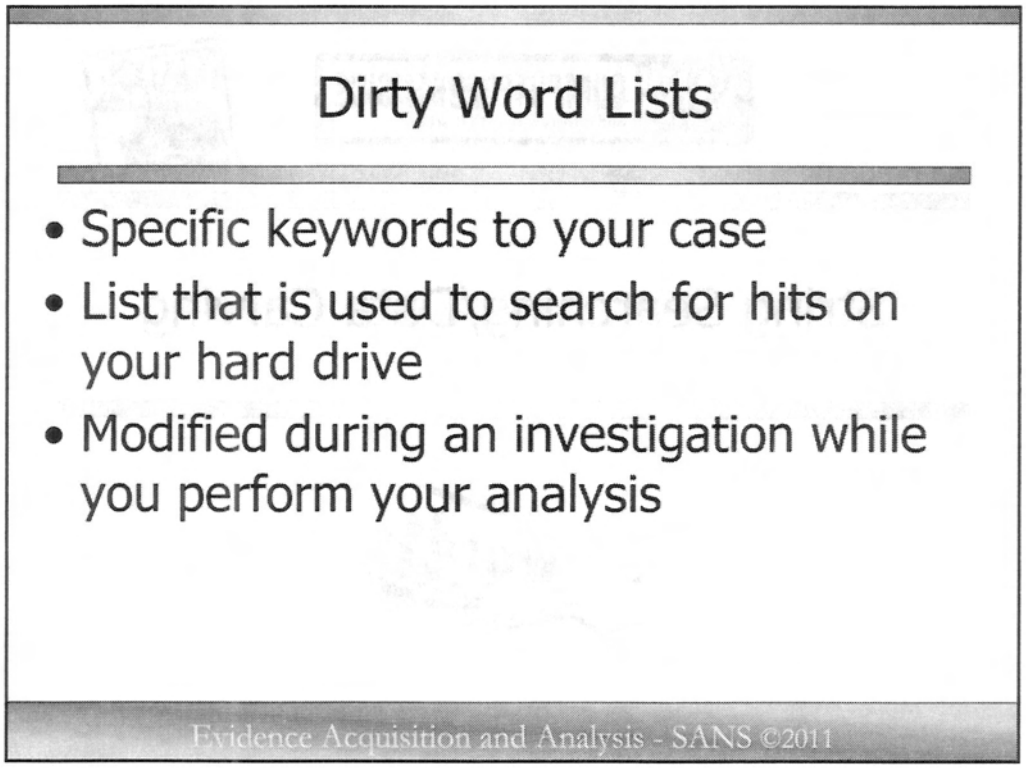
Special thanks to Chad Tilbury for his work on this day in helping create SEC408 Computer Forensics and E-Discovery Essentials in tech review and helping with slides for Browser Forensics and E-mail Forensics.



This page intentionally left blank.

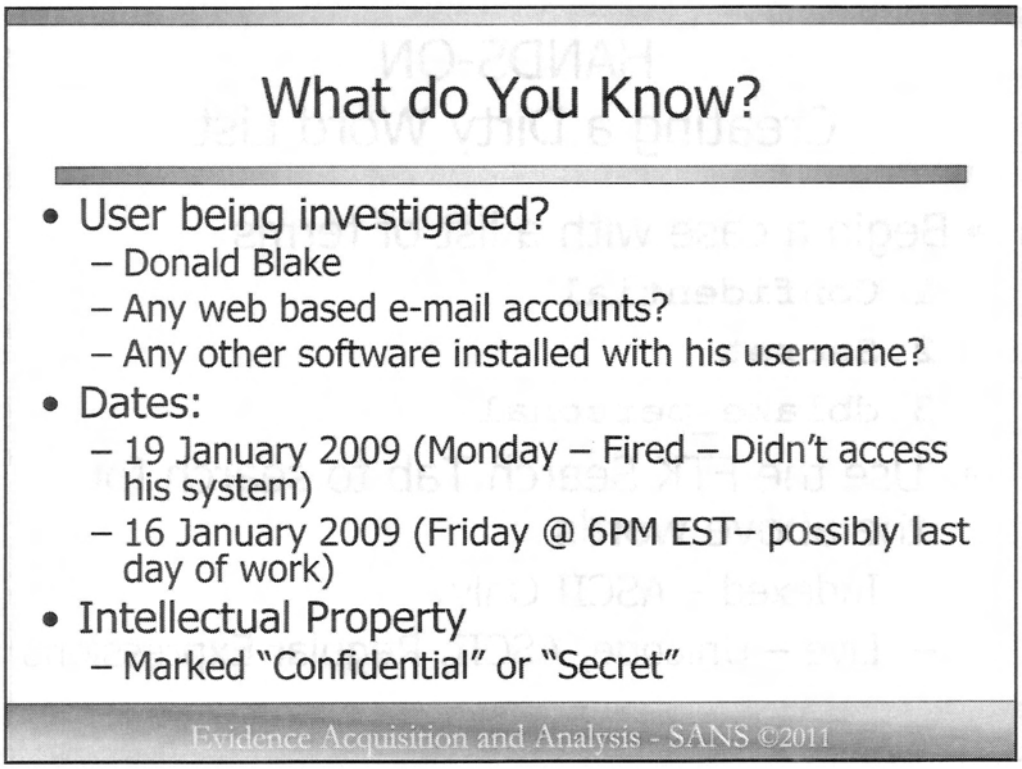


This page intentionally left blank.



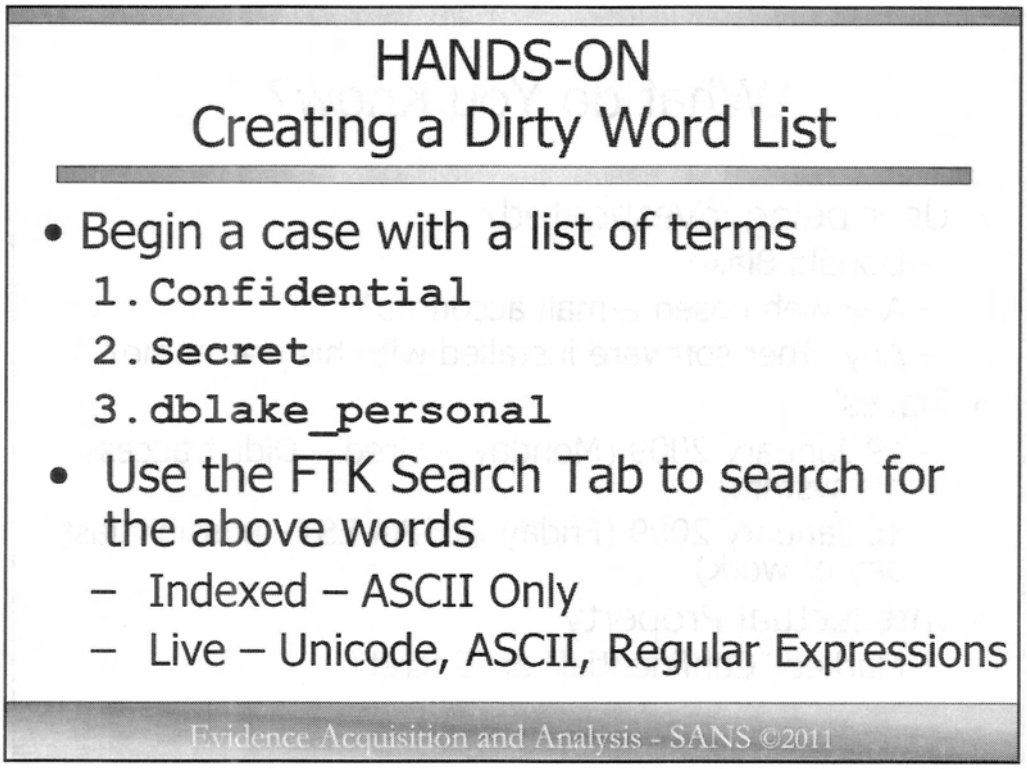
As you perform your investigation, you will begin to discover things that will enable you to find more information. For example, finding an IP address, a hacker handle, and an e-mail address would be items that are case-specific that would help you. In addition to the specific case key words, you could utilize generic key words such as hacker, IRC or Trojan, to perform a low level search on your hard drive or other media, looking for anything in a file that will hit on these key words.

This list of words is called a "Dirty Word List". These lists would be case-specific and invaluable in finding key information in your evidence. During your case, you should always be adding and subtracting keywords to this list.



By collecting some of the basic information from the case background, we can start a good baseline dirty word list. We have a user that we need to investigate his activity. We have dates/times associated with Donald Blake's last use of the system.

Donald Blake was fired on the 19th of January 2009. He did not access the system the day that he was fired. The last time that he was seen in his office was on January 16, 2009, around six in the evening. Donald Blake is under investigation for potentially stealing intellectual property. At Asgard Inc., most proprietary documents are marked with the words "confidential" or "secret".



