



SANS

www.sans.org

FORENSICS 408

COMPUTER FORENSIC
INVESTIGATIONS —
WINDOWS IN-DEPTH

408.1

Windows Digital Forensics and Advanced Data Triage

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

Copyright © 2014, The SANS Institute. All rights reserved. The entire contents of this publication are the property of the SANS Institute.

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.

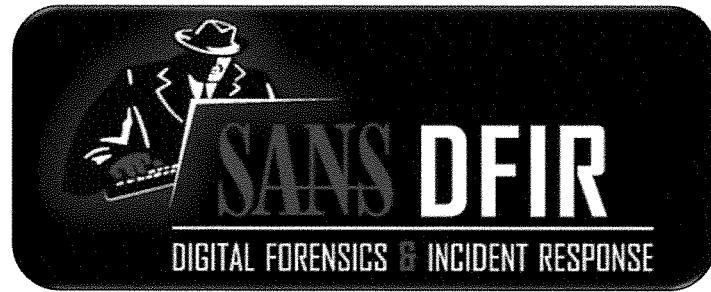
The SANS Institute reserves the right to terminate the above lease at any time. Upon termination of the lease, user is obligated to return all materials covered by the lease within a reasonable amount of time.



SANS Digital Forensics and Incident Response
CURRICULUM



FOR408: Windows Forensics



DIGITAL FORENSICS & INCIDENT RESPONSE

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

This page intentionally left blank.

SANS DFIR CURRICULUM

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

Website
<http://computer-forensics.sans.org>

SIFT Workstation
[http://computer-forensics.sans.org/
community/downloads](http://computer-forensics.sans.org/community/downloads)

Join The SANS DFIR Community

- Blog: <http://computer-forensics.sans.org/blog>
- Twitter: [@sansforensics](#)
- Facebook: [sansforensics](#)
- Google+: Search SANS DFIR
- Mailing list: <https://lists.sans.org/mailman/listinfo/dfir>

CORE

FOR408 Computer Forensic Investigations – Windows In-Depth GCFE	504 Hacking Techniques, Exploits, and Incident Handling GCIH
--	---

ADVANCED AND IN-DEPTH

FOR508 Advanced Computer Forensic Analysis & Incident Response GCFA	FOR572 Advanced Network Forensics and Investigations COMING SOON!
LEARN RFM New Content Added	FOR810 REM: Malware Analysis Tools and Techniques BREM

SPECIALIZATION

FOR518 MAC and iOS Forensics COMING SOON!	FOR526 Windows Memory Forensics In-Depth COMING SOON!
FOR559 Cloud Forensics and Incident Response COMING SOON!	FOR585 Advanced Smartphone & Mobile Device Forensics COMING SOON!

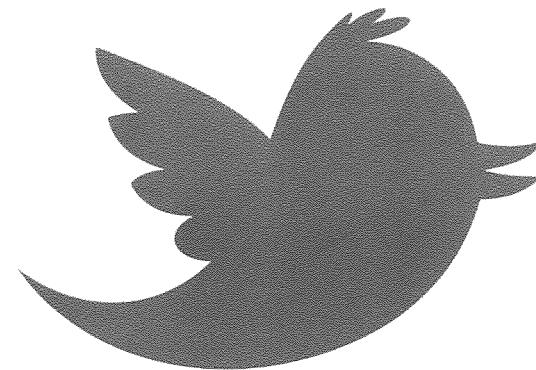
This page intentionally left blank.

Tweet During Class

- On Twitter?
- Meet Classmates
- Connect Online

@sansforensics

Hashtag: #408



Windows Digital Forensics and Advanced Data Triage © 2014 SANS

This page intentionally left blank.

Track Agenda

Section 1 Windows Digital Forensics and Adv. Data Triage

- Triage, Advanced FTK Imager Usage, Data Carving, String Searching

Section 2-3 Core Windows Forensics I

- E-mail, & Registry Analysis

Section 4-5 Core Windows Forensics II

- Artifact, Log File, & Browser Analysis

Section 6 Windows Forensic Challenge

- Putting Together A Real Case And Presentation

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

This page intentionally left blank.



Windows Digital Forensics and Advanced Data Triage

The SANS Institute
Ovie Carroll – oviecarroll@gmail.com
Rob Lee – rlee@sans.org

 @sansforensics <http://computer-forensics.sans.org>

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

Authors:

Ovie Carroll – oviecarroll@gmail.com
Rob Lee – rlee@sans.org

<http://twitter.com/robtleee>
<http://twitter.com/sansforensics>

Special Thanks to Chad Tilbury, Ovie Carroll, and Jenny Delucia. Your thoughts, opinions, research, and insight were invaluable to the creation of the course.

FOR408 - Section 1 - Agenda

The Donald Blake Case

Core Windows Forensics: Focus On Analysis

FTK Imager Advanced Techniques

Advanced Acquisition

Mounting Disk Images

File System Overview

Key Word Searching

File Metadata

Data Carving

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

The Donald Blake Case

Core Windows Forensics: Focus On Analysis

FTK Imager Advanced Techniques

Advanced Acquisition

Mounting Disk Images

File System Overview

Key Word Searching

File Metadata

Data Carving



Digital Forensics and Incident Response

CURRICULUM



The Donald Blake Case

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

This page intentionally left blank.

Asgard Inc. IP Theft Case

- Background

Employee Donald Blake was fired on Tuesday October 22nd 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 taking a key client with him – EvenBetterWidgets

Several clients switched to Donald Blake's new company

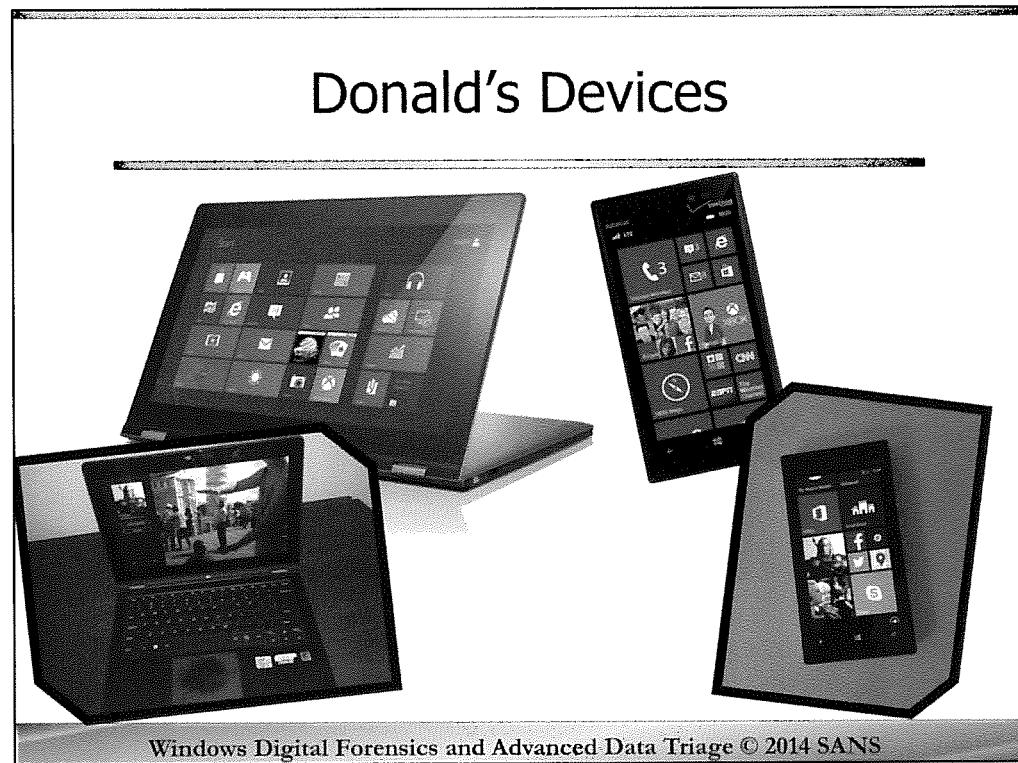
Some of the information that Donald Blake is currently using is assumed to have originated from Asgard Inc.

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

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

This page intentionally left blank.



Smartphone Details

- Nokia 928 – Windows Phone
- Office 365, SkyDrive, Skype, Sharepoint, and Exchange Integration

Laptop – Hybrid Tablet

Lenovo Yoga Series

Touch Screen ClamShell Laptop

- Windows 8.1 OS 64bit
 - 4 GB RAM
- Office 365, SkyDrive, Skype, Sharepoint, and Exchange Integration

Key Questions to Answer

Did Donald Blake steal Intellectual Property from ASGARD Inc.? (YES OR NO)

What did he steal?

Where did he put it?

How did you take it?

When did he do any of this activity?

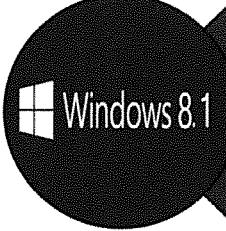
Did Donald Blake know he was going to be fired?

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

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. How did you take it?
5. When did he do any of this activity?
6. Did Donald Blake know he was going to be fired?

System and Setup Information



OS Type: Windows 8.1

- Fully Patched and Updated
- Single User System
- EST5EDT (Eastern Time)
- Office 365 Exchange E-mail
- dblake@asgard-venture-capital.com



Asgard Inc. Systems Include

- Office 365
- Sharepoint Server
- Skydrive Integration
- Exchange Online
- Microsoft Portal Online
- Whatever the employee wants to add

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

OS Type: Windows 8.1

Fully Patched and Updated

Single User System

EST5EDT (Eastern Time)

Office 365 Exchange E-mail

dblake@asgard-venture-capital.com

Asgard Inc. Systems Include

Office 365

Sharepoint Server

Skydrive Integration

Exchange Online

Microsoft Portal Online

Whatever the employee wants to add

Who is Who



Donald Blake

- Fired from work due to stock dumping of BetterWidgets due to suspected insider trading



Jordan Boone

- Chief Analyst



Derek Velez

- Sr. Business Analyst



Jamie Alexander

- CEO of Asgard Venture Capital Inc.

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

Donald Blake

Fired from work due to stock dumping of BetterWidgets due to suspected insider trading

Jordan Boone

Chief Analyst

Derek Velez

Sr. Business Analyst

Jamie Alexander

CEO of Asgard Venture Capital Inc.

FOR408 - Section 1 - Agenda

The Donald Blake Case

Core Windows Forensics: Focus On Analysis

FTK Imager Advanced Techniques

Advanced Acquisition

Mounting Disk Images

File System Overview

Key Word Searching

File Metadata

Data Carving

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

The Donald Blake Case

Core Windows Forensics: Focus On Analysis

FTK Imager Advanced Techniques

Advanced Acquisition

Mounting Disk Images

File System Overview

Key Word Searching

File Metadata

Data Carving



Digital Forensics and Incident Response

CURRICULUM



Core Windows Forensics: Focus On Analysis

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

This page intentionally left blank.

What We Learned in FOR108: Review

Digital Evidence Acquisition Essentials

- What is an Image?
- Evidence Acquisition Basics
 - FTK Imager & Previewing Data
- Types of Acquisition
 - Logical vs. Physical / Basic Windows Memory Acquisition/ Basic Disk-Based Acquisition

Legal Issues in Digital Forensics

- Rules of Evidence
- Admissibility
- Preservation of Evidence
- Chain of Custody
- Evidence Handling
- Evidence Integrity

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

We are going to talk for a few minutes about what evidence is and how and why it is important to maintain a chain of custody. Additionally, we will talk about proper evidence handling and how to ensure the integrity of any evidence you may come in contact with.

Establishing and following proper evidence preservation procedures is so critical to the outcome of your investigation.

In most criminal cases today, defense attorneys spend a majority of their efforts trying to find a flaw in the evidence preservation or handling. They know if the digital evidence is admitted in court, that it is very difficult to argue against the findings. Digital evidence almost speaks for itself.

Done properly, evidence preservation and handling will ensure your evidence is admissible in court.

We are going to talk for a few minutes about what evidence is and how and why it is important to maintain a chain of custody. Additionally, we will talk about proper evidence handling and how to ensure the integrity of any evidence you may come in contact with.

Establishing and following proper evidence preservation procedures is so critical to the outcome of your investigation.

In most criminal cases today, defense attorneys spend a majority of their efforts trying to find a flaw in the evidence preservation or handling. They know if the digital evidence is admitted in court, that it is very difficult to argue against the findings. Digital evidence almost speaks for itself.

Done properly, evidence preservation and handling will ensure your evidence is admissible in court.

Now that we know what evidence is, let's define Chain of Custody. Essentially, chain of custody is the ability to guarantee the identity and integrity of an item from collection through testimony of the evidence in court. It is the chronological documentation, and/or paper trail through the lifespan of an item of evidence from its seizure by law enforcement to final disposition.

The chain of custody officially starts when the item is identified by law enforcement as evidence or potential evidence. While it is always preferred to have a documented chain of custody from the moment a first responder identifies the item of evidence, the actual chain of custody does not officially start until law enforcement assumes control of the item.

In short, the whole idea behind the chain of custody is to guarantee the item of evidence has not changed since someone seized it.

There is something slightly different with digital evidence than other types of evidence typically do not have and that is the hash value. With digital evidence, once the documentation is accomplished as to who seized the evidence and any chain of custody until the item is forensically imaged, after the image has been created and the hash verifies, the hash essentially becomes the chain of custody from there through the testimony. What I mean by that is that you could theoretically upload the forensic image to a public FTP server, leave it there until trial, download it, hash the evidence, and verify the integrity.

For all evidence seized, taken, copied, etc., if it is to be introduced into court as evidence at some point, at a minimum, you will need some way to authenticate that the item of evidence is exactly what you claim it to be and it has not been altered from its original form. The most accepted practice for establishing an item's authenticity is by establishing its chain of custody. To establish a chain of custody the first step is to document at a minimum the following information:

Who seized the item/evidence? This should include the full name and contact information for the person who took control of the item. The purpose for this is to be able to testify what actions were taken with respect to the item of evidence. Establishing that the item of evidence was not changed in any way might require the testimony of each person that came into contact or had control over the item of evidence from the time it was seized. Each person might have to testify what their actions/interactions with the item were during the time the evidence was in their possession.

There may be situations where you are not the person who seized the item. Perhaps someone else responded to an incident and came back with a computer system or hard drive. The best case scenario would be for you to have that person who took the item create an evidence tag or property document. If this is not possible, you should create the document and start the chain of custody.

The next item to be documented is when the item was seized. This will establish the starting point for the chain of custody. With computer systems, there are TWO times that should be documented. The first is the actual time. This should be as accurate as possible and frequently seizing officials will synchronize their clock with something like the Naval Observatory. This time does not necessarily have to be to the second but should be as accurate as possible.

The second time that should be documented when dealing with or seizing computers is the system date/time. This is often obtained from the BIOS which receives the date/time from the Real Time Clock (RTC) that lives on the same chip as the CMOS (complementary metal oxide semiconductor). The "CMOS" is very low power static memory and its function is to store "Setup" information for the BIOS while the computer is turned off. A separate battery keeps the RTC and the CMOS information active.

WHY THIS IS IMPORTANT: As you know, the time on a computer system does not come from the hard drive, rather from a small chip called the CMOS, which is located on the mother board. If you remove a hard drive from the computer and do not seize the computer and no one documents the DATE/TIME of the RTC/CMOS it becomes much more difficult, perhaps impossible, to testify to the accuracy of the date time stamps on any of the files.

Next is the physical description of what is being seized. On your evidence tag or property document, you should describe the item with enough specificity to make sure there is no confusion about what was seized. Many agencies have their own policy but at a minimum the description should include the Make Model and Serial number of the item. It is also a good practice to annotate in the description the condition of the item, such as if there is any damage, dents, scratches, etc. This will help later if the property is returned to the owner and claims are made that the item was not returned in the same condition as it was taken. Many law enforcement agencies make it a practice to take digital photographs of all evidence seized.

Also, with physical items, it is a good idea to place a mark or sticker on the item or bundle of like items so you can later assert that you know this is the item you found/seized because you recognize your mark on the item. A good practice used by LE is to mark each item with your initials and the date you took the item. BE NICE – DON'T DESTROY THE ITEM. Would you be able to recognize the WRT54G router you took from the same router someone else took? I mentioned a bundle of like items. This is because, particularly with computer media like floppy disks and CD/DVDs, rather than documenting each CD/DVD, you may bundle several like items in a bag or container, seal the container with evidence or tamper-proof tape and document that you seized one bag of CD/DVDs containing 50 miscellaneous CD/DVDs.

Now that you have documented the seizure of your evidence, the next thing you must do is document everyone who takes control of the evidence. At a minimum you should document:

Full Name of the person releasing control

Full name of the person taking control of the evidence

Date/Time of the transfer of evidence

Ref: http://wiki.osdev.org/CMOS#Getting_Current_Date_and_Time_from_RTC

<http://www.pcguide.com/ref/mbsys/mobo/compRTC-c.html>

http://www.mitre.org/tech/cots/TIME_DATE.html

- * Purpose for the change of custody of the evidence (this might be to be transported to the lab)
- The condition – With the exception of the initial seizure, the condition will typically be 'UNCHANGED'

If you have an evidence custodian, you should also document the transfer of evidence to and from the evidence custodian.

It is important to document WHERE you found the item you are seizing. The location should include both physical addresses, such as the desk in the northwest corner of the master bedroom at 123 Main Street, Apartment 20. Many incident responders will carry a digital camera to take photographs of the search scene, while others still prefer to make sketches of the search scene. The location you find the item can also go a long way in demonstrating who had control of the item prior to seizure.

Photos are the best way to document exactly where you seized the item. As mentioned in the last slide, a photo will also document the condition of the item. Photographs are also useful for other things. There was a situation where a computer was seized along with all associated media on/in the desk. During the examination an encrypted folder was identified and the subject was unable to give the password because he had used the first letter of each of the 25 music CDs on his desk. When agents seized the disks, they had no idea and did not take photographs of the order in which they were stacked.

WHY – It is a good idea to document the authority by which you are taking the item. Documenting why is not as important as the other items but can be a great reminder later when you are trying to remember if you seized this item as a result of a search warrant or consent.

Evidence Integrity

If your goal is to prosecute the responsible parties, you must be able to ensure that the evidence has not been corrupted. The only way to do this is to take some [seemingly] extreme measures. Consider doing the following:

1. Create a cryptographic hash of the entire disk and each partition.
2. Create bit-image copies and analyze them.
3. Create a cryptographic hash of the copy and compare with the results obtained from the original. They MUST match, or else something's gone wrong and the copies are different from the original.
4. Be sure to lock the original disk in a limited-access room or container.
5. Utilize chain of custody forms to show who has current and previous control of original or best evidence utilized in a case.

The hashing process uses "hash" functions, which verify that the acquired image is an exact copy of the original media. The Message Digest 5 (MD5) and Secure Hash Algorithm-2 (SHA-2) are the two most common hash functions.

Hashing takes as input a message of arbitrary length, and produce as output an n-bit "fingerprint" or "message digest" of the input. The algorithm then produces a digital signature, which can be used to identify a uniquely given file, and therefore establish that the image is an authentic copy of the original evidence. Verification using hash algorithms is highly reliable. The odds of two random files having the same hash are astronomically small. Moreover, the use of the hashing algorithm is a one-way function. This means that it is easy to create a hash from a file, but almost impossible to create a file matching a particular hash.

Hash validation, when combined with evidence of a chain of custody between the time the original computer media was seized and the image was created, is strong authenticating evidence that the forensic image is an exact duplicate of the original. Hash algorithms fit the examples listed in Federal Rule of Evidence 901(b)(4) of "distinctive characteristics" that can be used to authenticate evidence.

Image files are essentially self-authenticating with their hash. You could image a drive, place the image on a public FTP server or pass it around to 1000 people and when you got it back as long as the hash matches, your chain of custody is intact. The hard drive is merely the container. Think of it as the evidence bag you place the bloody knife in at the crime scene. When you go to court, the knife does not have to be in the exact same brown bag, the bag is NOT your evidence, merely the container carrying the evidence.

Types of Hashes

The two most common hashes are the MD5 Hash and SHA-256 (sometimes called SHA-2).

MD = Message Digest

md5sum produces a 128-bit (16-byte) hash value, typically expressed in a 32-digit hexadecimal number.

SHA = Secure Hash Algorithm

SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely-used security applications and protocols.

SHA-256 produces a 256-bit (32-byte) message digest hash, typically expressed in a 64-digit hexadecimal number and is meant to provide 128 bits of security against collision attacks.

Hash Properties:

Cryptographic Algorithm

Non-reversible

i.e., given the hash, we can't compute the input file

These and other hashes can be used to verify that no modifications have been made to the data. When an analyst “hashes” the data, he is collecting the signature of the data to be used to verify that the data did not change during any analysis that was performed. It is also routinely utilized to ensure a copy is identical to the original copy of the file by comparing the original hash to the copy's hash.

If a single bit of data is different from one version to another, it will have a different md5 signature.

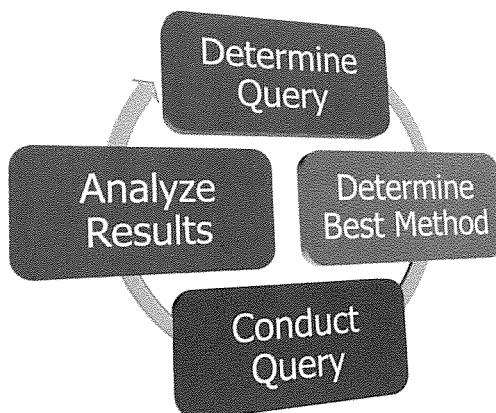
Every copy you make of digital evidence should show that the evidence is not changing as you are moving it or analyzing it. One way to perform this best practice is to use cryptographic hashes to show your bits that you collected have not changed.

Ref:

<http://en.wikipedia.org/wiki/MD5>

<http://en.wikipedia.org/wiki/SHA-2>

Investigative/Iterative Process



- Best Method
 - Keyword
 - Graphic review
 - Internet Analysis
- Best Tool
- Analysis of Search Results

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

Let's start the day off by talking about the computer forensic fundamental mindset.

When we speak of the computer forensic fundamental mindset, we will need to talk about the fact that computer forensics is as much of an art form as it is a science. We will discuss how computer forensics is also an Investigative/Iterative process, not a static discipline like DNA that can be done in a vacuum without any knowledge of the investigation. We will also discuss why computer forensics requires a solid understanding of both the operating system and the applications used by the subject and most importantly, we will discuss why computer forensics **REQUIRES** analysis.

Computer forensics, unlike most of the other forensic disciplines, is as much of an ART as it is a science. This fact has even been recognized by the courts in such cases as US v Brooks. In this decision, the courts concluded that “Given the numerous ways information is stored on a computer, [both] openly and surreptitiously, a search can be as much an art as a science.”

US v BROOKS - This case deals with law enforcement originally responding to an incident for the smell of marijuana and obtaining a search warrant to search the house for marijuana or items associated with marijuana use (paraphernalia). When looking in the trash can, they noticed a substantial amount of what appeared to be discarded photographs of child pornography that had been printed from a computer. Officers obtained a second warrant and asked for consent to search subject's computer for images of child porn to which the subject agreed. The subject signed a consent form which stated he authorized a pre-search and a complete search for **image files only** of child pornography.

The TWO most important things about this decision is that the courts understood that files can be stored both OPENLY and SURREPTITIOUSLY and that a search methodology or protocol need NOT be stipulated or detailed in the search authorization.

No Requirement to Detail Search Methodology - This surreptitious method of storing files can refer to any technique used to hide specific digital information that is evidence of a crime law enforcement have authorization to search for. One of these techniques might include the act of changing the file extension on a graphic file from something like a JPG to DOC. If you searched files only based on file extension this would prevent law enforcement from finding the evidence they are searching for. Additionally, if someone embedded a graphic file inside of a PDF or non-graphic file they might again thwart law enforcement's efforts to identify evidence of the crime. If you think about non-computer searches, in the US v Brooks case, the courts would never require law enforcement to list in detail which room they were going to search first or when they get to the bedroom, which order they were going to open the dresser drawers or that they were going to search the room in a counter-clockwise pattern. The same goes for computer searches however, we are seeing defenses raised to challenge or suppress the findings of a search because a search methodology was not detailed in the warrant.

Within the Scope of Search Authorization - If law enforcement had authorization to search for evidence of child pornography, do you think they could open or look inside a text file? An e-mail? An excel file? How about inside a zip file? If we think about this embedding of a graphic inside a text file, do you think you would be within the scope of a search authorization to look inside files other than graphic files? ANSWER: YES. Just like in a physical search of a room for drugs, officers may look through an underwear or sock drawer to make sure that drugs are hidden inside a sock or underwear. This search technique is referred to as taking a "brief perusal" (no underwear pun intended), and it is what authorizes you to briefly look inside each file to make sure the evidence you are authorized to search for is not surreptitiously hidden inside that file.

NOTE: This does not authorize you to read all e-mail or documents.

You should consider reading this case decision when you have some time because it emphasizes that which can be found at <http://laws.lp.findlaw.com/getcase/10th/case/044255.html>.

When presenting evidence in court or discussing digital evidence with the legal community, you will likely encounter people using the sub container perspective. While analogizing digital evidence as a file cabinet with drawers and files makes explaining certain computer concepts easy, this sub container perspective is causing significant problems with respect to the legal community applying search and seizure law to digital evidence.

The Berkley Journal of Criminal Law recently published an article written by Department of Justice Attorney Josh Goldfoot. This brilliant law article titled "The Physical Computer and the Fourth Amendment" is a must read by forensic examiners.

Search and seizure law is heavily based on physical facts. It controls what places law enforcement officers can enter and what things they can seize, but not what information they may learn. The sub-container perspective rejects that premise.

- The California Supreme Court recently used the physical perspective by viewing storage media as physical evidence.
- Under the physical perspective, a hard drive is an "object", not a place. It does not contain things; it is one thing.
- Like any other physical evidence, it is examined, not "searched."

As long as the storage medium is lawfully seized, the Fourth Amendment should not restrict how the forensic examination is conducted. Just as the Fourth Amendment does not govern the work of the technician analyzing seized blood stains, developing film, or testing suspected drugs, it also does not govern the work of the technician analyzing a lawfully seized hard drive.

As a digital evidence analyst, you should try to only use the physical perspective when discussing how the fourth amendment should be applied to digital evidence.

References:

<http://scholarship.law.berkeley.edu/bjcl/vol16/iss1/3/>
<http://cyberspeak.libsyn.com/cyber-speak-forensics-and-the-4th-amendment>
People v. Diaz. 244 P.3d 501, 509 (Cal. 2011).

Best Method –

When we say that computer forensic analysis is an Investigative or Iterative Process, we mean that while staying within the scope of the warrant, a great deal of thought must go into whatever you do. You must actually give great consideration to what the Best Method is to find the data you are searching for. Some of the things that go into your consideration are what type of data you have to analyze and what it is that you are looking for. Will just a straight key word search find everything you are looking for? What do you think would happen if you were to do a key word search for the word CHILD or KILL? You would likely get hundreds of thousands of hits. If it were graphics you were looking for, could you narrow your search by file size and not look at graphics smaller than 32k?

What is the Best Tool –

You will find that certain tools do a better job or at least make it easier for you to find certain types of files. You will find that a good forensic lab has several different tools. Some may even be developed in your lab, to make your job easier. If you are searching through e-mail, you will find that some forensic tools do a much better job of presenting MS Outlook PST files than others. Other forensic tools make it much easier for you to see compressed or zipped files while others require multiple steps just to see what is inside a zip file. This is where forensic blogs, list serves and courses like this come in real handy. Don't get locked on or tunnel vision when it comes to the tool you use.

Analysis of Search Results –

One of the worst things a forensic analyst can do is to blindly conduct a key word search and just dump the hits to media and give it to a case agent and never look at the data again. This action might be OK in some circumstances in e-discovery or other situation but this type of action is not considered ANALYSIS. As mentioned in the US v Brooks case, the courts understand that for every action you take on the computer (key word search, graphic review or analyzing Internet web surfing activity) when you review the results or question finding of a significant piece of evidence, you will (or should) almost inevitably develop a questions or an additional search that needs to be conducted or location that needs to be examined to solidify the previous finding. This type of iterative approach is the definition of a computer forensic analysis.

Let's take the finding of a key graphic file. Once you've found the graphic file, you should also want to know how that file got on the computer. Was it from web surfing? If it was, was it a result of a pop up or did the user conduct a Google search for specific key words describing the graphic you found? Did they have to navigate to the main web page where the graphic was located, or did they have to click several levels deep into a web page to find the graphic? Also, where was the graphic? Was it in the temporary Internet cache, or was it saved in a user directory that describes the type of graphic it is? All of this makes a significant difference in the outcome of your examination/analysis.

QUESTION: What else might you be thinking?

ANSWER:

Is there EXIF data that tells me what kind of camera took this photo?

Are there any other photos taken by the same camera on the computer?

What else was going on the computer when this graphic was created, modified, last accessed?

What applications were used to open, view, edit, create this file?

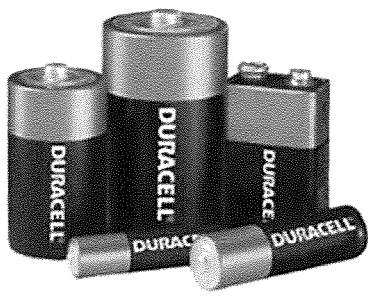
Is there any proof like a link file or registry entry that this graphic was opened, viewed or edited?

AND THE LIST GOES ON.

None of these questions are asked or answered if all you do is run key word search and dump the hits to a drive and give it to the case agent.

Analysis/Batteries Not Included

- Understanding OS & Applications & Investigation
- Evidence Created
 - User Action
 - System Action
- Problem Solving Skills
- Requires Analysis
 - NOT Just Data Extraction
 - W, W, W, W, W, H



Windows Digital Forensics and Advanced Data Triage © 2014 SANS

Understanding OS & Applications –

A forensic examiner/analyst should have a solid understanding of the operating system and the application they are examining. Only by understanding the OS and applications on the system you are examining will you understand where to go to look for evidence of an action. Many times you will find that you will have to conduct tests in your lab on applications to find out what evidence is created by the application when an action is taken, then go to the hard drive you are analyzing and look for that piece of evidence.

A forensic examiner should also UNDERSTAND the investigation for which she is doing the analysis for. Understanding what is being investigated will help guide an analyst in the direction evidence is likely to be found. In most law enforcement situations the analyst should have a copy of the search warrant, which will also have the affidavit which establishes the circumstances for which probable cause existed that convinced the courts to grant the search warrant. That search warrant also frames the boundaries of the search or “scope of the search”. When working with law enforcement, it is imperative that an examiner understand and stay within the scope of the warrant or any evidence they find may be suppressed and not allowed to be used in proceeding against the defendant.

As we have mentioned before about simply conducting a key word search and exporting the results for review by the case agent, do you think a non-technical non-forensic trained agent or investigator understands computer systems enough to ask for link files or know what in the registry could help his investigation? No.

Understanding Evidence Created –

Evidence of action or activity is created by both the user of the computer, as well as the system itself. An example of this might be a directory that is created by a user with the name describing the contents like “My Hacking Tools.” Another example of evidence created by the actions of a user might be the creation of a LINK file when a file is opened by the user.

Evidence created by a system action might be an audit log showing default system maintenance have run at the default time or file access times being changed by an antivirus scan automatically being run.

Understanding what kinds of evidence is created, how and why will help you be a better examiner.

Requires Analysis –

Findings are the result of your key word searches or individual items of significance you find during the course of your examination.

Analysis is the act of looking at all the individual findings, attempting to determine the 5 W's (Who What Where When Why) and How then based on the existence, lack of existence, location and time stamps of that information, determining what actions were taken on the computer that would have caused those items to exist.

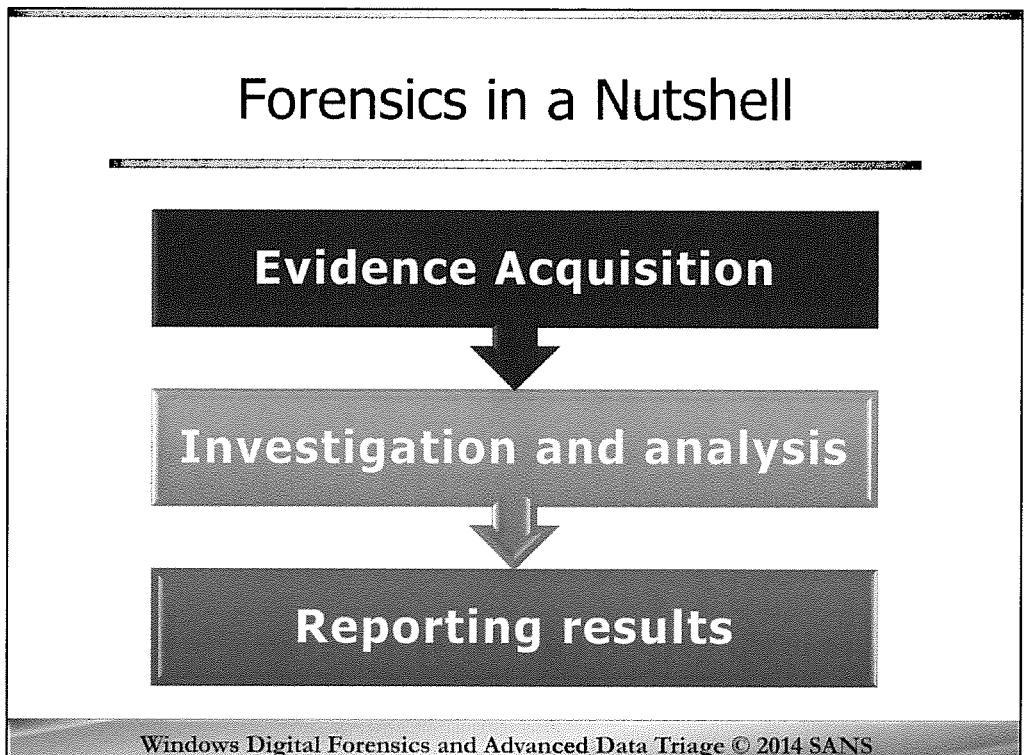
In a court of law, your expert opinion is based on conducting an analysis of the totality of your findings, and the information you have about the investigation as to what events took place and by whom. Your opinion must be in turn supported by your findings.

If you find someone that is only doing key word searches or exporting specific files for someone else to review, you should NOT be calling this person a forensic analyst. They are more of a DATA EXTRACTION SPECIALIST. This class is about giving you the skill and knowledge to understand what evidence is created by user and system actions so that you can find those pieces of digital evidence and form an opinion or conclusion as to what happened on a computer.

Problem Solving –

One of the most valuable skills a forensic examiner/analyst can have is their problem-solving skills. They should be masters of problem solving because for each investigation they should be asking themselves, what crime is being investigated, what actions might a user have taken to facilitate that crime. Of those actions what evidence would be created by the user, application or system when that action was taken. When analyzing a computer system, if you are not finding the evidence you know should be there based on the information you have about the investigation, you need to ask yourself, Why? What actions would a user have taken to hide their activities or prevent them from being where they should be? It may be a simple configuration setting a user changed that causes logs or files to be saved in a different location or it could be used some form of counter forensic programs. If the latter is true, what actions would you take to determine if a counter forensic program was installed or run? This goes right back to the problem solving and understanding of what evidence is created by a user, operating system or application when certain actions are taken.

So when we think about the computer forensic fundamental mindset, we know that computer forensics is as much an Art as it is a Science. That it takes an investigative and Iterative approach, with the forensic analyst looking at each item, file and finding and asking themselves if that finding warrants an additional search or inquiry to determine who, what, where, when, why and how that file originated on the computer and if that item was created or modified by a user or system action. All this can only be achieved by having a solid understanding of the operating system and applications being examined.



Computer forensics is more than just analyzing blocks of data. It is the effective gathering, examination, and reporting of your actions and findings. A seasoned investigator knows that if one step is overlooked, his case will not yield the results that he or she may desire.

Evidence seizure and acquisition generally occurs during the incident response phase where you must verify the incident, but you also begin your work to collect volatile and non-volatile data. Data that is volatile is lost if the system is adjusted prior to the collecting of that data. A memory dump of a process that might contain key IP addresses of the attacker or subject. Non-volatile data is a hard drive that is powered off, or static CD-ROMs.

Investigation and analysis occurs when the investigator takes what is collected and analyzes it to form a clear picture of the incident. This analysis uses tools and techniques that require data recovery, piecing together the puzzle of what happened, and forming a timeline of events.

Reporting your results becomes the most important step. Without accurate reporting, the investigator often finds himself unable to find anyone willing to prosecute his case or take action. Without action, why perform the investigation? Reporting is key.

"Gathering and analyzing data in a manner as free from distortion or bias as possible to reconstruct data or what has happened in the past on a system."

Farmer and Venema, 1999

Law is Not a Science

- Admissibility of Computer Evidence and MD5 Hashes
 - Using MD5 algorithm is completely acceptable.
 - Other algorithms?
 - Choose which algorithm you feel is best. (SHA1, SHA256, etc)
 - Accomplish any hashing of evidence and your evidence will usually see its day in court.
- WHY?
 - Hashing is not used for authenticity
 - Need Hashing for
 - Expert Witness Testimony
 - Tampering Claims
 - Weight of Evidence

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

FROM AN ARTICLE AT <http://computer-forensics.sans.org/blog/2009/01/07/law-is-not-a-science-admissibility-of-computer-evidence-and-md5-hashes/>

Law Is Not A Science: Admissibility of Computer Evidence and MD5 Hashes

Another day... another hashing discussion:

On the SANS GIAC Alumni list the other day, the question popped up from one of the individuals on the list:

"I'm assuming that this group has had the pleasure to consume the latest research focused on MD5 hash collisions. Discussions about hash collisions seem to carry the same energy as religion and politics. My question is regarding digital evidence and the use of MD5 hashes to establish digital evidence integrity. The use of hashes to ensure digital evidence integrity has legal precedence. However, as more research companies introduce concerns related to MD5 hashes, the courts will at some point, no longer consider this as a valid technology to ensure integrity."

Has anyone heard of a successful attempt to dismiss evidence due to concerns that MD5 is no longer considered tamper proof?"

This topic pops up from time to time in our **Computer Forensics** classes at SANS (*er... pretty much every time...*).

The answer:

First off, as of today, using MD5 algorithm as a form of hashing for digital forensic work is completely acceptable.

You can use additional means of hashing, but honestly, choose which algorithm you feel is best. As long as you are accomplishing hashing of evidence you are fine and your evidence, will usually see its day in court.

Why?

First off, admissibility guidelines do not differentiate between physical and electronic evidence. The U.S. Federal Rules of Evidence (FRE rules 901 and 902) guide authentication of evidence for admissibility. Nowhere does it state that electronic evidence will be treated differently than physical evidence for authentication purposes.

Could you get electronic evidence admitted without hashing? *Yep.*

Will hashing help admissibility of my evidence? *Certainly, but it is not legally required.*

What if someone brings up collisions in court? *Again, usually an attempt to confuse the jury. But you can turn this on them by stating that it is more likely that before showing up for jury duty, all the jurors randomly put the same 7 numbers into the Powerball Lottery and won. That has a much greater chance of happening than a naturally occurring collision. With folks being prosecuted on partial fingerprint matches or eye witness testimony from a guy driving by in a car at 30 MPH, do we really think this is a show stopper for courts?*

Interesting Rob, but anyone with some legal credentials to back up what you are telling us? *Yes, our very own author/senior instructor Richard Salgado for Computer Forensics at SANS wrote a wonderful paper on the topic several years ago for Harvard Law Review (http://web.archive.org/web/20090305231403/http://www.harvardlawreview.org/forum/issues/119/d_ec05/salgado.pdf) that states "...there is more than reasonable assurance that two different inputs will not have the same hash value."* (see footnotes 7 & 8)

If hashing is not legally required to prove authenticity, why do we use hashing, chain of custody, and proper storage of evidence in case of pending litigation? **Two point five reasons:**

1. Expert Witness:

Best practices are tested if you are deposed as an expert. Hashing (any form) is considered a best practice for digital forensic practitioners. If you take yourself seriously in this line of work and you do not perform any type of hashing then you open yourself up for a cross examination as an expert that would not be fun to sit through. "The court is called upon to reject testimony that is based upon premises lacking any significant support and acceptance within the scientific community,". If you would like your testimony to hold greater weight, HASH. 'nuff said.

2. Tampering:

Tampering can only be brought up if the opposing council has a strong argument that the evidence has been deliberately modified. Tampering cannot just be brought up because it is digital evidence and easily modified... the opposing side has to prove it happened. The burden is on the side claiming that tampering happened, not the side entering the evidence and do a search for "Authenticity and the Alteration of Computer Records"). With hashing (*even using an algorithm such as MD5*), you can reduce the threat that someone will claim the evidence has been tampered with if you can prove over time it has not changed. Which in this case, collisions are really not a big deal at all as long as you get the same hash every time you calculate it against the evidence.

Why is MD5 still ok? From the cited website: “*The existence of an air-tight security system [to prevent tampering] is not, however, a prerequisite to the admissibility of computer printouts. If such a prerequisite did exist, it would become virtually impossible to admit computer-generated records; the party opposing admission would have to show only that a better security system was feasible.*”

One last thought from Eoghan Casey on this topic: “On May 24, 2006, the DFRWS posted a challenge asking for anyone to produce actual files (or evidence) that have produced a collision and nobody has succeeded yet!”

2.5. Law Is Not A Science:

I tell students this regularly... We (*you and I*) are technical. We grew up loving math. We feel that if we add **1+1=2** we will always get **2**. This is why it is a science. **1+1=2** Repeatable. **1+1=2** Satisfying. Feels good doesn't it? **1+1=2**

Well, let's take that same formula from our nice scientific world and put it in the legal world.

Court 1: **1+1=2**

Court 2: **1+1=2**

Court 3: **1+1=3**

See what happened there? We ended up with some bizarre result. This drives us *crazy*. Well, in reality, this is not exactly what happens. What does happen? What if you take the SAME evidence, the SAME analysis, the SAME conclusions...you drop that into TEN separate courts, you will probably end up with the same verdict 9 times out of 10.

HOWEVER, (*comma, space, pause for additional dramatic effect*) there is always at least **one** jury/judge that will think differently and rule the other way given the SAME evidence, arguments, and testimony. We need to realize that we cannot force our mindset onto a system that is not a science, but rather, is an art. As a result, like the core question asks about MD5 hashing, we think we need to “fix” the courts or come up with a system that is FAIL proof.

In the instances where we might find that MD5 is attacked in court and subsequently not used for authentication in a courtroom, we can point to a variety of reasons. In the several cases my peers and I have reviewed, it appeared that the prosecution failed to produce an expert to discuss hashing. Generally all the expert would need to accomplish is to discuss the true likelihood of a collision... which is far less likely than even a collision with DNA evidence. It isn't whether the hashing standard has a fault, but whether it is GOOD enough... **1+1=3**. DNA analysis, fingerprinting, and eye witness testimony all have their faults... but are they good enough to convict? YEP. Have criminals been let off due to the fact that the prosecution could not produce a DNA expert to discuss the likelihood of a false positive? Even worse, the judge/jury listens to the explanation and still reject it. You don't have to dig far to find cases where individuals are not convicted despite the fact compelling scientific evidence points to the contrary.
1+1=3

And here is the kicker...even though one or two courts rule against the scientific facts such as DNA evidence (or countless others), it does not set precedence and invalidate DNA evidence for here to the end of time.

So... what do the lawyers think?

The best way to see why law and science do not mix well is to view it from a lawyer's perspective. This is an excerpt from one of my favorite legal blogs on the subject written by [Ralph Losey](#) who has a wonderful book called [e-Discovery Current Trends and Cases](#) (*worth a read if you deal with litigation and you work in IT*). It is a rather long blog entry, but read it if you have the time. It doesn't directly discuss MD5 hashing, but you will see why such a discussion about MD5 hashing being admissible or not due to collisions probably drives the lawyers crazy... just like it drives us crazy when we ended up with $I+I=3$ in their world.

...the practice of law is an art, not a science, and the human element can never be replaced by technology.

Unlike computer code, the rules of law are malleable and there are always exceptions. This in turn is one of the key reasons the two cultures of Law and IT have such a hard time understanding one another. It is also the reason a few inexperienced engineer types are delusional and arrogant enough to think that e-discovery can be "fixed" with the right software algorithms. It cannot because law is not a science, it is far too complex and chaotic for that. Or if it is a science, it is more like Quantum Physics, where electrons are unpredictable and can be in two places at once, not the orderly world of Newtonian Science that most engineers live in.

*Yes, there are many computer programs that can be used as effective tools in the pursuit of justice. We lawyers need to wake up to that fact. But so too do the technologists who think the right software alone will fix everything. **The human element is key in Law which is one reason that training is so important.***

Analysis is Not Artifact Recovery

Proper analysis is not about simply about:

- Finding Artifacts, Pictures, and Documents
- Or Recovering Deleted Files

Analysis requires understanding of how specific evidence will answer a key questions

- "Evidence of..." Categories (Download, Execution, File Opening, File Knowledge)
- Intersecting evidence and facts verifies results

Focus on which key questions need to be answered

- Build timeline based on key analysis questions
- Focus on detailing facts via analysis not theories

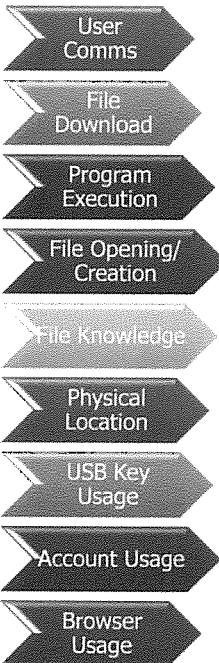
Windows Digital Forensics and Advanced Data Triage © 2014 SANS

One of the key ideas of this course is that proper analysis is essential to successfully navigate cases. The proper way to accomplish is not simply to recover a bunch of artifacts and recover some deleted items, paste them into a report, and hand to a prosecutor or management. You need to recover the artifacts and then analyze the data that they hold to determine a clear picture of what the user was doing, when they were doing it, why, and many other details that might go unnoticed unless your trained eye began to exam them.

Many artifacts you will uncover will help substantiate a fact. Multiple artifacts that all substantiate the same fact are much more effective at increasing the overall weight of your evidence.

This book will be useful to you as we begin to focus on "Evidence of..." analysis. This type of analysis relies on artifacts, but helps pair similar artifacts together that help answer a specific question or action. For example you will learn that there are commonly 4-6 locations on an average Windows system that will point to a user's File Opening or File Creation. We start to quickly build up the many artifacts that can answer many of the key types of questions on the next page.

"Evidence Of ..." - Categories



In this course, we begin to focus on answering the key questions. Did a user have knowledge a file existed on their machine? Did the user open the file and when? Did the user execute Regedit to delete registry entries? How and when did a user download a file wiper to a machine.

Seeing that there are specific questions that can be answered by these pairings we have created the "Evidence of ..." categories. We will continually build these categories in this class until they are populated fully. You will then be able to use this list as a "cheat guide" to help you remember where you can check to discover key items inside a Microsoft Windows Machine.

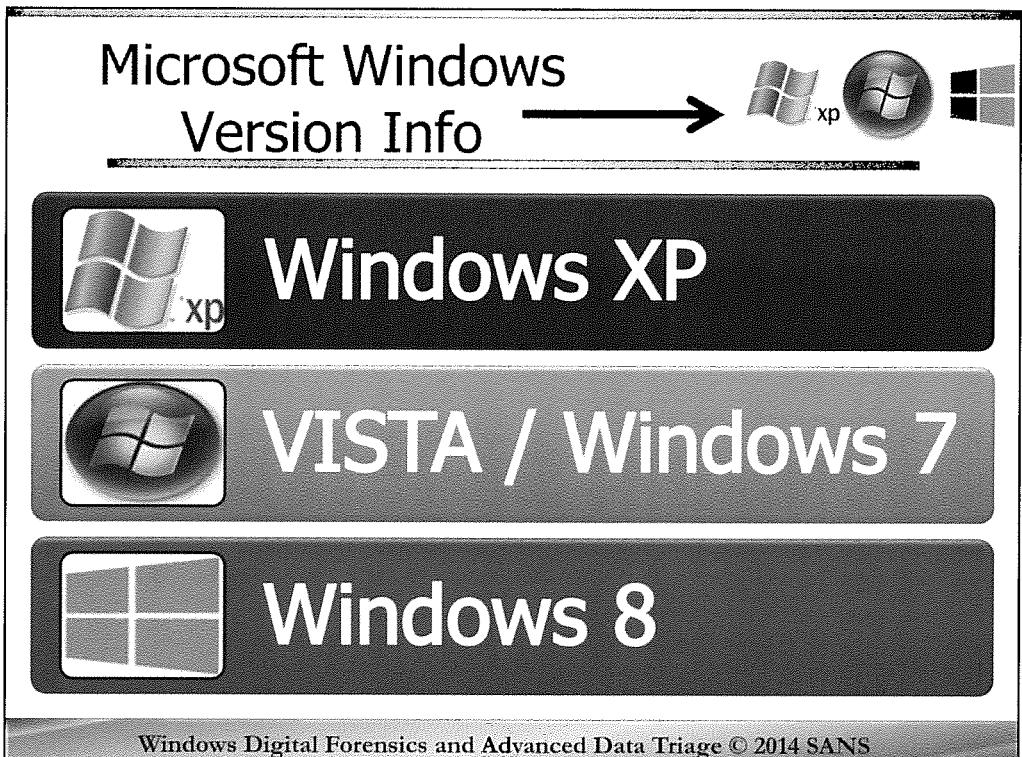
Evidence of Categories:

- User Communication
- File Download
- Program Execution
- File Opening/ Creation
- File Knowledge
- Physical Location
- USB Key Usage
- Account Usage
- Browser Usage

In a little bit, we will start to create our first timeline. The timeline will include major artifacts that make up facts from the case. The "Evidence of" slides will help you determine the activity that occurred as multiple artifacts should intersect for the same item. For example, when Office Word executes, you might Evidence of Execution via multiple

prefetch files and userassist entries. In the same example, you should see the document that Word opened up via File Opening Creation artifacts such as LNK files, Recent Docs, and more.

The idea behind this analysis technique is that instead of teaching you artifact after artifact and hoping you can figure out how they fit together. It focuses instead on the key question the artifacts help solve and categorizes them appropriately.



Over the course of the next few days, we will be examining the core Windows Operating Systems. Windows XP, Windows VISTA/7, and Windows 8. When an artifact is found only in a specific operating system, look for the Windows OS Icon to appear in the upper right hand side of the slide to note the specific operating systems that this artifact will be found in.

FOR408 - Section 1 - Agenda

The Donald Blake Case

Core Windows Forensics: Focus On Analysis

FTK Imager Advanced Techniques

Advanced Acquisition

Mounting Disk Images

File System Overview

Key Word Searching

File Metadata

Data Carving

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

The Donald Blake Case

Core Windows Forensics: Focus On Analysis

FTK Imager Advanced Techniques

Advanced Acquisition

Mounting Disk Images

File System Overview

Key Word Searching

File Metadata

Data Carving



Digital Forensics and Incident Response

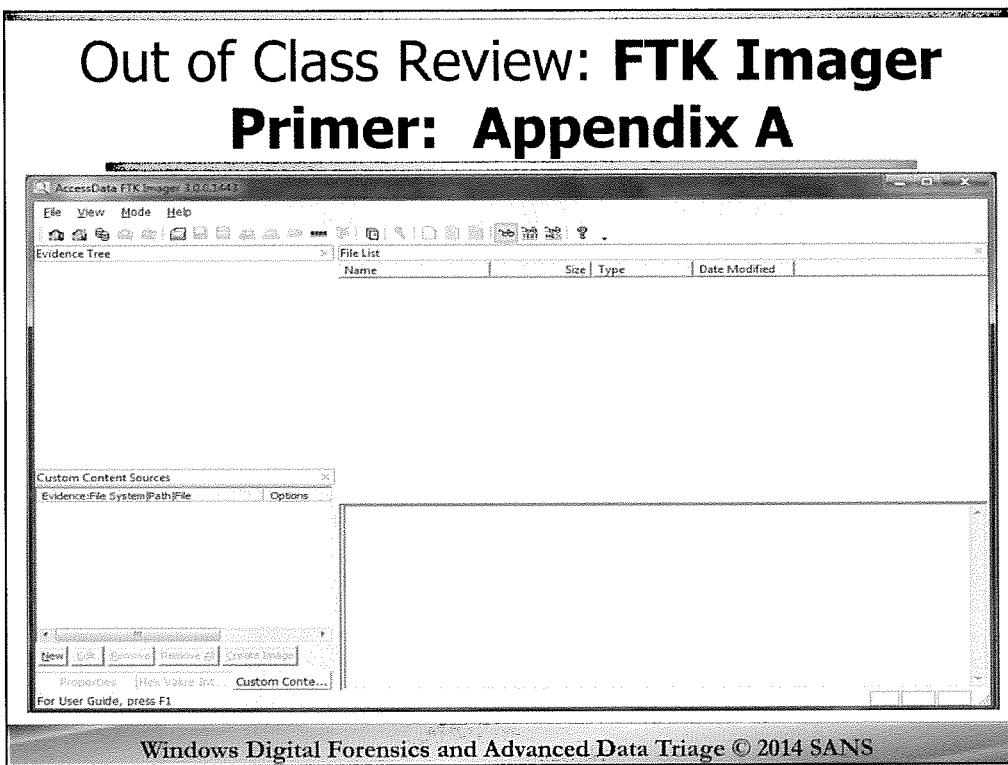
CURRICULUM



FTK Imager – Advanced Techniques

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

This page intentionally left blank.



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 that 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 is 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.

FTK Imager – Advanced Techniques

RAM Acquisition

Registry Extraction

Creating Custom Content Images

Triage Based Forensics – Fast Forensic Acquisition

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

RAM Acquisition

Registry Extraction

Creating Custom Content Images

Triage Based Forensics – Fast Forensic Acquisition

Memory Acquisition

- Memory Acquisition
 - Volatile Data
 - Will Change Evidence
 - Return outweighs Risk
- Soon to be Standard for all live response
 - WHY? – Without memory image there is little chance to bypass whole disk encryption



Windows Digital Forensics and Advanced Data Triage © 2014 SANS

Memory Acquisition has become one of the most important changes to the computer forensic field.

Memory acquisition is not new; it has been around for over 15 years.

Previously, and unfortunately, some even today resist memory acquisition because of its complexity. With new tools today, memory acquisition is no longer complex. Tools like F-Response have made it so that incident responders can image RAM as if it was a physical drive using whatever imaging tools they are comfortable with.

Surprisingly, there is still a lot of discussion about the most appropriate thing to do when responding to a computer system that is still powered on. Some law enforcement agencies are still teaching their agents to pull the plug from the back of the machine. Others are recommending collecting and documenting all volatile data, including RAM before powering the system down.

Because incident responders and investigative agencies may not be immediately aware what information is evidence when they arrive on scene, the Department of Justice advises incident responders to document and preserve as much information as they can. They suggest all incident responders be trained so they can collect/preserve as much volatile data as possible. The old argument that you are changing/altering evidence if you do anything other than pull the power plug is as ignorant as the assertion that the world is flat. It was OK when that was all we knew how to do, but we now have the capability to easily collect volatile data.

With the increased popularity of encryption programs, pulling the power plug has already resulted in investigative agencies having nothing to examine. Additionally, a growing popular claim from defense attorneys is that the system was being controlled by a remote administrative utility/Trojan or a virus was causing all the activity. Without the collection of volatile data, it becomes much more difficult to defend against or refute.

When responding to an incident involving digital evidence, the general rule for first responders should be to preserve as much data as possible in the way it was found when they arrived. The most immediate priority should be to capture volatile data.

Volatile Data – is what is referred to as data that will disappear or be destroyed once the computer system is powered off. Typically this is RAM, but it goes further. Volatile data is also current active network connections, running applications, open/listening network connections, etc. Much of this data is extremely valuable to determine or refute the claim that someone was remotely connected to the computer controlling its activity and therefore the suspect/defendant is innocent. It becomes extremely difficult (not impossible) to refute these claims if volatile data is not collected.

Will Change Evidence – Many use the argument that collection of volatile data will change/alter the current state of the evidence as the investigator found it and thereby make it inadmissible as evidence. This is simply NOT true. To the contrary. Not collecting volatile data is beginning to be seen by the courts as the incident responder intentionally destroying 3 gig of potentially exculpatory evidence (assuming the computer has 3 gig of ram).

So when you consider the legal challenges in defeating the Trojan defense or the SODDI defense (some other dude did it) the return far outweighs risk of the loss of data.

Soon to be standard for all live response.

There is currently no method to write block memory. For this reason, we obviously have to image RAM and collect Volatile data without a write block.

Now some might be saying that you will make changes to the system and won't this invalidate your evidence? NO.

As long as you can document your actions and what changes you caused, your evidence is still admissible and valid. As a matter of fact, the Department of Justice and some courts today are beginning to view the failure to collect RAM and Volatile data as the incident responder destroying potentially exculpatory evidence. Again, this goes back to the SODDI (Some Other Dude Did It) defense of a remote administrative utility being used to control the computer.

After memory acquisition, you can now make further assessments of the system to determine if it is safe to shut the system down and apply a write block. We will discuss some of the various types of write blocks later.

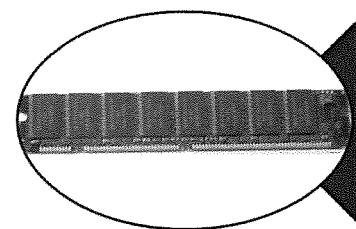
Incident responders responding to computer intrusions/hacks have for a long time now understood the need for conducting onsite triage. That is, immediately looking for specific items needed to immediately further your investigation. This tactic is now being recognized as critically useful in non-intrusion related investigations. Before conducting any further activity, you should apply a write block.

Triage's greatest benefits are the immediate identification of investigative leads.

The second benefit, particularly to responding law enforcement, is the ability to immediately confront a suspect and with the benefit of specific incriminating information obtained by the triage the likelihood of a confession is greatly increased.

After a triage, with the write block still attached you can initiate your physical or logical image of the drive.

Forensic Imaging Overview



Memory
Acquisition/Analysis



FTK Imager Device
Acquisition

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

This page intentionally left blank.

Why Collect System Memory

- What is in memory and why should we acquire it?
 - Processes
 - Network Connections
 - Open Files
 - Configuration Parameters
 - Encryption Keys -> Bit locker
 - Memory-only exploits/root kit technology

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

What is sitting in memory? 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 websites that the user surfed to. You might find residue from exited processes. And probably most importantly, you will likely have passwords for both encryption and other programs in clear text still sitting in memory.

With the increased use of encryption, particularly whole disk encryption utilities like Windows Bit locker, PGP and True Crypt, it is more important now than ever before for incident responders to image RAM and collect volatile data on any powered-on system they respond to. While it is the most volatile piece of evidence, it is also one of the most valuable.

In most cases, programmers will not obfuscate or encrypt these sensitive areas in memory. It will be merely sitting there in plain text. However, there won't be ASCII art surrounding it stating that "THIS IS THE PASSWORD", the string would exist though.

FOR508 should be the next course you take. There you will delve deeper into this advanced forensic technique and actually collect and analyze RAM and volatile data.

Encryption Keys -> Bit locker

(<http://jessekornblum.com/research/presentations/practical-cryptographic-key-recovery.pdf>)

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.

Tools for Memory Acquisition

FTK Imager

- By AccessData



dumpit.exe

- By Matthieu Suiche - MoonSols



Memoryze/Redline

- By Mandiant
- Acquire/Analyze physical memory (RAM)
- Compatible with Windows
XP/2003/VISTA/2008/Win7/2012/Win8



Windows Digital Forensics and Advanced Data Triage © 2014 SANS

There are currently a few tools available for memory acquisition. F-Response comes as both a USB human interface device (HID) that is inserted into the computer you want to acquire memory from or an application that is executed on the machine. RAM will show up as a physical drive on the examiner machine. The incident responder can then use any forensic imaging tool of their choice to image the RAM just as they would normally image a hard drive.

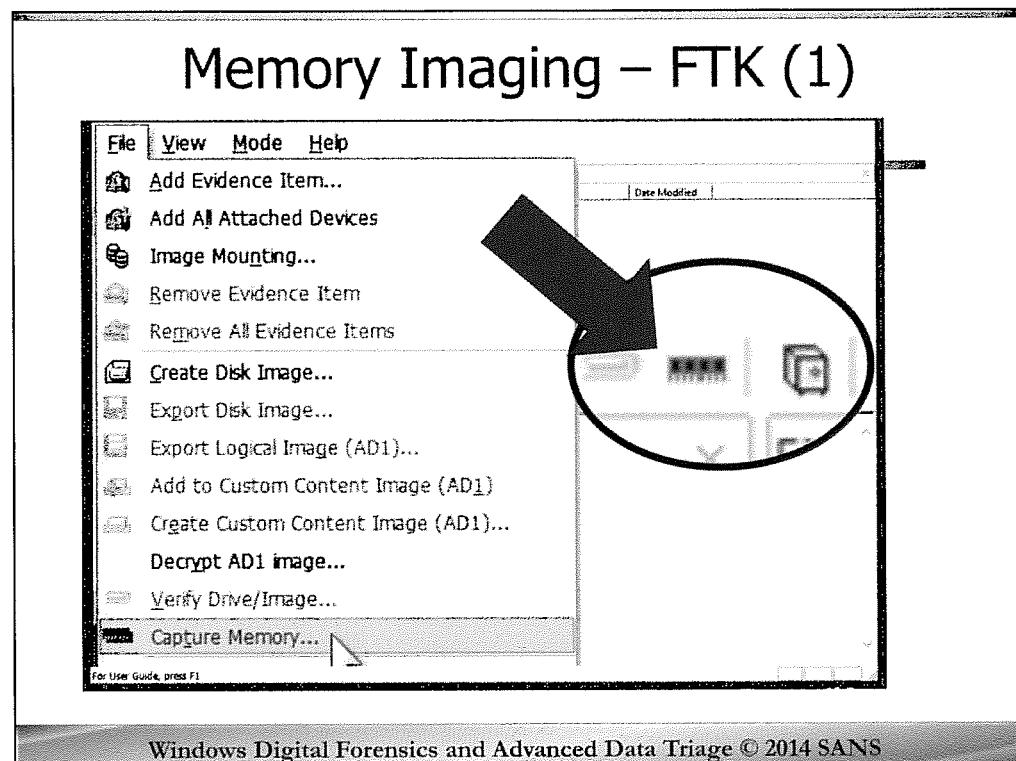
Access Data's FTK Imager is a free tool that is probably one of the most diverse in its capabilities.

During the RAM imaging process, FTK Imager will provide the option to also capture the Windows pagefile

Dumpit.exe is a standalone executable created by Matthieu Suiche that has one function; to create an image of Random Access Memory on any Windows 32 or 64 bit system.

Memorize is another free memory forensic software that can acquire including the paging file.

Ref: <http://www.moonsols.com/ressources/>



FTK Imager supports Random Access Memory (RAM) Acquisition and allows the capture of contents of the local machine's RAM to a file in a user-specified location. 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 (Win Vista/7/8 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.

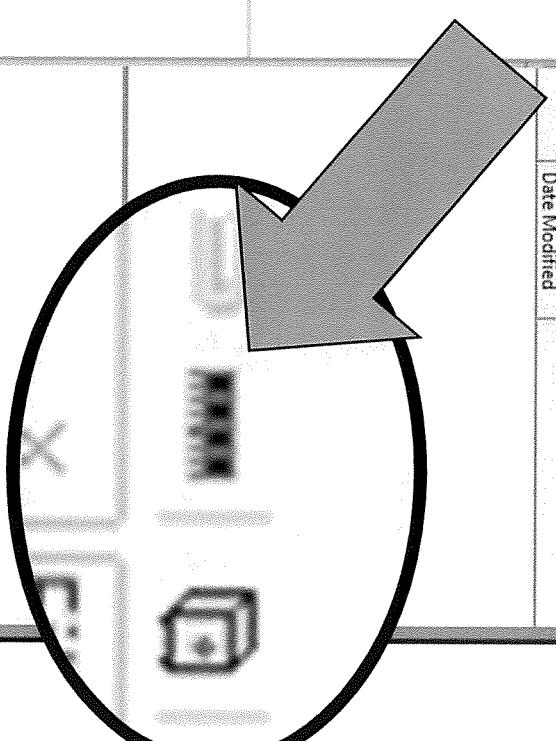
2

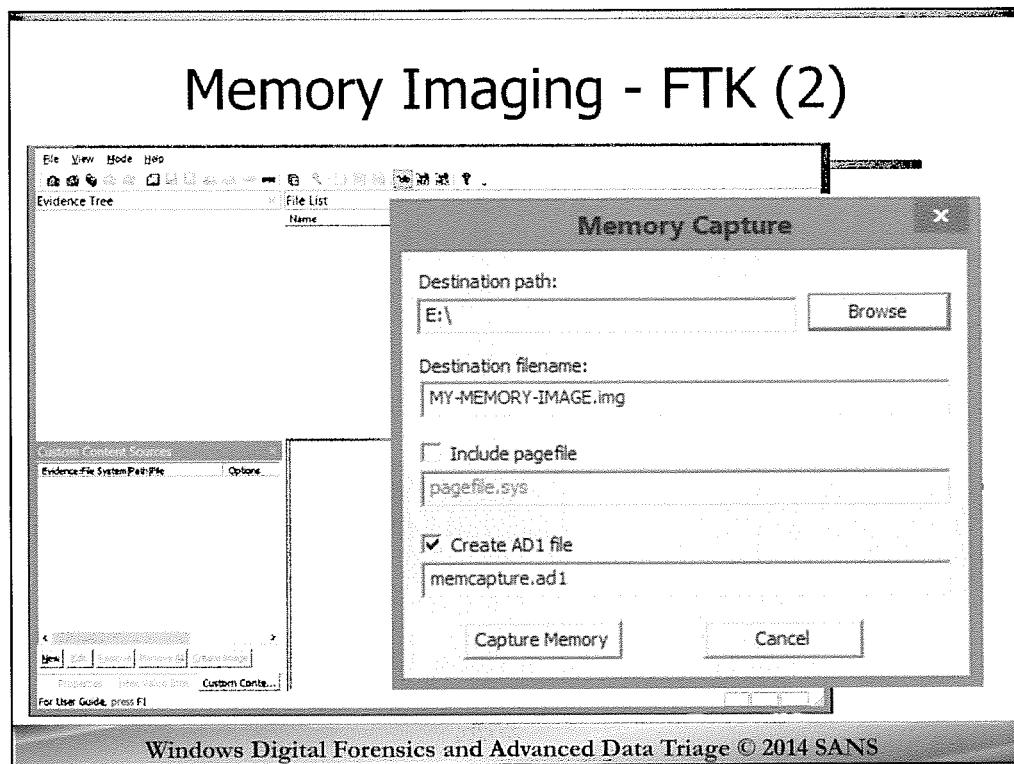
AccessData FTK Imager 3.1.4.8

- □ ×

FileViewModeHelp Add Evidence Item... Add All Attached Devices Image Mounting... Remove Evidence Item Remove All Evidence Items Create Disk Image... Export Disk Image... Export Logical Image (AD1)... Add to Custom Content Image (AD1) Create Custom Content Image (AD1) Decrypt AD1 image... Verify Drive/Image... Capture Memory...

For User Guide, press F1





With the Memory Capture dialog box open, select the “Browse” button to enter a location to create your memory image. When you image memory, you generally want to avoid exporting memory to the host system for a variety of reasons, including that you would be overwriting unallocated space with your memory image file, (destroying your ability to recover files in that portion of unallocated space). It is usually best to export memory to another networked machine or your attached sanitized USB device FTK Imager is running from, provided your USB device has sufficient storage capacity.

Is it possible to create a HASH of memory before and after imaging, like when imaging hard drives, to verify the memory captured was the same as it was on the system?

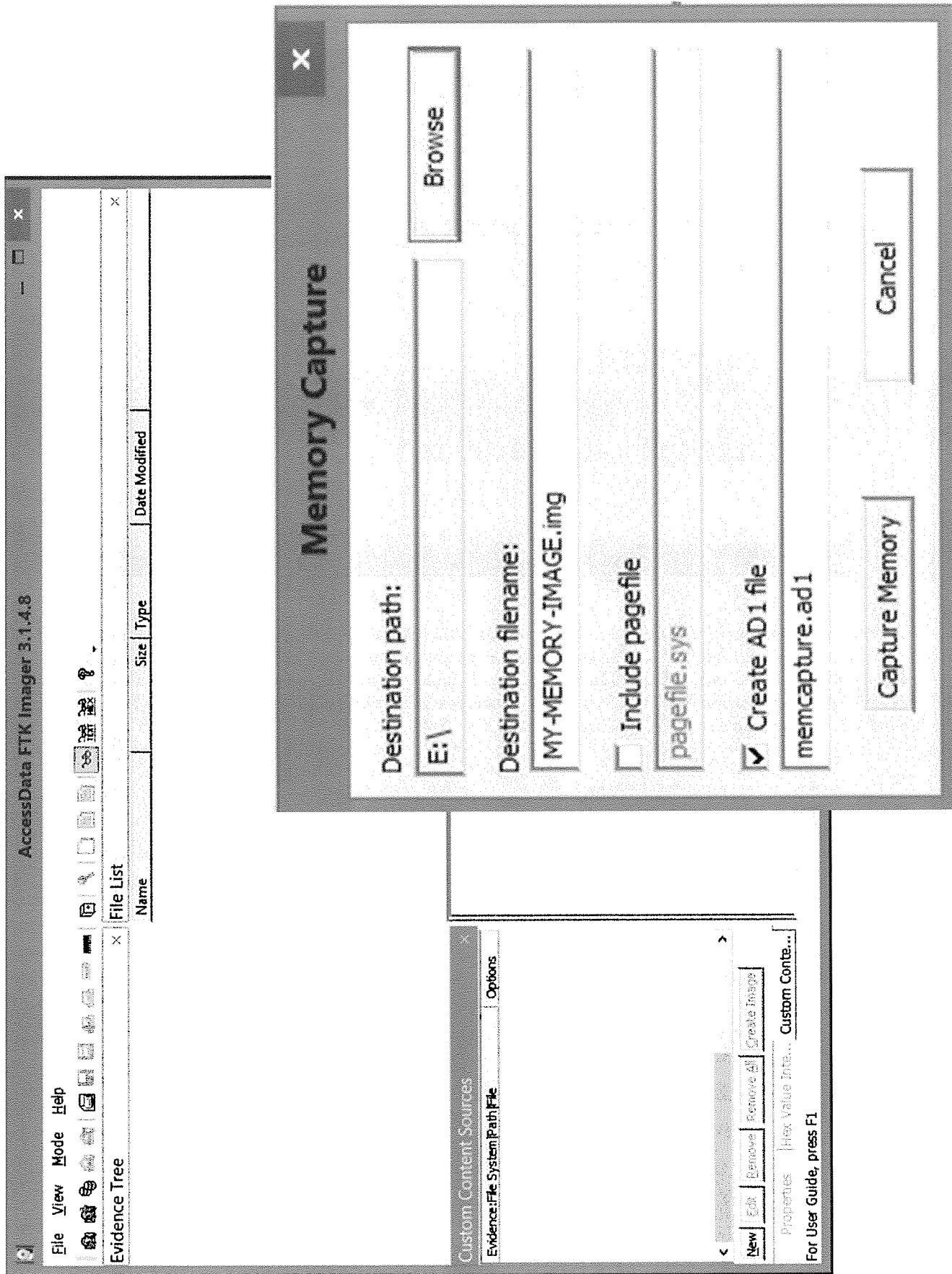
ANSWER: No. RAM is dynamically changing as you are capturing it, therefore, by the time you obtained a HASH, RAM would have changed and you could never obtain the same HASH again. We will discuss in a moment a possible mitigation strategy.

Save the file to your USB Key, name it MY-MEMORY-IMAGE.img, save this file till you need it later. After you save it to your USB key, transfer the file to your c:\cases\memory directory on your Windows SIFT Workstation.

FTK Imager also gives you the opportunity to Image the Pagefile.sys at the same time. The pagefile.sys is one of the memory-management scheme Microsoft uses to store frames from memory on your local hard drive. For forensic investigators, this is a common place we can find a variety of artifacts, from web surfing activity to encryption keys. Because pagefile.sys is saved on the local hard drive it may not be considered critical to capture immediately; however, because this is a dynamic file, it is a consideration for capturing before shutting down a live system.

We just discussed the challenge of verifying and authenticating the captured image of RAM. Because it is impossible to obtain a matching HASH of RAM from before and after capturing it, FTK Imager offers the ability to immediately image the copy of memory you just captured. It creates this second image in AccessData's proprietary image format known as AD1. The two advantages of doing this is that when creating an AD1 image of memory, FTK Imager also creates an audit log, complete with hashes. The second advantage is it compresses the original image of RAM (which is generally the same size as the amount of RAM imaged). In several test cases, the AD1 image of RAM was approximately one quarter the size of the original image.

Lastly, Select “Capture Memory” to start the memory capture.



Memory Imaging – Dumpit (1)

- Dumpit.exe – Command line executable
- Single purpose
- Capture to location executed



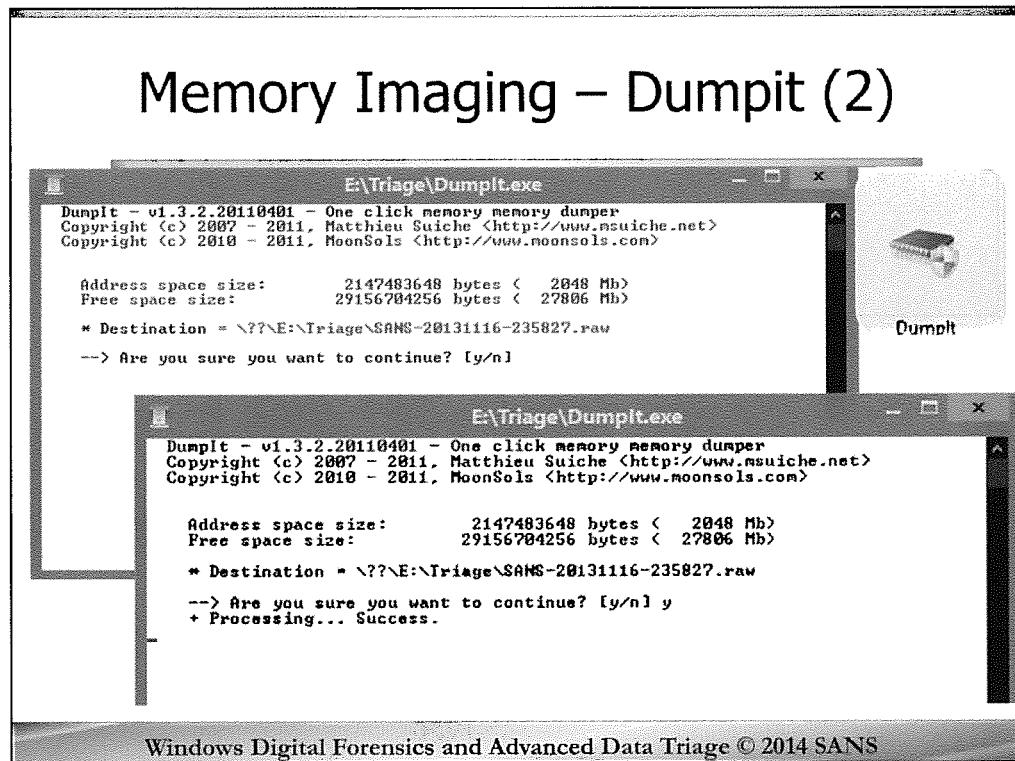
Windows Digital Forensics and Advanced Data Triage © 2014 SANS

One of the newest memory imaging tools was released by Matthieu Suiche. Dumpit.exe is a fusion of two of his previous tools, Win32dd and Win64dd and is designed to acquire a physical memory dump of both x86 (32-bits) and x64 (64-bits) Windows machines. The raw memory dump is generated in the same directory Dumpit.exe is executed from, which makes it ideal to deploy on a USB key or drive. Only a confirmation question is prompted before Dumpit.exe starts dumping memory.

Perfect to deploy the executable on USB keys, for quick incident response needs.

Reference:

<http://www.moonsols.com/resources>



To be prepared to respond at any time, I recommend keeping a sanitized 32 gigabyte USB drive with dumpit.exe, FTK Imager and a few other of your favorite incident response tools in a triage directory. Why 32G of RAM? This gives you the storage to potentially respond to more than one machine.

When you launch Dumpit you will see the destination directory where memory will be copied, then you will be offered one question, “**→ Are you sure you want to continue? [y/n]**”

Selecting the letter “y” will initiate the capture of RAM. Selecting “n” will terminate the dumpit program.

I have heard some suggest the reason they do not image RAM is either “it takes too long” or “I don’t need to worry about it, this is a <fraud case/child porn case/IP case>”.

I conducted several tests imaging RAM of a virtual machine with 8 G of RAM using Dumpit from an attached USB drive. Imaging to the local hard drive inside the virtual machine, 8 G of RAM took approximately :45 seconds. Imaging to an attached USB 2.0 USB drive the capture of RAM took 26 minutes. You can further reduce your imaging time by using a destination with higher throughput, such as USB 3. Additionally, if using USB, remember that all USB storage devices are not created equal. There are varying qualities of USB memory that have faster read and write times. While writing this document a review of USBFlashSpeed.com lists a Kingston DT HyperX 3.0 drive as having 186 MB/s write speed and 244 MB/s read speed, thereby theoretically reducing your 8G RAM image time to under a minute.

As for the second belief that RAM is not important, just remember two things. First, the person being accused of the crime can suggest to the court or the decision maker that the evidence that would prove them innocent, the evidence of remote control by someone other than the accused was intentionally deleted by the incident responder and second, the facts that the incident responder arrived on scene then made a conscious choice to

destroy evidence that was otherwise available to them is irrefutable. Regardless if the claims of SODDI (some other dude did it) are plausible, you cannot deny that evidence that was available to you when you arrived on scene was deliberately deleted/destroyed by you. In either case, it is better to spend the extra 20 minutes or so imaging RAM than potentially lose a case or have your credibility damaged by allegations of intentional destruction of evidence.

Reference:

<http://usbflashspeed.com> – Fastest USB Devices

http://en.wikipedia.org/wiki/USB_flash_drive#File_transfer_speeds

<http://usbspeed.nirsoft.net>

The image shows two windows side-by-side, both titled "E:\Triage\DumpIt.exe".

Left Window:

```
DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright <c> 2007 - 2011, Matthieu Suiche <http://www.msanche.net>
Copyright <c> 2010 - 2011, MoonSols <http://www.moonsols.com>

Address space size: 2147483648 bytes ( 2048 Mb)
Free space size: 29156704256 bytes ( 27806 Mb)

* Destination = \??\E:\Triage\SANS-20131116-235827.raw

--> Are you sure you want to continue? [y/n]
```

Right Window:

```
DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright <c> 2007 - 2011, Matthieu Suiche <http://www.msanche.net>
Copyright <c> 2010 - 2011, MoonSols <http://www.moonsols.com>

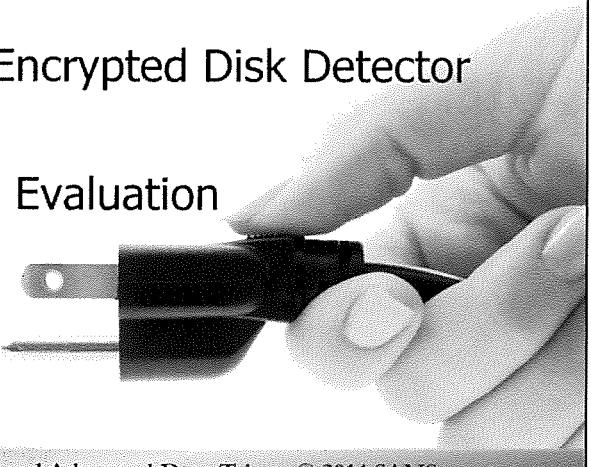
Address space size: 2147483648 bytes ( 2048 Mb)
Free space size: 29156704256 bytes ( 27806 Mb)

* Destination = \??\E:\Triage\SANS-20131116-235827.raw

--> Are you sure you want to continue? [y/n] y
+ Processing... Success.
```

One More Thing

- Evidence Encryption?
- Magnet Forensics Encrypted Disk Detector
- Live Logical Image Evaluation



Windows Digital Forensics and Advanced Data Triage © 2014 SANS

So you have imaged RAM and some of you may be thinking because you have collected the volatile data, it is time to pull the power plug.

There are two last things you should consider before pulling the plug.

First, is there anything that suggests the device may be using any encryption? Is there perhaps an encrypted folder/volume that is currently mounted and once you pull the power, you may not have access to the contents of that folder/volume?

What if the drive is full disk encrypted?

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 there were indications the drive was encrypted, 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.

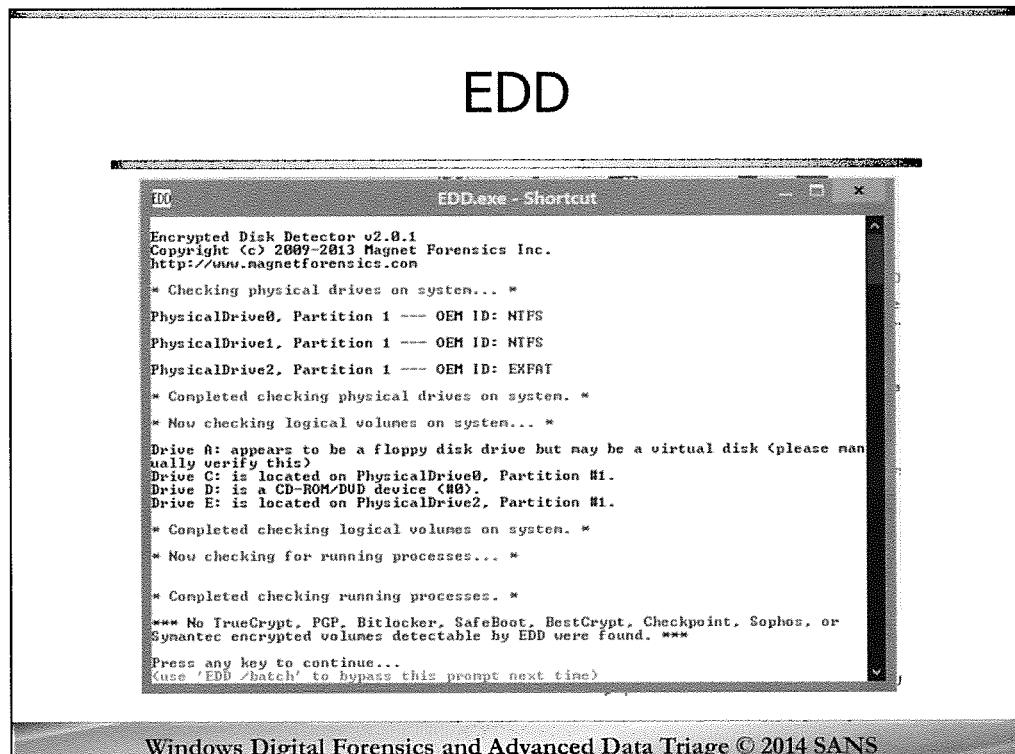
Remember, never make assumptions that a drive might not be encrypted... ALWAYS CHECK.

We will check for encryption using a tool called EDD found on your DVD under the D:\forensic-tools\edd - encrypted disk detector\edd.exe. This encrypted disk detector tool is also available at the Magnet Forensics website.

RIGHT-CLICK and RUN AS ADMINISTRATOR.

Ref:

<http://info.magnetforensics.com/encrypted-disk-detector>



Encrypted Disk Detector (EDD) is a command-line tool that checks the local physical drives on a system for TrueCrypt, PGP®, Bitlocker®, Safeboot, BestCrypt, Checkpoint, Sophos, or Symantec 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.

The newest version of EDD has added a splash screen asking for you to accept the End User License Agreement (EULA). You can create a shortcut to the EDD.exe with the /accepteula switch to bypass this EULA.

e.g. edd.exe /accepteula

Reference: <http://info.magnetforensics.com/encrypted-disk-detector>

EDD

EDD.exe - Shortcut

Encrypted Disk Detector v2.0.1
Copyright (c) 2009-2013 Magnet Forensics Inc.
<http://www.magnetforensics.com>

- * Checking physical drives on system... *
 - PhysicalDrive0. Partition 1 --- OEM ID: NTFS
 - PhysicalDrive1. Partition 1 --- OEM ID: NTFS
 - PhysicalDrive2. Partition 1 --- OEM ID: EXFAT
 - * Completed checking physical drives on system. *
 - * Now checking logical volumes on system... *
 - Drive A: appears to be a floppy disk drive but may be a virtual disk (please manually verify this)
 - Drive C: is located on PhysicalDrive0. Partition #1.
 - Drive D: is a CD-ROM/DVD device (#0).
 - Drive E: is located on PhysicalDrive2. Partition #1.
 - * Completed checking logical volumes on system. *
 - * Now checking for running processes... *
 - * Completed checking running processes. *
- *** No TrueCrypt, PGP BitLocker, SafeBoot, BestCrypt, Checkpoint, Sophos, or Symantec encrypted volumes detectable by EDD were found. ***
- Press any key to continue... this prompt next time> (use 'EDD /batch' to bypass this prompt next time)

Analyzing Memory Images

- Data Carving / String Searching
 - Recover Images/Files based on headers and keywords
 - FTK (Day 2 408)
 - Internet Evidence Finder (IEF – Day 4 408)
 - Chat Sessions
 - Internet History
 - Web E-mail
- Memory Analysis
 - Memoryze/Redline (Day 2 FOR508)
 - MANDIANT (www.mandiant.com)
 - Volatility (Day 2 FOR508)
 - In Downloadable Linux SIFT Workstation (Ubuntu Based)
 - <http://computer-forensics.sans.org>
 - HBGary Responder
- Recover Encryption Keys
 - Bitlocker/Truecrypt
 - Passware Kit (<http://lostpassword.com>)

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

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.

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.

FTK Imager – Advanced Techniques

RAM Acquisition

Registry Extraction

Creating Custom Content Images

Triage Based Forensics – Fast Forensic Acquisition

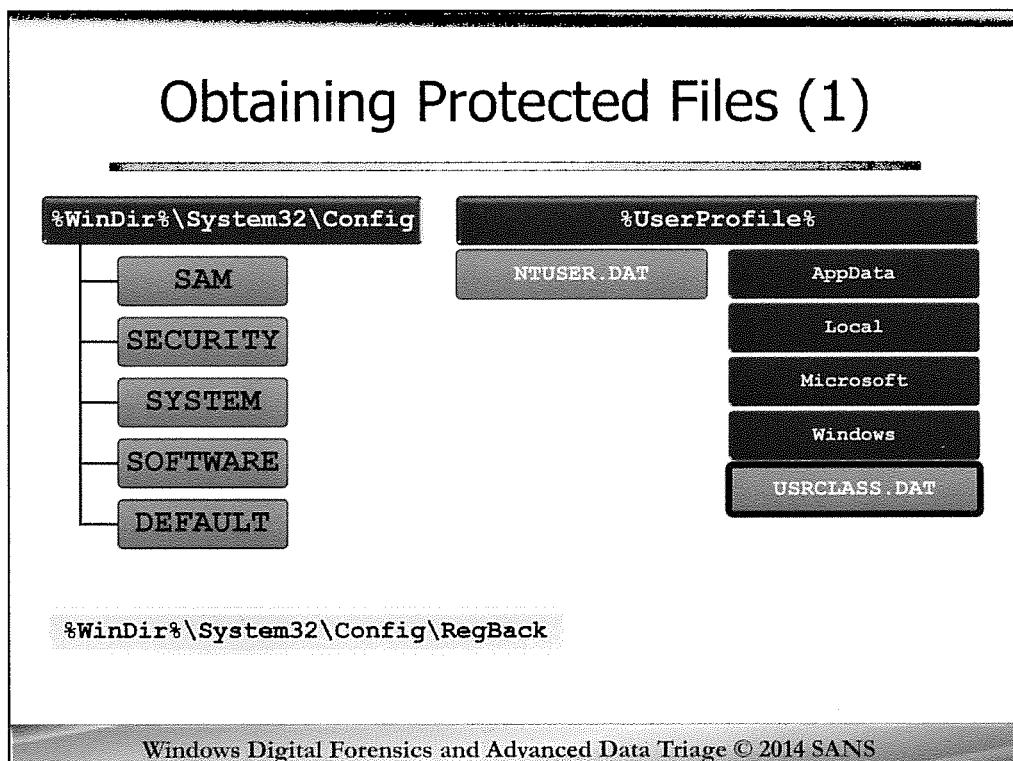
Windows Digital Forensics and Advanced Data Triage © 2014 SANS

RAM Acquisition

Registry Extraction

Creating Custom Content Images

Triage Based Forensics – Fast Forensic Acquisition



FTK Imager also provides you the ability to easily extract most of the 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.