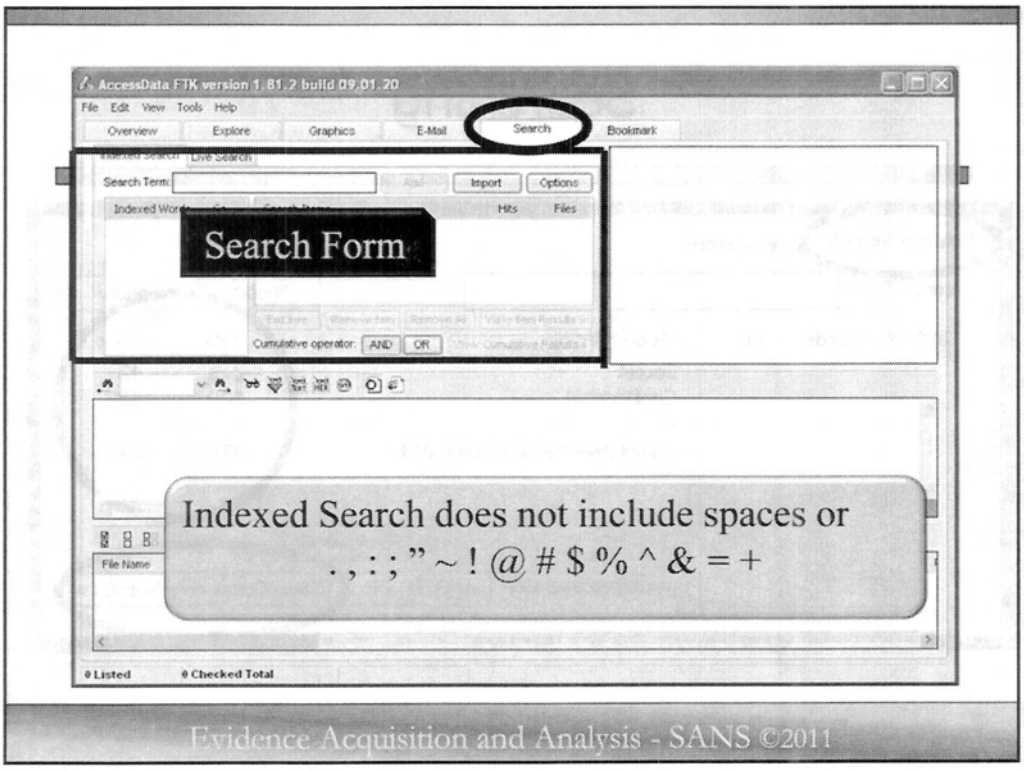
Let us first start by creating a dirty word list. We need to ask several questions.

The items in your list based on the case background should include: confidential, secret, and dblake_personal.

1. Which confidential or secret documents existed on this machine?
2. Did Donald Blake send any documents from his machine to another location?

You can perform searches in FTK utilizing two methods, indexed searching or live.

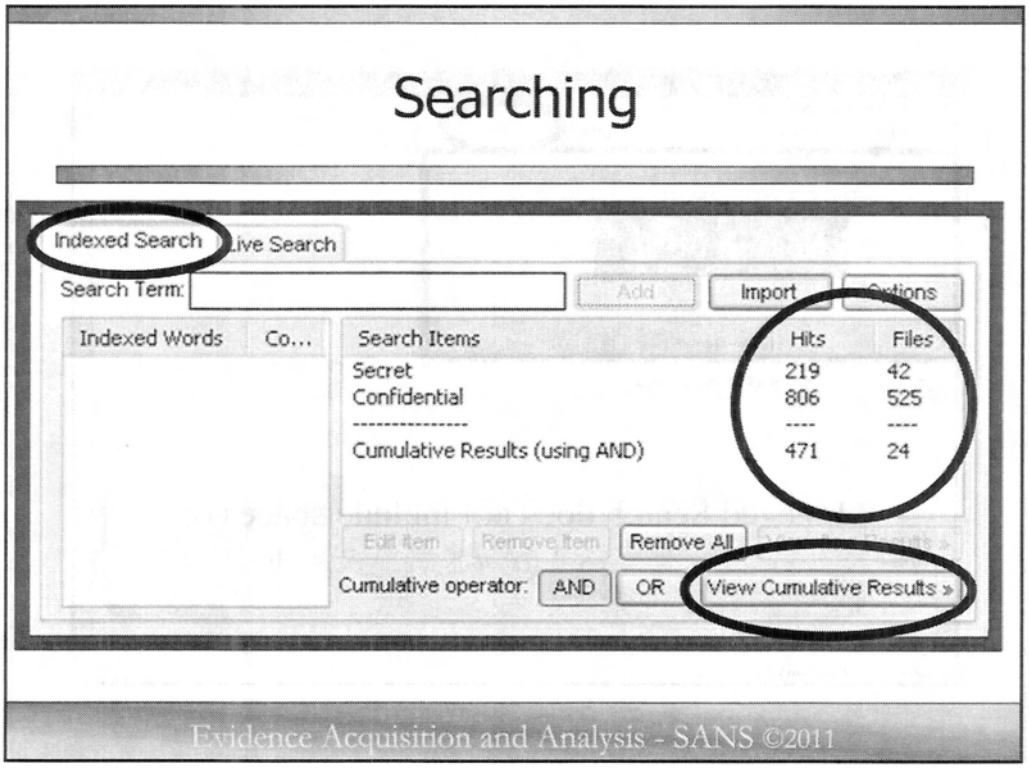
Indexed searching is an extremely fast way to identify data that contain the ASCII search strings you will input. The Live Searching will allow you to perform unicode, ASCII, or regular expressions searches. The latter is more inclusive since many files on Microsoft based operating systems will include unicode characters.



Click on the Search tab.

When you look at the search form you notice there are two types of searches that you can do in FTK.

The first and most common type of search is the "Indexed Search". This is where you are searching the media that was indexed in the pre-processing of FTK. The indexed search will search all discrete words or number strings found in both allocated and unallocated space. It does not capture spaces or symbols, including . , : ; " ~ ! @ # $ % ^ & = +



Once you have clicked on the Search tab, select the Indexed Search tab, then click inside the Search Term field.

Conduct a search for each of the three search terms: confidential, secret, and dblake_personal. You can get creative by seeing if the results can be paired down even more by including the "AND" operator to search for more than one term in a single file.

As you type your search word(s) you will see FTK instantly displaying below the number count of words matching what you have already typed. Indexed searches are not case-sensitive.

After typing your word, you then click "**ADD**" to add the word to your search query.
You can then modify that search further by adding additional words, and then adding those to your search.

So here you can see that we started by searching for the word Secret and received 219 hits, or instances of Secret, that were contained inside 42 different files.

By adding the additional word "Confidential", which has 806 hits inside 525 files, we have now reduced our cumulative total hits of files containing BOTH Secret AND Confidential down to 24 files. This is because the Cumulative operator "AND: is selected, if you changed the Cumulative operator to "OR", you would see the Cumulative Results change.

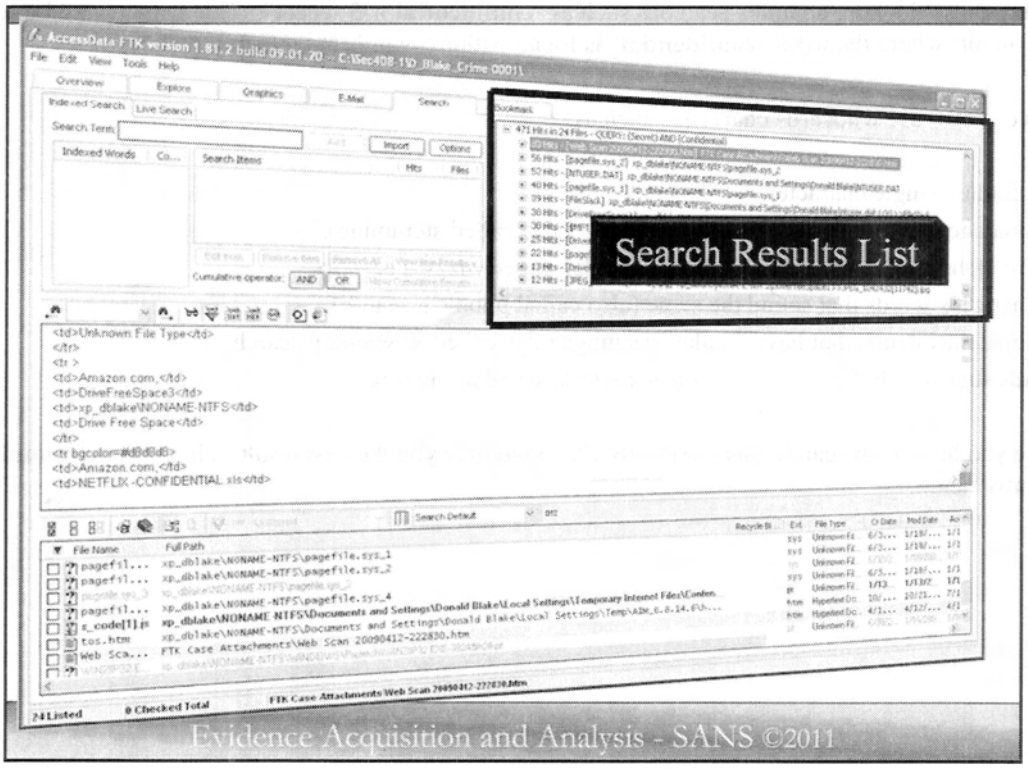
FTK supports Boolean searches consisting of a group of words or phrases linked by connectors such as "AND", "OR", and "NOT".