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?

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. A password injection attack on original evidence to blank the password may forever deny you the ability to access EFS encrypted files.

The NTUSER.dat hive contains all the keys related to the specific user. It is found on your system at %UserProfile%.

There is an additional hive on Vista and Windows 7/8 machines that was created located at **C:\Users\<username>\AppData\Local\Microsoft\Windows\UsrClass.dat**. This hive is very important because it contains some key information regarding additional program execution information and will give us the ability to tell which folders a user has opened or closed. Additionally, on Windows 7/8, the registry is backed up every 10 days to %WinDir%\System32\Config\RegBack. We will discuss later how you can grab all these and other significant artifacts.

As mentioned before, FTK Imager will grab the core registry hives and each users NTUser.dat hive. Great, so we now know a couple of reasons why we might want to collect the registry. Let's use FTK Imager to see how easy it is to extract the core registry hives.

%WinDir%\System32\Config

SAM

SECURITY

SYSTEM

SOFTWARE

DEFAULT

%UserProfile%

NUSER.DAT

AppData

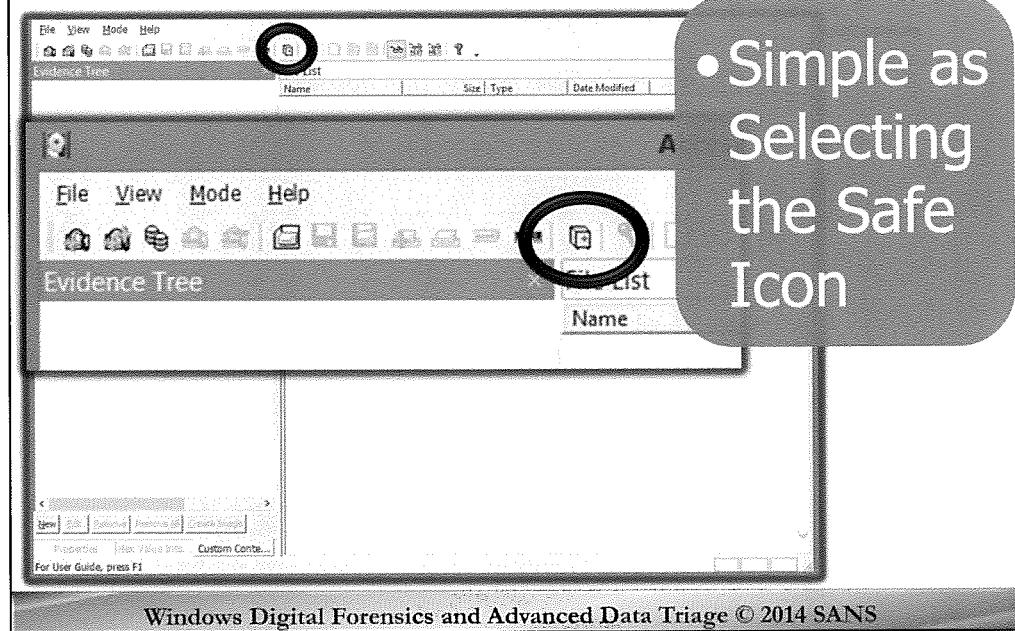
Local

Microsoft

Windows

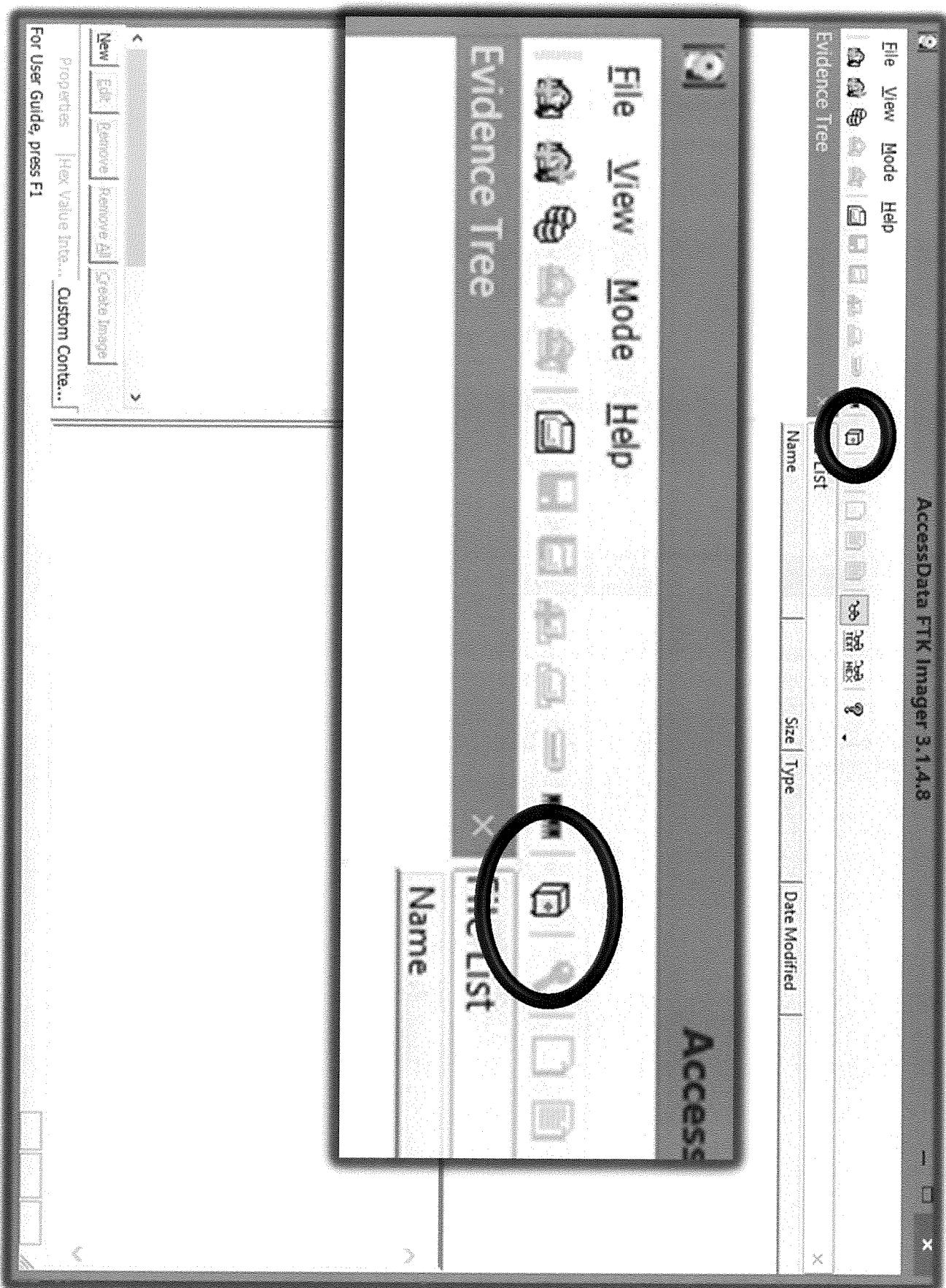
USRCLASS.DAT

Obtaining Protected Files (2)

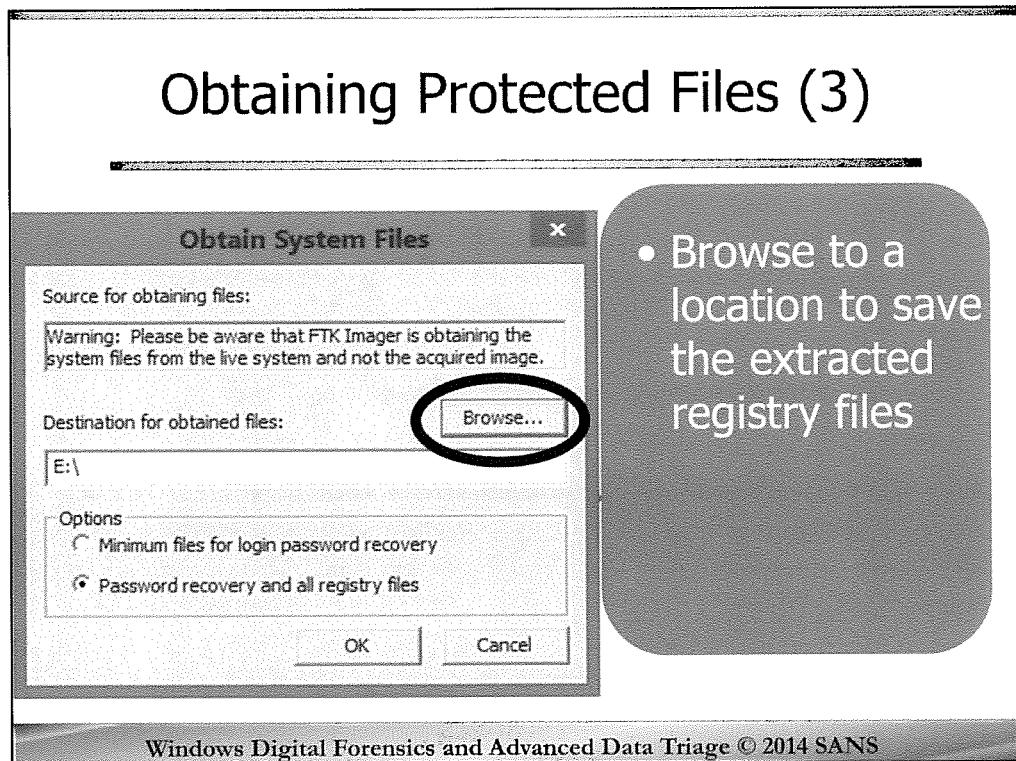


To obtain the protected registry files using FTK Imager, you would insert your thumb drive containing FTK Imager Lite on a running Windows system. From the thumb drive you would launch FTK Imager Lite.

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.

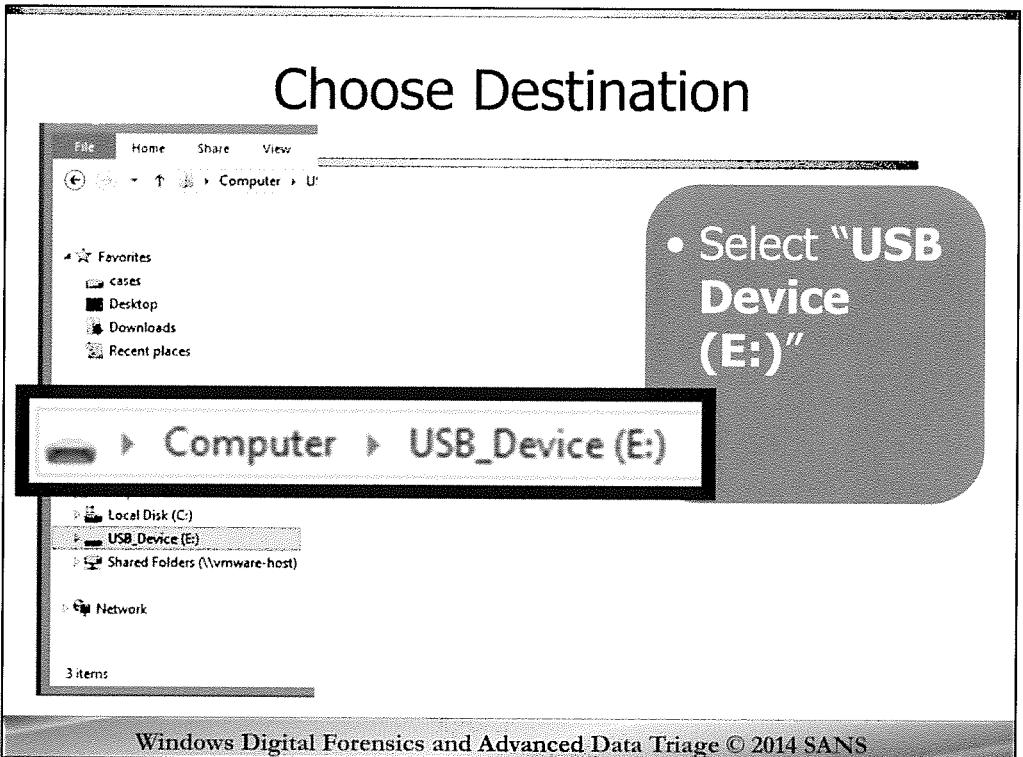


Obtaining Protected Files (3)

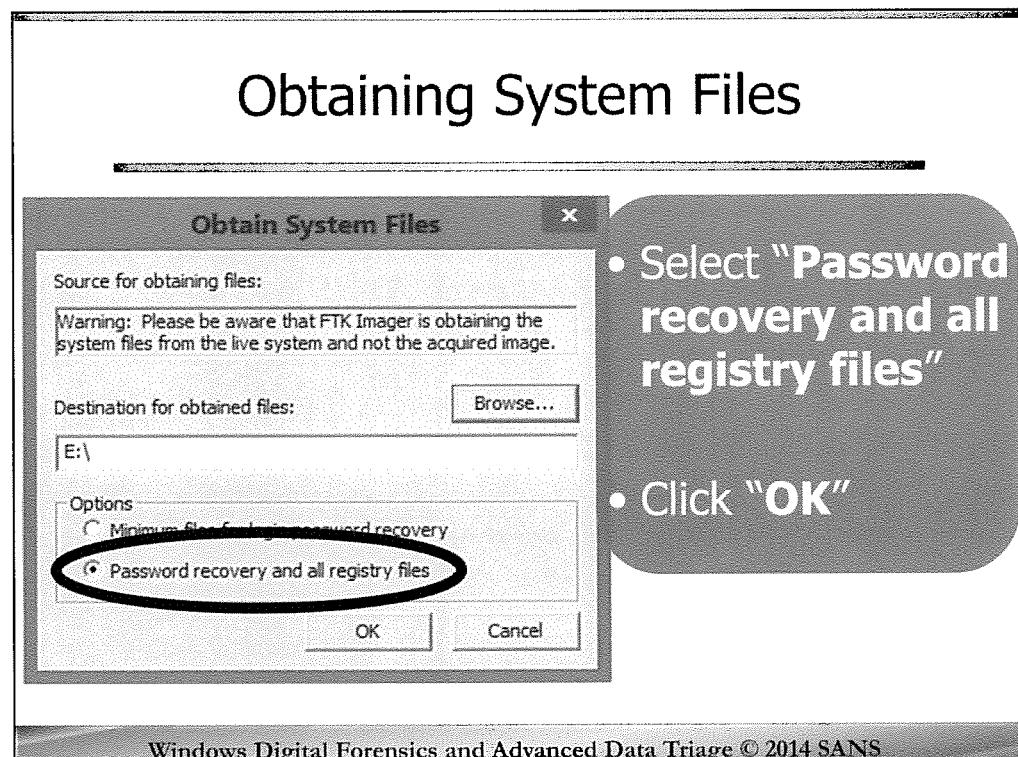


- Browse to a location to save the extracted registry files

As we have already discussed in class, every effort should be made to minimize the changes to the system so you would not want to export and save the registry hives to the victim system.
Select the “**Browse...**” button to navigate to the destination directory you want to save the registry files (a network drive or USB thumb drive, etc.).



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 USB Device you brought with you. Again, remember that the only rule on this is that you would never save or export a file anywhere on the subject's 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, if necessary, to stick your thumb drive into the running computer system, extract the registry files, then assess the system to determine if it is safe to shut the system down.



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

If you only want to crack the password file, all you have to do is accept the default “**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**”, 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.

Selecting “**OK**” and FTK Imager exports the selected files to the designated location.

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

Obtaining Protected Files (1)

Name	Date modified	Type	Size
Users	11/19/2013 11:05 ...	File folder	
default	11/18/2013 1:23 AM	File	512 KB
SAM	11/18/2013 1:23 AM	File	256 KB
SECURITY	11/18/2013 1:23 AM	File	256 KB
software	11/18/2013 1:23 AM	File	55,552 KB
system	11/18/2013 1:23 AM	File	10,240 KB

Name	Date modified	Type
All Users	11/19/2013 11:05 AM	File folder

Name	Date modified	Type	Size
Crypto	11/19/2013 11:05 ...	File folder	
Protect	11/19/2013 11:05 ...	File folder	
NTUSER.DAT	11/18/2013 1:23 AM	DAT File	1,280 KB

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

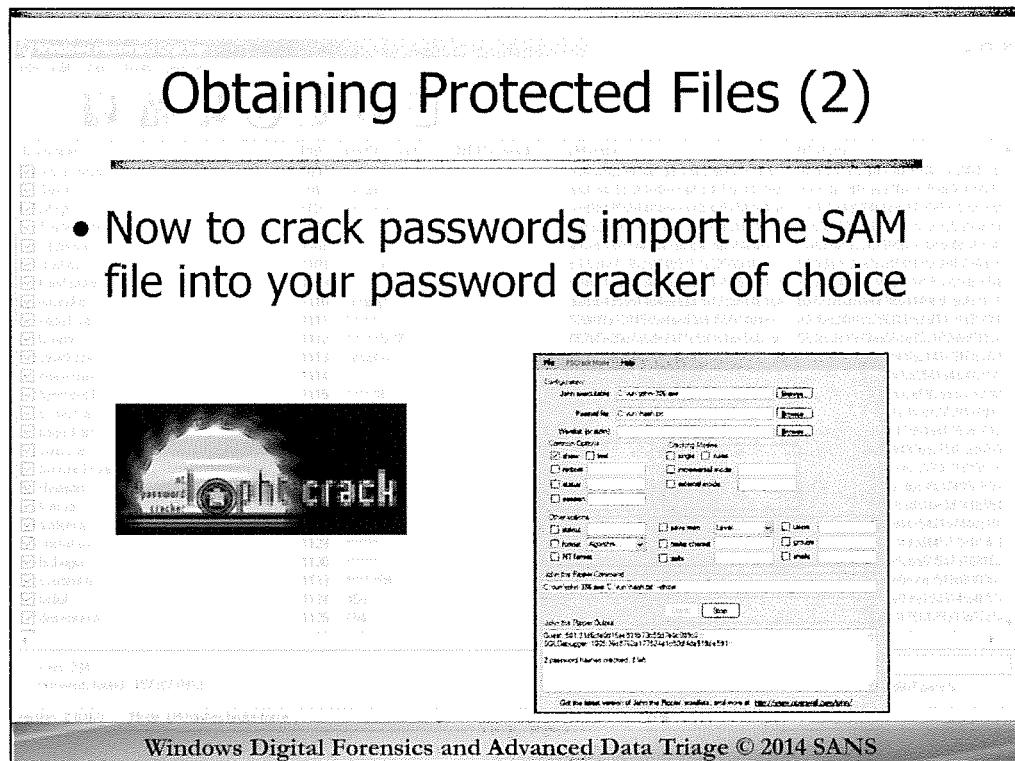
- All registry hives are extracted
- NTUser.dat hive from each user account extracted

Navigating to the location you exported the registry hives 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 primary registry hives, 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, 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.

FTK Imager – Advanced Techniques

RAM Acquisition

Registry Extraction

Triage Based Forensics – Fast Forensic Acquisition

Creating Custom Content Images

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

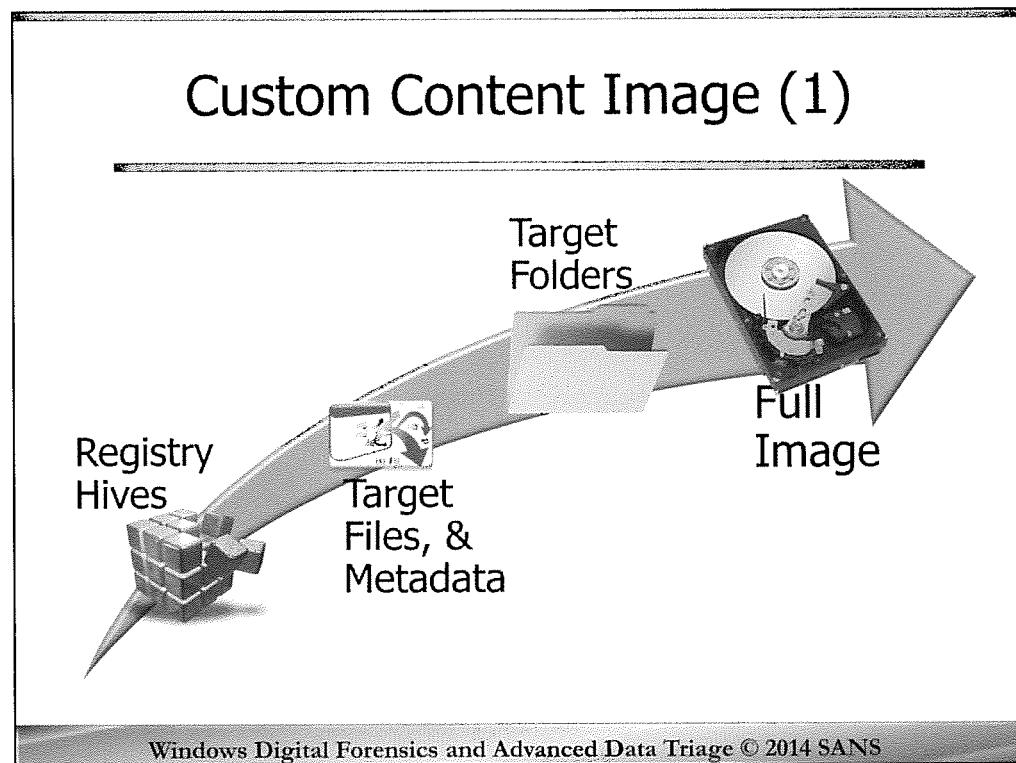
Computer Forensics Primer

SIFT Kit Essentials

Forensic Investigation Methodology

Evidence Fundamentals

Evidence Acquisition



There are many instances where a speedy triage is needed or you need to capture and preserve critical files with all their associated metadata to later prove access, knowledge or control of a file.

As the capacity of hard drives increase, the challenge for incident responders to identify actionable information quickly increases. While most in the forensic community recognize the risk of not imaging the entire hard drive, there are two forces working against us that may result in the end of full drive imaging (let's hope not). The first is the size of the data and the courts who are increasingly becoming more uncomfortable with what can be interpreted as an over collection and subsequent invasion of privacy. Some courts have already taken a strong stance with respect to e-mail servers, requiring the government to seize only e-mails of the target of the investigation rather than the entire mail server.

Imaging an entire file server of a business has also become the exception rather than the rule. Surgically preserving only specific files or folders has also become the norm when investigating only specific individuals in a large business. The days of imaging an entire file server of a business are nearly gone. In such a situation most incident responders identify the permission the target of the investigation has and selectively image those folders.

In some situations, all that may be needed is seizing individual files or folders off a system. Most forensicators know that logically copying the files or folders off of the system onto a thumb drive or other sanitized media is not sufficient, as it would change among other things the file timestamps. One option might be to use forensic tools (a forensic write block and FTK Imager) to create an image of the file(s) in question.

With this phased approach to imaging in mind, combined with the need for rapid analysis, you may not want to initiate a full disk image immediately. In these situations a custom content image may be the perfect solution.

QUESTION: On an NTFS formatted file system; if you did use your hardware write block and FTK Imager to create a custom Content Image, Would all the file integrity be maintained?

ANSWER: The process of creating a custom content image would maintain the integrity of the file “contents” and the file timestamps, but what about the file ownership permissions?

QUESTION: Does proving a file was present on a hard drive do anything toward proving the file was accessed by a user of the computer?

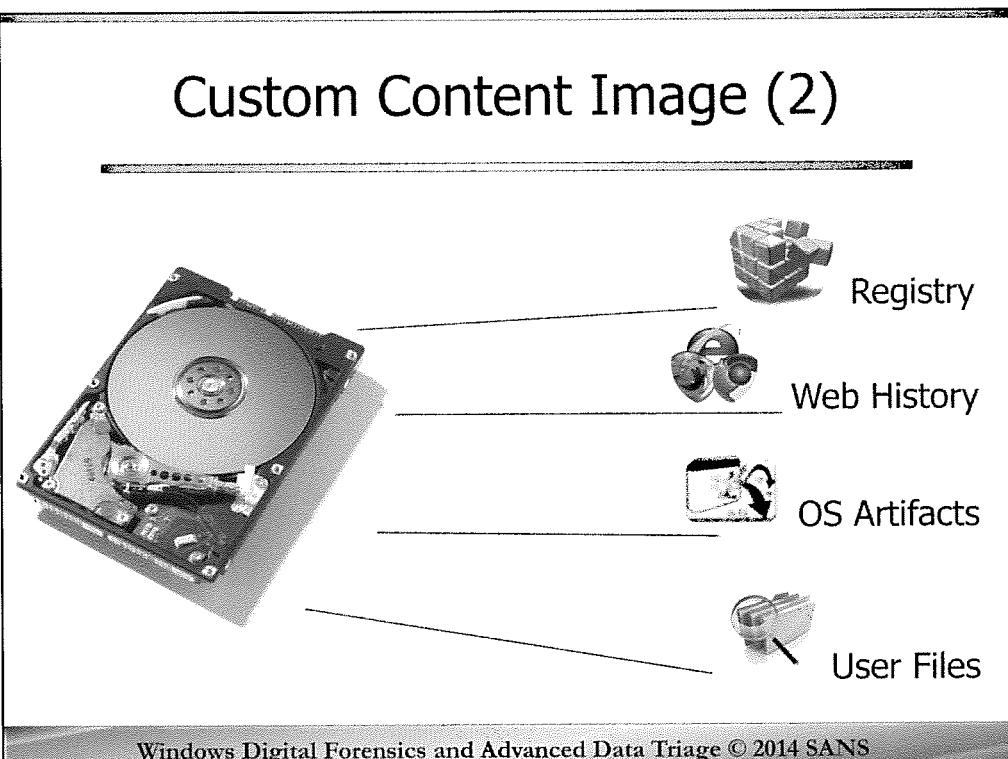
ANSWER: No. Additional forensic artifacts are needed to suggest a user of the computer had accessed the file. We will be discussing in depth throughout this course many of the forensic artifacts that can help demonstrate a file was accessed, when it was accessed, how many times and more.

The NTFS file system consists of several system (metadata) files such as \$MFT — Master File Table, \$Bitmap, \$LogFile and others, which contains information about all the files and folders on the NTFS volume. We need to keep this in mind when not imaging the entire drive and instead targeting specific files or creating a triage image.

Ref:

http://www.ntfs.com/ntfs_basics.htm

Custom Content Image (2)



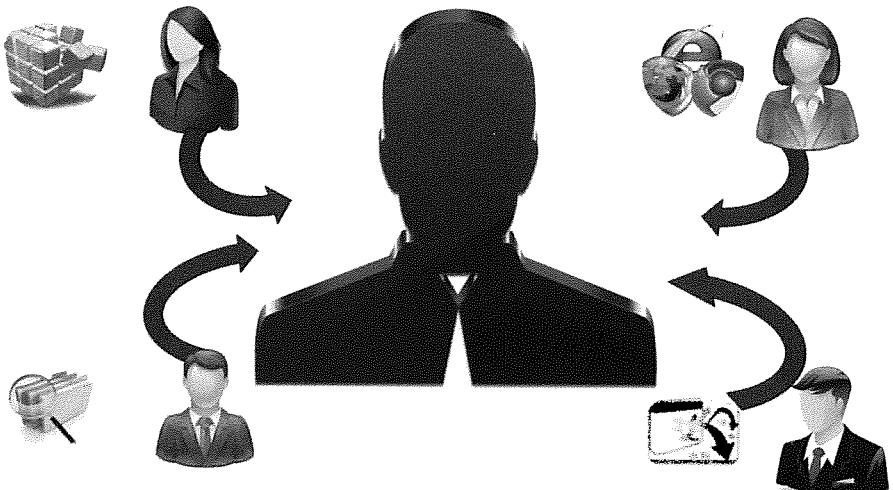
Let's assume you have a high priority case and a suspect computer with a 1-terabyte drive. Time is of the essence and you need to identify actionable information as quickly as possible. Imaging the entire drive would take several hours, then loading the drive into your forensic software for indexing would take several more hours, potentially causing a bottleneck in your workflow of 20 or more hours before you could even start your analysis.

Even after imaging and indexing, one fatal mistake many in the forensic community make is assigning a single examiner to review terabytes of data. This is neither efficient nor wise, especially if somewhere in that mountain of data is a piece of digital evidence that could thwart a terrorist attack, rescue an abducted victim, or identify the location of additional evidence that was scheduled to be destroyed. If that search involved thousands of boxes of paper documents rather than electronic copies, we would not hesitate to commit additional people to the review. But in the world of digital evidence, we often are still relying on a single forensic examiner to review the entire contents of multiple hard drives.

The solution to the first problem of imaging the entire hard drive is imaging selected portions and artifacts, those areas we know are most likely to have the highest potential for the information we are looking for and the areas that contain some of our most valuable forensic artifacts to tell us what was happening on the computer.

By selecting only specific content, informed by the investigation and your knowledge of forensic artifacts, we can create an image of significantly fewer files resulting in a much smaller image. This smaller image can be created significantly faster and analysis can begin immediately.

Distributed = Faster

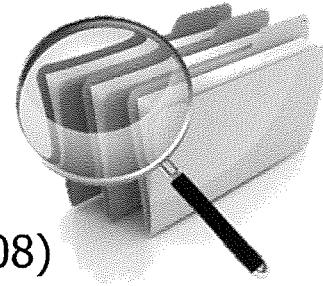


Windows Digital Forensics and Advanced Data Triage © 2014 SANS

The solution to the second problem is to use this distributed approach to analysis. In nearly every analysis of digital evidence, there are a series of actions that must be performed. With only one examiner, these actions happen in tandem. Depending on what you are looking for, first the examiner might triage the user's folders, then looks at specific windows artifacts, then examines several registry artifacts, perhaps next they will look at Internet history, and the list of tasks go on. Using a coordinated distributed and collaborative approach you can identify critical evidence faster. Separating the otherwise tandem tasks between examiners, each with a copy of the custom content image will result in identifying critical information faster.

What Content to Image

- Registry hives & backups (FOR408)
- Link files (FOR408)
- Jump lists (FOR408)
- Prefetch (FOR408)
- Event logs (FOR408)
- Master File Table (FOR408/508)
- Log files and Journal log (FOR508)
- Pagefile & Hibernation files (FOR508)



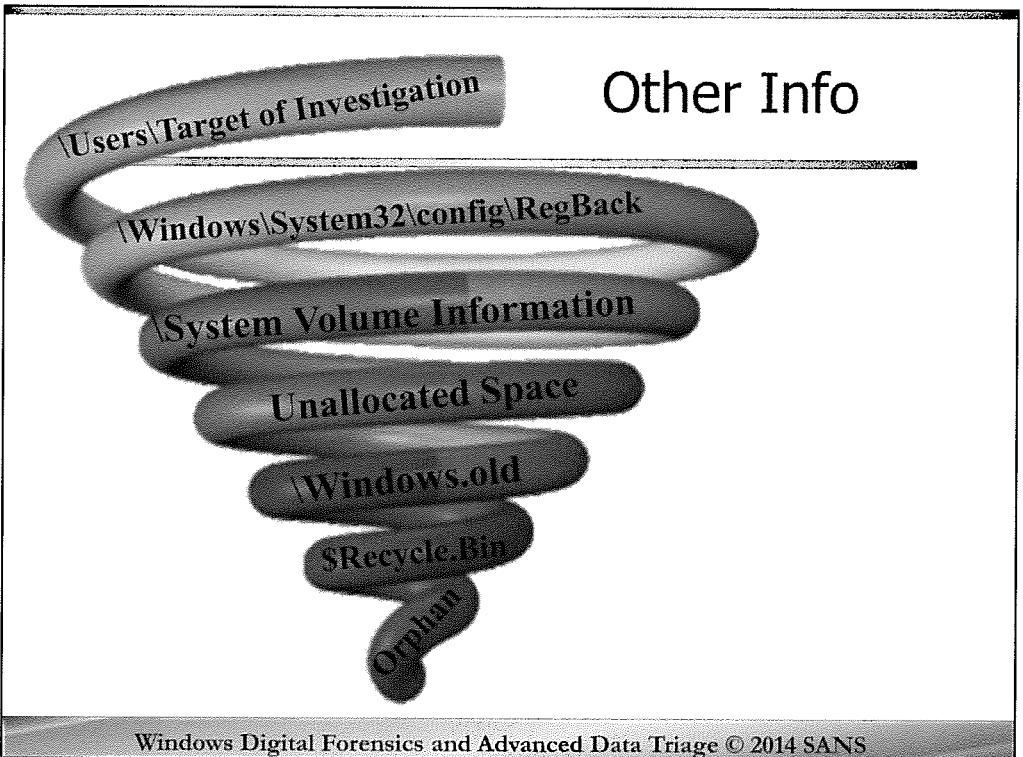
Windows Digital Forensics and Advanced Data Triage © 2014 SANS

So the million dollar question is what do we grab?

This is obviously based on the facts of your investigation but for nearly any custom content triage we would take the below listed files/artifacts. Using FTK Imager's Custom Content Creation feature (we will show you how to do this next) you can use wild cards to locate certain files by their file extension, regardless where they are on the drive.

- \$MFT – The master file table (Index of every file and folder on the system)
- \$LogFile and \$USN \$J (journal) file recording file activity (File open, close, creation, deletion)
- All registry hives and perhaps backup registry hives. Don't forget that using FTK Imager's "Obtain Protected File System" (safe icon), misses the USRCLASS.DAT hive in Win7/8 images.
 - SAM
 - SYSTEM
 - SOFTWARE
 - DEFAULT
 - NTUSER.DAT
 - USERCLASS.DAT
- *.evt – Event Logs by their file extension, located in the %WinDir%\System32\winevt\Logs folder
- *.lnk Files – All link files by extension .lnk
- *.pf – All prefetch files by extension .pf
- Pagefile.sys – The Windows Pagefile (an extension of RAM)
- Hiberfile.sys – The hibernation file is a compressed image of RAM the last time the system was placed into hibernation
- The RECENT Folder and sub folders that include jumplist (Win Vista/7/8)

Between FOR408 and FOR508 we have a lot of artifacts to cover. We list which course will cover, IN-DEPTH, the examination of that specific artifact for processing. That way it makes sense as to why we are obtaining it.



Windows Digital Forensics and Advanced Data Triage © 2014 SANS

With each file you add the size of your custom content image increases, so as with many things in digital investigative analysis, it is a judgment call. For our purposes in class, this is all we need to capture, however, based on your preview of the drive folder structure, you may also consider including the entire specific User folder and subfolders. This would capture web surfing cache, all user files stored in the default location, etc. The only caution for collecting the specific user's folder is that it can be large, depending on how many user files and web surfing they have cached, thus increasing the image creation time.

A quick file to grab if your preview reveals it contains any information is the "\$Recycle.Bin". The "System Volume Information" directory (depending on the OS version) may include system restore points, previous versions of the registry, and other data.

One last possible directory for inclusion on Windows 8 systems is the "Windows.old" directory. This directory is used when a System Reset or Restore has been performed and may be a gold mine of all previous user files.

In summary, what you include in your Custom Content image depends on the circumstances of the investigation and your triage analysis during a preview of the system. Just remember, the more files, the longer it is going to take to create the image.

\$Recycle.Bin
\System Volume Information
\Users\<target_of_investigation>
\Windows\System32\config\RegBack
\Windows.old
Unallocated Space
Orphan

\Users\Target of Investigation

\Windows\System32\config\RegBack

\System Volume Information

Unallocated Space

\Windows.old

\$Recycle.Bin

Orphan

FTK Imager – Advanced Techniques

RAM Acquisition

Registry Extraction

Triage Based Forensics – Fast Forensic Acquisition

Creating Custom Content Images

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

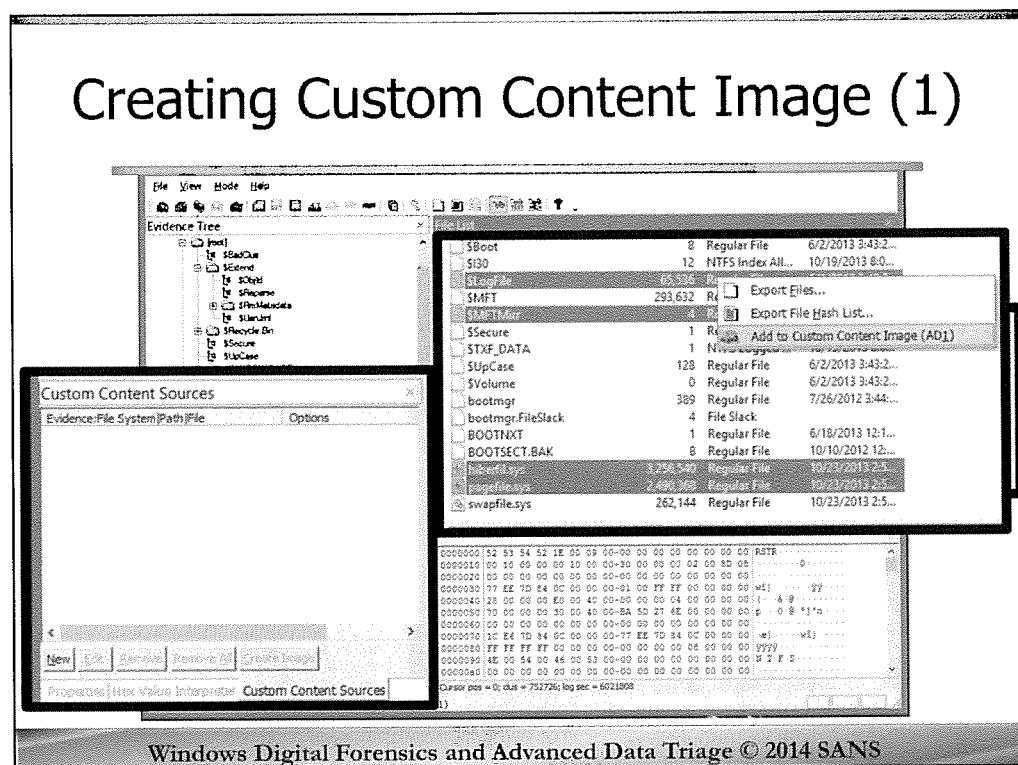
Computer Forensics Primer

SIFT Kit Essentials

Forensic Investigation Methodology

Evidence Fundamentals

Evidence Acquisition



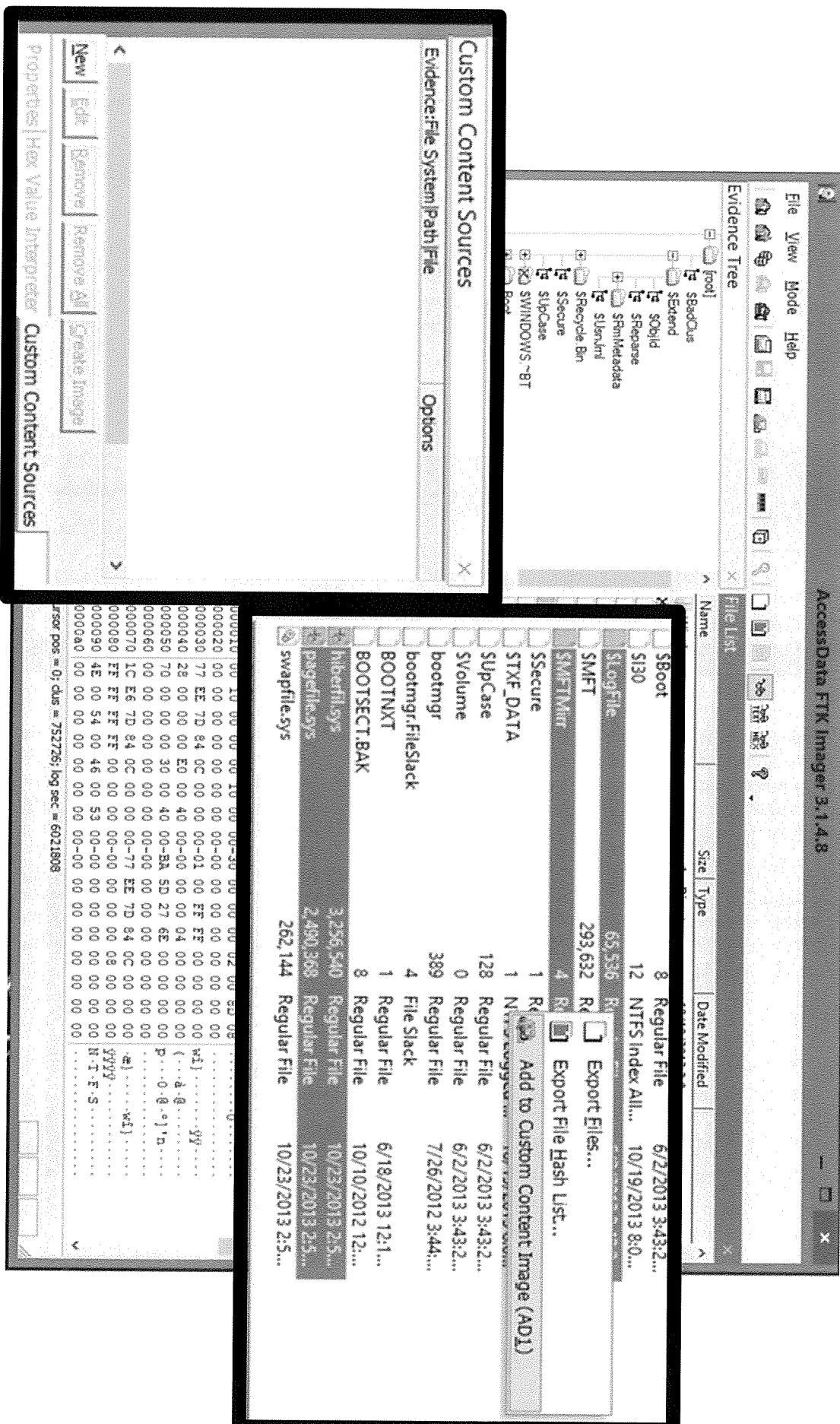
One of the least known features of FTK Imager is its ability to easily create custom content images. Custom content images contain only selected files, folders and file type based on file extension. You can create a custom content image from a live system, a dead system (attached to a write block), or from an image file. The process of creating a custom content image starts by using the preview feature to view and select the files you want included in your image.