You can also do more complex searches such as "**confidential w/5 secret**". This search would result only in hits where the word "**confidential**" is found within 5 words of "**secret**".

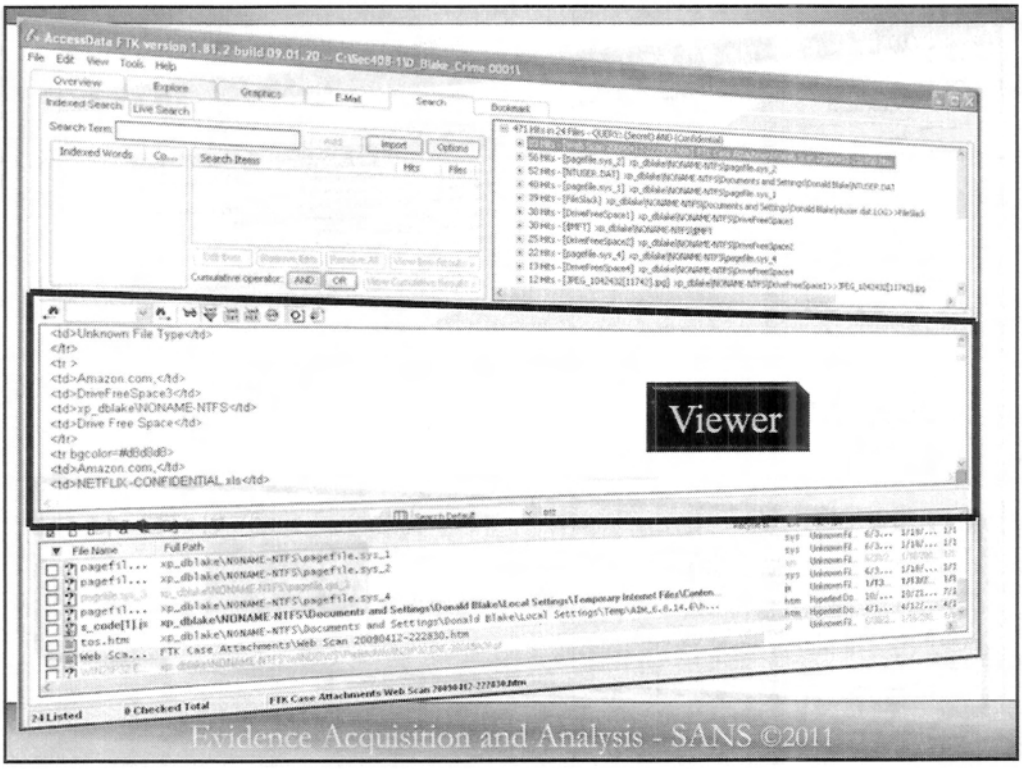
You can also use wildcards characters such as:

"?" for any single character,
"~" matches words that contain the same root (also called stemming),
"%" matches words with similar spellings (also called fuzzy a search),
"#" matches words that sound the same (also called phonic a search),
"&" matches words that have similar meanings (also called a synonym search)
Words such as "the" and "if" are considered noise and are ignored.

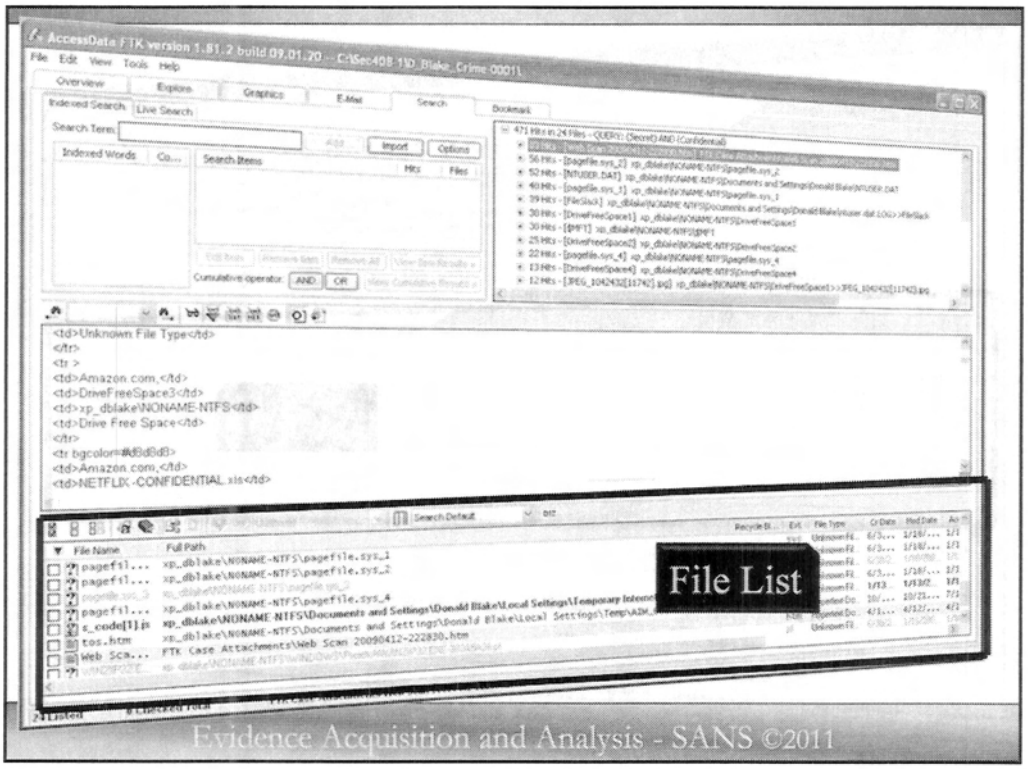
Once you have your search query carefully crafted to give you the best results, click "**View Cumulative Results**" and...



Your results will display in the "**Search Results List**" windows. All your hits are organized in descending order by file. Here you can review all the files, and as you click on each of the files and subsequent hits, the file containing the hit will be displayed with the hit highlighted in the Viewer window.

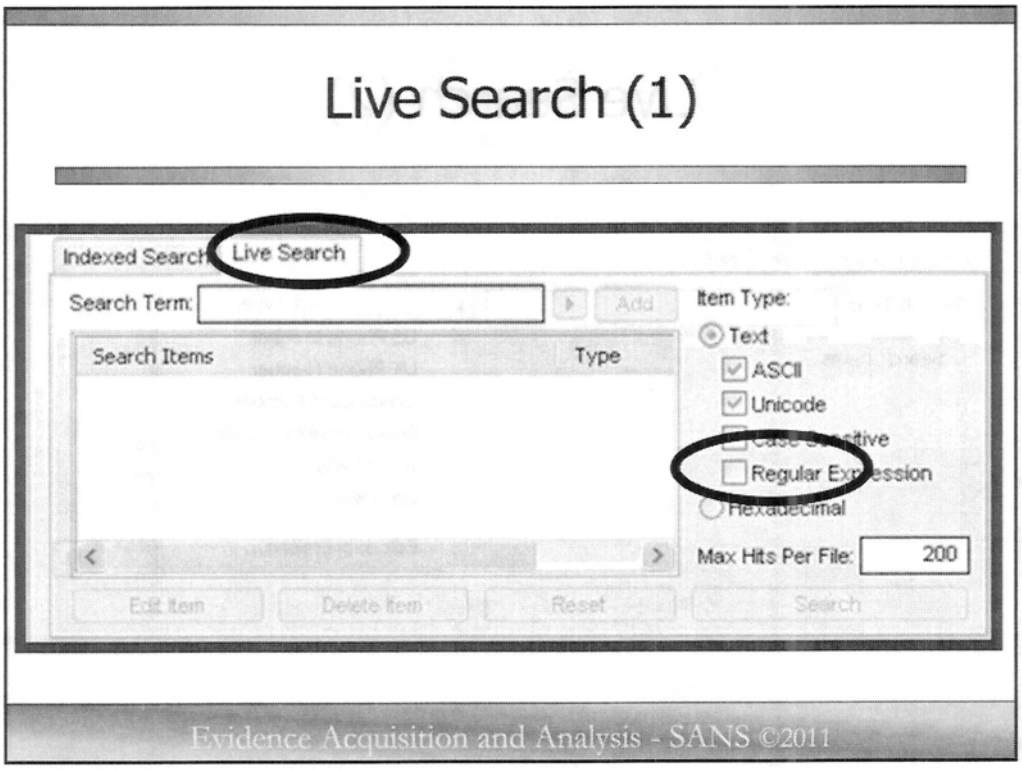


The middle window is where the file containing the hits will be displayed with the hits highlighted in yellow in the Viewer window. You can either navigate through this window to review each of the hits or click each consecutive hit in the Search Result List window. Remember that you will often find multiple hits in a single file. As you click on each hit in the search file results window, the file will move to that location in the viewer window.



Now turning your attention to the very bottom of the FTK application, you will find the **File List** window.

As you click on any of the graphics in the Search Results List window, the file will also be highlighted in the File List window. As we discussed in the previous tabs, it is here that you will find where the file is located on the drive, what directory, etc. You will also be able to look here in the File List window to see the MAC times and other interesting details about the selected file.



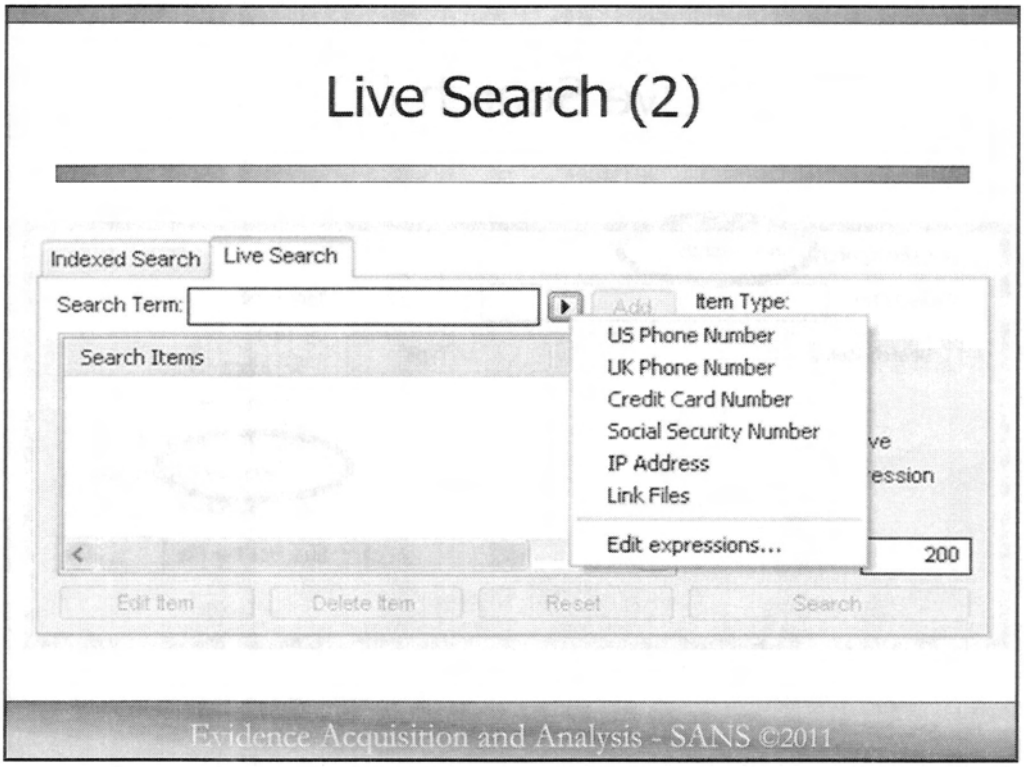
The second way you can do searches in FTK is through the **Live Search** function.

The reason this is important is that as we said earlier, FTK only indexes discrete words or number strings found in both allocated and unallocated space.

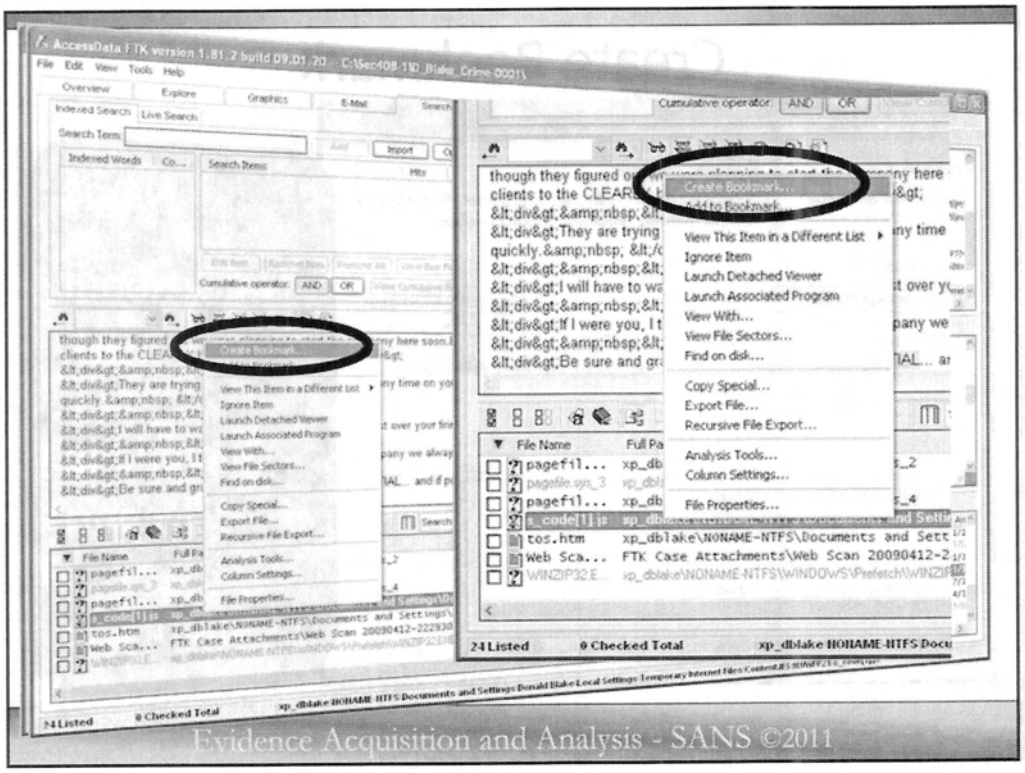
Live Search can be used to search for special characters, case sensitive words, Hexadecimal or Regular Expressions. Live Search should be used judiciously since it is a time intensive process that involves an item-by-item comparison with the search term. One big advantage of Live Search is that it can find patterns of non-alphanumeric characters.

Some regular expressions have already been included in FTK for you. You can find them by first clicking on "**Regular Expression**" then ...

Click on the Arrow to the right of the search dialog box and you will see a drop down menu that you can select from or edit and add your own regular expressions.



Click on the arrow to the right of the search term field and you will see a drop down menu where you can select from, edit, and add your own regular expressions.

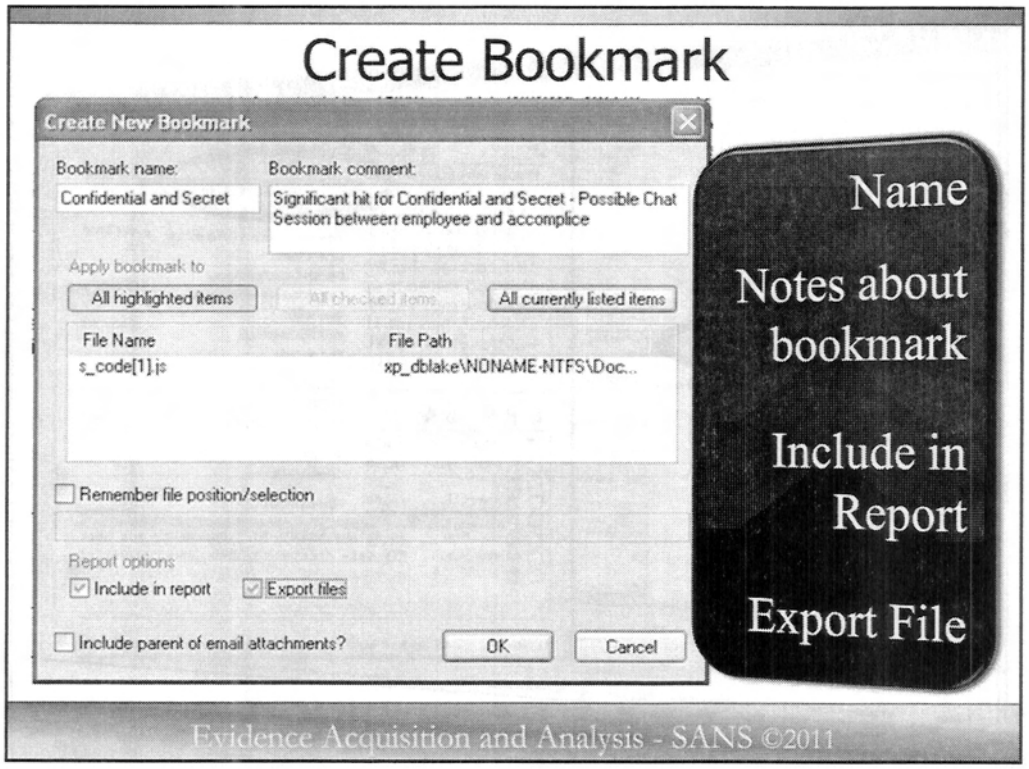


Now before we go to the Bookmark tab, let's first go over how to create a bookmark. There are two primary ways to create bookmarks.