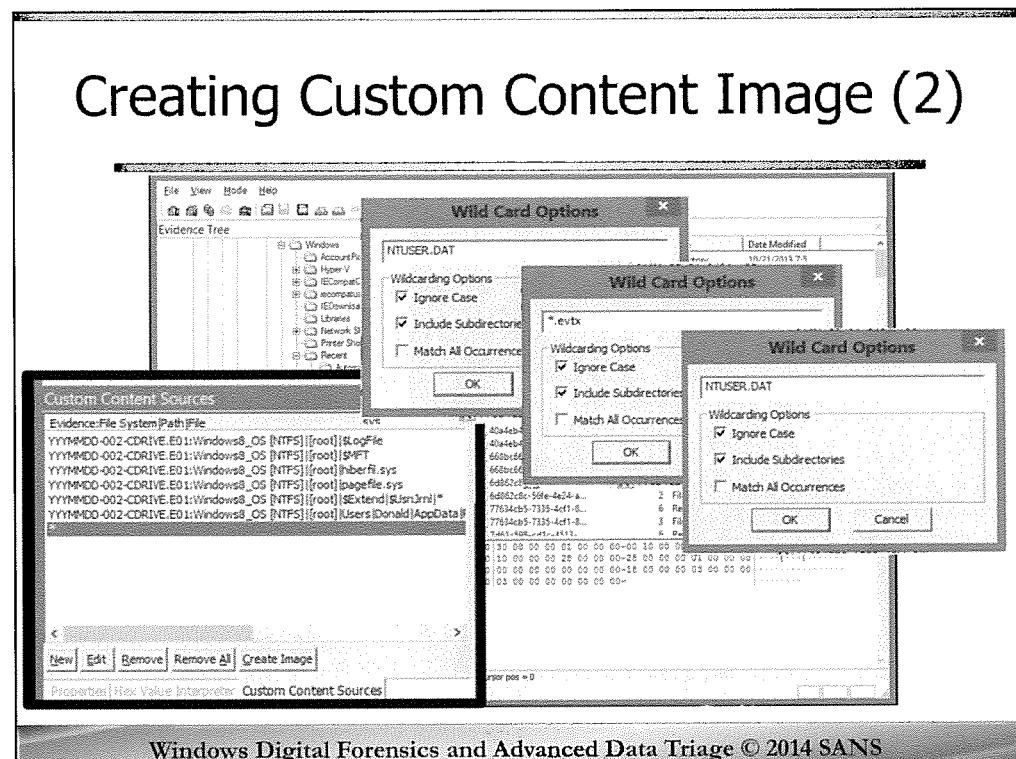
In the lower left corner of FTK Imager is a 3-function window. Along the bottom of this 3-function window are 3 tabs labeled “Properties”, “Hex Value Interpreter” and “Custom Content Sources”. You can select the “Custom Content Sources” tab or it will be automatically selected when you add your first item for inclusion in the custom content image.

There are three ways to select files for inclusion in a custom content image. First, while previewing the drive or image, you can navigate to the specific file desired, right click on the file in the “File List” window and select “Add to Custom Content Image (AD1)” in the dialog box.

Standard Windows file selection shortcuts are available when selecting files. To select several contiguous files, select the first file then hold down the Shift key and select the last file. All the files in between will be selected. To select several non-contiguous files, hold down the Control key while you select each file or folder.

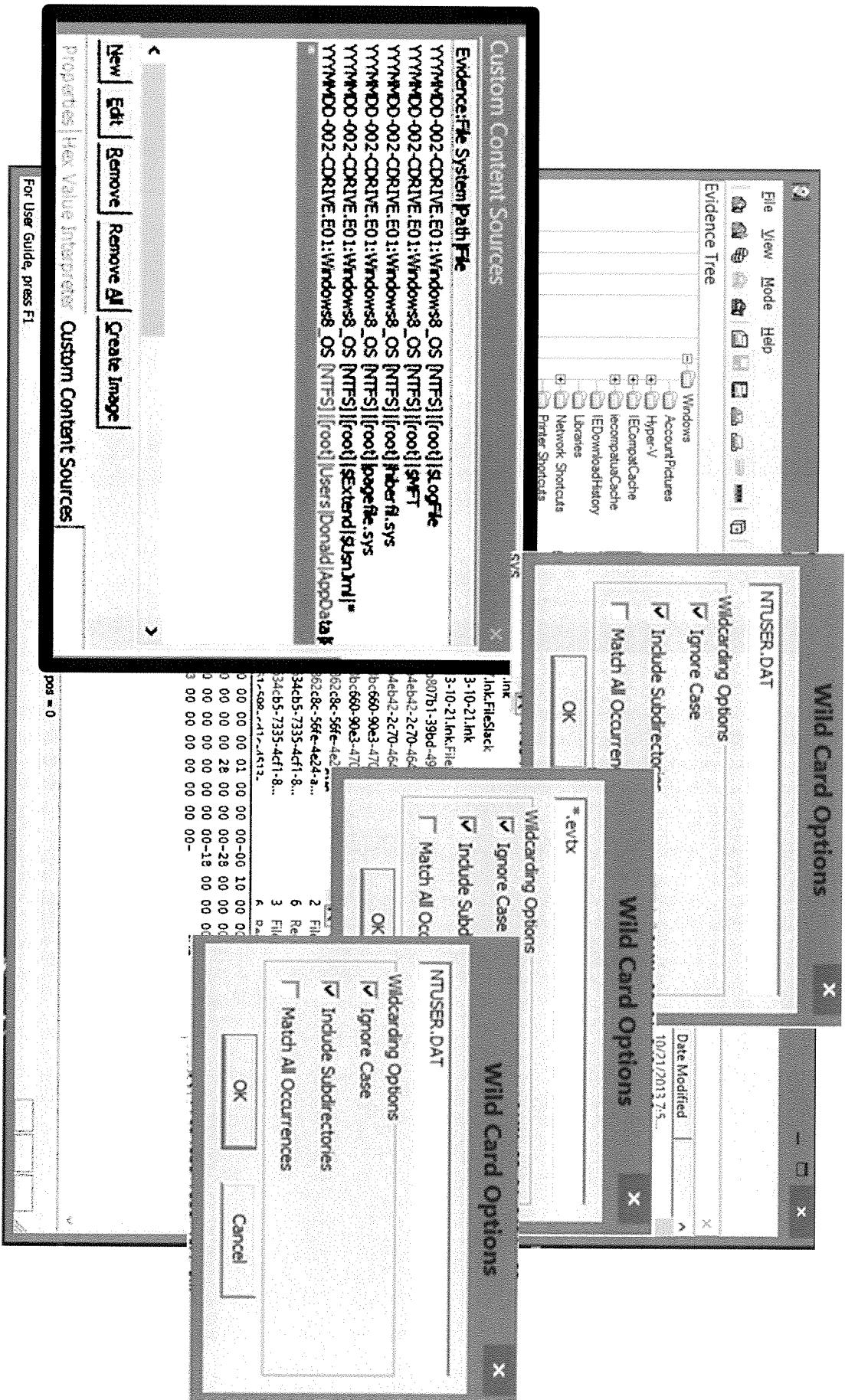
The second method is to select and right click a folder in the “Evidence Tree” window, then choose “Add to Custom Content Image (AD1)” in the dialog box. When adding a folder to the custom content image all files and subfolders are automatically included.

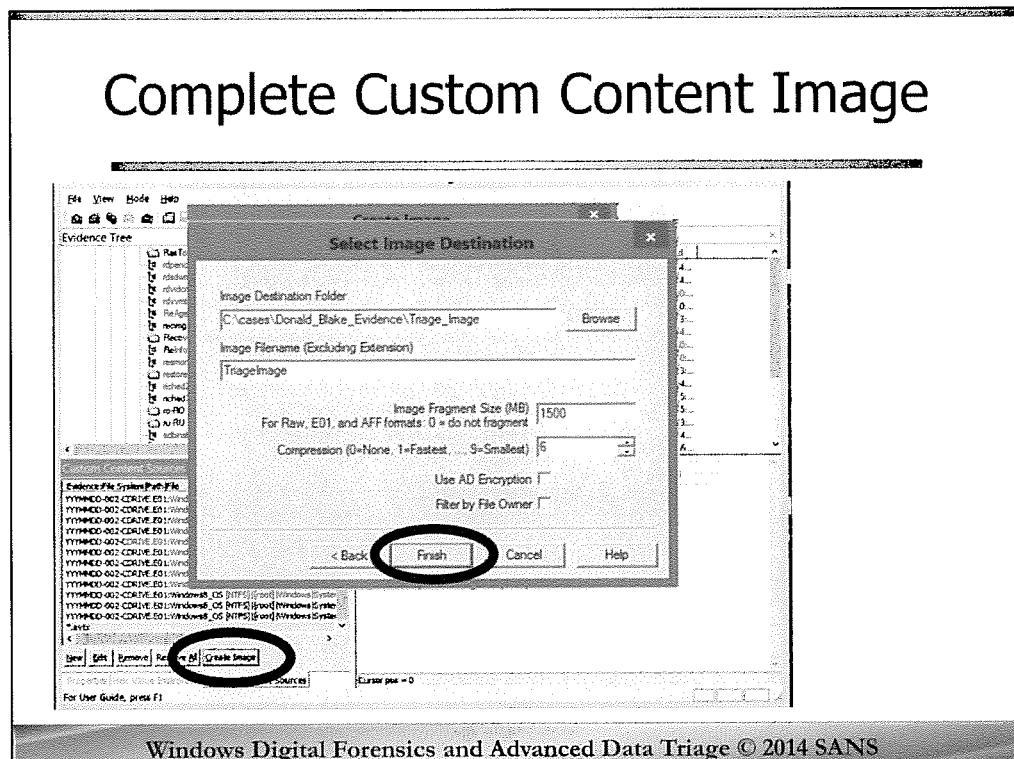




The third method is to create and edit a new wild card entry. To create a new wild card entry, select the “New” button in the lower left corner of the Custom Content Sources window, or use the “Alt+N” keyboard shortcut. An asterisk “*” will appear in the Custom Content Sources window. Select the asterisk, and then select the “Edit” button, or use the “Alt+E” keyboard shortcut.

The “Wild Card Options” dialog box will appear where you can type the exact name of the file (e.g. NTUSER.DAT would add every instance of “NTUSER.DAT” to the custom content image) or any variation of a filename with a wild card (e.g. *.evtx” would include any file with the “.evtx” file extension). You also have the option to ignore case, and match all occurrences.





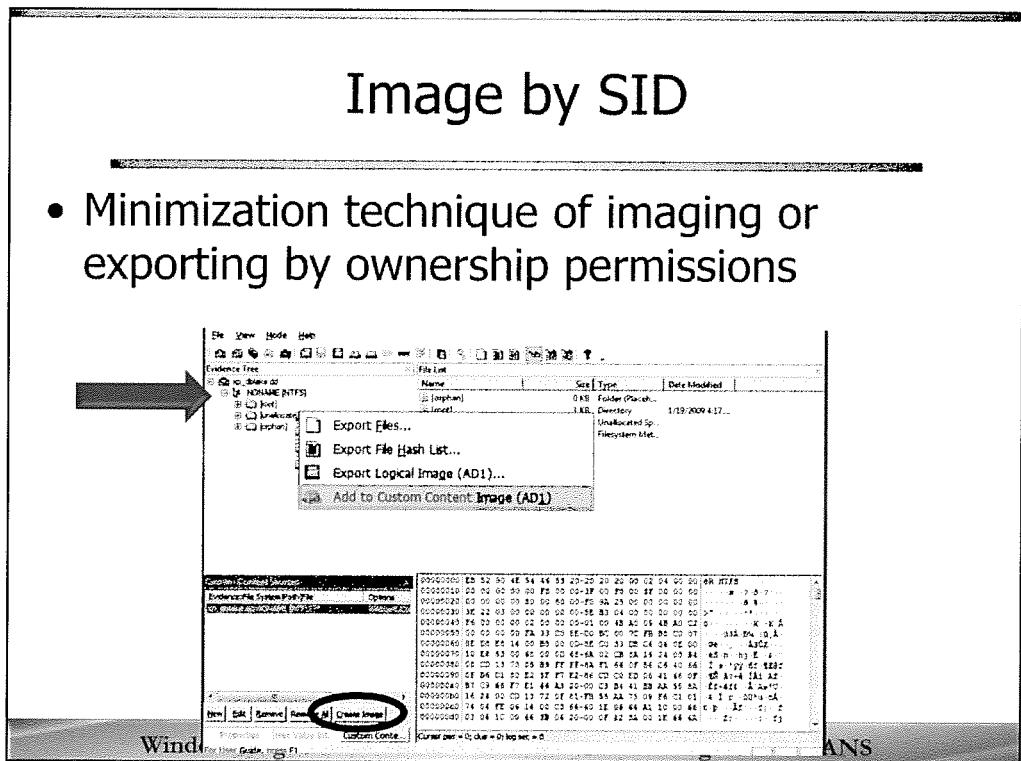
After you are satisfied you have selected all the important files, folders and artifacts for your Custom Content Image, complete your image by clicking on the “**Create Image**” button located on the bottom left of the Custom Content Sources window pane. The subsequent dialog boxes are the same as when you create any other image using FTK Image.

Fill in the appropriate information in the “Evidence Item Information” dialog box and click “**Next**”.

Select the “**Browse**” button and navigate to a location to save your image, then give the image a name and select “**Finish**”.

Image by SID

- Minimization technique of imaging or exporting by ownership permissions



Another great feature of FTK Imager is that you can create custom images of all files with specific ownership permissions by selecting the desired user SID. This is an excellent technique to use when either imaging files on a file server where you want to collect all files with specific user permission, or when you have to provide a discovery copy of an image containing multiple defendants. If you seized a multi-user computer where each of the users had an expectation of privacy for their files and then provided the entire drive to one of the defense attorneys without providing adequate protection to the other users files you could find yourself in a bit of legal trouble.

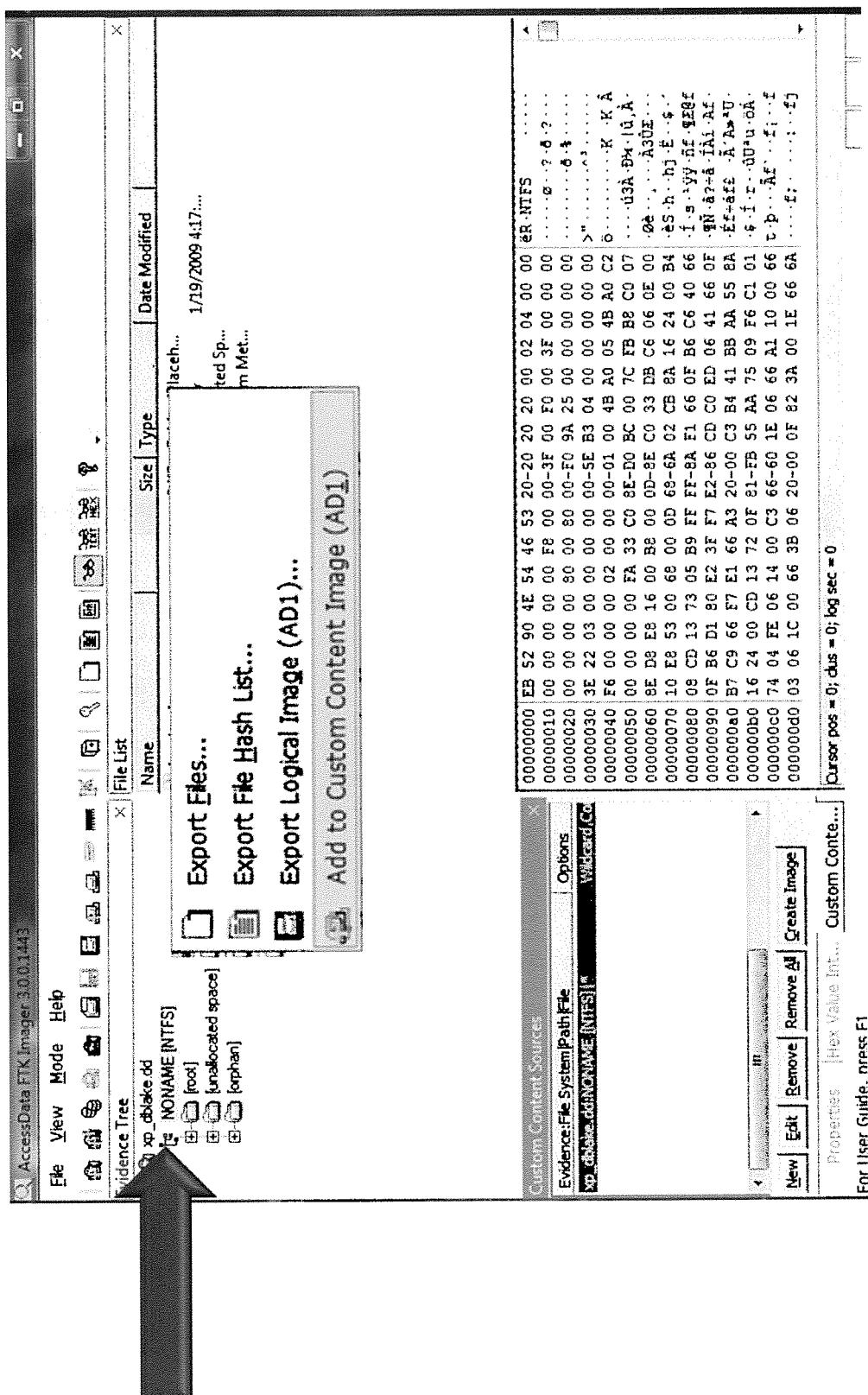
Recognizing that hard drive capacity is getting larger each year and more of our personal information is on our computers, the United States Courts have expressed concern recently about potential invasion of privacy. Where possible, this may be an excellent way to minimize collected data.

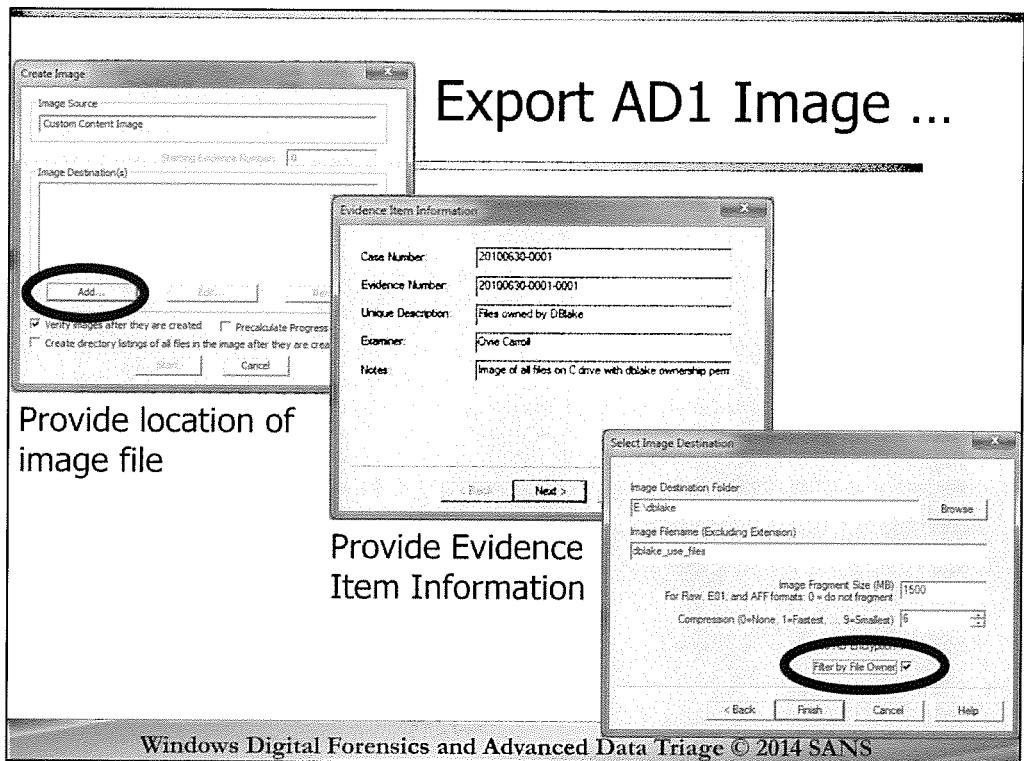
You can also use this technique to **extract** all files owned by particular users from a forensic image previously created.

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.



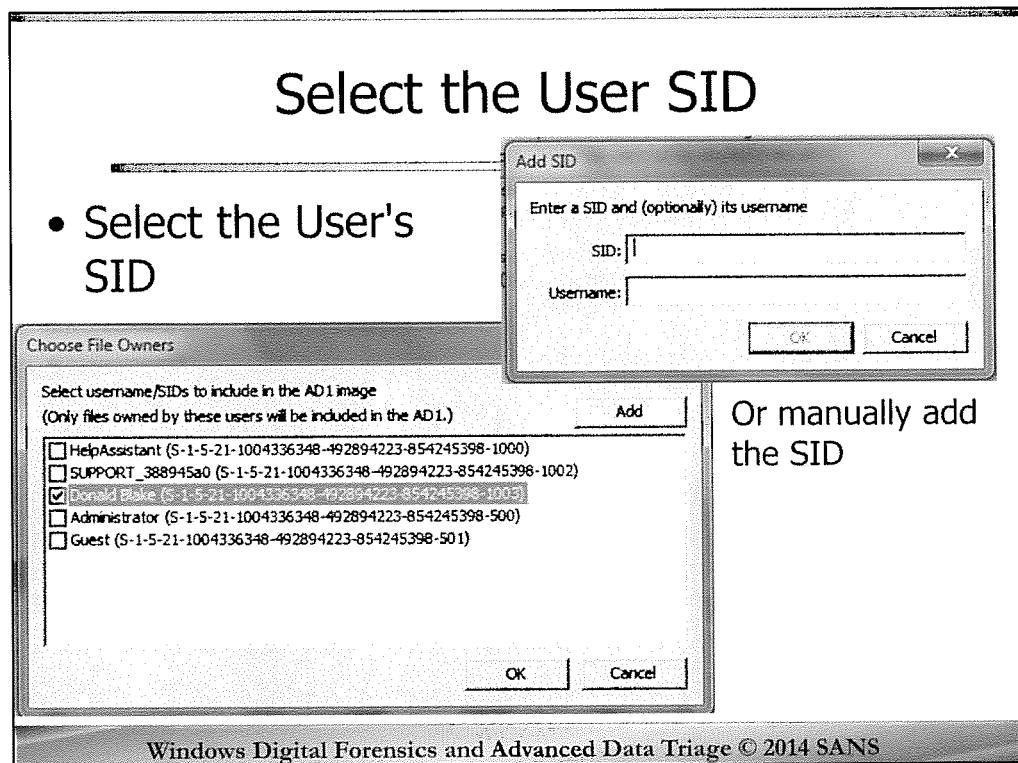


Next, select “Add...” to add a location for your evidence item/image file.

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.

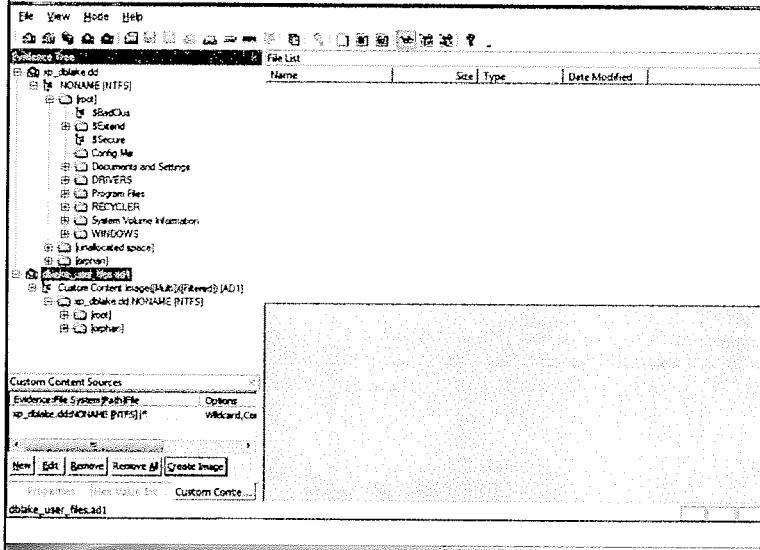
Select the “**Filter by File Ownership**” box.



Or manually add
the SID

When using the “Filter by File Ownership” feature, you will be presented with a new dialog box that lists all the users on the system. Simply select the users whose 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.

Image by SID



Windows Digital Forensics and Advanced Data Triage © 2014 SANS

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 be to zoom in on the user activity without the noise of hundreds or thousands of other users or system files?

Example Step-by-Step: Minimize by SID

1. Add an Evidence item
2. Select "Image file" and browse to the evidence image
3. Expand the evidence tree and select the NONAME[NTFS] partition
4. Right click and select "Add to Custom Content Image AD1"
5. In the Custom Content box, select "Create image"
6. Add an Image Destination
7. Select an Image Destination Folder and give the image file a name
8. Select "Filter by File Owner" and select User SID
9. Select the "Create directory listing of all files in the image after they are created"
10. Review files in directory listing and compare results to original full image

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

1. Add the an Evidence item
2. Select "Image file" and browse to the evidence image
3. Expand the evidence tree and select the NONAME[NTFS] partition
4. Right click and select "Add to Custom Content Image AD1"
5. In the Custom Content box, select "Create image"
6. Add an Image Destination
7. Select an Image Destination Folder and give the image file a name
8. Select "Filter by File Owner" and select User SID
9. Select the "Create directory listing of all files in the image after they are created"
10. Review file directory listing and compare results to original full image



Digital Forensics and Incident Response

C U R R I C U L U M



Exercise 1

Data Triage and Extraction

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

This page intentionally left blank.

FOR408 - Section 1 - Agenda

The Donald Blake Case

Core Windows Forensics: Focus On Analysis

FTK Imager Advanced Techniques

Advanced Acquisition

Mounting Disk Images

File System Overview

Key Word Searching

File Metadata

Data Carving

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

The Donald Blake Case

Core Windows Forensics: Focus On Analysis

FTK Imager Advanced Techniques

Advanced Acquisition

Mounting Disk Images

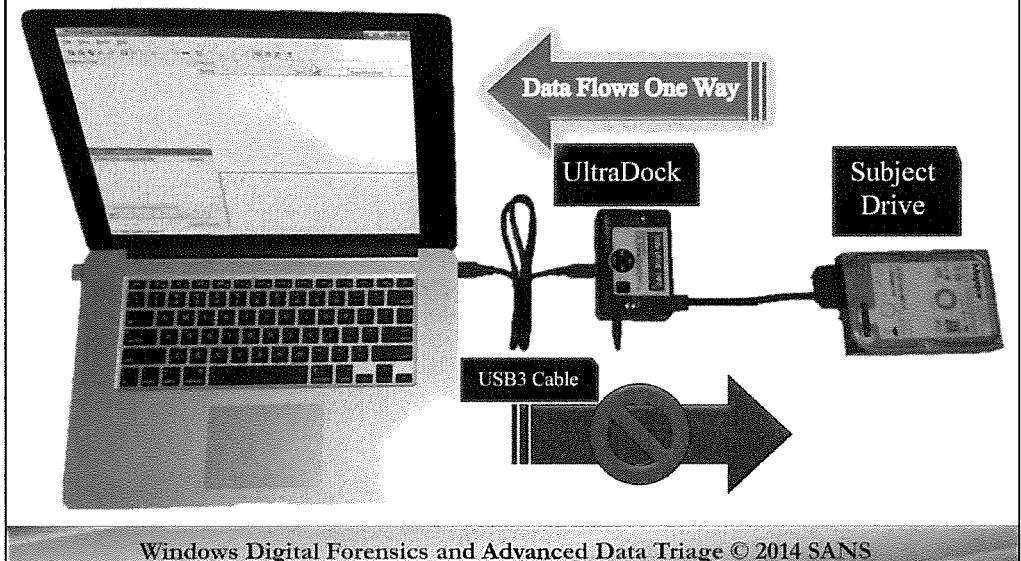
File System Overview

Key Word Searching

File Metadata

Data Carving

Out of Class Review: Hard Drive Acquisition w/Write Blocker – Appendix B



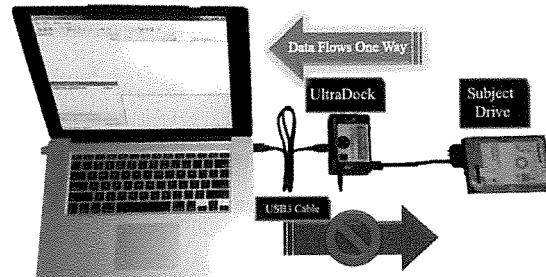
Once you have this all connected, you simply plug in the firewire cable as shown here into your forensic machine. In my experience, before you actually plug in the fire wire or USB device to your forensic machine, you should power up the entire device so that the drive gets to speed. If you don't do this you can sometimes have problems with your forensic machine recognizing your connected device.

(The actual power device for the UltraDock is not shown here to in an attempt to keep the example as visually clean as possible.)

Out-of-Class Exercise

HANDS-ON: Drive Acquisition

- What you need:
 - Practice Evidence Hard Drive (Used, Ebay, Instructor's Extra Drive)
 - External USB Drive (*Large capacity*) labeled "WORKING COPY"
 - UltraDock write blocker
- Use step-by-step on next slide
- Image your ORIGINAL Evidence hard drive to the large capacity "WORKING COPY" USB drive
- Fill out chain of custody form for the seizure



Windows Digital Forensics and Advanced Data Triage © 2014 SANS

Out-of-Class Exercise: HANDS-ON: Drive Acquisition

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: Depending on the size of your subject drive, this exercise will take some time to complete. To ensure your system is available for other exercises, we recommend you practice this in your room tonight and bring any questions to class in the morning.



Digital Forensics and Incident Response

CURRICULUM



Advanced Acquisition: Solid State Drives

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

This page intentionally left blank.

Solid State Drives

Better speeds

Quieter than ordinary hard drives

No cooling on the fly

No mechanical parts

Consume less power during operation



Windows Digital Forensics and Advanced Data Triage © 2014 SANS

Over the past 5 years, the adoption rate of the Solid State Drives (SSD) has been incredibly high. From desktops to laptops, the increase in speed achieved and additional power savings have made these drives highly attractive. When first released SSDs were very expensive (The first 32Gb SSDs sold for \$2,000 a drive), had limited capacity, and the adoption rate was minimal. But as the capacity of the SSD drives has increased and the costs have become more affordable, many businesses and individuals have started to use the drives in larger numbers. The benefits of solid state drives include increased speed of access. No longer do you have a motor moving a head of a hard drive across a spinning platter to read the polarity of binary data stored on it. As a result, the access to data is instantaneous.

For today, the term SSD has come to mean that it has emulation of an IDE. A memory stick does not emulate IDE because it does not have an IDE connector; however, it has no moving parts so still qualifies as an SSD. The flash drive or SSD (solid state device/drive) knows nothing about your files and is not aware in any way of the content. That is the job of the Operating System.

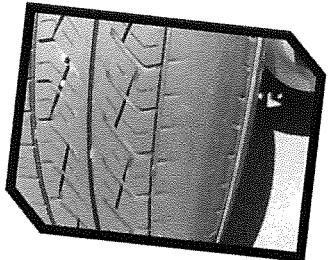
SSD has no moving parts. With no moving parts, solid-state drives are less fragile than hard disks and are also silent. SSDs usually employ low access time and latency. SSDs are relatively cool compared to hard drives.

Most SSD manufacturers use non-volatile flash memory to create more rugged and compact devices for the consumer market. SSD's do not require batteries. Non-volatility allows flash SSDs to retain memory even during sudden power outages, enduring data persistence. SSD design is proprietary. Most every detail is proprietary on process and format for the data stored on SSD. Every vendor wants to be the winner in the format for the best SSD device, so no one is helping anyone learn about their layout and division of the device

SSD Trim and Wear Leveling

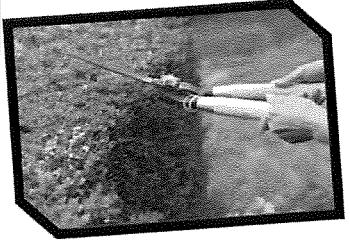
Wear Leveling

- SSD storage only good for X # of writes
- Data around to ensure even use of SSD storage around drive



Trim

- Clear data stored in flash that is deleted
- Effectively “Clearing Free Space”
- Once a week on Win7/8



Windows Digital Forensics and Advanced Data Triage © 2014 SANS

SSDs have limited number of writes and as a result will need two different capabilities that are used to help reduce the overall wear and tear of the SSD: Trim and Wear Leveling

In flash-based solid state disks the write endurance is the number of write cycles to a block of flash memory. Once you have met the write endurance limit, the disk may become unreliable or unable to use any of the cells. Many of the consumer based flash media is not even the best that is available. In many cases, we have the lower quality flash used for consumer drives and keys. As a result, there is a tendency for repeated writes to eventually corrupt the flash memory. How long will it last? Again it is variable; it should last for years, but not forever.

From Archive.org:

“The first step is to evaluate only the highest quality NAND flash available on the market today. Changes in flash die geometries, cell structure and address control functions impact yield rates from the wafer during the fabrication process. The concept that certain spots on a wafer are more likely to produce a higher quality chip is prevalent throughout the semiconductor industry. When flash memory wafers are tested and probed, a distribution of bad, weak, and strong die are identified across the wafer. Bad cells are marked, and the remaining cells are sorted into consumer and industrial quality flash. Adtron selects only industrial quality flash identified at the ie sort stage. Consumer grade flash makes it into flash disks that are mass marketed through retail outlets.”[1]

Wear Leveling

Wear leveling is a technique for prolonging the service life of some kinds of erasable computer storage media, such as flash memory. When content is changed it must be moved to a new location before the data can be saved, and then the data will be stacked in the garbage collection queue. Once the data has been moved the original location is then free to be cleared.

The data on a Solid State Device is virtualized and the Physical Sector that you are asking for is not actually the sector it was 5 minutes ago. The data moves around using wear leveling schemes, and when you ask for Sector 125, it's physical block is not the same block, it is converted to an logical block, and every 5 write cycles the data is moved to a new and empty previously erased block. This destroys some data used in forensics such as file slack. Slack space disappears, you can no longer be sure that the exact physical sector you are recovering is in the same location or has not been moved.

Drive Trimming or Trim

Windows 7/8 has a new feature for Solid State Drives called TRIM. If the SSD supports the TRIM calls it should improve speed and the lifetime of the SSD.

"Microsoft and SSD manufacturers are adopting the Trim operation. In Windows 7, if an SSD reports it supports the Trim attribute of the ATA protocol's Data Set Management command, the NTFS file system will request the ATA driver to issue the new operation to the device when files are deleted and it is safe to erase the SSD pages backing the files. With this information, an SSD can plan to erase the relevant blocks opportunistically (and lazily) in the hope that subsequent writes will not require a blocking erase operation, since erased pages are available for reuse. As an added benefit, the Trim operation can help SSDs reduce wear by eliminating the need for many merge operations to occur. As an example, consider a single 128 KB SSD block that contained a 128 KB file. If the file is deleted and a Trim operation is requested, then the SSD can avoid having to mix bytes from the SSD block with any other bytes that are subsequently written to that block. This reduces wear. Windows 7 requests the Trim operation for more than just file delete operations. The Trim operation is fully integrated with partition- and volume-level commands like Format and Delete, with file system commands relating to truncate and compression, and with the System Restore (aka Volume Snapshot) feature."^[2]

"Of course, device manufactures and Microsoft want to maintain superior performance characteristics as best we can. One can easily imagine the better SSD manufacturers attempting to overcome the aging issues by pre-erasing blocks so the performance penalty is largely unrealized during normal use, or by maintaining a large enough spare area to store short bursts of writes. SSD drives designed for the enterprise may have as high as 50% of their space reserved in order to provide lengthy periods of high sustained write performance.

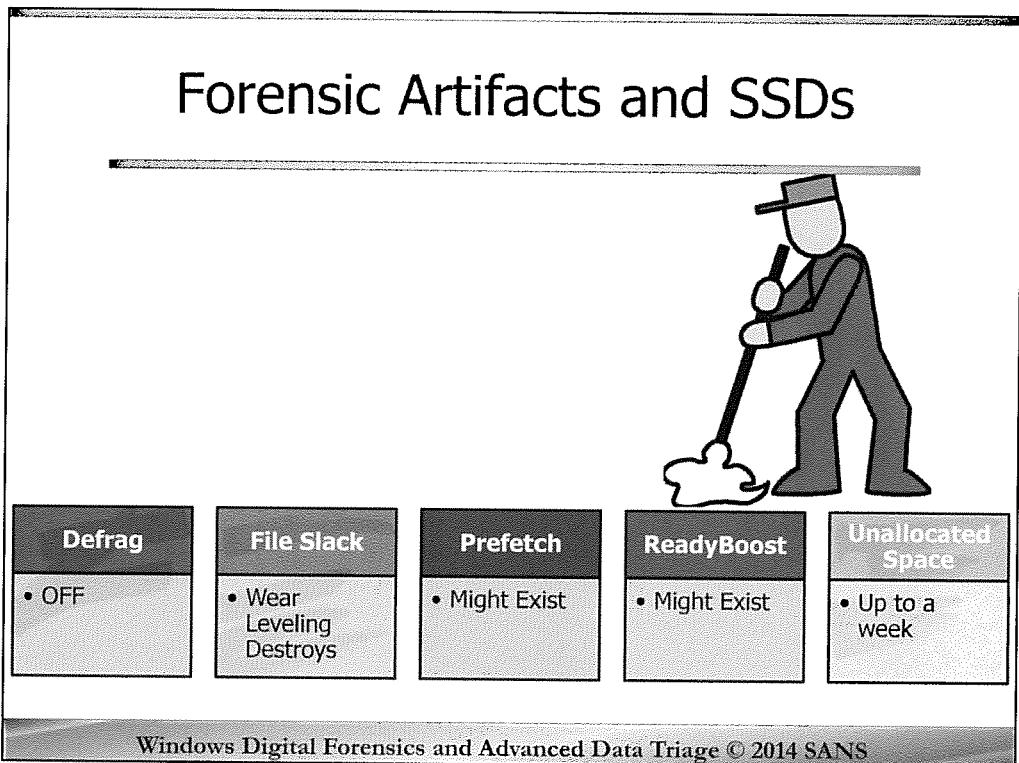
In addition to the above, Microsoft and SSD manufacturers are adopting the Trim operation. In Windows 7, if an SSD reports it supports the Trim attribute of the ATA protocol's Data Set Management command, the NTFS file system will request the ATA driver to issue the new operation to the device when files are deleted and it is safe to erase the SSD pages backing the files. With this information, an SSD can plan to erase the relevant blocks opportunistically (and lazily) in the hope that subsequent writes will not require a blocking erase operation since erased pages are available for reuse.

As an added benefit, the Trim operation can help SSDs reduce wear by eliminating the need for many merge operations to occur. As an example, consider a single 128 KB SSD block that contained a 128 KB file. If the file is deleted and a Trim operation is requested, then the SSD can avoid having to mix bytes from the SSD block with any other bytes that are subsequently written to that block. This reduces wear.

Windows 7 requests the Trim operation for more than just file delete operations. The Trim operation is fully integrated with partition- and volume-level commands like Format and Delete, with file system commands relating to truncate and compression, and with the System Restore (aka Volume Snapshot) feature."^[3]

References

- [1] <http://web.archive.org/web/20070115073812/http://adtron.com/products/flash-disk.html>
- [2]: <http://blogs.msdn.com/e7/archive/2009/05/05/support-and-q-a-for-solid-state-drives-and.aspx>
- [3]: <http://blogs.msdn.com/b/e7/archive/2009/05/05/support-and-q-a-for-solid-state-drives-and.aspx>



Many forensic artifacts could be affected by the utilization of an SSD drive. As mentioned, slack space will not exist on a flash drive as a result of wear leveling. Defrag is disabled by default but driving optimization (trimming) replaces that operation. Trimming will occur on a weekly basis per the scheduler. Also, prefetch and ready boost generally are sometimes disabled. We have found that on many systems, prefetch and readyboost is still enabled and that is due to the over confidence in Microsoft in the ability of SSDs to boost execution performance. Apparently that they have turned prefetch and readyboost back on and found an improvement in the speed of the system. Typically, I have found more systems with an SSD that have prefetch and readyboost turned on than off, but your experience might be different.

From MSDN:

“Will disk defragmentation be disabled by default on SSDs?

Yes. The automatic scheduling of defragmentation will exclude partitions on devices that declare themselves as SSDs. Additionally, if the system disk has random read performance characteristics above the threshold of 8 MB/sec, then it too will be excluded. The threshold was determined by internal analysis.

Will Superfetch be disabled on SSDs?

Yes, for most systems with SSDs.

If the system disk is an SSD, and the SSD performs adequately on random reads and doesn't have glaring performance issues with random writes or flushes, then Superfetch, boot prefetching, application launch prefetching, ReadyBoost and ReadDrive will all be disabled.

Initially, we had configured all of these features to be off on all SSDs, but we encountered sizable performance regressions on some systems. In root causing those regressions, we found that some first generation SSDs had

severe enough random write and flush problems that ultimately lead to disk reads being blocked for long periods of time. With Superfetch and other prefetching re-enabled, performance on key scenarios was markedly improved.

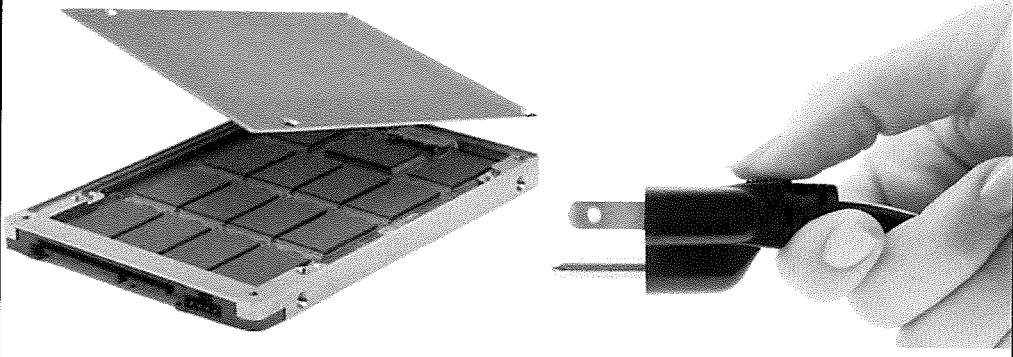
Does the Windows Search Indexer operate differently on SSDs?

No.” [1]

[1] <http://blogs.msdn.com/b/e7/archive/2009/05/05/support-and-q-a-for-solid-state-drives-and.aspx>

To Pull or Not to Pull

- Risk to SSD Associated with Power Loss
- Live Acquisition – Best Practice
- Possible Remediation



Windows Digital Forensics and Advanced Data Triage © 2014 SANS

Many discussions about proper acquisition techniques have always discussed whether or not to pull the power from a running system to “freeze” the state of the hard drive from accidentally erasing data. For the most part, this is a good idea—except when it comes to solid state drives. This action could cause some serious problems. [1] SSD drives are not meant to immediately cease functioning. In fact, there is a good chance that you could brick your SSD drive with a power failure.[2] Most drives can repair themselves automatically if re-connected to a power source, but it leads to another thought. If the SSD can self-write and self-repair its own data, then an investigator has very little control over the actual data while it is stored on a SSD hard drive.

In fact, cutting the power could be the worst option for trying to ensure proper collection of data on the drive. The repair operation could be doing many things including performing trimming operations and wear leveling while the drive is self-repairing after a power loss. Some thinking have recommended that the best options might include to image the system live. The longer you leave the solid state drive running in any form might corrupt the data. Powering off the system using a normal shutdown could also engage drive trimming/optimization or additional wear leveling as a result of data being close and written as a result of the shut down process. The only option that might result in the best evidence would be similar to imaging memory – doing it on a live system through live acquisition.

There are no firm recommendations as to what best practices are as of yet, however, many in the forensics community might discover that their procedures need updating when they would deal with drive acquisition of solid state drives.

If you lose your drive due to a power loss it is recommended to follow these guidelines from Crucial. [3]

A sudden power loss is most common cause for a system to fail to recognize an SSD. In most cases, your SSD can be returned to normal operating condition by completing a power cycle, a process that will take approximately one hour.

We recommend you perform this procedure on a laptop or desktop computer because it allows you to only connect the SATA power connection, which improves the odds of the power cycle being successful. However, a USB enclosure with an external power source will also work. Apple and Windows desktop users follow the same steps.