Let's first go over creating a bookmark of a single file.

While reviewing any evidence, you can create a bookmark by RIGHT clicking on any file in any of the File List windows.

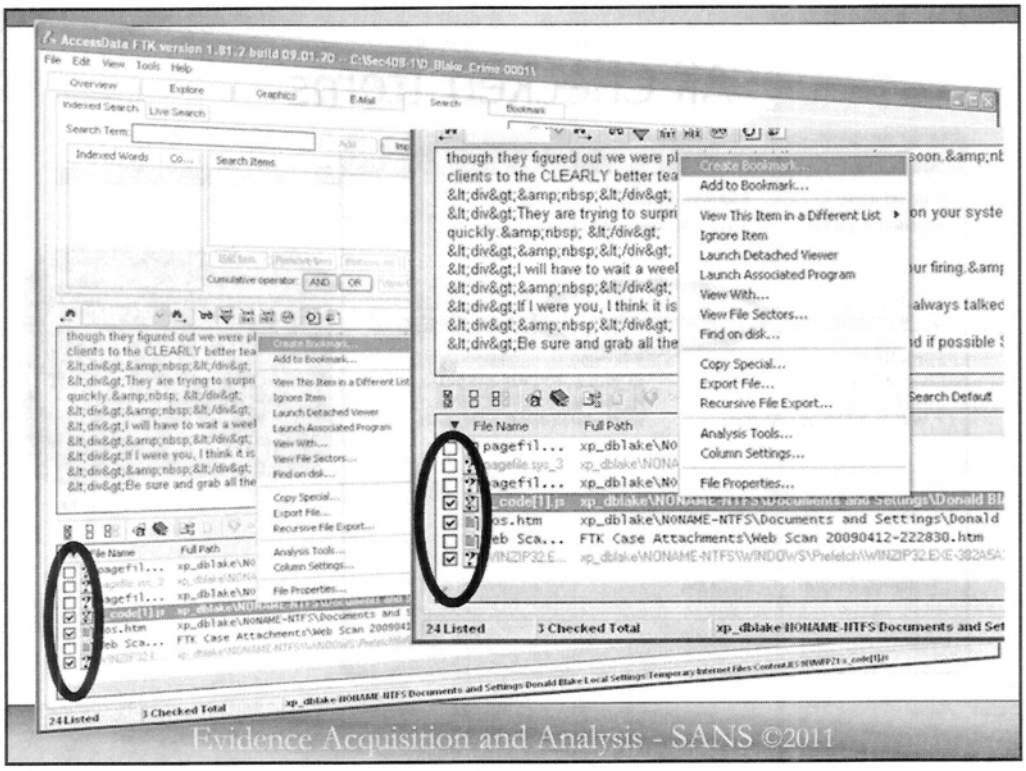
This will bring up a dialog box that will allow you to select "**Create Bookmark...**"



Now you receive the **Create New Bookmark** dialog box where you will give your bookmark a name. You also have a comment box to make notes about what the file is or why you think this item is significant.

CAUTION: Do not put anything in here that you would not want to explain in court. These comments will also be exported to the FTK automated report.

You can then choose to include this bookmark in your report, and you have an option to export the file.

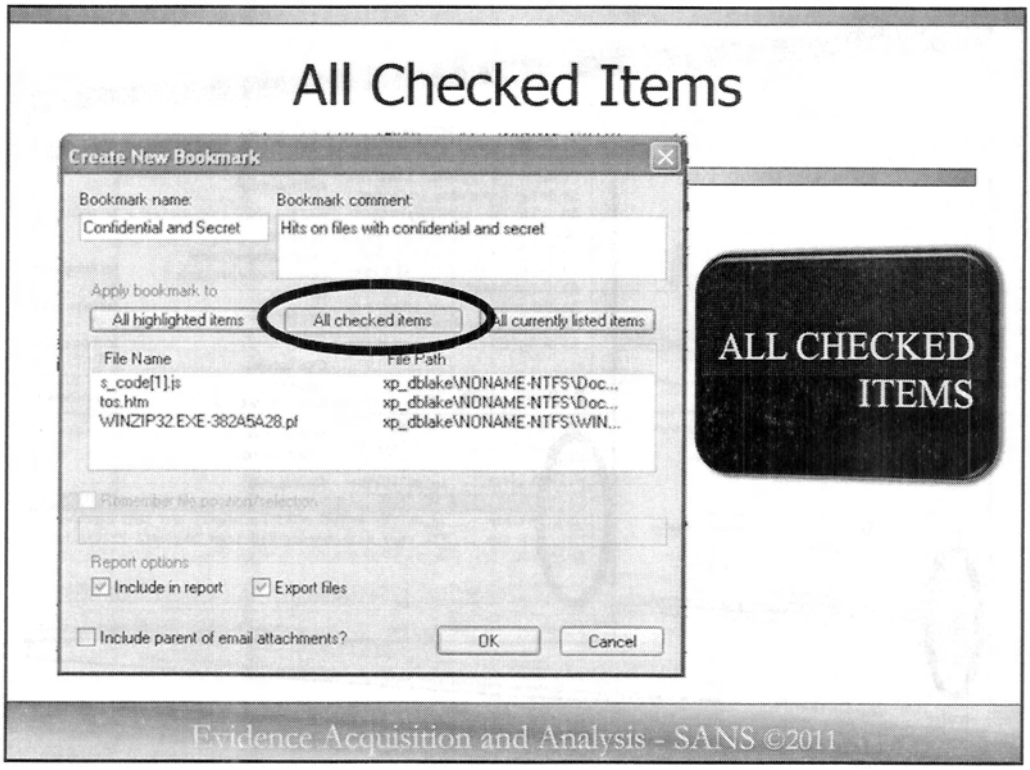


Now, I told you there are two ways to create bookmarks. The first way was for a single file where we right clicked on that file and selected "Create Bookmark…". What if there are multiple files you want to bookmark, all at one time. It is quite easy to do in FTK.

There are actually two ways to bookmark multiple files – by highlighting multiple files the same way you would in any Windows program (by holding down the shift or control key while selecting files), OR you can CHECKMARK them in FTK.

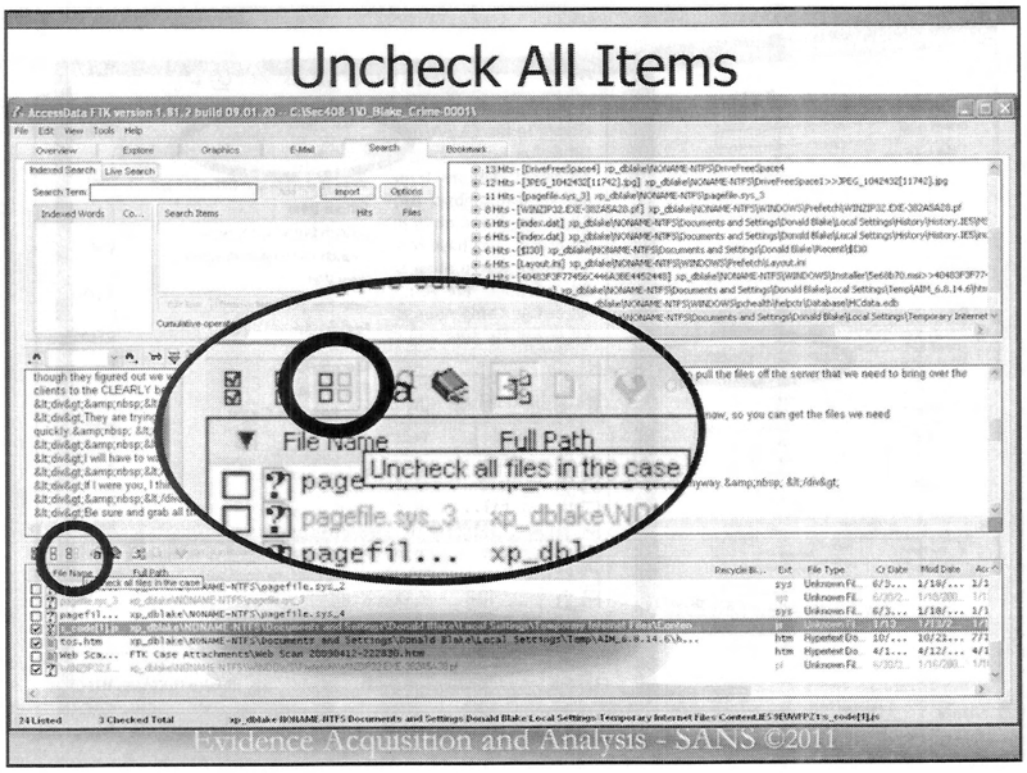
To the Left of every file in the File Viewer window is a box. By clicking in that box you place a check mark in the box.

Here I have checked three files. This time when I right click on any of these files and select "Create Bookmark", we will be bookmarking all three files, into the same bookmark.



This time, select the middle button to create your bookmark with "**All Checked Items**" Or "**All Highlighted Items**".

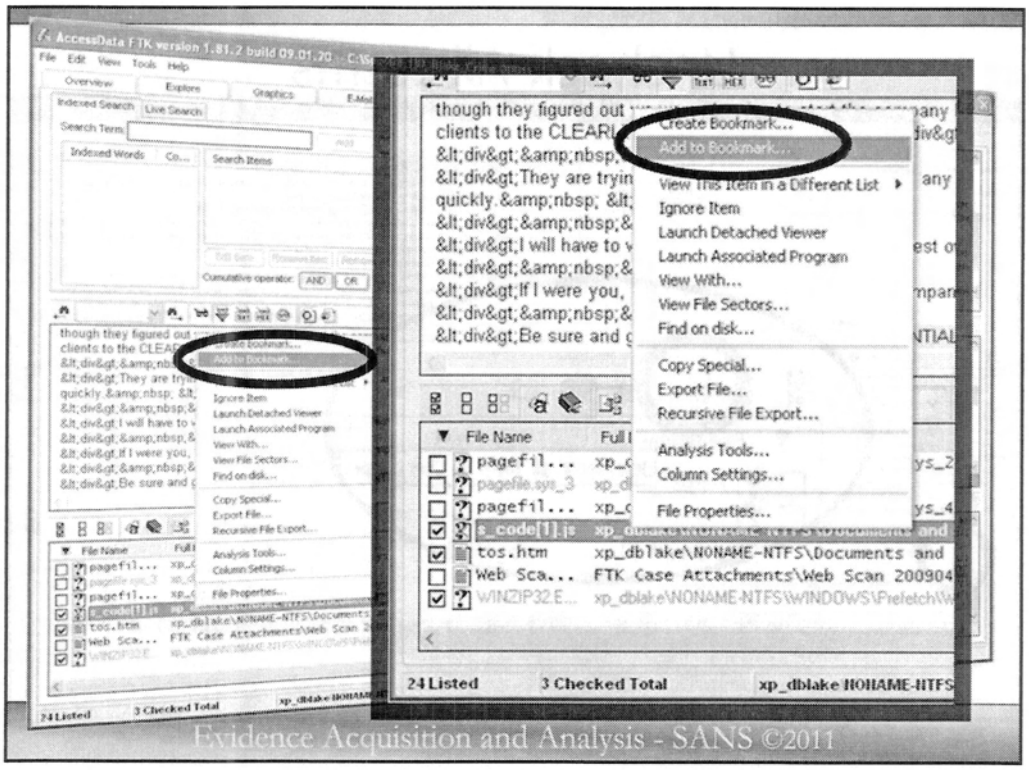
This is an area where mistakes can easily be made, so always be careful and review the files listed in the middle window to make sure the files you wanted are actually listed.



One thing to remember is that if you use the check box method, after each bookmark you probably want to reset or erase ALL your checked items. There is an easy way to do this.

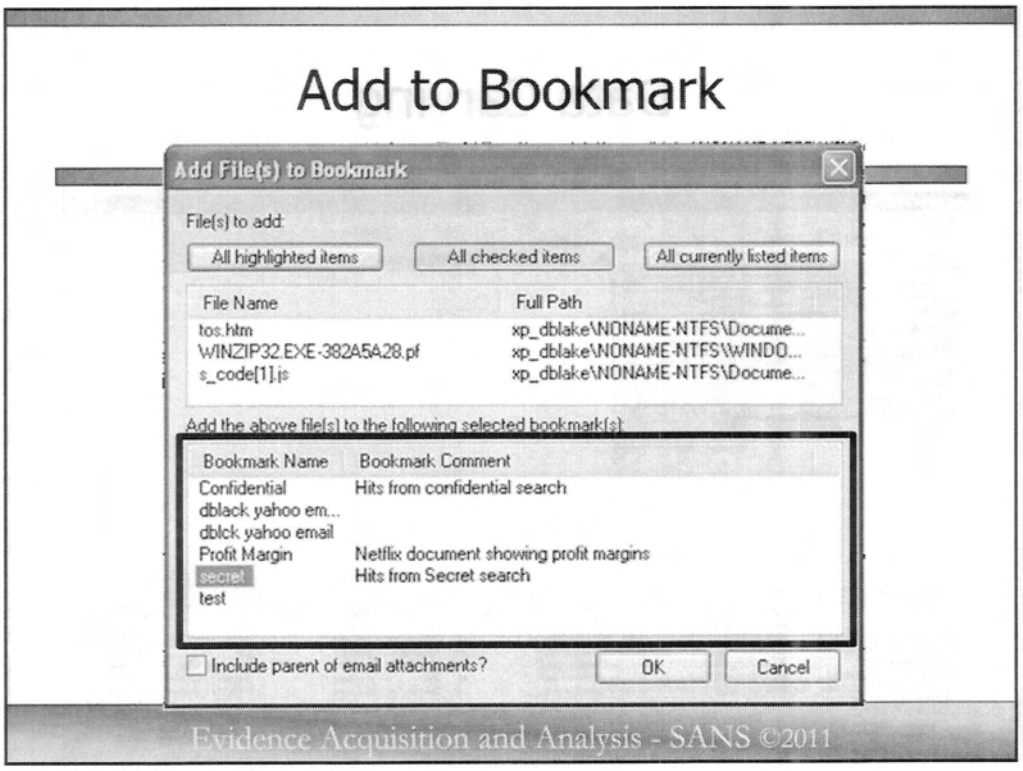
At the bottom left of FTK, above the File List window, you will see what looks like four empty boxes, two black and two gray. Click this and it will UNCHECK ALL ITEMS IN THE CASE.

Now you are reset to start making new checkmarks for a new bookmark.



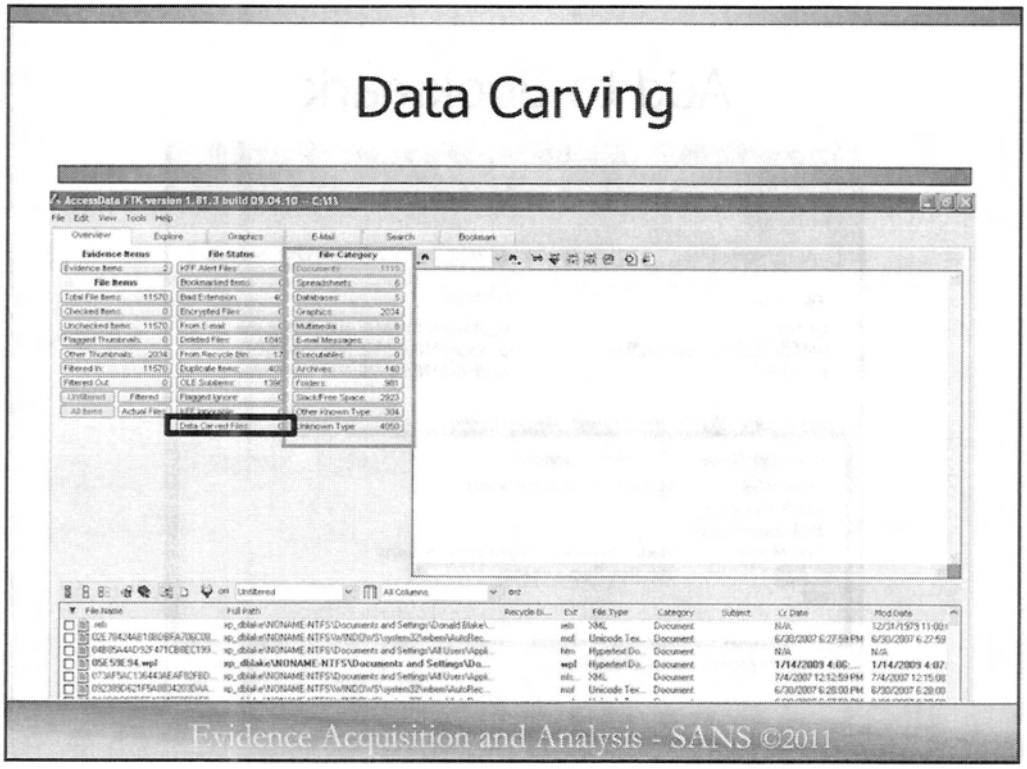
Now while we are talking about bookmarks, there is one additional feature I would like to show you.