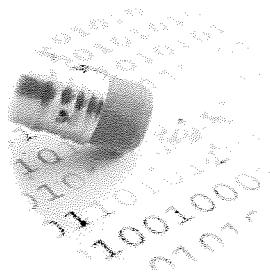
1. Once you have the drive connected and sitting idle, simply power on the computer and wait for 20 minutes. We recommend that you don't use the computer during this process.
2. Power the computer down and disconnect the drive from the power connector for 30 seconds.
3. Reconnect the drive, and repeat steps 1 and 2 one more time.
4. Reconnect the drive normally, and boot the computer to your operating system.
5. If the latest firmware has not been updated to your drive, do so.

References:

- [1] <https://www.usenix.org/system/files/conference/fast13/fast13-final80.pdf>
- [2] <http://www.extremetech.com/computing/169124-the-mysteriously-disappearing-drive-are-power-outages-killing-your-ssds>
- [3] <http://forum.crucial.com/t5/Solid-State-Drives-SSD-Knowledge/Why-did-my-SSD-disappear-from-my-system/ta-p/65215>

Write Blocking SSDs

- Powered On Drives
- No Control Over
 - Wear Leveling
 - Controller Initiated Trimming
 - Other Unknown Controller Actions
- Drive Integrity Not Met
 - Drive md5 would change over time
 - Data loss will occur



Windows Digital Forensics and Advanced Data Triage © 2014 SANS

The usual process of write blocking drives using a standard write blocker will only protect the drive from accidental writes from the connected operating system. However, the drive's controller itself is fairly robust and is likely to perform wear leveling and trimming operations when the drive is powered on. Given that so much is unknown on each vendor's implementation of their own SSD drives, it is likely that there is a good risk associated with assuming that the SSD drive integrity will be achieved with a write blocker for prolonged periods.

As a result, it is recommended that a write blocker is used, it is used to image the hard drive only. It is probably not recommended to perform analysis on a SSD drive connected via a write blocker as it might be plugged in for an extended period of time increasing the chances that controller initiated SSD drive management could occur resulting in a loss of integrity.

FOR408 - Section 1 - Agenda

The Donald Blake Case

Core Windows Forensics: Focus On Analysis

FTK Imager Advanced Techniques

Advanced Acquisition

Mounting Disk Images

File System Overview

Key Word Searching

File Metadata

Data Carving

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

The Donald Blake Case

Core Windows Forensics: Focus On Analysis

FTK Imager Advanced Techniques

Advanced Acquisition

Mounting Disk Images

File System Overview

Key Word Searching

File Metadata

Data Carving



Digital Forensics and Incident Response

CURRICULUM



Image Mounting

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

This page intentionally left blank.

Image Mounting



- New image mounting capability
- Mount read-only as drive or physical Device
- Mount types
 - RAW/DD, E01, S01, AD1, and L01 Images
- Encrypted images cannot be mounted

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

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.

Benefits to Mounting Images



- Interact with files with their native or associated application
- Run anti-virus and malware detection applications
- Share with remote computers
- Copy files out of image
- Forensically sound

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

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 review 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 computer 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.

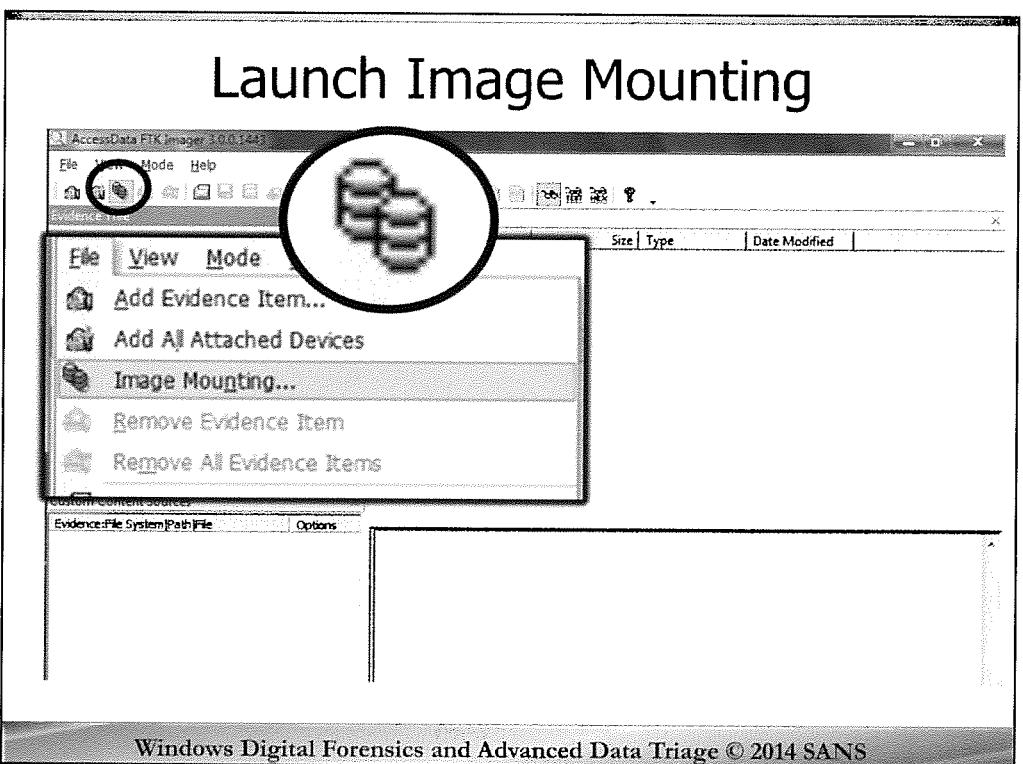
Characteristics of Mounted Images

- Logically Mounted Images
 - Windows file systems (NTFS/FAT) can be mounted to a drive letter
 - AD1 and L01 images have no drive geometry so must be mounted logically
- Physically Mounted Images
 - Cannot be viewed by Windows Explorer
 - Can be viewed with Windows application that performs Physical Name Querying

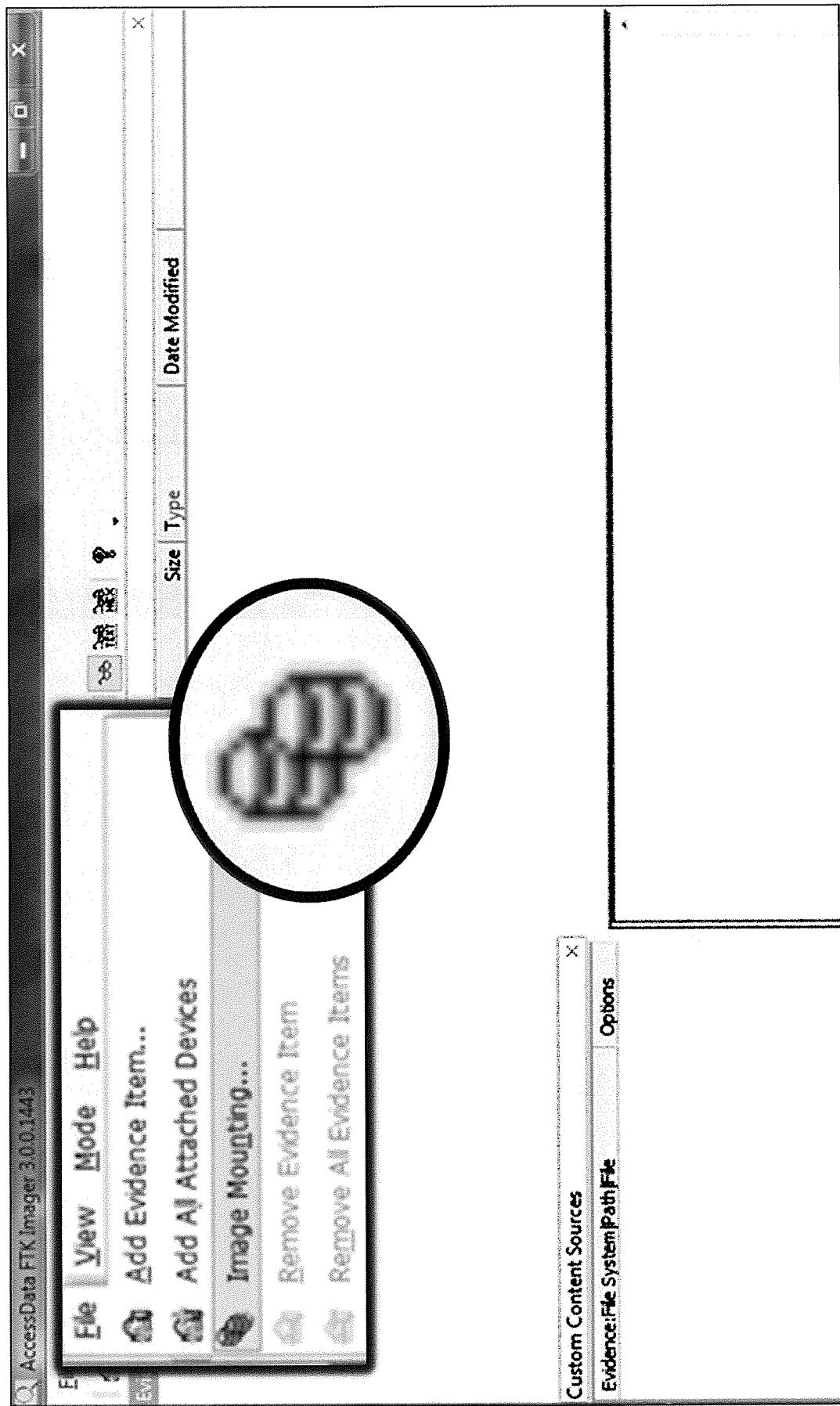
Windows Digital Forensics and Advanced Data Triage © 2014 SANS

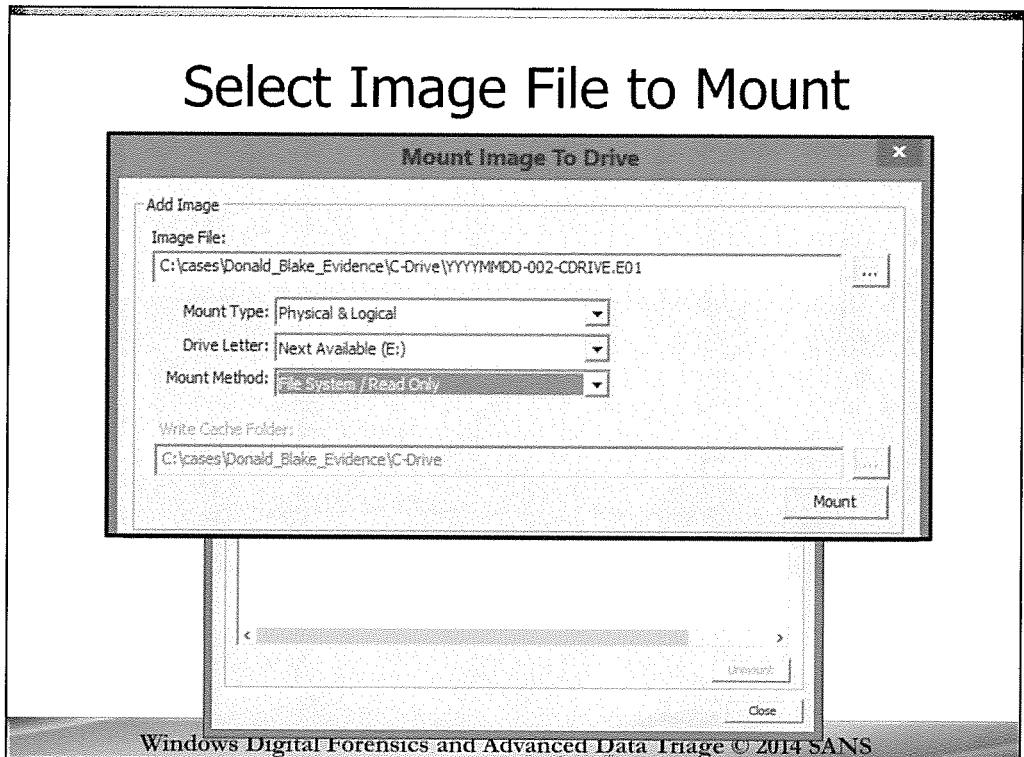
When you create AD1 or L01 custom content images, they contain full file structures but do not have any drive geometry or any other physical drive data. This will prevent them from being mounted physically. Additionally, when you mount them logically, the drive or partition size will not be displayed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



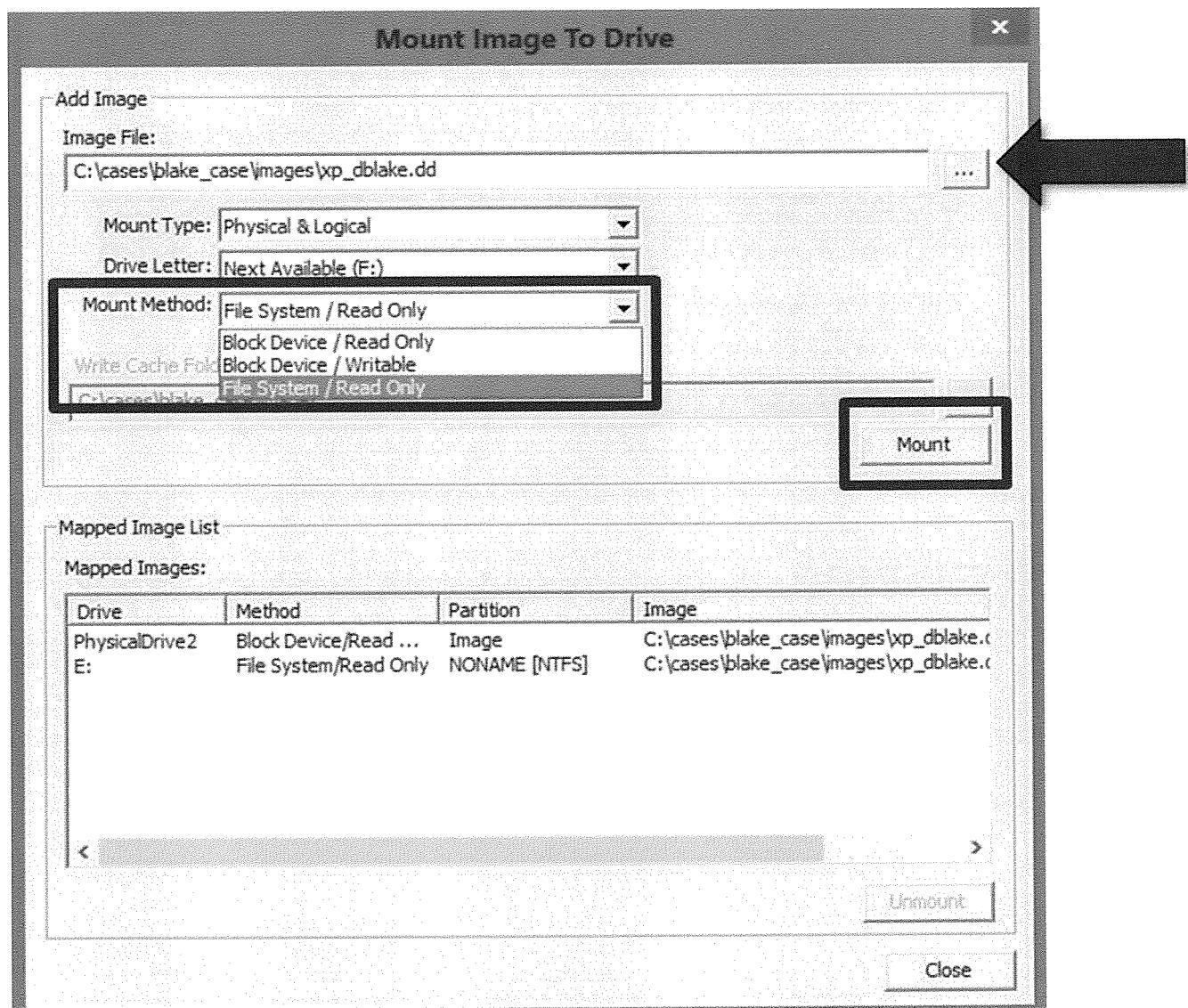


Click the “...” adjacent the “Image File” field. Browse to the location your image file is located.

Click “**Open**”.

Now that you have selected the image file, the “Mount 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.

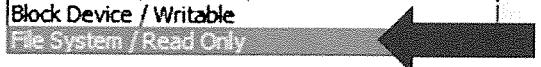
Click “**Mount**” and the selected image file will be mounted. You can see in the bottom half of the “Mount Image to Drive” area the details of the mounted images in the “**Mounted Image List**”.



FTK Imager Mount Method

Mount Method: File System / Read Only

Block Device / Read Only
Block Device / Writable
File System / Read Only



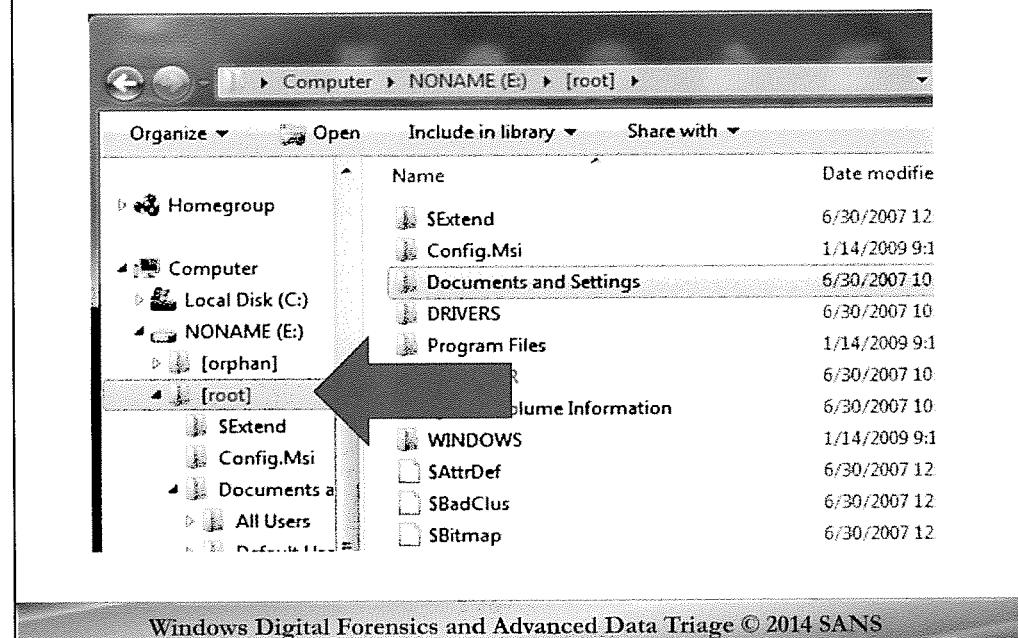
Block Device / Read Only	Treats the mounted image as a block device (disk). Image will be subject to NTFS permissions and Windows file/folder protections.
Block Device / Writable	Mounts image as a writable device, saving any changes in a cache file (no changes made to original image).
File System / Ready Only	Creates a virtualized folder structure, circumventing Windows file/folder protections. File system starts in [root] folder.

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

From the FTK Imager User Guide:

- **Block Device/Read:** Only Reads the device as a block device, meaning that the mounted device must be viewed using any Windows application that performs Physical Name Querying.
- **Block Device/Writable:** Allows you to write to the evidence, make notes, and so forth. The changes and notations are saved in a cache file, but no changes are made to the original. If selected, provide path information for the cache file in the Write Cache Folder field.
- **File System/Read Only:** Reads the device as a read-only device that you can view using Windows Explorer.

Exploring a Mounted Image



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

Organize ▾			Open	Include in library ▾	Share with ▾
	Name	Date modified	Type		
▶	Homegroup	6/30/2007 12:50 PM	File f		
▶	Computer	1/14/2009 9:10 PM	File f		
▶	Local Disk (C:)	6/30/2007 10:36 PM	File f		
◀	NONAME (E:)	6/30/2007 10:42 PM	File f		
▶	[orphan]	1/14/2009 9:10 PM	File f		
▶	[root]	6/30/2007 10:54 PM	File f		
▶	SExtend	6/30/2007 10:34 PM	File f		
▶	Config.Msi	1/14/2009 9:10 PM	File f		
▶	Documents	6/30/2007 10:54 PM	File f		
▶	All Users	6/30/2007 12:50 PM	File		
▶	Default Use	6/30/2007 12:50 PM	File		
▶	Donald Bill	6/30/2007 12:50 PM	File		
▶	LocalService	6/30/2007 12:50 PM	File		
▶	NetworkSer	6/30/2007 12:50 PM	File		
▶	DRIVERS	6/30/2007 12:50 PM	File		
▶	SMFTMirr	6/30/2007 12:50 PM	File		
▶	... ~ ...				
Volume Information					
▶	WINDOWS	1/14/2009 9:10 PM	File f		
▶	SAttrDef	6/30/2007 12:50 PM	File		
▶	SBadClus	6/30/2007 12:50 PM	File		
▶	SBitmap	6/30/2007 12:50 PM	File		
▶	SBoot	6/30/2007 12:50 PM	File		
▶	SB0	6/30/2007 12:50 PM	File		
▶	SLogFile	1/19/2009 4:17 AM	File		
▶	SMFT	6/30/2007 12:50 PM	File		
▶	SMFTMirr	6/30/2007 12:50 PM	File		



Exercise 2

Mounting Disk Image

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

This page intentionally left blank.

FOR408 - Section 1 - Agenda

The Donald Blake Case

Core Windows Forensics: Focus On Analysis

FTK Imager Advanced Techniques

Advanced Acquisition

Mounting Disk Images

File System Overview

Key Word Searching

File Metadata

Data Carving

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

The Donald Blake Case

Core Windows Forensics: Focus On Analysis

FTK Imager Advanced Techniques

Advanced Acquisition

Mounting Disk Images

File System Overview

Key Word Searching

File Metadata

Data Carving



Digital Forensics and Incident Response

CURRICULUM



Windows File Systems

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

This page intentionally left blank.

Windows File System Evolution

FAT 12/16

- MS-DOS, Win95/98/NT/2000

FAT 32

- Win95 (OSR 2), Win2000
- WinXP/2003/Vista/Win7/Win8

ExFat

- 2008/2012/Vista/Win7/Win8

Windows NT file system (NTFS)

- WinXP/2003/2008/2012/Vista/Win7/Win8

ReFS

- Server 2012

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

A file allocation table (FAT) is a table that Windows maintains on a hard disk that provides a map of the clusters that a file has been stored in.

The number at the end of the FAT is a multiple of how many clusters can be addressed on the file system. For example, on a FAT16 system, it can address 2^{16} or 65,536 clusters.

Windows creates a FAT entry for a new file that records where each cluster is located and its sequential order. When you read a file, the operating system reassembles the file from clusters and places it as an entire file where you want to read it. For example, if there is a long web page, it may very well be stored on more than one cluster on your hard disk.

With 32-bit FAT entry (FAT32) support in Windows 95 OSR2, the largest size hard disk that can be supported is two terabytes!

The FAT file system has been around since the early 1980s and is one of the most simple file systems. It contains no security features, few time stamps, and several hacks that have allowed it to still be used today. There are four variations of FAT: FAT12, FAT16, FAT32, exFAT. The major difference in each is the size of addressable entries in the FAT, which will be described later. The exFAT file system is the newest version and can be found in Windows versions after VISTA SP1 and latest versions of Windows CE 6.0.

FAT32 was introduced with Windows 95 OSR2 or later.

The FAT file system is one the most common PC file system around as it is compatible with so many different computers. FAT is very reliable since it keeps a table of files and free space. If your system crashes, the FAT

does not lose data, but may not have written the data before the crash. Typically, running CHKDSK or SCANDISK recovers these lost fragments.

FAT32 is an enhancement of FAT16 and is based on 32-bit file tables instead of 16-bit. FAT32 uses much smaller clusters of 512 bytes to 32 kilobytes supports drives up to 8 terabytes. The smaller clusters result in better file efficiency and reduced wasted space.

FAT32

Cluster Size = 512 bytes to 32 KB

32 bit cluster numbers

Reserves the high 4 bits it really has a 28-bit cluster identifier

2^{28} addressable clusters

268,435,456 clusters max for a theoretical maximum volume size of 8 Terabytes

Windows will only allow you to format a disk up to **32 GB**

Windows will recognize disk larger than 32 GB formatted on other operating systems

MBR Limitations only allow partitions that are **2 TB** in size

No security - anyone can access every file

Root directory ordinary cluster chain - no limit on size

Limited error recovery

File Size Limit

4 GB – 1 byte (2^{32} bytes minus 1 byte)

Maximum volume size

FAT12 32 MB

FAT16 4 GB

FAT32 32 GB

Theoretical Max is 8 TB; MBR limitations places limit at 2 TB.

Windows will strictly allow a user to format a partition at 32GB. However, Windows can recognize larger partitions created by other operating systems.

Files per volume

FAT12 4096

FAT16 65536

FAT32 4,177,920

Overview of FAT Filesystem's Limits.

<http://technet2.microsoft.com/windowsserver/en/library/810c3217-77bb-4553-b6ce-3ff10dbdbac91033.mspx?mfr=true>

What Data Still Exists Upon File Deletion for the FAT Filesystem?

FILENAME LAYER

File Name will be preserved minus the first letter

METADATA LAYER

Modification/Creation Times and Access Date (Preserved)

File Type, Size, and Cluster addresses (Preserved)

DATA LAYER

Data clusters in FAT will be marked as unallocated but data will be preserved at the original cluster locations

Slack Space will exist

ExFAT – Improves upon the FAT filesystem – eliminating the 4GB file size limit and reduces the overhead of the FAT file system by removing the continual use of the File Allocation Table (FAT) to keep track of cluster allocations for contiguous files. It is not FAT64, as some call it, as it uses FAT32 (32 bit cluster addresses).

NTFS

NTFS includes many features not found in the FAT system and was designed to be reliable and efficient even when used on large disk volumes. NTFS provides a great balance of performance, reliability and compatibility. Its design lets it quickly perform file operations like read, write, and search. NTFS allows long file names and maintains an 8 plus 3 file name for a given file so DOS programs can use it.

File Size Limitations

Theoretically: 16 exabytes minus 1 KB (2^{64} bytes minus 1 KB)

Reality: 16 terabytes minus 64 KB (2^{44} bytes minus 64 KB)

Maximum volume size

Theoretically: 256 terabytes minus 64 KB (2^{32} clusters minus 1 cluster)

Reality: 16 terabytes

OS Limitations:

MBR partitions only support partition sizes up to 2 TB

Dynamic NTFS disks and 64-bit computers can support larger than 2 TB

Files per volume

4,294,967,295 (2^{32} minus 1 file)

NTFS --What Data Still Exists Upon File Deletion?

FILENAME LAYER

File Name will be preserved

METADATA LAYER

Data Modification, Access , Creation, and MFT Change times (Preserved)

File Type, Permissions, Size, and Cluster addresses will generally be kept depending on the file system

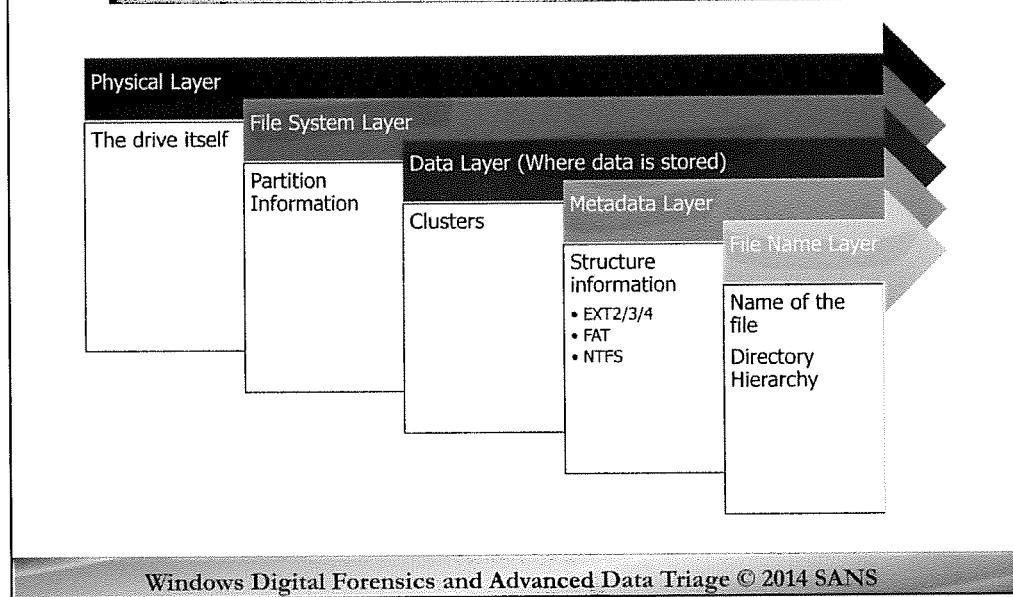
DATA LAYER

Data clusters will be marked as unallocated but data will be preserved

Slack Space will exist

ReFS – Resilient File System - Initially intended for file servers (Server 2012 and after) only. It is an improvement on NTFS. It maximizes data availability, despite errors that would historically cause data loss or downtime.

File System 5-Layers



This is the overview of the file system 5 layers that we will be examining over the next few sections. We start with the physical and the partition details of a drive themselves which leads us to the actual file system. The file system will be made up of 3 layers (Data, Metadata, and File Name Layers). In order to understand how to best recover data during a case, we should understand how it is intentionally structured. Anti-Forensics techniques tend to overlook some of the more obvious structural foundations of a system because they are designed to fool a casual user, not someone familiar with the inner workings a file system forensics.

To extend that theory we will begin by breaking down the 5 layers initially.

In the 1st two layers we will examine the Physical layer and the File System layer will be used to discuss how a drive is initialized, partitioned, and then formatted. We will discuss the Master Boot Record, the partitions themselves, and how the Windows Operating system will identify a specific physical drive that is attached to it.

We then will discuss from a very high level how the 3 layers of the file system work together to actually store file data.

Data Layer

Allocated or Unallocated?

- Data will be either
 - Allocated
 - Data block is actively being used by a file
 - Data exists in a file on the system
 - Not deleted
 - Unallocated
 - Data block is not being used by a file
 - Data may or may not exist in the block or cluster
 - May contain deleted or unused data
 - Pieces of files are called file fragments

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

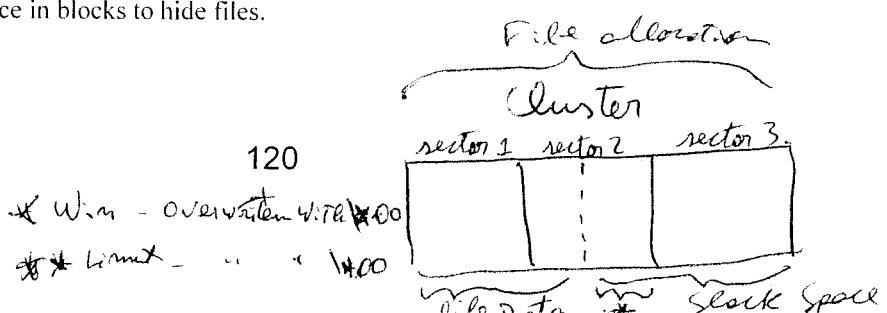
Data chunks will be in one of two states on file system: used or not used. Each chunk of data (cluster or block) is either owned by an existing file or is waiting to be used. This is generally referred to as free space. Even though the space is free, it does not necessarily mean that it is free of data. Files that were deleted on the system could have written to these blocks at one point. This space is considered unallocated by the file system. Even though the space is unallocated, critical evidence can be recovered from these blocks despite not being recoverable by ordinary file recovery.

If a file is not fully recoverable, a piece of that file may still be recoverable. That piece of the file is called a file fragment. A fragment may be one or more blocks of data, but alone would not be the full file. For example, an e-mail found on a system may be recoverable, however, you may only obtain half of the e-mail. The other half was written over when the file system needed the data block that the e-mail portion resided in.

Slack space is the unused space in a cluster. Windows file systems use fixed-size clusters. Even if the actual data being stored requires less storage than the cluster size, an entire cluster is reserved for the file.

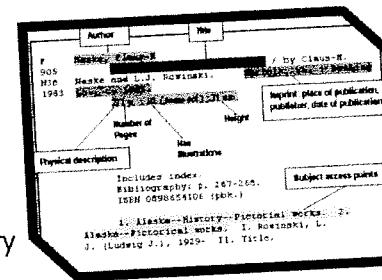
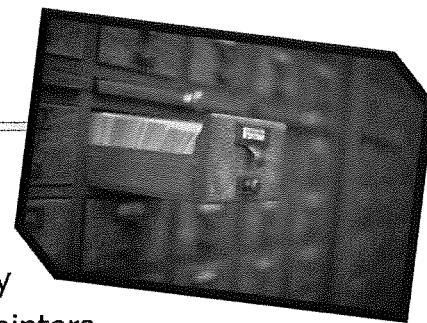
Windows write file information in sector sized chunks. If the file is 1280 bytes in length and the clustersize is 2048 then windows will write into the first three sectors. Notice that the third sector is only partially written, when that occurs, windows will use the null byte \x00 as a filler until the end of the sector not the cluster. Any extra sectors not used in writing data for the file is slack space. Slack space could contain data from the previous file that was stored at that location.

Slack space exists on Unix based file systems, but slack space is overwritten to the end of the block with the null byte. This means that naturally occurring data in slack space is rare. However, data hiding tools, such as BMAP, might utilize slack space in blocks to hide files.



Metadata Layer

- The Metadata layer contains the values that describe files
- Acts like a Card Catalog in a Library
- The Metadata structures contain pointers to the data layer and information such as MACtimes and permissions
- Each metadata structure is given an address
- Structure names include
 - Master File Table entry (NTFS)
 - File Allocation Table (FAT) Directory Entry



Windows Digital Forensics and Advanced Data Triage © 2014 SANS

Typical file systems store virtually all data in files. The most important of these are a set of special files, which are typically called *metadata structure* or *inodes*. The prefix "meta-" means self-referring. So "metadata structures" are structures that contain data *about* data. And that's exactly what these structures do. They contain internal information about the real data stored on the file system. For example, it could contain a listing of directory, timestamps, and file owners.

All file systems have some structure that is used to describe a file. The metadata layer contains those structures. These structures are called different things in different file systems:

NTFS: Master File Table (MFT) entry

FAT: Directory Entry

These structures typically do not contain the actual name of the file. They contain descriptive information such as MACtimes, permissions, owner user id, and size. This layer also has some method of referring to the data units that have been allocated to the file. For Unix-based file systems, there are a series of pointers to the different fragments. For FAT, the File Allocation Table is used to find "Chains" of clusters.

Each structure is given an address. We will use this address when referring to structures in this layer. This structure is typically hidden (especially for deleted files) from users, but there is a lot of useful information in them.

Deleted File? Wiped File?

- What does this mean if someone deletes a file?
 - The data still exists on disk and is fully recoverable until the free space is over-written
- Bottom Line: We're usually successful at recovering deleted data
 - Unless someone has overwritten or wiped the disk blocks before deleting a file
 - One wipe is all that is necessary to stop any forensic tool from recovering the data on modern hard drives
 - NIST Guideline for Media Sanitization (Sept 2006)

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

This is important for one reason. If a file is deleted, the contents are not overwritten immediately. The data still exists on disk and can be recovered until the free space is re-allocated by the OS and overwritten.

You might think that the lifespan of deleted data is short, and that storage space that has been freed is used again quickly. This isn't necessarily the case. In fact, because of the inode and disk block allocation algorithms, this sort of collision occurs infrequently.

The bottom line is that we can usually recover most (if not all) of a file even though it has been deleted. Studies have been done that indicate that about 80% of the time you will be able to recover files unless they have been deleted using a tool like srm.

Srm defeats recovery techniques by wiping (or overwriting) the contents of file after the file is deleted. Only one wipe is necessary to stop any forensic tool from being able to recover the data that was once written there. Recently, the NIST guideline, **Guidelines for Media Sanitization** September 2006, states that "Studies have shown that most of today's media can be effectively cleared by one overwrite."

Ref:

<http://srm.sourceforge.net/>

http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf

Marked MAC Meaning by File System

- The MACB column changes depending on the filesystem that is being examined
- NTFS and EXT2/3 Systems identify "C" as the metadata change time
- File creation time is listed as a 'B' for file "Birth"

File System	Time Stored	Time Resolution	Data Modified	Data Accessed	Metadata Change	Metadata Birthdate
FAT	Local	Jan 1, 1980	Modified (2 sec)	Accessed Date (1 day)		Created (10 ms)
NTFS	UTC	100 ns since Jan 1, 1601	Modified	Accessed	MFT Modified	Created
exFAT	UTC	10 ms since Jan 1, 1601	Modified	Accessed		Created

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

Depending on the filesystem, the meaning of the letters in the MAC column might change a bit. The largest change occurs in the "C" column. On NTFS and UNIX filesystems, the "C" stands for the last time the metadata contents have been updated. This would occur when a file size changes, security permissions change, or even if the owner of the file is updated.

The time stored value is also important to understand. Specifically, the FAT filesystem is the most odd since it stores a time in local time and does not account for changes in time zones. This means that if a FAT filesystem the written time will always be the same regardless of the time. 3 PM EST would also be 3 PM PST.

NTFS stores time in UTC -> 12:00 A.M. January 1, 1601 Coordinated Universal Time (UTC). The time format is a 64-bit FILETIME format that includes the interval of 100-nanoseconds since 12:00 Jan 1 1601 in UTC. [1]

Ext2/3 stores time in Epoch Format -> 12:00 A.M. January 1, 1970

Modified – Last Time File Data Was Modified

Accessed – Last Time File Data Was Opened

Change in Metadata – Change in File Attributes

Birthdate – File Volume Creation Date/Time

It is important to remember the meaning behind the letters as it changes the context surrounding the event in the timeline. For example, a file might be created on a NTFS volume and then transferred to a USB key with a FAT32 volume. The modified time of the file should remain constant, but the C time on the USB key, will be the time the file was created one the volume. This is noteworthy because an investigator can tell if a file originated from the volume using a combination of the context surrounding all of the timestamps. Being able to tell a file is copied onto a volume from another location or if it created on the volume is an important distinction.

In the latest version of the sleuthkit, the “B” letter stands for the files “BIRTH” or creation time.

References:

[1] FILETIME structure <http://msdn.microsoft.com/en-us/library/ms724284%28v=vs.85%29.aspx>

Ref: http://www.iau.org/static/resolutions/IAU1976_French.pdf RESOLUTION NO. 3 BY COMMISSIONS 4 AND 31 which defines the official abbreviation for Coordinated Universal Time is *UTC*. This abbreviation arose from a desire by the International Telecommunication Union and the International Astronomical Union to use the same abbreviation in all languages. English speakers originally proposed *CUT* (for "coordinated universal time"), while French speakers proposed *TUC* (for "temps universel coordonné"). The compromise that emerged was *UTC*,[11] which conforms to the pattern for the abbreviations of the variants of Universal Time (UT0, UT1, UT2, UT1R, etc.)

FOR408 - Section 1 - Agenda

The Donald Blake Case

Core Windows Forensics: Focus On Analysis

FTK Imager Advanced Techniques

Advanced Acquisition

Mounting Disk Images

File System Overview

Key Word Searching

File Metadata

Data Carving

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

The Donald Blake Case

Core Windows Forensics: Focus On Analysis

FTK Imager Advanced Techniques

Advanced Acquisition

Mounting Disk Images

File System Overview

Key Word Searching

File Metadata

Data Carving

Core Windows Forensic Analysis



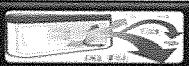
Part 1 String Searching/Data Carving



Part 2 Registry Forensics



Part 3 E-mail Forensics



Part 4 Windows Artifact Analysis



Part 5 Log File Analysis



Part 6 Browser Forensics

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

This page intentionally left blank.



Digital Forensics and Incident Response

CURRICULUM



Key Word Searching



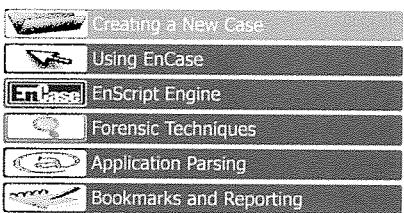
Windows Digital Forensics and Advanced Data Triage © 2014 SANS

This page intentionally left blank.

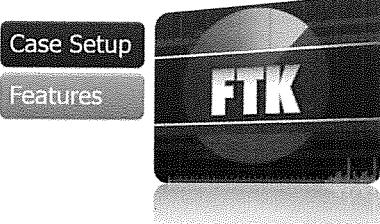
Forensics Suites

- EnCase – Appendix C
- FTK – Appendix D

EnCase Overview



FTK Overview



Windows Digital Forensics and Advanced Data Triage © 2014 SANS

There are two commercial suites that compete with each other for the top position for the most used commercial forensic application: Guidance Software's EnCase and Access Data's Forensic Toolkit (FTK). Both suites speed up the analyst to tackle large scale deep dive forensics capability relatively quickly. One of the core capabilities in these tools is the capability to automatically index every keyword on a system image provided and make it incredibly fast to perform searches through adding the extracted strings to a database for efficiency and speed purposes.

In this next example, we will demonstrate on the core benefits to the commercial tool suites. While we could easily demo it with both EnCase and FTK, we have chosen FTK for this exercise. In Appendices C and D, we have a short tutorial for those in the course who would like a quick primer on how to use these tools. SANS does recommend that if you want a full overview and in-depth course in how to use these tools in the best possible manner, we recommend each of the vendor's training courses that step an analyst through the best usage of their toolset in a variety of situations. In this class, we like to expose you to both toolsets in a neutral way so you can compare and contrast both tools and make a conclusion on your own which tool might be best suited to your needs.

While commercial tools are great, there is usually an equivalent open-source or free capability that also might exist. In many cases, it might not be as intuitive or have the level of support a commercial forensic product might have; but in many cases, if you need to do forensics on a cheap budget, there are many options available to you. This course aims to expose you to as many free and commercial capabilities as possible so you can reach your own conclusions as to which tools you may wish to frequently use in your own investigations.

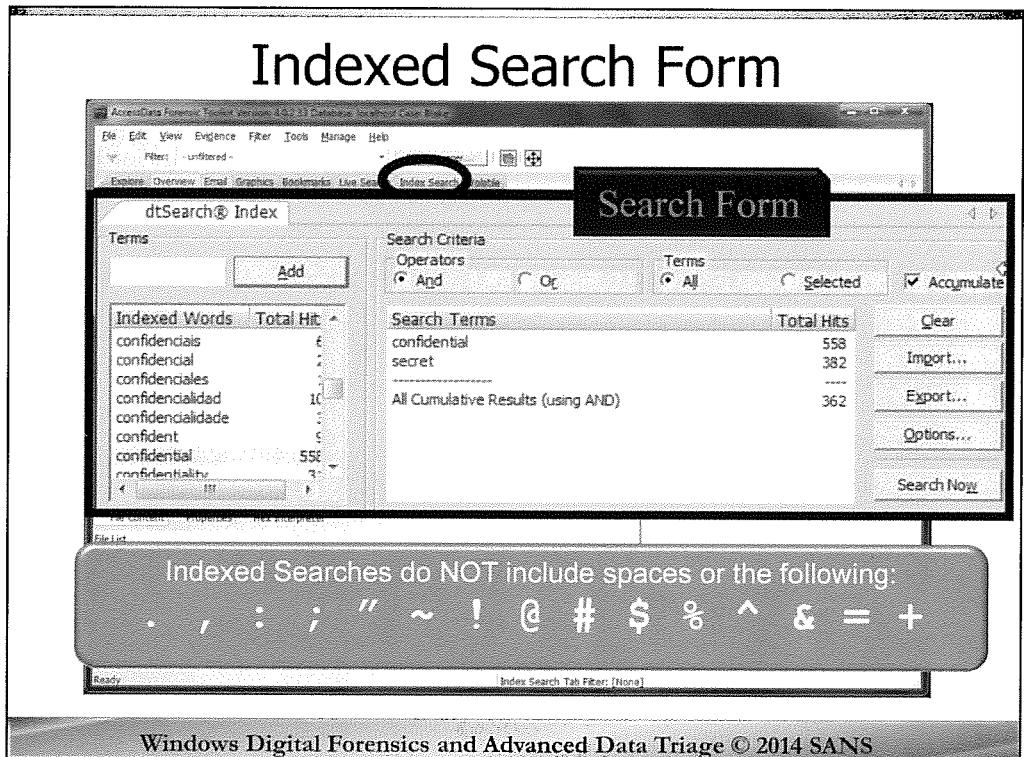
Key Word Lists

- Keywords specific to your case
- List that is used to search for hits on your hard drive
- Modified during an investigation while you perform your analysis

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

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 keywords, you could utilize generic keywords 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 “Key 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.