What if you have created bookmarks for secret items, then you find another file or image that you would like to add to a previously created bookmark. It is almost the same technique as creating a new bookmark, but instead of right clicking and selecting "Create Bookmark", this time, right click and select "**Add to Bookmark**".



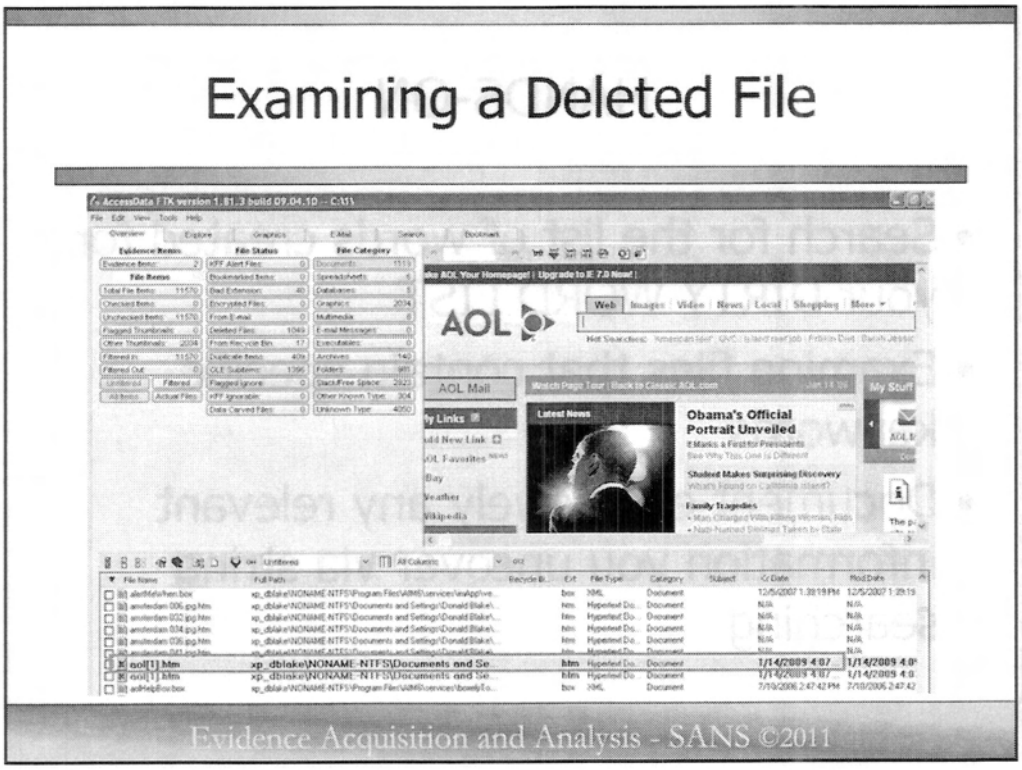
At the bottom of the "Add File(s) to Bookmark" dialog box, you will see all the already created bookmarks you have in your case. Just select the already created bookmark you want to add the newly bookmarked files to and then click OK. Once you click OK the file(s) selected will be added to that bookmark.

This will come in very handy as you analyze your evidence.



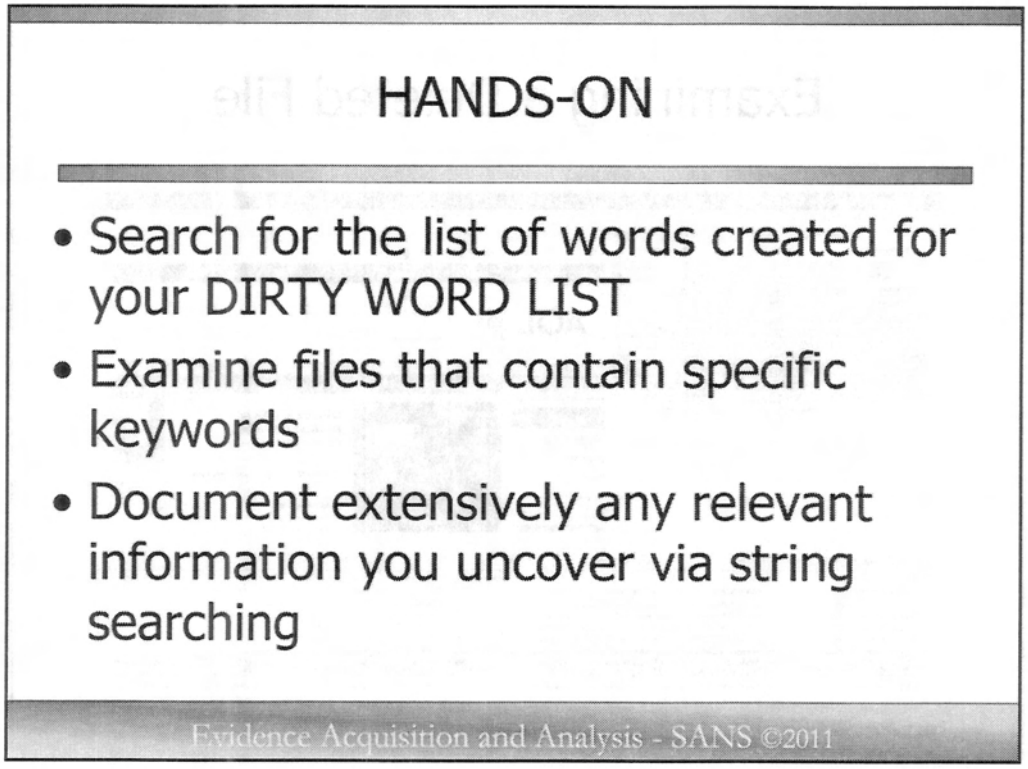
Above in red you can see the File Category location inside of FTK. This is where you will be able to examine both existing and deleted data of the specific document type. Once you click on the type of file you are looking for, the Viewer window below will list all of the files case wide that match that criteria.

Using FTK to perform data sorting such as this can save time in many cases. For example, in inappropriate use of the Internet cases, you will be able to look at the graphics files and see if the user went anywhere that was objectionable fairly quickly.

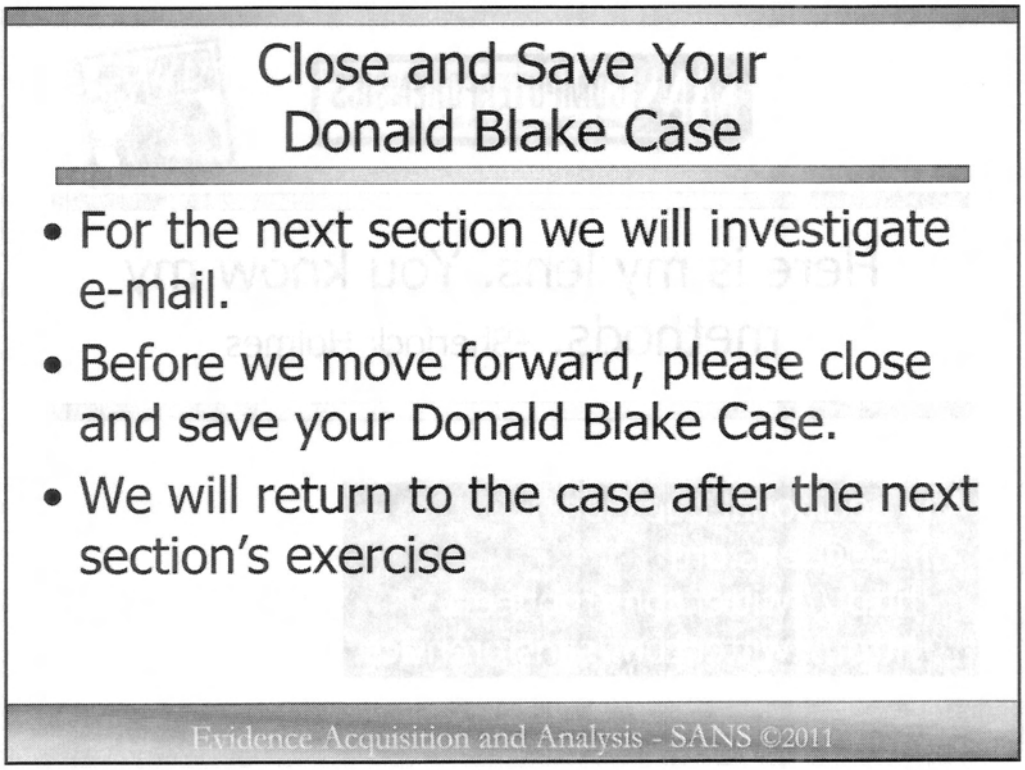


This is an example of utilizing the framework of FTK to view a deleted file. The deleted files are marked in red in your version of FTK. It makes them easier to spot. In this case you can see the page that was viewed by Donald Blake on January 14, 2009. It is an AOL home page with news on it.

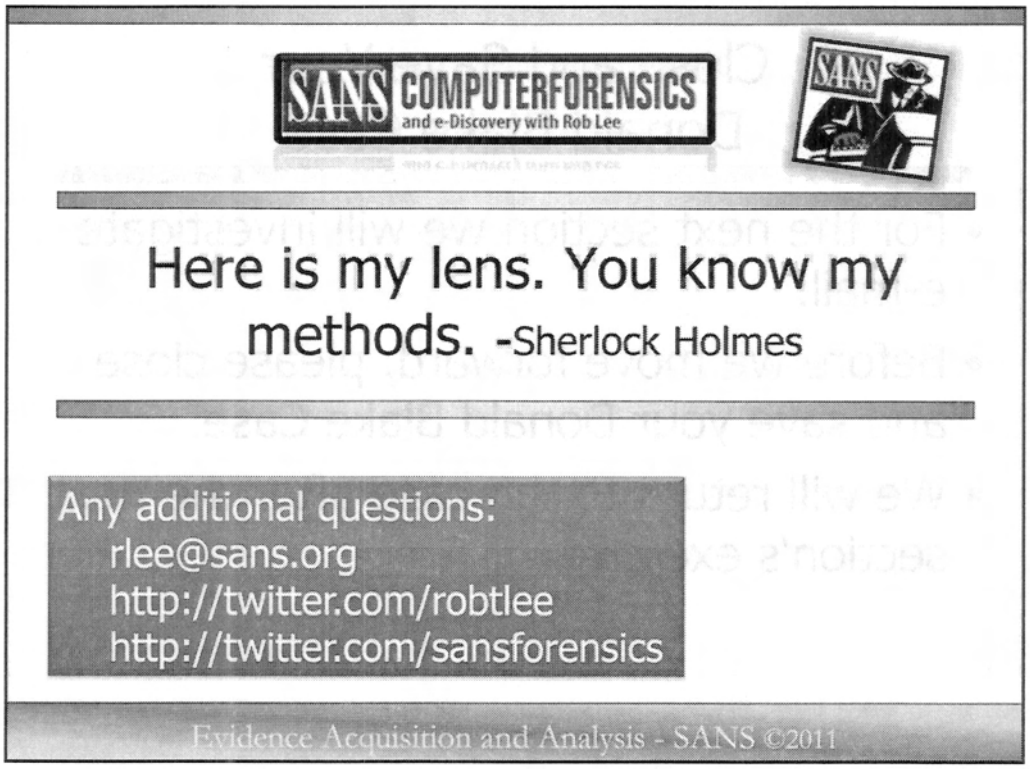
Spend some time here looking for deleted files that have been carved out of the file system or that have been categorized for you automatically. Pay special attention to files that have been marked confidential or secret. Also pay special attention to any files that might have been created on the last day of work for Donald Blake.



This page intentionally left blank.



This page intentionally left blank.



This page intentionally left blank.

ABOUT SANS

SANS is the most trusted and by far the largest source for information security training and certification in the world. It also develops, maintains, and makes available at no cost the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system – the Internet Storm Center. The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world. A range of individuals from auditors and network administrators to chief information security officers are sharing the lessons they learn and are jointly finding solutions to the challenges they face. At the heart of SANS are the many security practitioners in varied global organizations from corporations to universities working together to help the entire information security community. SANS provides intensive, immersion training designed to help you and your staff master the practical steps necessary for defending systems and networks against the most dangerous threats – the ones being actively exploited. This training is full of important and immediately useful techniques that you can put to work as soon as you return to your office. Courses were developed through a consensus process involving hundreds of administrators, security managers, and information security professionals, and they address both security fundamentals and awareness and the in-depth technical aspects of the most crucial areas of IT security. **www.sans.org**

IN-DEPTH EDUCATION AND CERTIFICATION

During the past year, more than 17,000 security, networking, and system administration professionals attended multi-day, in-depth training by the world's top security practitioners and teachers. Next year, SANS programs will educate thousands more security professionals in the US and internationally.

Earn your Master of Science Degree in Information Security from the SANS Technology Institute (STI)

SANS Technology Institute offers two postgraduate degrees to help you solidify your knowledge and further your career. **www.sans.edu**

Global Information Assurance Certification (GIAC)

GIAC was founded in 1999 with a mission to validate the real-world skills of IT security professionals. GIAC's purpose is to provide assurance that a certified individual has practical awareness, knowledge, and skills in key areas of computer, network, and software security. GIAC currently offers certifications for more than 15 job-specific areas reflecting the current state of information security and includes five ANSI accredited certifications in key areas such as Incident Handling, Forensics, Leadership, Essential Security Knowledge, and Intrusion Analysis. GIAC is unique in measuring specific knowledge areas instead of general purpose information security knowledge. Over 34,000 students have obtained GIAC certifications with hundreds more in the process of doing so. Get the most out of your training with the GIAC certification process! Find out more at **www.giac.org**.

SANS BREAKS THE NEWS

SANS NewsBites is a semi-weekly, high-level executive summary of the most important news articles that have been published on computer security during the last week. Each news item is very briefly summarized and includes a reference on the Web for detailed information, if possible. **www.sans.org/newsletters/newsbites**

@RISK: The Consensus Security Alert is a weekly report summarizing the vulnerabilities that matter most and steps for protection. **www.sans.org/newsletters/risk**

Ouch! is the first consensus monthly security awareness report for end users. It shows what to look for and how to avoid phishing and other scams plus viruses and other malware using the latest attacks as examples. **www.sans.org/newsletters/ouch**

The Internet Storm Center (ISC) was created in 2001 following the successful detection, analysis, and widespread warning of the Li0n worm. Today, the ISC provides a free analysis and warning service to thousands of Internet users and organizations and is actively working with Internet Service Providers to fight back against the most malicious attackers. **http://isc.sans.org**

TRAINING WITHOUT TRAVEL ALTERNATIVES

Nothing beats the experience of attending a live SANS training event with incomparable instructors and guest speakers, vendor solutions expos, and myriad networking opportunities. Sometimes though, travel costs and a week away from the office are just not feasible. When limited time and/or budget keeps you or your co-workers grounded, you can still get great SANS training close to home.

SANS OnSite *Your Location – Your Schedule*

With SANS OnSite program you can bring a unique combination of high-quality and world-recognized instructors to train your professionals at your location and realize significant savings.

Six reasons to consider SANS OnSite:

1. Enjoy the same great certified SANS instructors and unparalleled courseware
2. Flexible scheduling – conduct the training when it is convenient for you
3. Focus on internal security issues during class and find solutions
4. Keep staff close to home
5. Realize significant savings on travel expenses
6. Enable dispersed workforce to interact with one another in one place

DoD or DoD contractors working to meet the stringent requirements of DoD-Directive 8570? SANS OnSite is the best way to help you achieve your training and certification objectives. **www.sans.org/onsite**

SANS Simulcast now available for OnSite classes

Now broadcast your OnSite classes to multiple locations using the Simulcast feature. Perfect for distributed workforces. Learn more at www.sans.org/simulcast.

SANS OnDemand *Online Security Training & Assessments*

When you want access to SANS' high-quality training 'anytime, anywhere', choose our advanced online delivery method! OnDemand is designed to provide a very convenient, comprehensive, and highly effective means for information security professionals to receive the same intensive, immersion training that SANS is famous for. Students will receive:

- Up to four months of access to online training
- Integrated lectures by SANS top-rated instructors
- Assessments to reinforce your knowledge throughout the course
- Hard copy of course books
- Access to our SANS Virtual Mentor
- Labs and hands-on exercises
- Progress reports

www.sans.org/ondemand

SANS vLive! *Live Online Training with Top SANS Instructors*

Do you like the idea of online training but want to interact with SANS' world-class instructors? Then vLive! is for you. vLive! uses cutting-edge Webcast and collaboration technology to deliver a live classroom experience directly to your desktop. Let SANS' top instructors train you in the comfort of your own home or office... on vLive! **www.sans.org/vlive**

For additional training options, visit www.sans.org/security-training/delivery.php

For group programs, please contact us at groupsales@sans.org