Click on the Search tab.

The Indexed 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 and UNICODE strings and indexes them.

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 . , : ; " ~ ! @ # \$ % ^ & = + unless you specifically configure it to recognize and those special characters.

AccessData Forensic Toolkit Version: 4.02.33 Database: localhost Case: Blake

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered -

File Search Index Search Options...

dtSearch® Index

Search Criteria
Operators
And
Or
All
Selected
Accumulate

Total Hits
558
382

362

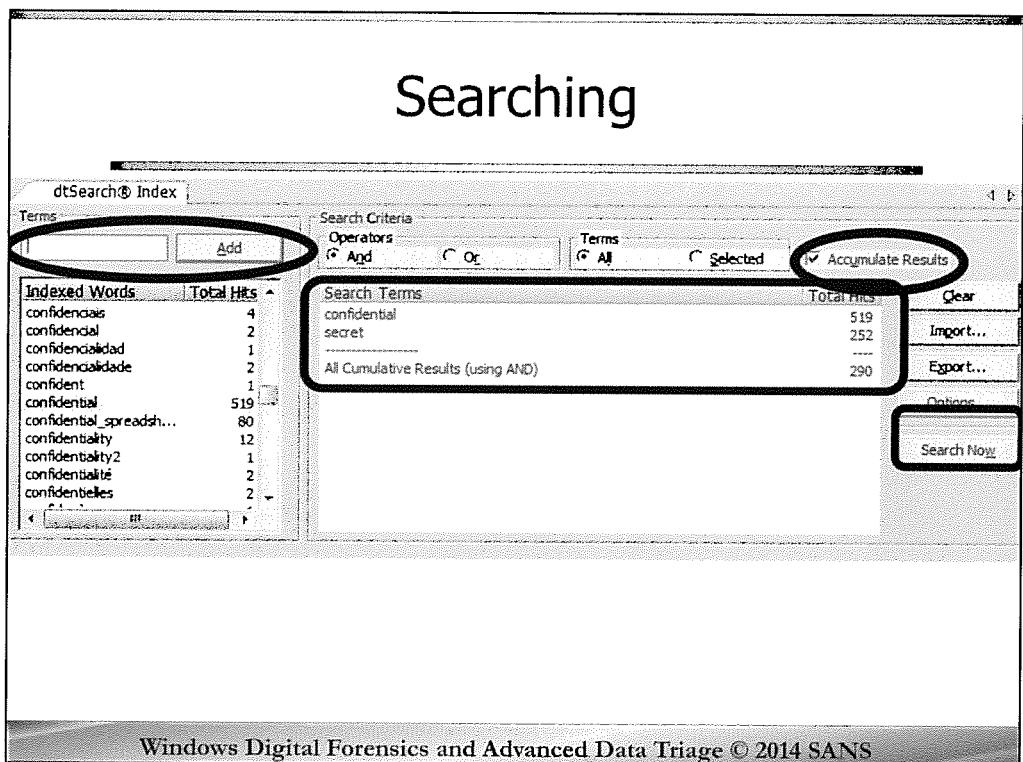
Search Terms
confidential
secret

All Cumulative Results (using AND)

Indexed Words	Total Hits
confidenciais	6
confidencial	1
confidenciales	1
confidencialidad	10
confidencialidade	1
confident	1
confidential	1
confidentiality	1

File Content
File List
Name
\$130
\$MFT
121311
Ready
Index Search Tab Filter: [None]

Indexed Search does not include spaces or
 . : ; , ~ ! @ # \$ % ^ & = +



Once you have clicked on the Index 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 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 252 hits, or instances of Secret.

By adding the additional word “Confidential”, we see that the key word “Confidential” has 519 hits. By checking the “Accumulative Results” box we have now reduced our cumulative total hits of files containing BOTH Secret AND Confidential down to 290 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**”.

44

dtSearch® Index

Search Criteria
Operators
• And
○ Or
Terms
C All
C Selected
Search Terms
confidential
secret
.....
All Cumulative Results (using AND)

Indexed Words Total Hits

Indexed Words	Total Hits
confidenciais	4
confidential	2
confidentialidade	1
confident	2
confidential	1
confidential_spreadsheet	80
confidentiality	12
confidentialité	1
confidentialités	2
confidential	2

519
252

290

Clear
Import...
Export...
Options
Search Now

Index Search Wildcards

Wildcard	Explanation	Example
*	Matches any number of characters	*blake*
?	Matches any character	?blake
~	Stemming (contain the same root)	frack~
%	Fuzzy search (misspellings)	b%%anana
#	Phonic search (similar sounding words)	#giving
&	Synonym search (similar meanings)	quick&
w/5	Word1 within 5 words of Word2 (number is variable)	big w/10 problem
not w/10	Word1 not within 10 words of Word2	help not w/4 desk

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

One of the most powerful features of the FTK dtSearch indexing technology is the capability to perform complex searches within the case index.

You can use wildcard characters such as:

“*” for any number of characters (*blake* matches dblake_personal)

“?” for any single character (?blake matches dblake)

“~” matches words that contain the same root, also called stemming (frack~ matches fracking and fracked)

“%” matches words with similar spellings, also called fuzzy search (b%%anana matches words starting with b and within two different characters of banana)

“#” matches words that sound the same, also called phonic search (#giving matches living)

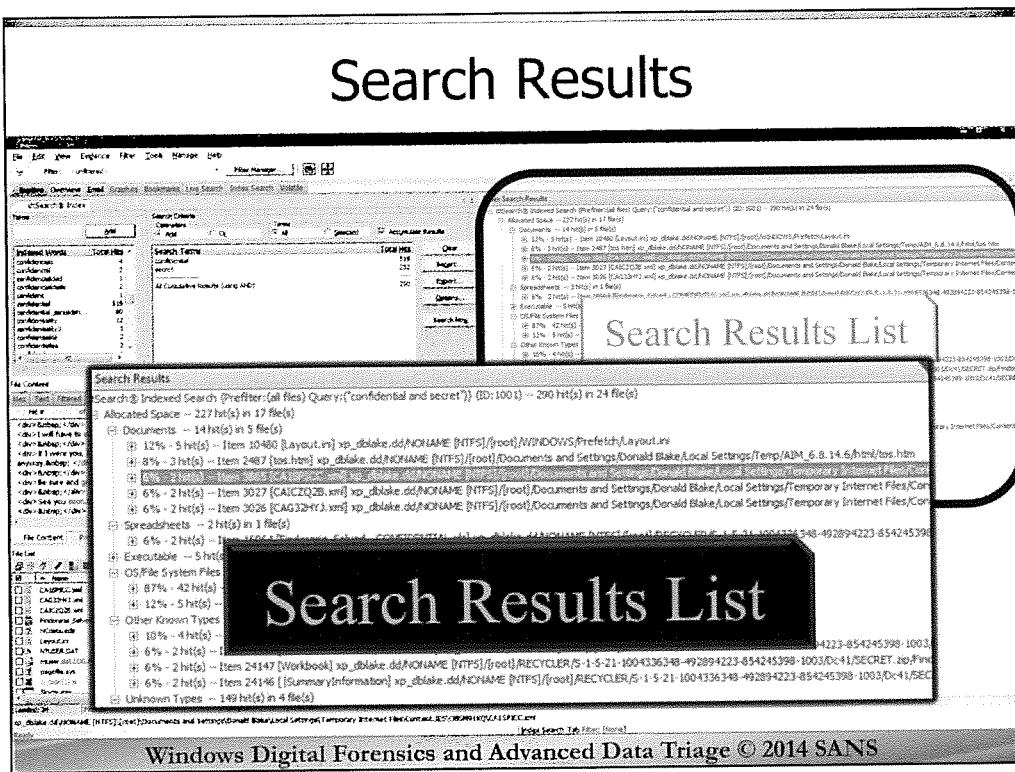
“&” matches words that have similar meanings, also called a synonym search (quick& matches fast)

“Word1 w/5 Word2” - Word1 must occur within five words of Word2 -- number is variable (big w/10 problem matches big darn problem)

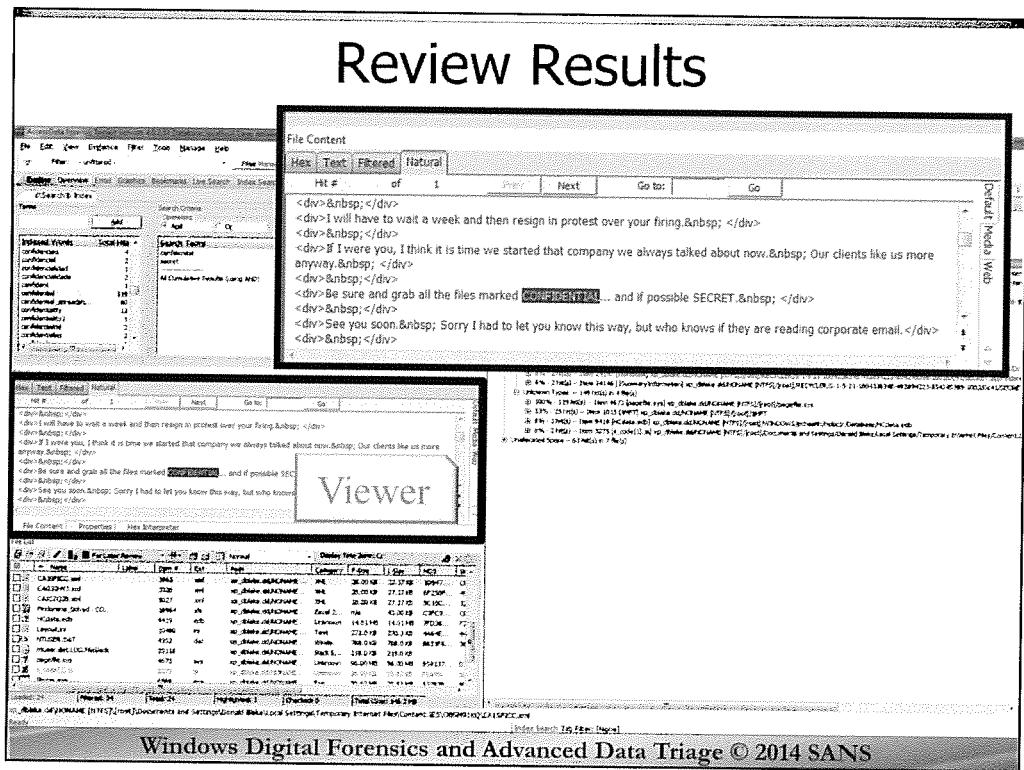
“Word1 not w/10 Word2” - Word1 must occur, but not within ten words of Word2 – number is variable (help not w/4 desk will not match help desk)

Words such as “the” and “if” are considered noise and are ignored.

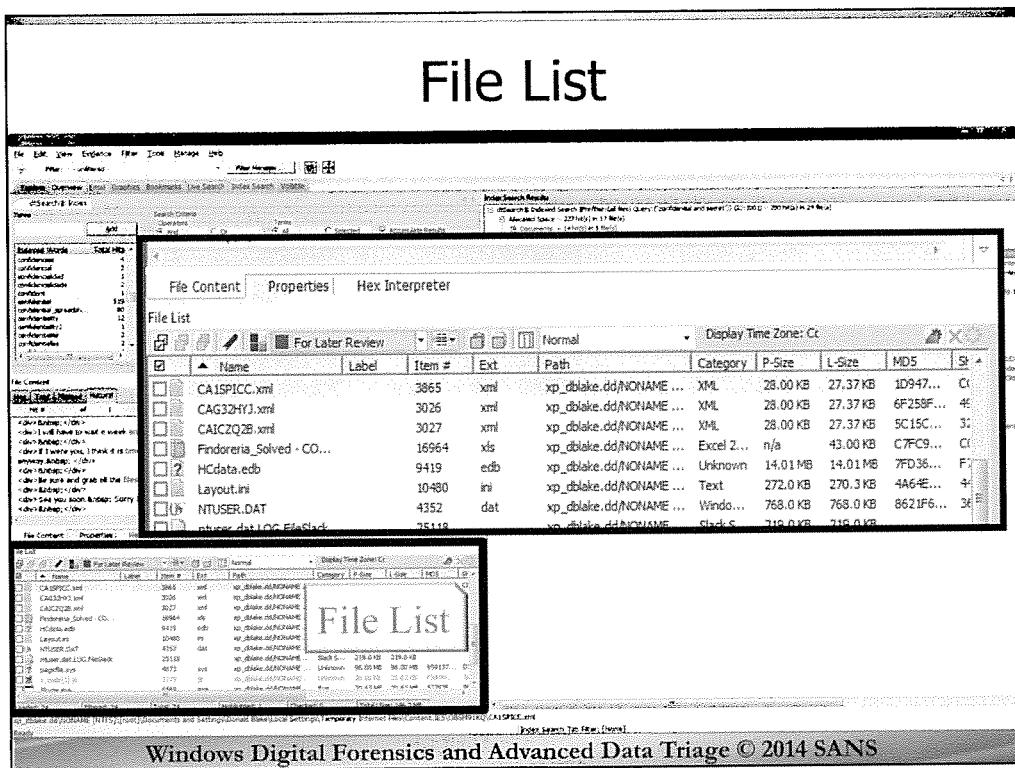
Once you have your search query carefully crafted to give you the best results, click “Search Now” and...



Your results will display in the “**Search Results List**” windows. All your hits are organized by hits found in Allocated and Unallocated Space. Further, the hits are organized by file category. You will see we found 15 hits in 5 document files listed. 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 left 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 left 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. This is where customizing the file list columns can be of value, by only showing those column headings that you feel are most important will help evaluate the information faster.

Triage Review of Hits

- Reconsider your key word
- Review every hit (good luck with that)
- Triage review hits

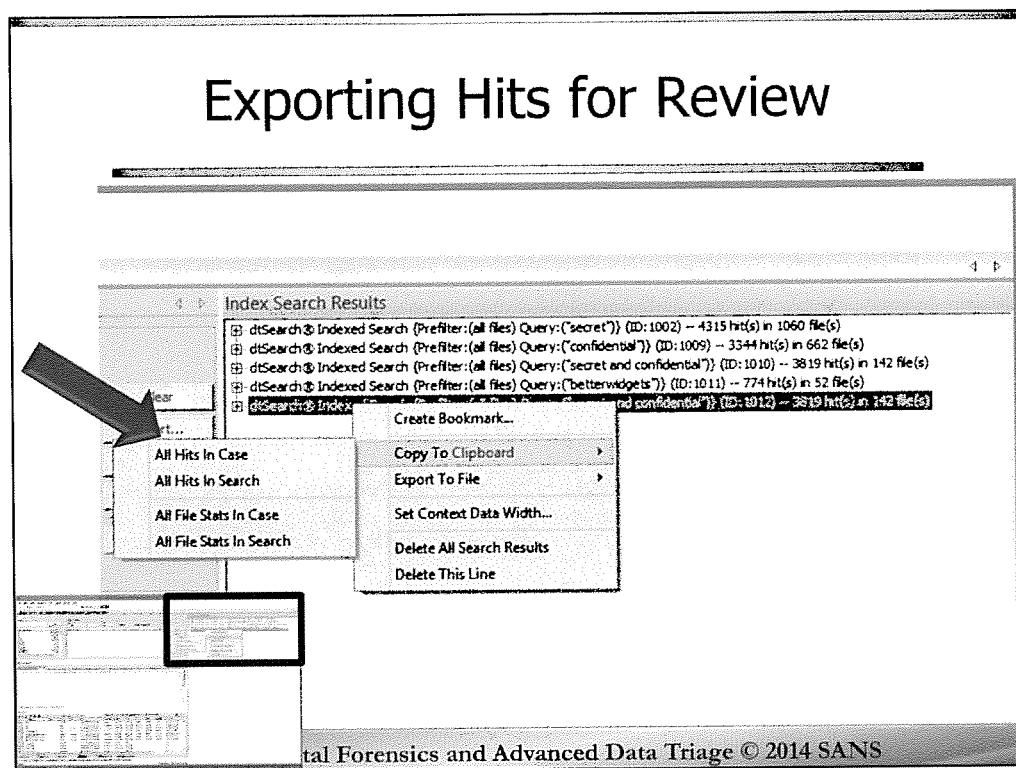
The screenshot shows two side-by-side panels of search results from FTK. The left panel is titled 'Index Search Results' and shows a list of hits under the category 'Spreadsheets'. The right panel is also titled 'Index Search Results' and shows a list of hits under the category 'Documents'. Both panels include a breakdown of hits by file type and item ID. Two arrows point to specific hits in the 'Documents' panel: one arrow points to 'Item 125908 [WACC Calc Spreadsheet.xls]' and another arrow points to 'Item 125908 [WACC Calc Spreadsheet.xls] YYYMMDD-002-CD'. The bottom of the interface displays the text 'Windows Digital Forensics and Advanced Data Recovery © 2014 SANS'.

Many times you will receive thousands of hits for a single key word. There are three ways to deal with this.

First – You can re-evaluate your key word selection. Perhaps there is a better way to search for the intended information. Some words are just bad words to search for on a windows operating system because they will appear thousands of times in a brand new system. In these cases, you may consider making your search term more complex by combining wildcards or filters such as searching for the word “secret” only when it appears within 2 words of the word “confidential”. This technique works best when you have specific information you know about your case and can draw from that information to create complex search terms.

Second – You can review every single hit. This will take forever and is highly accurate however highly inefficient.

Third – You can conduct a triage review of your hits by first looking at the file the hit was found in. This is identified in the FTK Indexed Search Results brackets (e.g. [WACC Calc Spreadsheet.xls]). This is where your training and experience and knowledge of operating systems comes in handy to recognize many operating systems files that may contain a hit for the key word but are highly unlikely to contain information significant to the investigation. After identifying file likely to have significant hits, you can expand the hit to reveal the 10 words surrounding the key word hit. This in many cases is enough to determine if the file warrants further analysis.



FTK is a very resource intensive program. When reviewing search hits, FTK attempts to display all each file and highlight each hit in each file you select to review and sometimes these background tasks can overwhelm the database while and cause FTK to become unresponsive. Thankfully you can export a comma-separated file with all the search hits listed in 6 columns:

Search Term

File Name

File Path, Item Number

Hit Number

and 4 words on both side of the search hit.

Reviewing the 10 words surrounding the search hit in many cases give you context enough to determine if you need further review. You can then go back into FTK to conduct further analysis or examine the file by virtually mounting the image with FTK Imager.

You can export all your search hits at one time (remember, depending on the number of hit you have, be patient) or you can export just the hits for a specific key word search.

To export search hits, right click on one of the search hits in the Indexed Search Results and select “**Copy To Clipboard**”, then select either “**All Hits In Case**” to create a comma separated value (CSV) file with every hit for every key word search conducted or “**All Hits In Search**” to create a CSV file with all hits for ONLY the selected key word search.



Digital Forensics and Incident Response
CURRICULUM



Exercise 3

String Searching

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

This page intentionally left blank.

FOR408 - Section 1 - Agenda

The Donald Blake Case

Core Windows Forensics: Focus On Analysis

FTK Imager Advanced Techniques

Advanced Acquisition

Mounting Disk Images

File System Overview

Key Word Searching

File Metadata

Data Carving

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

The Donald Blake Case

Core Windows Forensics: Focus On Analysis

FTK Imager Advanced Techniques

Advanced Acquisition

Mounting Disk Images

File System Overview

Key Word Searching

File Metadata

Data Carving



Document and File Metadata

String Searching

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

This page intentionally left blank.

Evolution of File Forensics

Document/File Metadata

- Files/Documents Contain Internal File Metadata
 - .LNK Files
 - Location
 - Timestamps
 - Type of Location
 - Office Documents
 - Document Title
 - Version of MS Office Word
 - Last Author
 - Document Creation Date/Time
 - Last Saved Date/Time
 - Last Printed Date/Time
 - Picture/Media Files
 - EXIF Data
 - Camera Make/Model
 - Creation Time
 - Modification Time
 - Photo Information
 - GPS Coordinates (iPhone and other newer cameras)

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

Office internal metadata is a key point of discussion for e-discovery related cases. This metadata is embedded into the file itself and includes information that might be quite useful for a variety of litigation reasons. In many court cases, the judges have ruled that metadata specifically needs to be requested; otherwise, the party is under no obligation to provide it.

What kind of metadata might be included within Microsoft Office documents, picture files, and link files? In most cases, it is data about the file itself. Similar to MP3 metadata (artist, album, rating), metadata would include items that have nothing to do with the actual file, except it helps describe how the data was created, the location, and author.

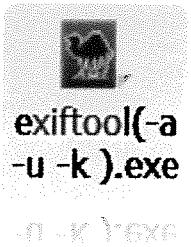
This type of information might be key to a case where one side might want to show a picture was taken at a particular location from a specific camera. Office documents that are stolen and show up inside a different company could be examined to prove that the document originally came from another company.

It is no wonder that many judges are wrestling with metadata requests surrounding e-discovery. It could make or break a case.

Metadata in Media Files

Exif Parsing

- The metadata tags defined in the internal metadata standard cover a broad spectrum including:
 - Pictures
 - Office Documents
 - Audio Fields
 - Video Fields
 - Executable Files
- Tool needed to pull metadata from these data formats easily and quickly
 - `exiftool`
 - Drag and drop file on `exiftool` or execute from command line against picture.
- <http://owl.phy.queensu.ca/~phil/exiftool/>
- Updated Regularly – Update Often!
- Location: Icon on Desktop



Windows Digital Forensics and Advanced Data Triage © 2014 SANS

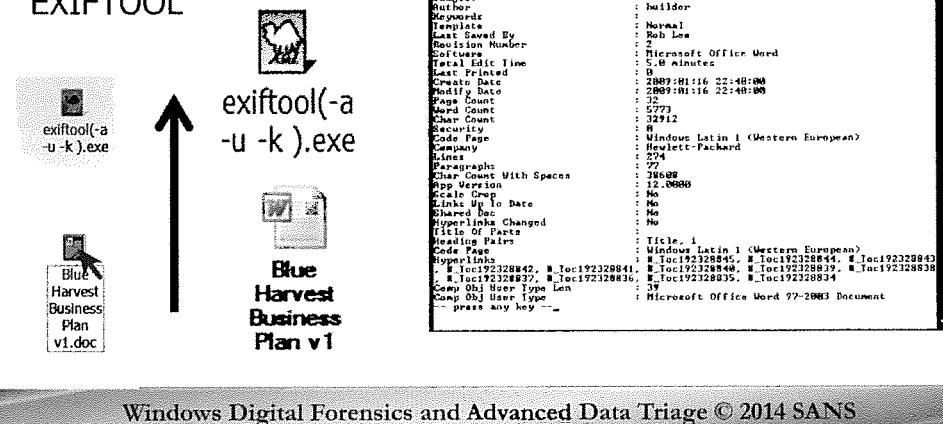
Every picture will have information embedded inside the picture about how the picture was taken. This useful information will include the original picture creation date and the type of camera that was used to take the picture. This information could be critical to an investigation especially if you are trying to link a user's camera to pictures that have shown up somewhere on the Internet. This fingerprint can be pulled out using a tool to parse the Exif data embedded in the picture, audio, or video file.

One of these tools is the exiftool, which is a universal parser for these types of files. The program can be downloaded from <http://owl.phy.queensu.ca/~phil/exiftool/>.

You can simply drag and drop a picture file on top of the exiftool icon to get it to parse the picture's Exif data.

Examining MS Office Metadata

- Browse to a folder containing documents
 - Drag and Drop on EXIFTOOL



Examining the metadata of Microsoft Office documents in the SIFT Workstation is fairly trivial. Simply browse to the folder containing Microsoft Office documents and click on a document of interest. Drag and drop it on top of the EXIFTOOL on your desktop. When you do, in the viewing pane summary information will show the relevant metadata for that Microsoft Office document.

The metadata of the Microsoft Office document will include: author information, creation time, last print time, and in some cases the Microsoft Office version that created it.

Examining PowerPoint Presentations

- Send To: Exiftool
- Examine:
 - Title
 - Author Information
 - Last Author
 - Edit Time
 - Created Time
 - Last Saved Time
 - Last Printed
 - And More

ExifTool Version Number	8.18
File Name	UEAPR_Preso.ppt
Directory	C:/Documents and Settings/sansforensics/Desktop
File Size	11 MB
File Modification Date/Time	2010:04:17 13:51:03 -05:00
File Permissions	r--r--r--
File Type	PPT
MIME Type	application/vnd.ms-powerpoint
Current User	rob
Code Page	Windows Latin 1 (Western European)
Title	Bob
Author	2009 Mandiant presentation template
Template	rob
Last Saved By	rob
Revision Number	1.0
Software	Microsoft Office PowerPoint
Total Edit Time	4.1 days
Create Date	2009:09:19 07:18:06
Modify Date	2010:04:17 18:51:02
Word Count	16752
The file name is...	Copy of 072709_CS_Pensacola_Sec500_Briefing_Sco
File Name suffix	.ppt
File Name Extension	.ppt
File Directory	C:/Documents and Settings/sansforensics/Desktop
Byte Size	148 kB
Exif File Modification Date/Time	2009:09:19 07:06:24 -05:00
No File Permissions	r--r--r--
File Type	XLS
MIME Type	application/vnd.ms-excel
Code Page	Windows Latin 1 (Western European)
Sheet Title	Eval Master Track 1
Screen Reader	Zebra Data
Last Saved By	Bob
Software	Microsoft Excel
Hyperlinks Printed	2009:04:22 19:00:05
Title	2009:09:19 07:18:06
Modify Date	2009:09:19 12:00:24
File Security	0
Code Page	Windows Latin 1 (Western European)
Name	SANS Institute Northcutt
Company	SANS Institute
App Version	12.0000
Scale Crop	No
Links To Date	No
Shared Doc	No
Hyper-links Changed	No
Title Of Parts	Summary, 500.1, 500.2, 500.3, 500.4, 500.5, 500.6
File	Worksheets, 7
Heading Pairs	38
Comp Obj User Type Len	Microsoft Office Excel 2003 Worksheet
Comp Obj User Type	

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

Starting in the upper right-hand corner is an example of using EXIFTOOL to examine a PowerPoint presentation. In this case, you can see similar information in the Microsoft Office PowerPoint presentation that you see in a Microsoft Office Word document.

One of the interesting metadata properties present in this PowerPoint presentation is something called Edit Time. This metadata property fascinates me. If someone creates a new PowerPoint presentation and copies slides into that presentation, then the edit time would be extremely small. However, if someone actually wrote the PowerPoint presentation, the edit time would be quite large.

Examining Office Files (1) (.docx, .pptx, .xlsx)

- Office 2007 Files are compressed archives
- XML Format
- View in FTK
- Summary Data is stored in a .xml file

- docProps/core.xml

The screenshot displays the file structure of an Excel 2007 file (NPV.xlsx) in a file browser. The file contains three main XML files:

- core.xml (selected)
- app.xml
- xl.xml

The XML content of the core.xml file is as follows:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<cp:coreProperties
  xmlns:cp="http://schemas.openxmlformats.org/package/2006/metadata/core-properties"
  xmlns:dc="http://purl.org/dc/elements/1.1/"
  xmlns:dcterms="http://purl.org/dc/terms/"
  xmlns:dcmtypes="http://purl.org/dc/dcmitype/"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <dc:creator>Rob Lee</dc:creator>
  <cp:lastModifiedBy>Rob Lee</cp:lastModifiedBy>
  <dcterms:created xsi:type="dcterms:W3CDTF">2008-03-06T03:38:57Z</dcterms:created>
  <dcterms:modified xsi:type="dcterms:W3CDTF">2008-03-06T03:39:53Z</dcterms:modified>
</cp:coreProperties>
```

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

Starting with Microsoft Office 2007, a new format for Microsoft Office files was released. This format had an “x” extension on the back of the traditional three letter extension (.DOC,.PPT,.XLS)->(.DOCX,.PPTX,.XLSX). The new files are merely compressed archives with embedded XML files.

Inside one of these XML compressed files you will see three directories. One of the directories is called docProps. It is inside this directory where you're going to find a file called core.XML. Inside the file core.XML, you will see your XML formatted summary information and document properties for this particular file.

Notice in the lower right-hand corner, is a new Excel 2007 spreadsheet. After examining the core.XML file inside the docProps directory, you can see that I created the file on March 6, 2008 at 3:38 UTC. You can also notice the last modification time is about a minute later. Notice that the creator is Rob Lee and the last author is also Rob Lee. If someone else had modified the file other than Rob Lee, their name would show up instead.

Examining Office Files (2) (.docx, .pptx, .xlsx)

- Office 2007 Files are compressed archives
- Parsing via EXIFTOOL

File Name	: Forensic Summit EU_v_1.0.xlsx
Directory	: C:/Documents and Settings/sansforensics/Desktop
File Size	: 22 kB
Last Modification Date/Time	: 2010-01-27 00:26:00-05:00
File Permissions	: rw-rw-rw-
File Type	: XLSX
MIME Type	: application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
Creator	: Bob
Last Modified By	: Bob
Create Date	: 2010-01-19 03:08:52Z
Modify Date	: 2010-01-27 05:26:00Z
Title	: Slide 1
Creator	: RobLee
Last Modified By	: rob
Revision	: 579
Last Printed	: 2004-04-22T02:58:01Z
Create Date	: 2001-11-20 21:11:13Z
Modify Date	: 2009-06-13 20:42:49Z
Template	: UrbanReport
Total Time	: 38 minutes
Pages	: 2881
Words	: 15967
Characters	: Microsoft Office Word
Application	: 0
Doc Security	: 133
Lines	: 37
Paragraphs	: No
Texts	: No
Heading Pairs	: Title_1
Titles Of Parts	:
Company	:
Links Up To Date	: No
Characters With Spaces	: 18731
Shared Doc	: No
Hyperlinks Changed	: No
App Version	: 12.0000

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

In this example, we are utilizing the EXIFTOOL to parse the metadata of an Office 2007 Excel document. You can see that Rob Lee is the author and when the file was last printed, created, and last modified. You also see the file path embedded in the document, which could help verify the location of the current file when it was last saved. This could be an important piece of information if trying to identify drive letters and directories.

Exiftool iPhone Picture Analysis

- iPhone Pictures

- Internal GPS

- Time and Date

- Questions:

- When was this picture taken?
 - Where was this picture taken?

```
C:\Documents and Settings\anforensics\Desktop>exiftool.exe IMG_0284.JPG
ExifTool Version Number : 6.94
File Name               : IMG_0284.JPG
Directory              : .
File Size               : 331 kB
File Modification Date/Time : 2009:05:15 00:43:02
File Type               : JPEG
MIME Type               : image/jpeg
JFIF Version            : 1.1
Make                    : Apple
Camera Model Name      : iPhone
Resolution X           : 72
Resolution Y           : 72
Resolution Unit        : inches
Modify Date             : 2009:05:15 00:43:02
File Number              : 1
Date/Time Original     : 2009:05:14 19:45:42
Create Date              : 2009:05:14 19:45:42
Color Space              : sRGB
Exif Image Width       : 1280
Exif Image Length      : 1280
GPS                     :
  GPS Latitude Ref   : North
  GPS Latitude        : 38 deg 59' 8.40" N
  GPS Longitude Ref  : East
  GPS Longitude       : 77 deg 6' 15.00" E
  GPS Altitude        : 5600.1000
  GPS Units           : meters
  GPS Process         : Microsoft Windows Photo Gallery 6.0.6001.18000
  GPS Creator          : Microsoft Windows Photo Gallery 6.0.6001.18000
  GPS Software         : Microsoft Windows Photo Gallery 6.0.6001.18000
Orientation             : Horizontal (normal)
Image Width             : 1280
Image Height            : 1280
Encoding Process        : Baseline DCT, Huffman coding
Bits Per Sample         : 8
Color Components        : 3
YCbCr Cr Sub Sampling : YCbCr4:2:2 (2.1)
Aperture                : 2.8
Exposure Compensation  : 0
Exposure Program        : Program AE
Exposure Value          : 2.8
Flash                   : Off
Focal Length             : 3.6 mm
Focal Length 35mm       : 3.6 mm
Focal Length Fit        : 3.6 mm
Focal Length 35mm Fit   : 3.6 mm
GPS Latitude             : 38 deg 59' 8.40" N
GPS Longitude            : 77 deg 6' 15.00" E
GPS Altitude              : 5600.1000
GPS Units                 : meters
Thumbnail Image          : (Binary data 3559 bytes, use -b option to extract)
```

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

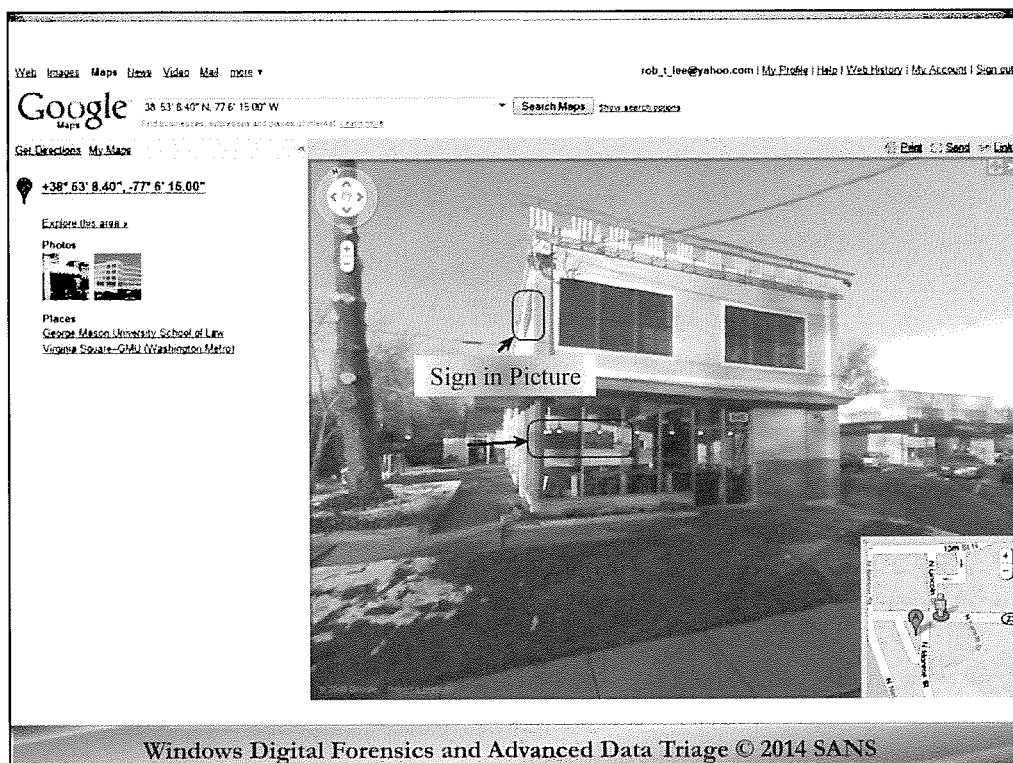
In order to show the true capability of the EXIFTOOL, we will take a look at one of the most popular cell phones on the market, the Apple iPhone. With version 2 of the Apple iPhone, which has an embedded GPS device, every picture taken will be embedded with the GPS coordinates of the location where that picture was shot.

So the two key questions one would have with iPhone pictures would be: 1. When was this picture taken? And 2. Where was this picture taken?

This is example output from an iPhone picture that was taken recently on my iPhone. Notice that you have the device make and manufacturer in addition to the creation date and time, as well as the GPS coordinates embedded inside this picture. Let's take a look at where those GPS coordinates point to using Google maps.

ExifTool Version Number	: 6.94
File Name	: IMG_0284.JPG
Directory	: .
File Size	: 331 kB
File Modification Date/Time	: 2009:05:15 00:43:02
File Type	: JPEG
MIME Type	: image/jpeg
JFIF Version	: 1.1
Make	: Apple

Camera Model Name : iPhone
X Resolution : 72
Y Resolution : 72
Resolution Unit : inches
Modify Date : 2009:05:15 00:43:02
F Number : 2.8
Date/Time Original : 2009:05:14 19:45:42
Create Date : 2009:05:14 19:45:42



Plugging the GPS coordinates into Google maps is a fairly simple process. I switched from map view to Google Street view so I could tell what I'm looking at. I rotated the viewing camera to the left and can see the location where the picture was taken. On the picture we saw a sign called Rocklands barbecue. Notice on the side of the building you actually see the same sign. The picture was actually taken next to the tree that you see in the lower left-hand side of the picture.

As you can tell, being able to use the exiftool to mine the metadata, including the GPS coordinates out of a picture, could prove fairly useful during the computer investigation.

FOR408 - Section 1 - Agenda

The Donald Blake Case

Core Windows Forensics: Focus On Analysis

FTK Imager Advanced Techniques

Advanced Acquisition

Mounting Disk Images

File System Overview

Key Word Searching

File Metadata

Data Carving

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

The Donald Blake Case

Core Windows Forensics: Focus On Analysis

FTK Imager Advanced Techniques

Advanced Acquisition

Mounting Disk Images

File System Overview

Key Word Searching

File Metadata

Data Carving



Digital Forensics and Incident Response

CURRICULUM



File Carving

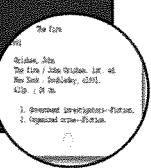
Windows Digital Forensics and Advanced Data Triage © 2014 SANS

This page intentionally left blank.

How File Carving Works: Recovering Deleted Files

- Using file pointers to recover data of file
- Metadata includes
 - MFT Entry
 - FAT Directory Entry
- Uses
 - Cluster Starting Address
 - File Length
- Can handle fragmented files

Metadata Method



- File headers
 - Example (.exe = "MZ" Header or "4d 5a 90 00" in Hex")
- Scanning at cluster start
 - Look for "MZ" header at beginning of every cluster
- Guesswork at best to figure out end of file unless footer exists
 - Look for footer or end at max size
 - whichever comes first

Data Layer Method



Windows Digital Forensics and Advanced Data Triage © 2014 SANS

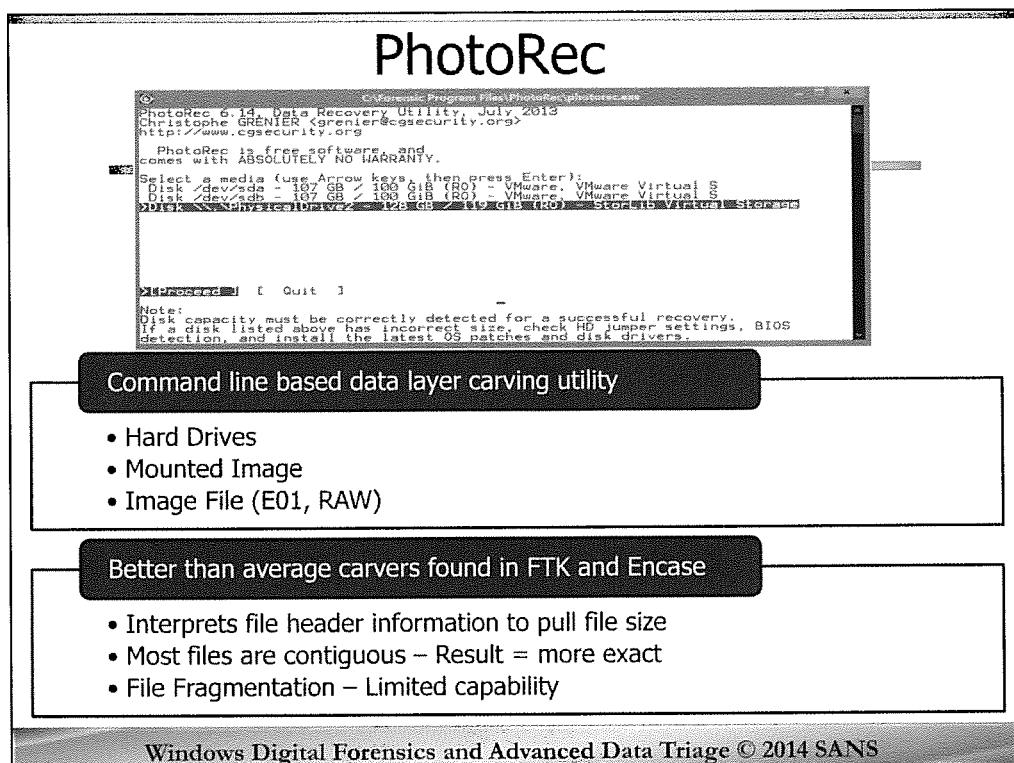
Forensics is probably best known to the average individual for the ability of investigators to recover lost or deleted files from a file system. However, most of the time the recovery of files is limited to Metadata layer extraction. What this means is that a file is recovered by examining the file properties such as the starting cluster, the file size, file name, and parent directory. On an average system, extracting deleted data is easiest using this methodology. The difficulty is that many modern operating systems recycle these deleted metadata locations quickly and as a result over write the data that is stored there.

Even if the metadata of a file is overwritten, in many cases it is still possible to recover a file from the data layer and clusters of a file system volume. Tools that focus on unallocated space extraction can scan the beginning of every cluster looking for file headers that match known file types.

A file header is how a file usually identifies itself to the application trying to interpret the unique data. These common headers have key file information that is passed to the application so that the application can perform a sanity check to ensure the file is indeed valid. File headers become unique as a result and become similar to a fingerprint for a file. The file header can be as small as two bytes and as large as 64 bytes in some instances.

When a program is used to scan a file system volume looking for these headers, it has a good chance at carving the deleted files out of unallocated space by carving the file once a header it is looking for is found. For example, a Windows Executable has a file header commonly called the "MZ" header. In bytes it is 0x4f, 0x5d, 0x90, 0x00. The 4f corresponds to an ASCII "M". The 5d corresponds to an ASCII "Z". If a carving utility finds the exact header above, the file in unallocated space that has found is likely to be a windows executable (.exe) or a dynamic library (dll).

Once the file carving begins, the file is carved out until it finds a file footer. If a file footer does not exist, then it usually makes a guess as to an appropriate file size usually based on similar files. In some cases, the file carving tool might be able to scan the header of the file for the exact size of the file. Certain files will embed the file size into the header itself and this information can be used to accurately extract the exact file from unallocated space.



PhotoRec is a file carving program that is command line based. Files carved using PhotoRec use prebuilt internal signatures targeting many media file types. PhotoRec can be used directly against a hard drive or against a mounted drive image using FTK Imager. Photorec can be downloaded here:

<http://www.cgsecurity.org/wiki/PhotoRec>

One of the better features of PhotoRec is the ability of the tool to read the header of the files in order to do a much better job of accomplishing file carving by being able to interpret file size that is possibly stored in the header. PhotoRec will truncate the size of the file to exact specifications. If a carved file ends up being smaller than what the file size shows in the header then the file would be discarded.

It also has some limited capability to handle fragmentation. It can accomplish this by looking at the previous clusters to see if a file signature was found and the file was not able to be carved out. It will attempt to try and carve the file again with the additional data. However, even with this additional capability to look back and attempt to join the data together, if a file is severely fragmented more than 2 places, I have found that it recovery of the file is probably going to fail. However, it is one of the few tools out there that even attempts to accomplish this and is unique in that perspective.

©
PhotoRec 6.14 Data Recovery Utility, July 2013
Christophe GRÉNIER <grenier@cgsecurity.org>
<http://www.cgsecurity.org>

PhotoRec is free software and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys then press Enter):
Disk /dev/sda - 107 GB / 100 GiB (RO) - VMware, VMware Virtual S
Disk /dev/sdb - 107 GB / 100 GiB (RO) - VMware, VMware Virtual S
Disk \\.\PhysicalDrive2 - 128 GB / 119 GiB (RO) - StorLib Virtual Storage

>[Proceed] [Quit]

Note:

Disk capacity must be correctly detected for a successful recovery.
If a disk listed above has incorrect size, check HD jumper settings, BIOS
detection, and install the latest OS patches and disk drivers.

How Does PhotoRec Work?

- Reads Boot Sector to Determine Cluster Size
- Identifies files by header information
 - Knows over 320 file types
 - Media Files
 - Executables
 - Shortcut (LNK)
 - Index.dat
 - Archives (.rar, .zip, 7z)
 - And many, many more ...

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

How does PhotoRec work? PreBuilt Signatures

PhotoRec reads the Boot Sector of the NTFS or FAT partition to determine the cluster size. Once the cluster size has been determined it reads the target file system volume by cluster and examines the initial header of a file. The signatures are prebuilt inside PhotoRec.

PhotoRec has the ability to carve out over 320 different types of files. Almost every windows based media file is already specified to be carved out included executables, shortcut (LNK), and Internet Explorer index.dat files. Not only that, it does a wonderful job at carving out archives and multimedia file types. While not having the most intuitive and pretty interface, photorec is a very powerful tool indeed.

PhotoRec File Types

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

This page intentionally left blank.

Archives	Multimedia	Multimedia2	Multimedia3	Multimedia4	Multimedia5	Others	Others2	Others3	Others4	Others5
.7z/.Zip file	3dsmax	ctb Custom shapes	.iso CD/DVD iso image	.pcx PCX file format	.sld AutoSketch drawing 1cd	.dbx Outlook Express	.frm MySQL table definition	.mdb xlsx PassX	.ods Diazo • Sonar Data	
a Unix/Linux	3gp Video	ctg Canon catalog	.it Impulse Tracker	.psb Photoshop Image	.smil	.acdpc	.dt TSC Survey	.frm	.pdf files holding PKCS#12 key	
ace ACE	3gp Video	cue Cue sheet	.iTunes	.psd PentaX Raw picture	.psps SPS	.ad Mac Address Book	.dfi Division	.fsl QuickBook	.lrf SQL Server	
.ari	abr Brush	db Thumbs.db	.inf JPEG Network Graphics	.pgm Portable GrayMap	.sr2 Sony Raw picture	.adr Opera Hotlist	.dav Davik	.fs Zone data	.lrc ITUT/LIS	
bifMS	abb Color Book	dri Kodak Raw picture	.jpe JPEG 2000	.png	.svg Scalable Vector	.agn Autogen	.dgm Microstation	.fwd FWD Sports Computer	.lnk Link (shortcut)	
bz2 bzp2	ado Duotone Options	dif Dvu	.jpg JPEG picture	.pmf Portable anmap	.swc Flash	.ahn Ahnenblatt	.dlf Lotus Data	.gam Gam's Factory	.lzo Logic Platinum File	
cam MS cabinet	bmp After Effects	drg Digital Negative	logic Apple Logic Studio	.ppm Portable PFM Map	.swf Flash Compiled	.amb Licom AlphaCAM	.dim Sun/CAD DistImage	.gcs Guitart	.lwo 3d model	
dar dar3	aif Apple Audio	dpr Designer	m2t Blu-ray/MPEG-2	.pproj Premiere project	.tif Tag Image File Format	.ard AlphaCAM	.diskimage Sun/FCI Disk Image	.ext XFI	.lwo (two 3d model)	
deb Debian	album MP Photomatix	dpx	m2ts Blu-ray/MPEG-2	.psd Photoshop Image	.tivo video record	.amr Adaptive Multi-Rat. DLL	.dynamiclink Library	.gbo Ghost Image file	.ly LilyPond	
dump	ai! Cubate Sceneformat	dz2	m3u Movie Picture Expert	.psf Print Shop File	.ted Blu-ray/MPEG-2	.amr AlphaCAM	.dmp Oracle Dump (export)	.jmg6 Game Maker	.mat Matlab	
EZip Data	ais Ableton Live Sets	dic Nikon DSC	max 3ds	.pspl P	.tpl Tool Preset	.apa APAtile Helper	.drw Pro/ENGINEER Drawing	.jmd Game Maker	.mcu Vector Fields	
fb2fbf/fArc	ani Animated Cursor	dss Digital Speech Standard	max Paperport	.ptb PowerTab	.ts MPEG-2 Transport	.apple	.dwf Drawing Interchange File	.scf GPG/OpenPGP	.mdf SQL Server	
iso ISO	ape Monkey's Audio	dta SPSS	mb Waya	.pts PTSU	.wav RIFF audio	.asm	.e01 Encase	.grb Scribus	.mdl Matlab Model	
pa2	arn Sony raw image	dr0f Digital Video	mfa The Games Factory	.wpd Php Video Pro	.wpd JPEG XR	.asp ASP script	.scr Encrypted file by eCrypts	.h Header	.pst Outlook	
.jar Rat	asf, wma, wmv	divi AutoCD	midb iTunes	.qcpl The QCPL File Format	.webm Marosia	.ard AgeLine	.hdri Hierarchical Data Format	.mif Pro/ENGINEER	.pri Pro/ENGINEER Model	
.rpm RPM package	asf Layer Style	emi Enhanced Metafile	mid MIDI	.qtl Apple QuickTime 100	.wmf Metaphie	.ard AlphaCAM	.adb Exchange Database	.hdri ENV	.pmr Delcam PowerSHAFT	
.rtf StuffIt	auSurf/Next! audio data	ersF Mapper Rasters	mkv Matroska	.qd DarkXpress Document	.wlpk OpenCanvas files	.axx Ax:Crpt	.hdri Parallel disk image	.mmi Memosync Data Base	.pri Python Compiled Script	
.tar tar	avi RIFF video	ers-A Apple Logic	mmg Multiple-image	.qpl QuarkXpress Document	.wpf PlayList	.bic Bacula backup	.emka ENKAI DX	.mif Migration Backup	.pcx Python Compiled Script	
.tar.gz tar	bimov Binov VoiceFile	fcf Final Cut Pro	mov Quicktime Movie	.z3d RED 3d camera	.wt Media Center TV	.bit Dos/Batch	.emk Mac OS X Mail format	.mif Custom CAD-CAM	.pri GraphPrism 4	
.wim imaging	blk blender	fn10 Freehand 10	mp3 MP3/ACT	.tarw Fujifilm picture	.wt Media Center TV	.bam WaWPack	.epi Encapsulated PostScript	.http HTTP Cache	.pri Mozilla "mark database"	
x2v	blend Blender	fn5 Freehand 5	mp4+MPEG 4	.tarw Real Media	.x3f	.bd	.ext Event Log	.ics vCalendar	.pri Mozilla "mark database"	
.zip zip	bmp BMP bitmap image	flac	mpeg Moving Picture	.tarw Real Audio	.xcf GIMP XCF File	c	.exe executable (PE)	.imbinedmail	.pri Mozilla "mark database"	
caf Core Audio Format	fla Flash Project File	mpl Maya	raw Contact picture	.xm			.fsl SymBackup	.img levault	.pri Mozilla "mark database"	
.cam image	flp Fruity Loop	mpo Multi-picture format	rdc Collie picture	.xm			.fsl Dynamics NAV	.imm Incredimail	.pri Mozilla "mark database"	
CATDrawing CATIA	.fv	mrw Minolta Raw picture	rm Real Media	.msc Reason Music Score			.fsl Dynamics NAV	.fcs Flow Cytometry Standard 3 inf Autoren	.pri Mozilla "mark database"	
.cds CD Audio	.gif		msi Finale Music Score	msi Reason			.cls VB	.fsl Dynamics NAV	.pri Mozilla "mark database"	
.cdd Concept Draw Document	.ipb Guitar Pro 5	mwz MetaStock	rms Reason Audio File	.cm Comic Life			.ini	.ini	.pri Mozilla "mark database"	
cdl Concept Draw Library	.icc Color profiles	naf Nikon Raw Picture	rp2 Reader Project				.fsl TwiNES Disk Image	.jad Java application Descriptor	.pri Mozilla "mark database"	
.cdf Corel Draw	.ico Icon	oci OpenCanvas image	rv2 Panasonic Raw 2				.fsl Fortran	.jav Java	.pri Mozilla "mark database"	
.cot Concept Draw Template	.idf MDI Instruments	ogg OGG Verbs audio	rx2 Zortech RX 2,				.cp_ MS File (Z2D)	.fsl Freehand 10	.pri Mozilla "mark database"	
comicdoc ComicLife	.indd InDesign File	ogm OGGS audio	sas Tool Edit/				.dts Diabol	.fts	.pri Mozilla "mark database"	
.cpr Cubase Project File	.ifo DVD Video manager	orf	shn Shorten audiofile				.dat Index dat	.fsl Dynamics NAV	.pri Mozilla "mark database"	
.crc Canon Raw 2 picture	Indd IndDesign	phm Portable Bitmap	subbelius				.def Disease 3	.ip2 File Maker Pro	.pri Mozilla "mark database"	
.crw Canon Raw picture	Info ZoomBrowser	.ppt Macintosh Picture	.sit Nitron				.dbi DriftBox	.xdblesp AtX	.pdf Portable Document Format	

Adding Signatures to PhotoRec

- PhotoRec searches for the signature file named
 - **photorec.sig** in %USERPROFILE
 - C:\Documents and Settings\rob\
 - C:\Users\rob
 - File must contain one signature per line
 - Signature contains
 - Extension name
 - Offset
 - Signature in hex or text strings
 - Use **fidentify.exe** to verify

EXT	OFFSET	SIGNATURE
pfx	0	0x1100000053434341
pf7	0	0x1700000053434341
pf8	0	0x1a00000053434341

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

PhotoRec searches for the signature file named

photorec.sig in the USERPROFILE or HOMEPATH directory, i.e.. C:\Documents and Settings\rob\ or C:\Users\rob.

photorec.sig in the current directory

The file must contain one signature definition per line. A signature is composed of the extension name, the offset of the signature, and the signature or magic value. The magic value can be composed of a string, i.e. "data". Special characters can be escaped like "\b", "\n", "\r", "\t", "\0" or "\\". Hexadecimal data, i.e. 0x12, 0x1234, 0x123456... Note that 0x123456, 0x12 0x34 0x56 and 0x12, 0x34, 0x56 are equivalents. Note, space or comma delimiters are ignored

By using a hexadecimal editor, you can see that the pf file from our example begins by a distinctive string.

The signature can be written as

ext 0 "TEXT String"

or

pfx 0 0x1100000053434341

pf7 0 0x1700000053434341

pf8 0 0x1a00000053434341

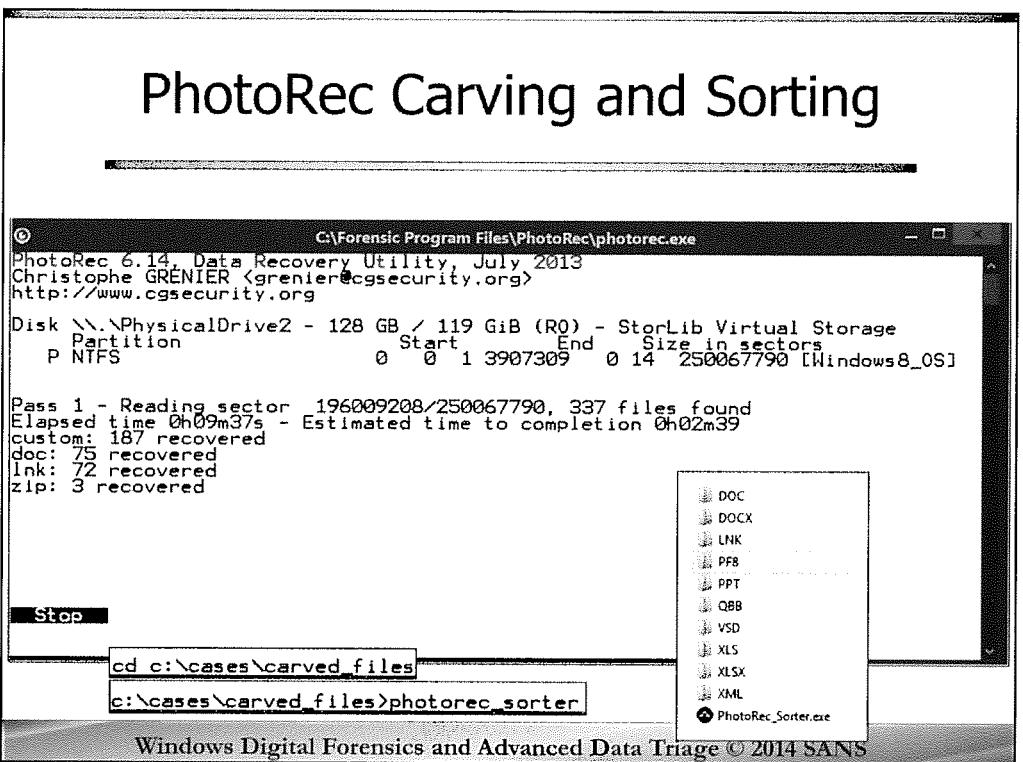
In this next step, we will use the photorec tool called **fidentify** to verify the signatures we just added to our tool. It accomplishes this by using real files and makes sure that when those files are scanned the signature of the header will match. To do this simply run **fidentify.exe *.pf** to scan all the prefetch files found in the exercises directory. Once completed each of the CSRSS prefetch files harvested from different versions of Windows should match their equivalent operating system. A correct execution is shown below

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd c:\cases\exercises\prefetch
c:\cases\exercises\prefetch>_
```

```
C:\Windows\System32\cmd.exe
c:\cases\exercises\prefetch>fidentify.exe *.pf
CSRSS.EXE-WIN7.pf: pf7
CSRSS.EXE-WIN8.pf: pf8
CSRSS.EXE-XP.pf: pfx

c:\cases\exercises\prefetch>_
```



You end up with a bunch of numbered folders prefixed with “recup_dir.” and each folder has different file types (unless you only chose to recover one file type – in that case, this utility is not much use to you).

PhotoRec Sorter (this script) is executed from the same directory as the “recup_dir” folders and moves each file into a new folder matching the name of the file extension (in upper case, ex. PDF, DOC, PPT)

So you end up with all the recovered files being sorted into folders by file extension.

Move PhotoRec_Sorter.exe to the directory containing the “recup_dir” folders created by PhotoRec.

Run PhotoRec_Sorter.exe and pay attention to the console output.

Once PhotoRec Sorter has finished executing, be sure to look through the “recup_dir” folders for any files that did not get properly sorted.



Digital Forensics and Incident Response

CURRICULUM



Exercise 4

File Carving

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

This page intentionally left blank.

Forensic Links/References

SANS

- <http://computer-forensics.sans.org>
- http://www.sans.org/reading_room/white_papers/forensics/
- <http://www.sans.org/newsletters/>

Computer Forensic BLOGS

- <http://windowsir.blogspot.com>
- <http://www.forensickb.com/>
- <http://cfed-ttf.blogspot.com/>
- <http://seccure.blogspot.com/>
- <http://jessekornblum.livejournal.com>
- <http://computer.forensikblog.de/en/>
- <http://www.forensicblog.org>
- <http://geschonneck.com/index.php>
- <http://www.forensicblog.org>
- <http://www.forensicfocus.com>
- <http://forensicir.blogspot.com>

- <http://www.msuiche.net>
- <http://volatilesystems.blogspot.com/>
- <http://blog.mandiant.com>
- <http://computer.forensikblog.de/en/>
- <http://digfor.blogspot.com/>

Legal Blogs

- <http://ralphlosey.wordpress.com>
- <http://www.granick.com/blog>
- <http://idethelightning.senseient.com>
- <http://commonscold.typepad.com/eddupdate/>
- <http://www.ediscoverylaw.com>
- <http://www.ediscoverylaw.com>
- <http://legal-beagle.typepad.com>

Computer Forensics Podcasts

- <http://cyberspeak.libsyn.com>
- <http://forensic4cast.com>

Computer Forensics Wiki <http://www.forensicswiki.org>

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

This page intentionally left blank.



Digital Forensics and Incident Response

CURRICULUM



Here is my lens. You know
my methods. -Sherlock Holmes

Any additional questions:

oviecarroll@gmail.com twitter @ovie

rlee@sans.org

twitter @robtleee

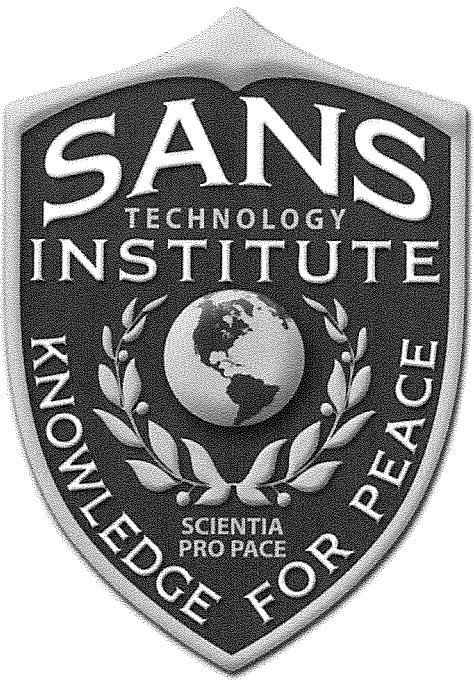
ctilbury@sans.org

twitter @chadtilbury

twitter @sansforensics

Windows Digital Forensics and Advanced Data Triage © 2014 SANS

This page intentionally left blank.



This Course is Part of the SANS Technology Institute (STI) Master's Degree Curriculum.

If your brain is hurting from all you've learned in this class, but you still want more, consider applying for a Master's Degree from STI. We offer two hands-on, intensive Master's Degree programs:

- Master of Science in Information Security Engineering
- Master of Science in Information Security Management

If you have a bachelor's degree and are ready to pursue a graduate degree in information security, please visit www.sans.edu for more information.

www.sans.edu

855-672-6733

info@sans.edu



FTK Imager Primer

The SANS Institute
Ovie Carroll – oviecarroll@gmail.com
Rob Lee – rlee@sans.org

 @sansforensics <http://computer-forensics.sans.org>

Appendix A - FTK Imager Primer © 2014 SANS

Authors:

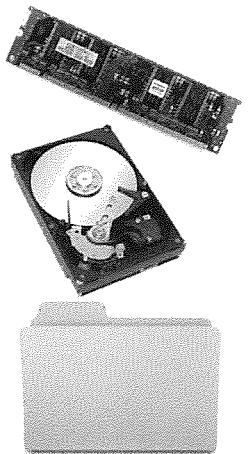
Ovie Carroll – oviecarroll@gmail.com
Rob Lee – rlee@sans.org

<http://twitter.com/robtleee>
<http://twitter.com/sansforensics>

Special Thanks to Chad Tilbury, Ovie Carroll, and Jenny Delucia. Your thoughts, opinions, research, and insight were invaluable to the creation of the course.

Types of Acquisition

- Memory Acquisition



- Physical – Entire Drive

- Logical – Just a Partition

- C:\

Appendix A - FTK Imager Primer © 2014 SANS

When we talk about acquisition, we are talking about typically three types of acquisitions that you will conduct as a forensic examiner and incident responder.

The first is memory acquisition, which is also sometimes referred to as volatile data collection. For incident responders investigating hacking cases this is not really anything dramatically new but for non-hacking cases, cases like child porn or any other type of crime, in the past, incident responders have typically taken a hands-off approach to running computers with respect to documenting the volatile data including RAM.

The second is the most common, called a physical acquisition. This is what all forensic examiners are familiar with and that is the imaging of hard drives and other disk based or solid state memory.

The last type of acquisition is a more targeted type of acquisition that is referred to as a Logical acquisition. This is when incident responders go into businesses and image portions of a server, perhaps only imaging certain directories that the subject/user has write permissions to access and store data.

Physical/Logical Device Names

Name	Definition	Windows
Physical	Entire Hard Drive	PhysicalDrive0
Logical	Partition Only	C:

Appendix A - FTK Imager Primer © 2014 SANS

This is a chart to easily show you the differences in architecture between a typical Linux-based system and a Windows one.

The first physical drive is referred to as \\PhysicalDrive0 and subsequent drives would be identified as 1,2,3 etc. As you may have learned when looking for computers on your network neighborhood, the nomenclature for your local drive is “\\.”

The physical volume or partition on a hard drive is commonly referred to as a drive letter. C: is the common value for the system's main partition. In the Unix world, this would be equivalent to the /dev/hda1 or /dev/sda1.

For dd.exe to work correctly you need to become familiar with how Windows calls the nomenclature of these entire drives instead of looking for a single file on these drives. The entire drive C: is called “\\.\C:” or the entire D: is called “\\.\D:”

Typically, time will be a factor in determining if doing an entire copy of a volume is necessary. Based on how fast your hardware is, I have seen this process take as slow as a gigabyte an hour. A helpful hint here to save space on your target media is to use an NTFS file system with file compression enabled. A 20-gigabyte volume could be reduced to a 3-gigabyte image.

Physical Images

- Physical drive imaging
 - Grabs entire drive (MBR to the final sector)
 - Unless obtaining a RAID or special device, grab the physical partition

Appendix A - FTK Imager Primer © 2014 SANS

You should at least know what kind of drives you would need to backup. In most cases, imaging the entire physical drive would be the best choice. This is a bit more difficult in a Windows environment than a Unix one since you do not have access to the raw devices. However, you will have access to the logical drives that are partitioned on your system.

Physical backups are recommended since you will be able to grab the entire drive contents which would include swap space that is being used by your computer.

Logical Images

- Logical imaging
 - File System Partition Only (NTFS, FAT, EXT)
- WHY Logical
 - Targeted partition, folder/directory or file extraction
 - RAID devices (Striped Array)
 - Encrypted Physical Drive

Appendix A - FTK Imager Primer © 2014 SANS

Logical backups are most commonly used when imaging RAID systems or corporate systems where you only need or are authorized to image/extract a specific partition, directory/folder or set of files.

Later in the course, we will demonstrate how you can use FTK Imager to image a specific partition, directory/folder or set of files, yet still do this in a manner that each file, or partition, is imaged in such a way that you can later verify their integrity.

Logical backups are also recommended if you have a RAID system that has multiple hard drives in it. It would be incredibly hard to piece this back together using each individual drive. At a minimum, you would need a similar RAID system. However, in this case, by simply imaging each logical drive onto a separate media would accomplish your goal in evidence seizure.

Logical backups are also recommended if you discover your Physical Drive is Encrypted.

Labeling and Types of Evidence Copies

Evidence Tag = YYYYMMDD-(case##)-(Seq#)

- Casename-Evidence Number
- Year/Month/Day-Evidence Number
- Example = **20090716-001-001**

Original Evidence

- Name says it all. The original evidence that copies were made from

Best Evidence

- Evidence you should secure and never touch
- If original evidence is damaged or had to go back into production, this is the copy of the evidence that all other copies would be made

Working Copy

- Made from copy of original evidence or best evidence
- Working copy is the evidence you analyze using forensic tools

Appendix A - FTK Imager Primer © 2014 SANS

This naming convention will allow you to immediately date the evidence and know which case and evidence tag number it is from. The original collection information should be stored on a chain of custody form. You should also create and maintain a log of all evidence items you create at the search scene. This log should list the name of the image, person who created the image and location where the image was originally located. This log will be a great reference tool later when you have 100 image files from one search and want to know the name of the image file from the computer located in Mr. Smith's office.

NOTE: Great caution should be taken when considering the naming conventions. The above listed naming convention would be detrimental if you were creating or moving image files on a system with an 8.3 file name limit. All your images would essentially be the same name of YYYYMMDD. In these cases, you may want to consider reversing the naming convention leading with the evidence sequence number, then case number, then YYYYMMDD.

One suggestion is to label the evidence using a YYYYMMDD## format. It will allow you to immediately date the evidence and know which evidence tag number it is. The original collection information should be stored on a chain of custody form.

Evidence Tag = **YYYYMMDD - (case##) - (Seq#)**

Casename-Evidence Number

Year/Month/Day-Evidence Number

When you initially acquire evidence you should always try and retain the original evidence if possible. In many cases, this will not be possible. In some cases the system will need to be put back into production and other cases it will need to go back to the original owner. A copy might be the only piece of evidence you have. This first copy of the evidence should be labeled the BEST EVIDENCE. The BEST EVIDENCE is critical to your case.

Best Evidence

Evidence you should secure and never touch

If original evidence is damaged or had to go back into production, this is the copy of the evidence that all other copies would be made

The second copy of the evidence you make should be labeled the WORKING COPY. The WORKING COPY is the evidence you will actually examine.

Working Copy

Made from copy of original evidence or best evidence

Working copy is the evidence you analyze using forensic tools

Store the original evidence, if possible, and the BEST EVIDENCE in a secure safe/room utilizing the chain of custody properly along the way.

Most guidelines state that it requires the use of an original, which also provides that a "duplicate" is admissible.

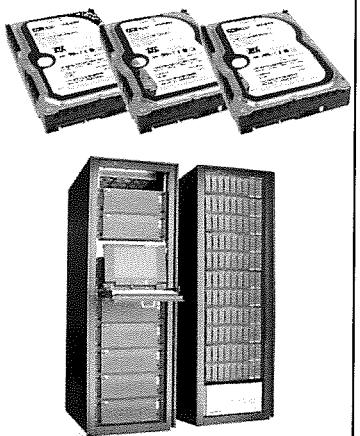
Defines a duplicate as a copy of the original made by, among other things, "mechanical or electronic re-recording . . . or by other equivalent techniques which accurately reproduces the original."

We must focus on whether the image is an accurate, verifiable and reproducible reproduction of the original.

As we have discussed before, hash algorithms are the answer to evidentiary issues.

Storing Images

- Prevailing Method
 - Storing Multiple Hard drives on Shelf
- Carnegie Mellon Drive Failure Study*
- Suggested Method**
 - Upload to managed RAID with tape backup and off site disaster recovery



*<http://www.cs.cmu.edu/~bianca/fast07.pdf>

**http://www.usdoj.gov/usao/eousa/foia_reading_room/usab5601.pdf

Appendix A - FTK Imager Primer © 2014 SANS

The prevailing method of storing images of seized computer systems are to place them on a shelf or in an electronic media safe in a climate controlled room. When computer forensics was new to law enforcement this was the only thing they knew how to do.

Several studies about the number of drive failures have brought attention to this practice of placing the original or only copy of evidence on a shelf in a room. Carnegie Mellon did a study of over 100,000 different types of hard drives and found that the failure rates are much higher than stated in manufacture data sheets. Additionally, because hard drives can sit in evidence rooms for years before they go to court, the likelihood of failure after sitting in evidence increases.

With digital evidence, we have an opportunity like no other type of evidence to safeguard against a tragic event such as 911. When the World Trade Center towers collapsed, they took with them evidence from several law enforcement agencies and many of those cases had to be dismissed because the evidence was destroyed.

A safer, more advanced method of storing and maintaining digital evidence is to upload the image file to a managed RAID (Redundant Array of Independent (or Inexpensive) Disks) systems that has backups conducted. Since the primary purpose of a RAID is for redundant storage that eliminates the potential loss of data due to a single drive failure, this storage technique provides the most advanced and safer method for safeguarding digital evidence. The RAID methodology of storing evidence images also adheres to the National Institute of Justice, Office of Programs recommendations that investigators preserve evidence "*in a manner designed to diminish degradation or loss*" Department of Justice, Office of Justice Programs, National Institute of Justice, Crime Scene Investigation: A Guide for Law Enforcement (2000).

The Department of Justice Computer Crime and Intellectual Property Section published an article in the January 2008 issue of the United States Attorney's Bulletin, Volume 56, No 1 which can be found online at the link listed.

FTK Imager Features

- Preview Digital Data
- Image in Multiple Image Formats
- View/Extract Contents of Images
- Convert Image File Formats
- Generate Hash Reports
- Extract Protected System/Registry Files
- Image RAM

Appendix A - FTK Imager Primer © 2014 SANS

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 3.0.0.1443 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 and 64-bit operating systems

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

Image File Formats

- There are several ways to store a disk image
- Some allow metadata to be stored:
 - Acquisition date
 - Drive serial number
- Some allow the data to be compressed
- Some are proprietary
- Sleuthkit and SIFT Workstation compatible with multiple image evidence formats

Appendix A - FTK Imager Primer © 2014 SANS

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/>

Supported Imaging Formats

- **Raw: Original True Bit Image**

- Same size as original drive
- Contains no metadata
- No compression
- Also called 'dd' format
- Images in raw ends in **.dd** or **.img**

- **EnCase Evidence File Format (E01):**

- Proprietary format created for EnCase (Guidance Software)
- EnCase Evidence File format ends in **.E01**
- Contains acquisition metadata and can compress data

Appendix A - FTK Imager Primer © 2014 SANS

One of the things that make FTK Imager many investigator's 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.

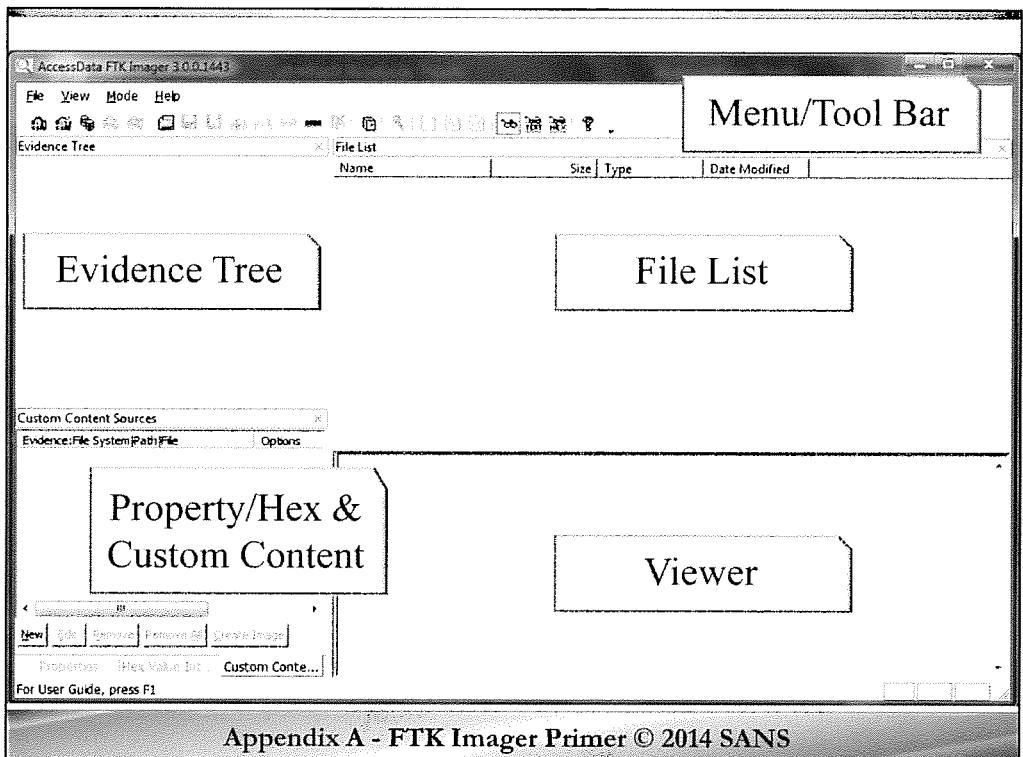
S01 – Smart – Andy Rosen's SMART technology

CUE – ISO buster

ISO – ISO BUSTER

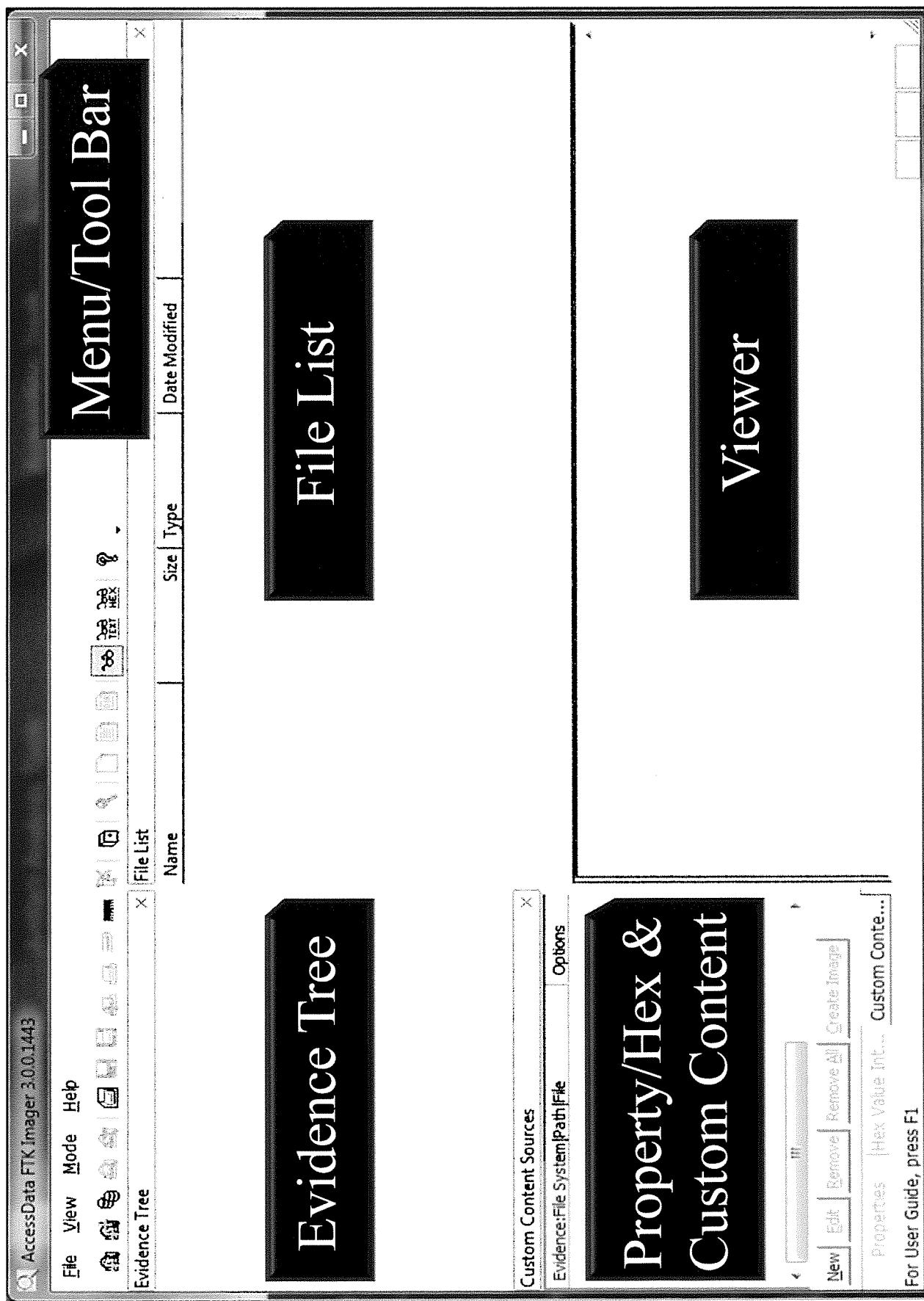
ADI – Access Data Proprietary Format – Great for targeted imaging rather than full drive imaging.

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.



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 that 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.

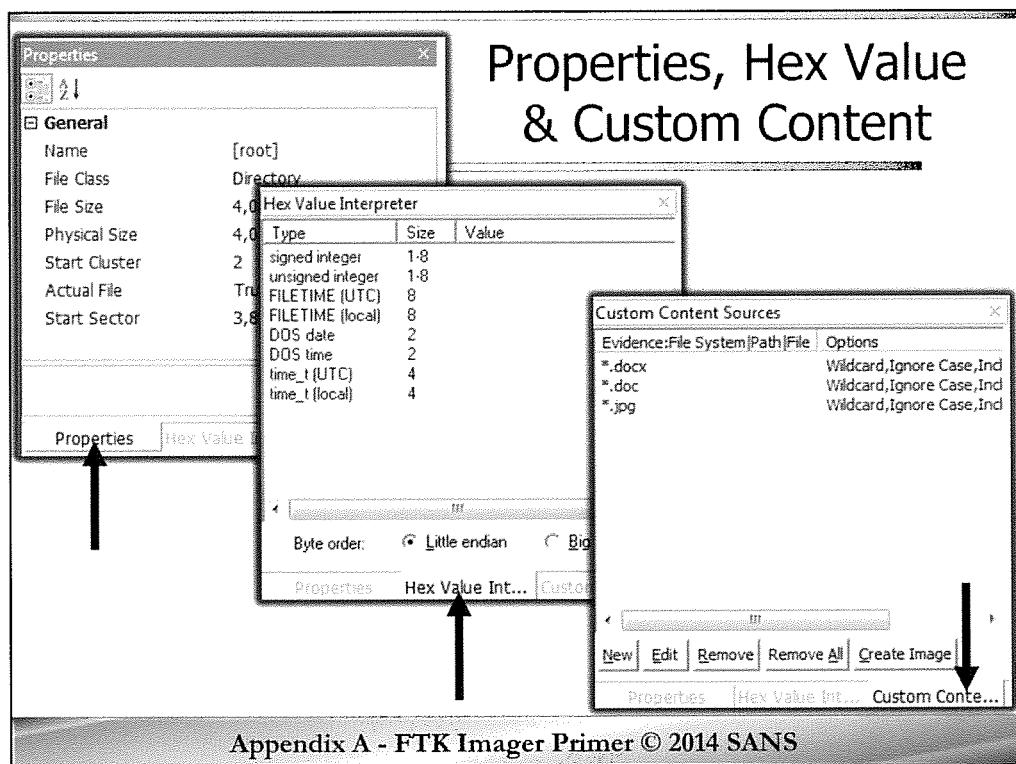


- The Viewer (bottom right)

The Viewer - which is located just below the File List window is 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:

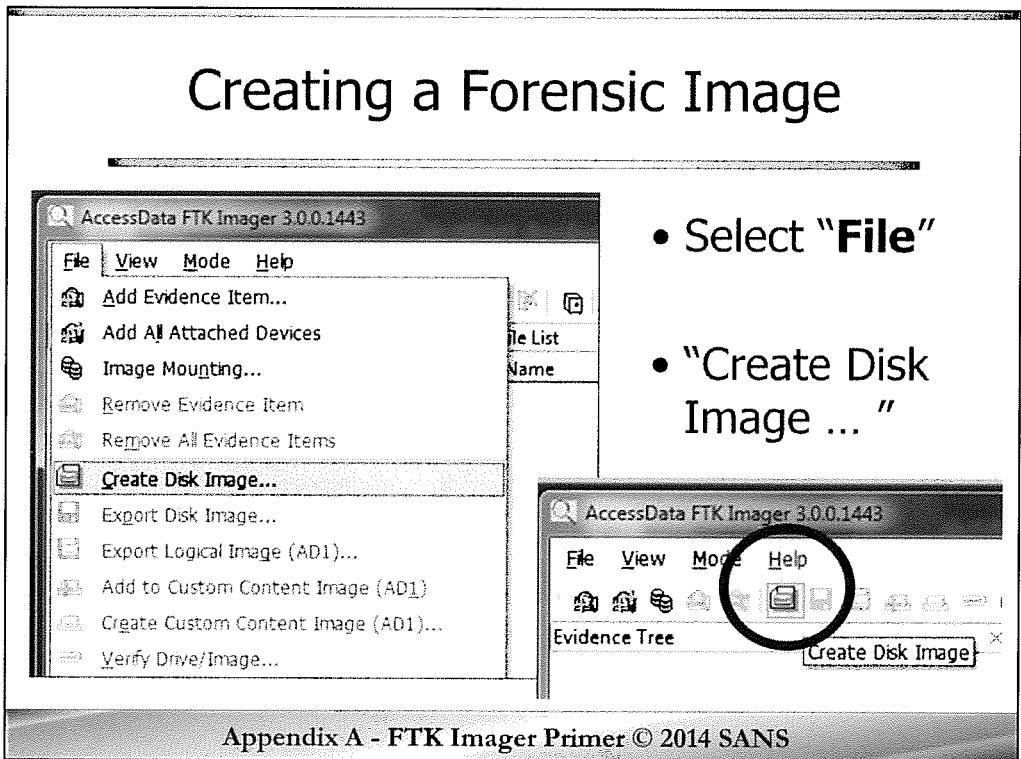
- The Properties pane
- The Hex Value Interpreter
- The Custom Content Sources

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 its 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.

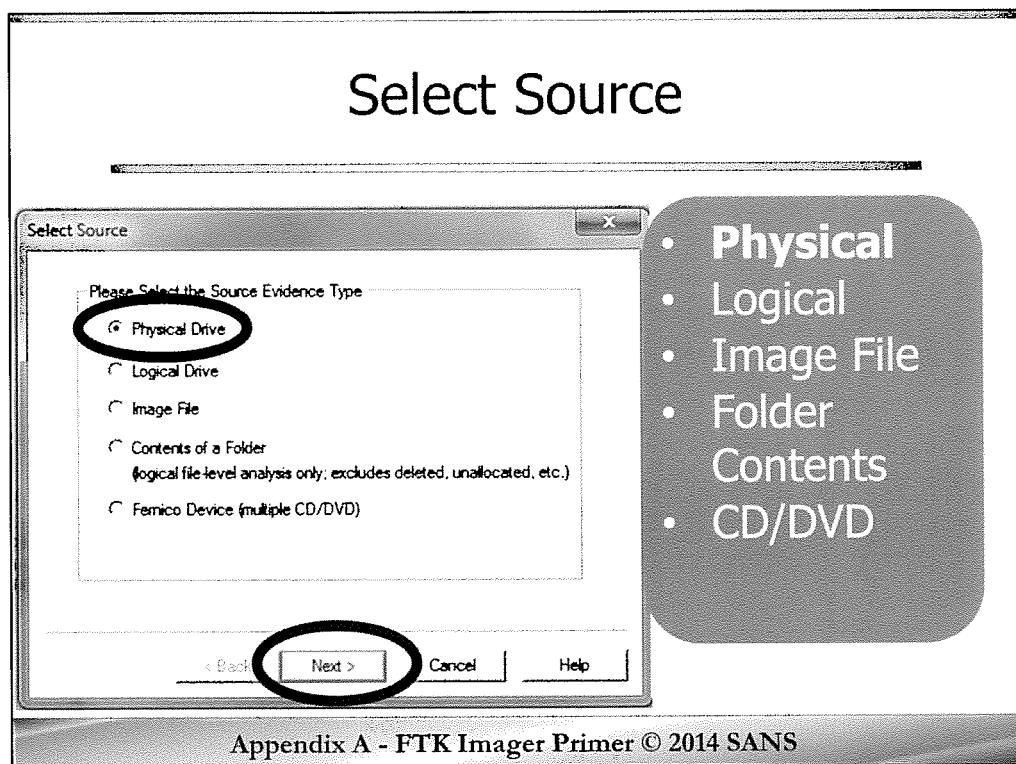
Custom Content Sources: This is an extremely valuable feature that will allow you to create custom images containing only the files you need or select. You can individually select files from a live file system to add to a Custom Content image or you can create filters to search for and image only specific items like jpg or doc files. So, if you wanted to create a forensic image of all the Microsoft Word documents and picture files with the jpg file extension, you could create three filters as you see in the slide. Thus it will create a 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\system32\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.



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.

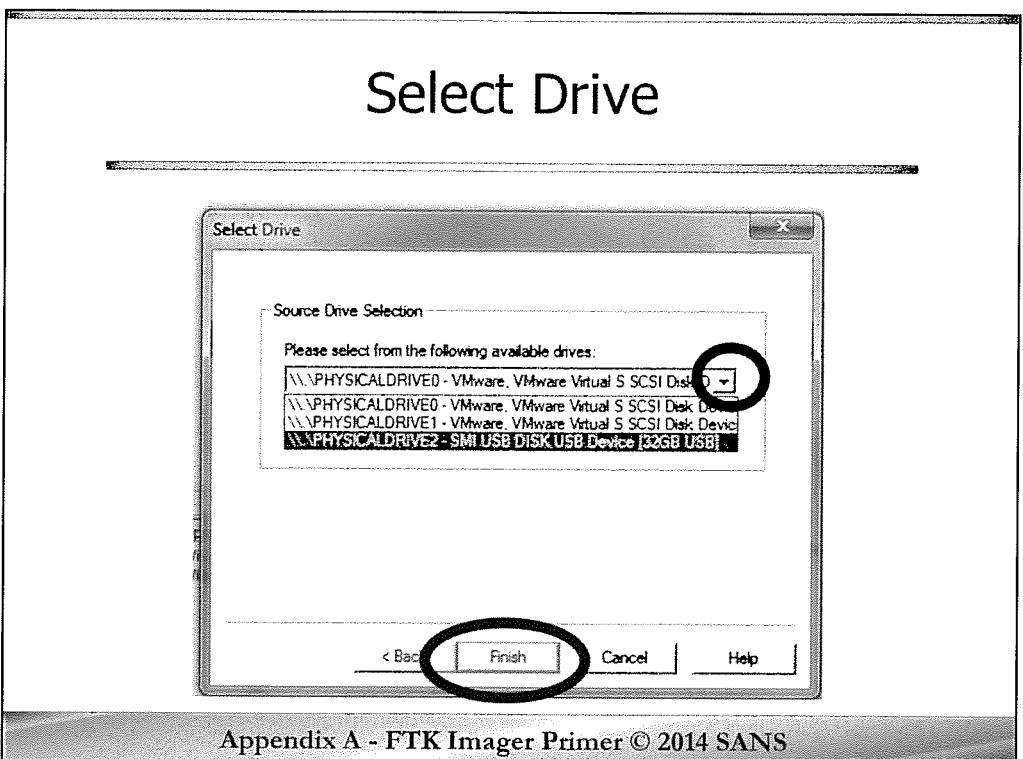
In the forensics world, you almost always want to see everything, so you will usually choose PHYSICAL drive. This will image all the allocated and unallocated space, active and deleted files, etc.

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**”.

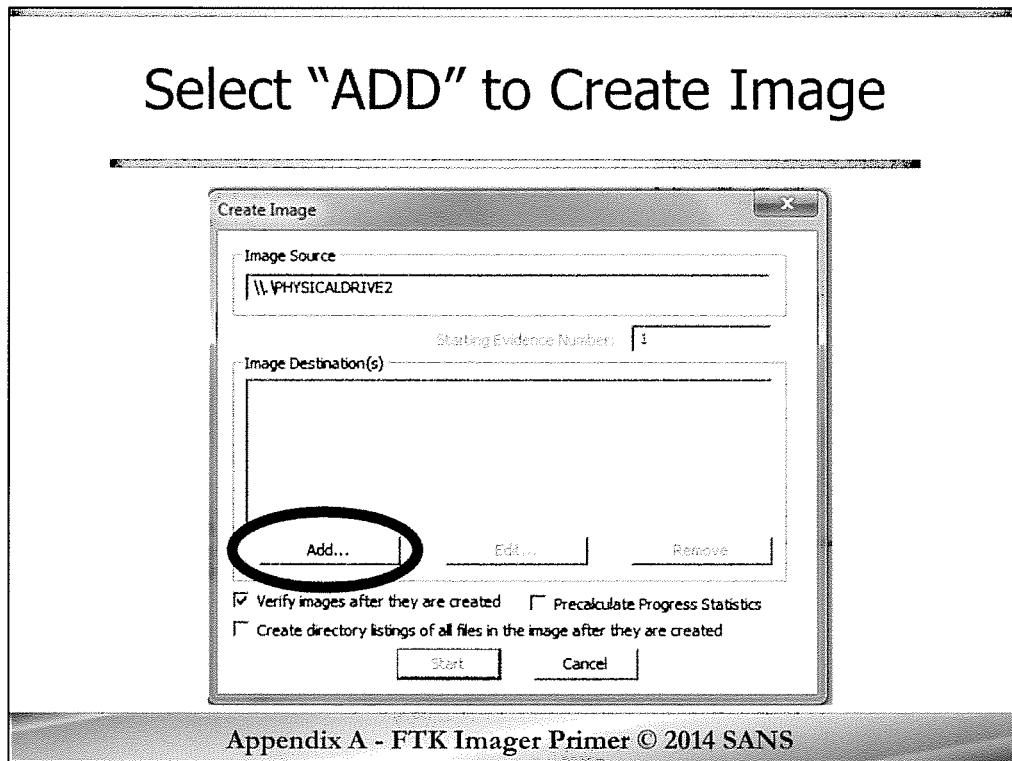
Then select “**Next >**”.



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.

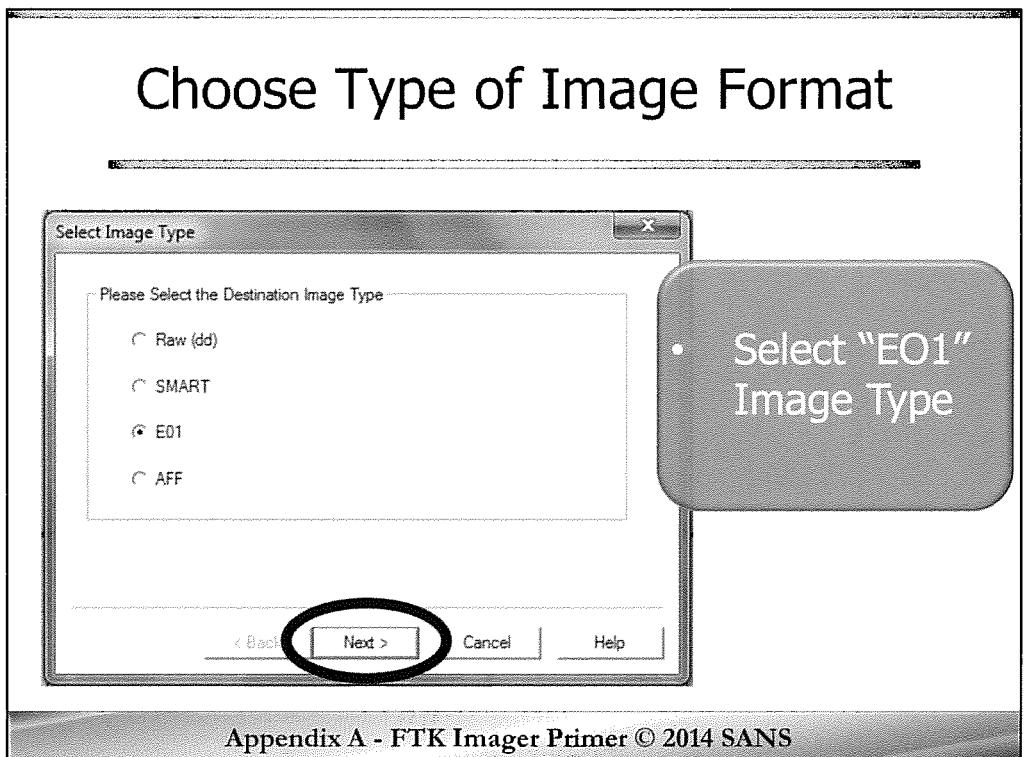
If you have your thumb drive attached and see the Physical Drive 1, go ahead and select it.

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.

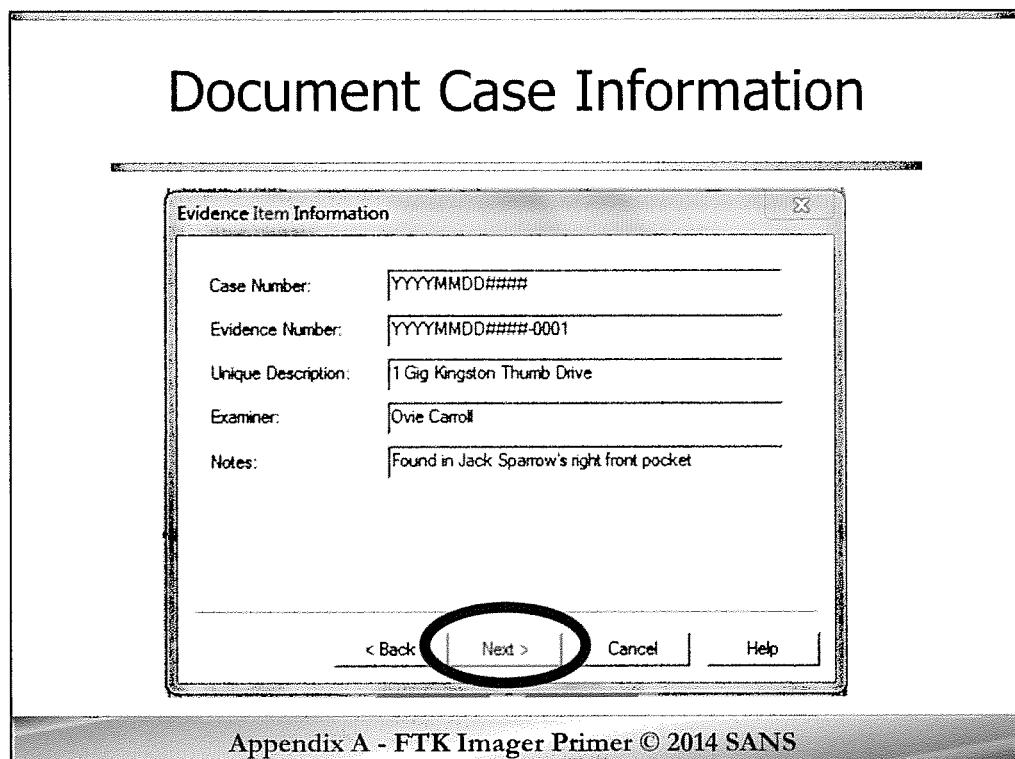
For now, don't worry about the other radio buttons below the add button. We will get to those after selecting a destination.



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 if 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”.



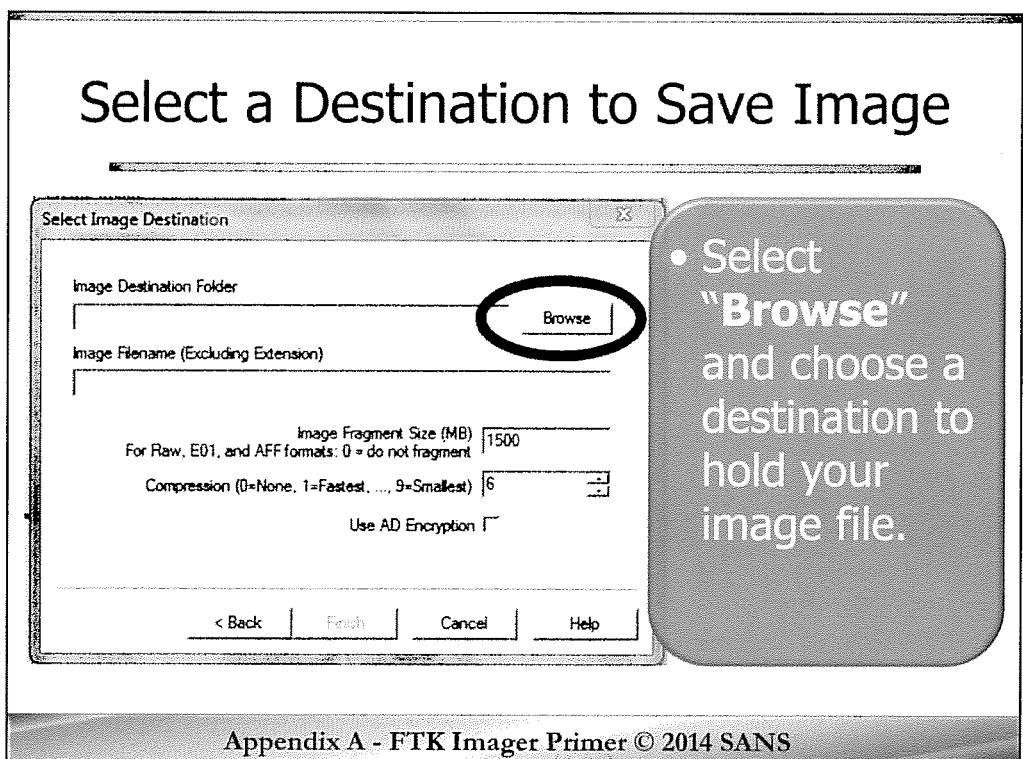
Now you should receive a dialog box allowing you to fill in information about your case or device you are imaging.

The format most commonly used for case and evidence numbers is 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.

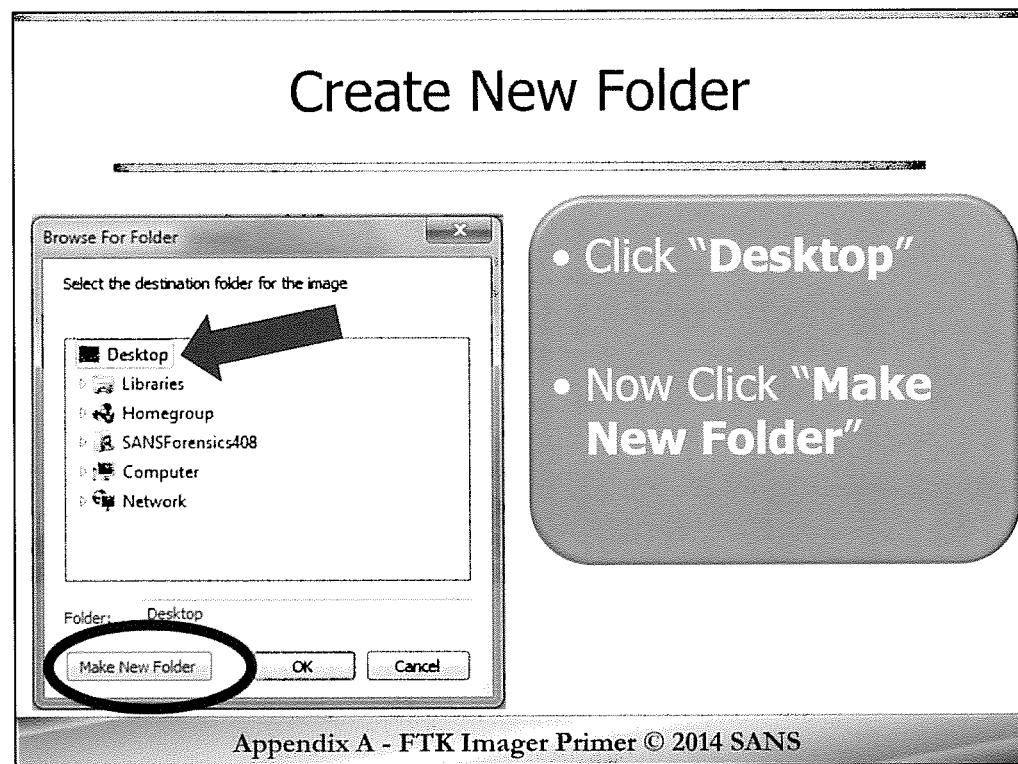
It is also common in large seizures that you create a log file with each image file name and where you found that device (e.g. image file YYYYMMDD####-0001 – thumb drive found in Jack Sparrow's right front pocket). This helps when you look at 20 image files and want to quickly start looking at certain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

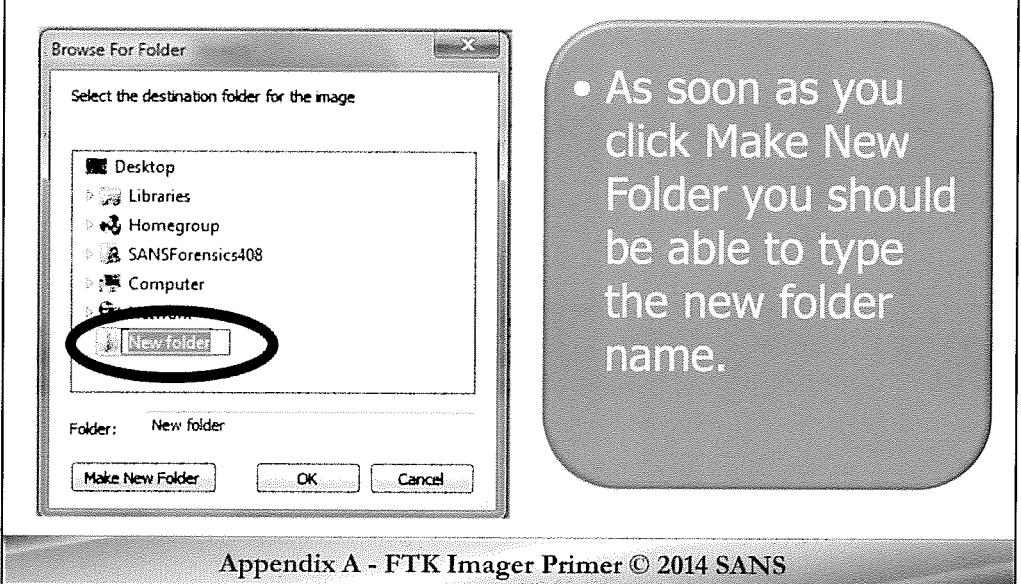


Let us create a folder, and put it on our desktop, so we can easily find it and examine the contents.

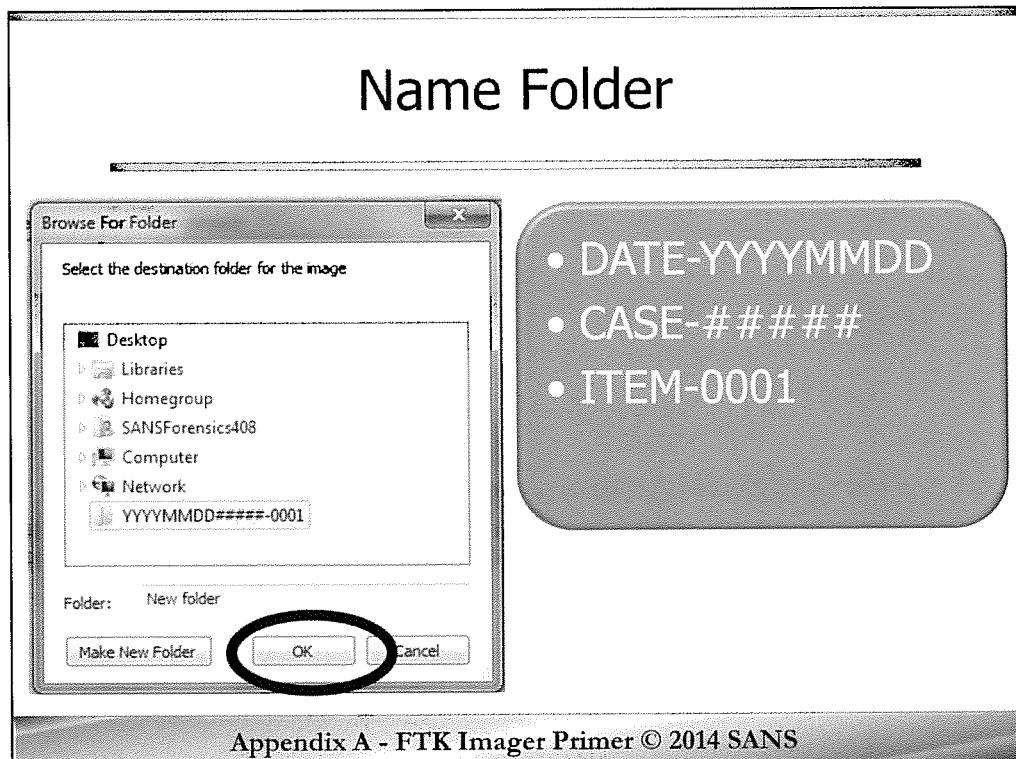
Click on "Desktop".

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

Name Destination Folder



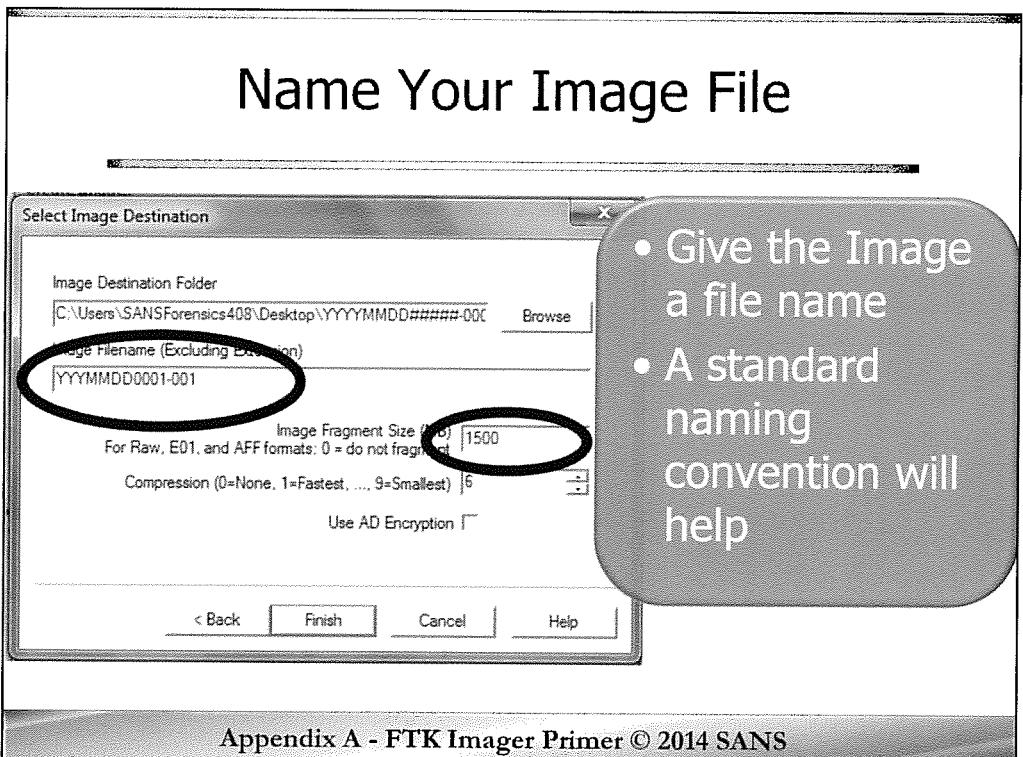
Now, let's name that folder the same name as our case: "YYMMDD#####-0001".



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 subject's name, or even the search location's 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.

Note: SMART S01 images are limited to image sizes between 1MB and 2GB.

FTK Imager - Encryption

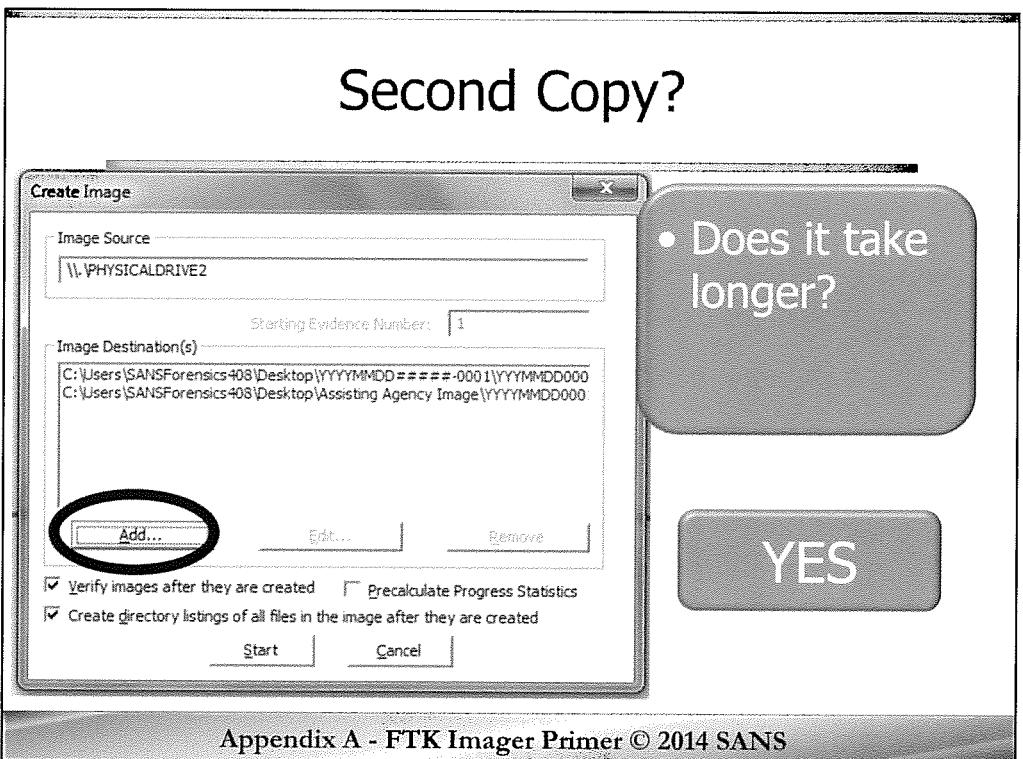
- Protect image files through encryption
 - Supported Image Types
 - AD1, E01, S01 and RAW/DD
 - AD Encryption Supports
 - Hash SHA-512
 - Crypto algorithms: AES 128, 192, and 256
 - Key Types: pass phrases, raw key files and certificates

Appendix A - FTK Imager Primer © 2014 SANS

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.

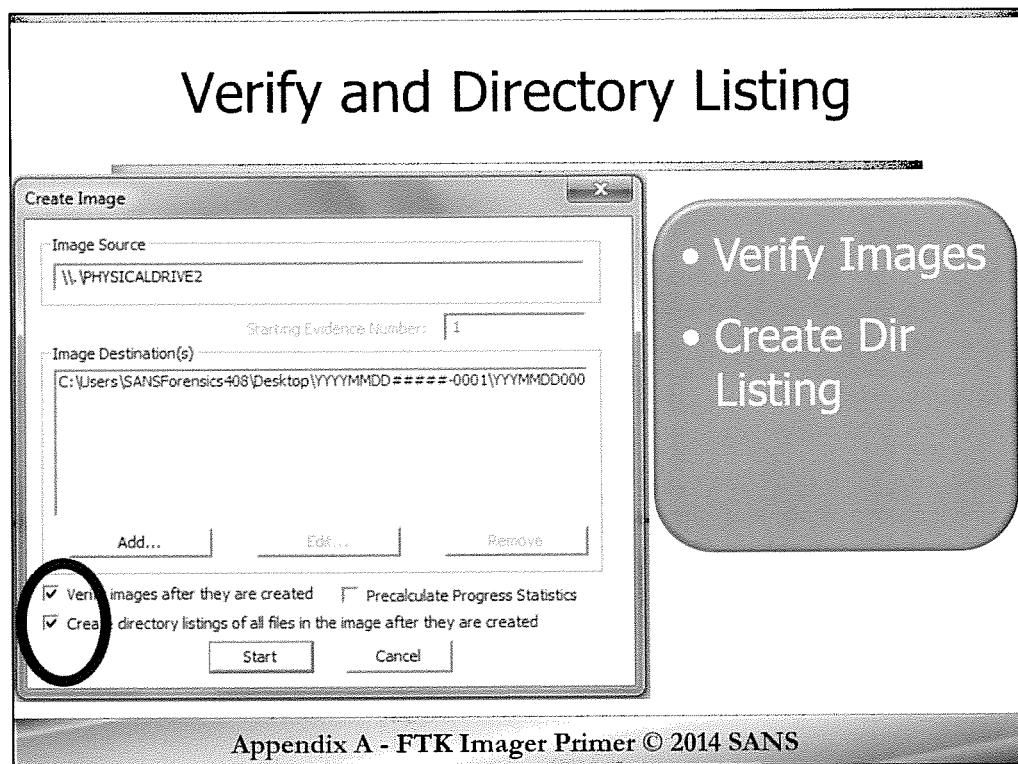
This is particularly useful if you need to produce one forensic image copy for you and one for another party such as the defense attorney or another agency. I have heard a lot about some law enforcement agencies that will create the forensic image, but when it comes time to share a copy of that image 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.

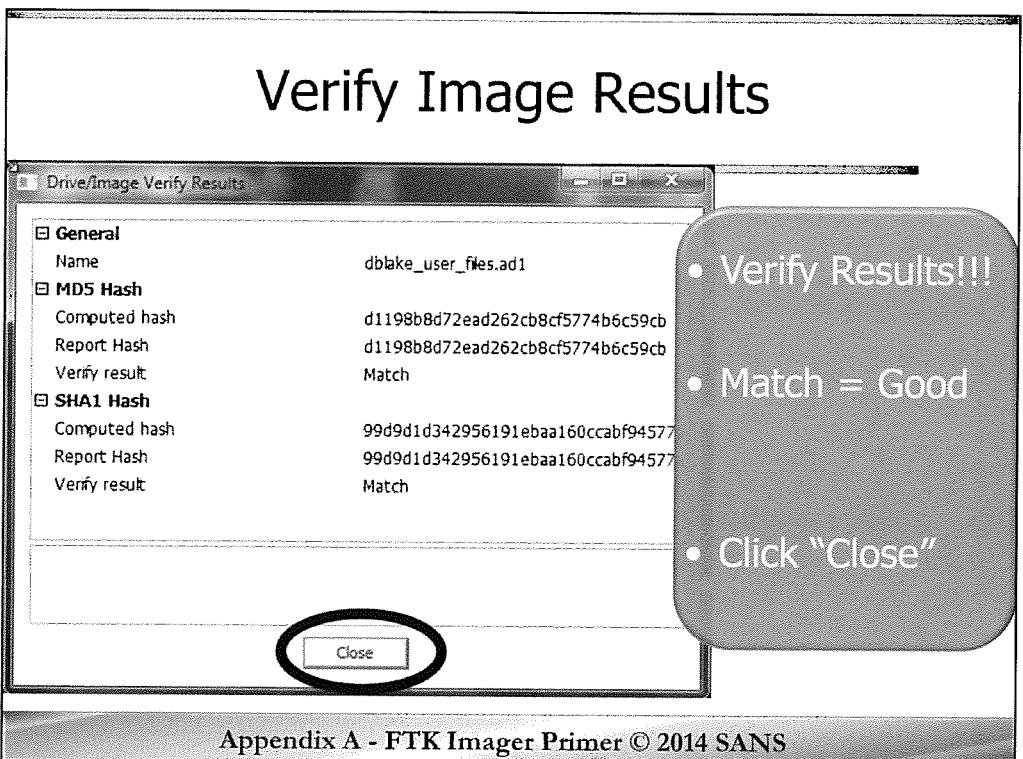
Be careful not to misrepresent what this TSV file is. Some might want to consider it a complete list of everything that is on the drive...

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**.

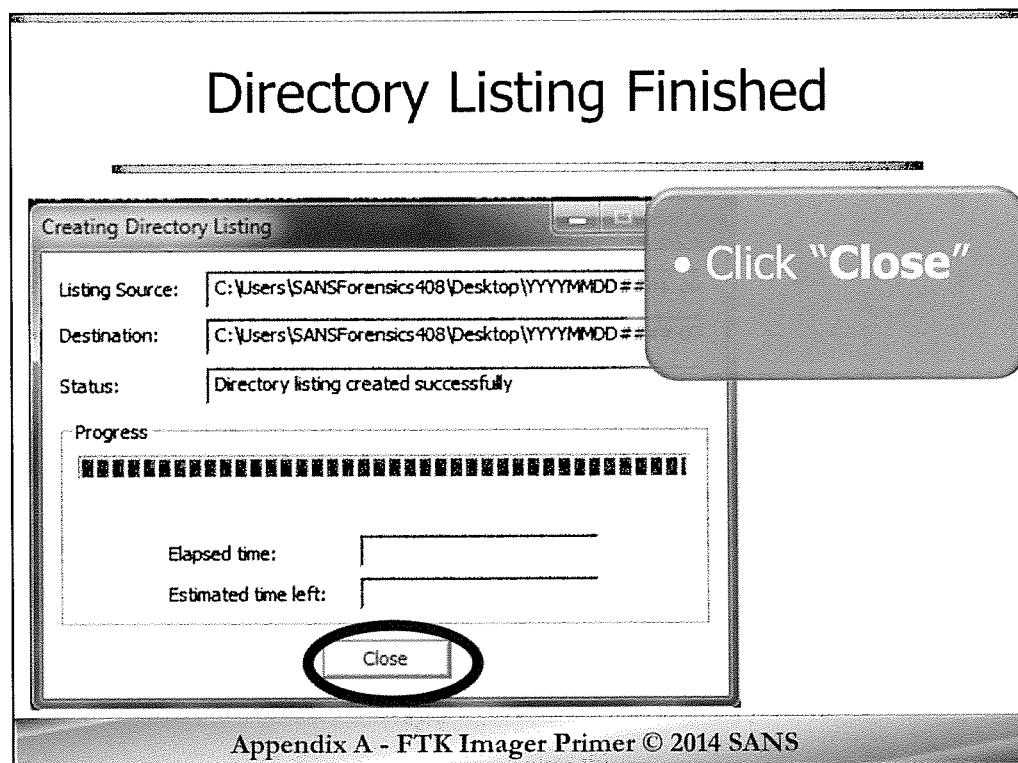


When FTK Imager is finished creating all the images and verifying that the hashes match, FTK Imager will display the Drive/Image Verify Results. This does not take much effort, but it is the most critical part of the imaging process. If FTK reports that the image hashes do NOT match and you just blow 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 want 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 accidentally 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.

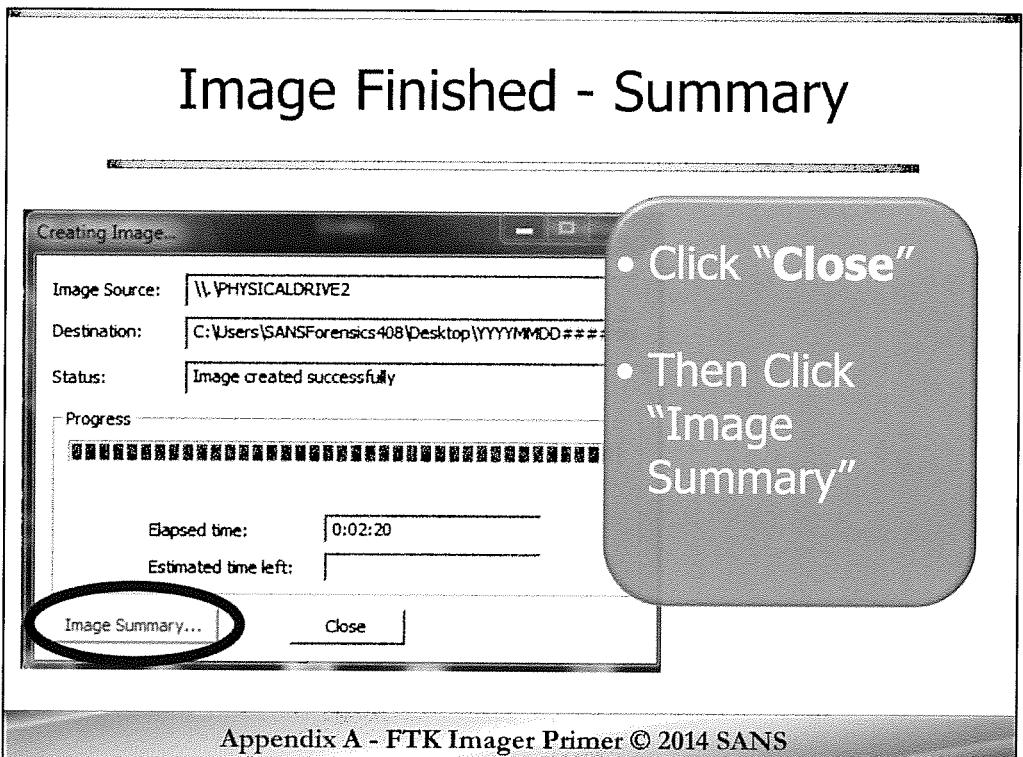
Select Close.



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.

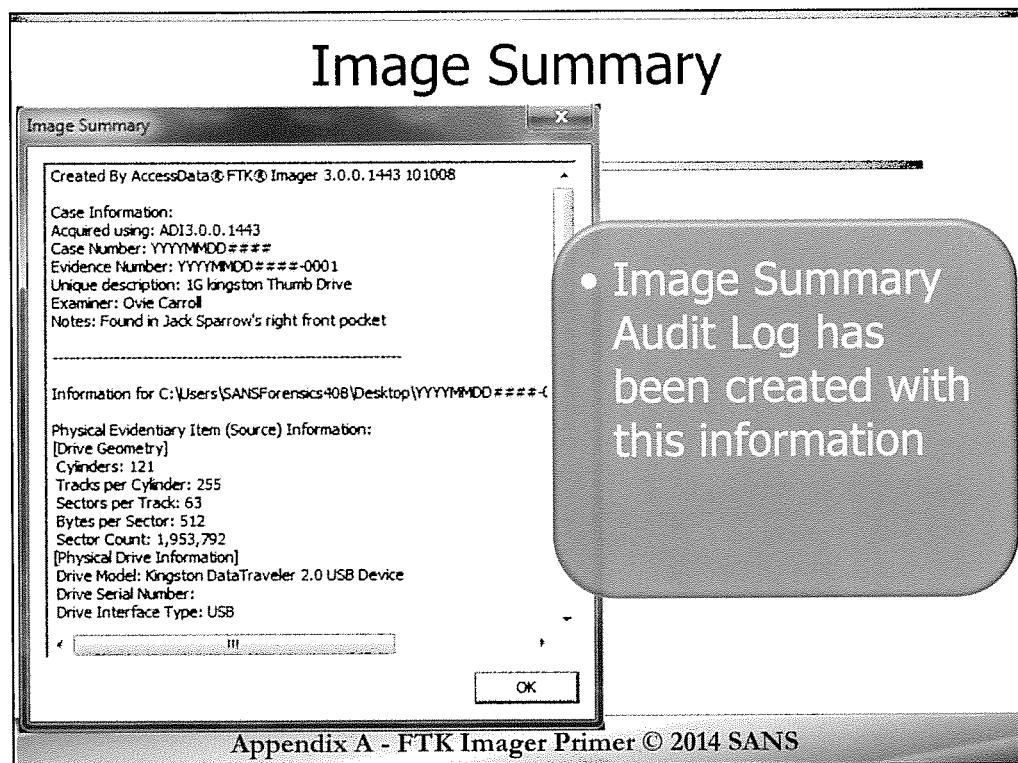
More and more, I am finding that a directory listing is a good thing to go ahead and create. It can be used in a number of ways. First, if the judge wants to require a “Return” on the search warrant, you would typically only provide a list of what items you seized from the scene, which would state: one 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 insist 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.cfti.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.

Open Output Folder



- Open the folder your image is in

Appendix A - FTK Imager Primer © 2014 SANS

Now that you have reviewed the Image Summary, you can close it and also close FTK imager. If you followed our instructions, on your host 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.

Why Review Audit Log

The screenshot shows a Notepad window titled "YYYYMMDD#####-0001-001.txt - Notepad". The content of the file is as follows:

```
File Edit Format View Help
Created By AccessData® FTK® Imager 2.5.4.16 080324

Case Information:
Case Number: YYYMMDD#####
Evidence Number: YYYMMDD#####-0001
Unique Description: 1 Gig Kingston Thumb drive
Examiner: civie Carroll
Notes: Found in Jack Sparrow's right front pocket

Information for C:\Documents and Settings\Administrator\Desktop\YYYYMMDD#####-0001\  

Physical Evidentiary Item (Source) Information:  

(Drive Geometry)  

Cylinders: 121  

Tracks per cylinder: 255  

Sectors per track: 63  

Bytes per Sector: 512  

Sector Count: 393,792  

Physical Image Information:  

Drive Model: Kingston DataTraveler 2.0 USB Device  

Drive Interface Type: USB  

Source data size: 954 MB  

Sector count: 1953792  

[Computed Hashes]  

MD5 checksum: f2217981e6479072fb1c+b0c7afc48de  

SHA1 checksum: 2767b76263a428523f80ee1cbecc1627f1669764

Image Information:  

Acquisition started: Sat Jan 10 21:16:02 2009  

Acquisition finished: Sat Jan 10 21:23:53 2009  

Segment list:  

C:\Documents and Settings\Administrator\Desktop\YYYYMMDD#####-0001\YYYYMMDD#####-0001\  

Image verification Results:  

Verification started: Sat Jan 10 21:23:54 2009  

Verification finished: Sat Jan 10 21:24:51 2009  

MD5 checksum: f2217981e6479072fb1c+b0c7afc48de : verified  

SHA1 checksum: 2767b76263a428523f80ee1cbecc1627f1669764 : verified
```

A callout bubble on the right side contains the following text:

- Audit logs are useful to document date/times image created & hash value

Appendix A - FTK Imager Primer © 2014 SANS

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.

Why Use Imager to Preview

- Triage
 - May aid in determining which device to image/seize
- Examine Specific Files
- Extract Specific Files
- Recover Deleted Files

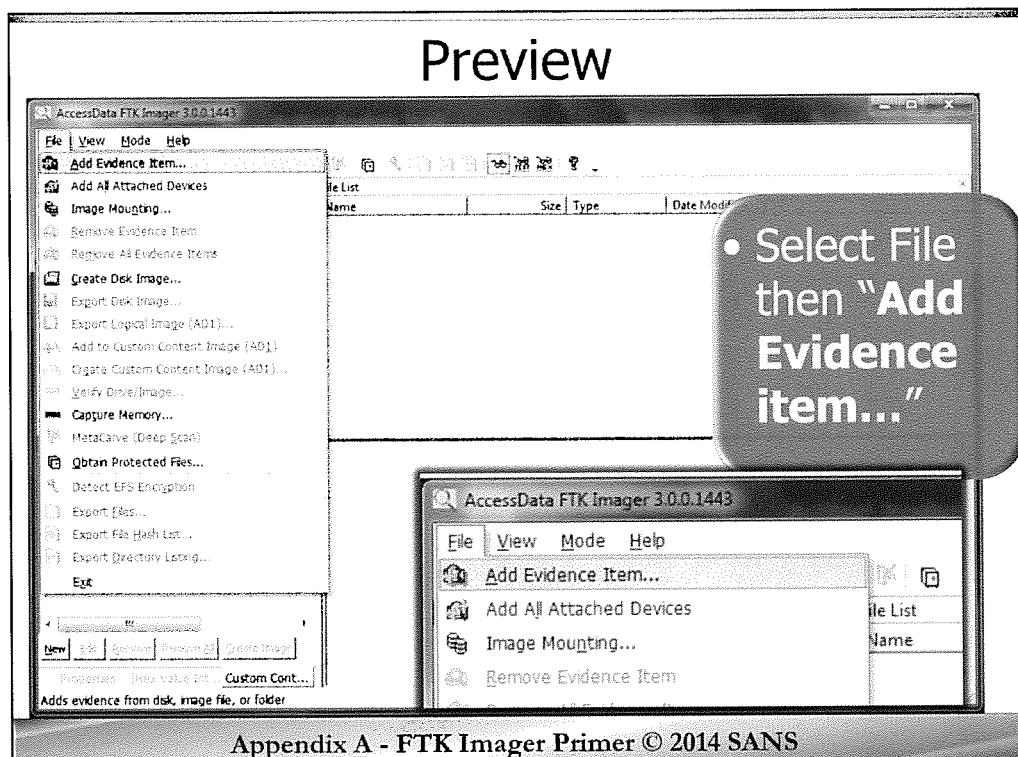
(Please Note: Start your virtual machine and launch FTK Imager from your desktop – Upper Right Corner)

Appendix A - FTK Imager Primer © 2014 SANS

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.

In many situations you generally know what you are looking for and by conducting a brief triage prior to starting the imaging process, you may be able to quickly identify (and export if needed) information key information. Information that could be identified during the triage could either quickly answer critical questions (was this the computer involved in the matter being investigated), identify investigative leads for potentially volatile information (identifying web based accounts that must be preserved), or provide information to an investigator that could significantly aid during an on-site interview being conducted (documents about the matter being investigated, specific Google search or inappropriate pictures organized in a My Pictures directory).

(Please Note: Start your virtual machine and launch FTK Imager from your desktop – Upper Right Corner.)

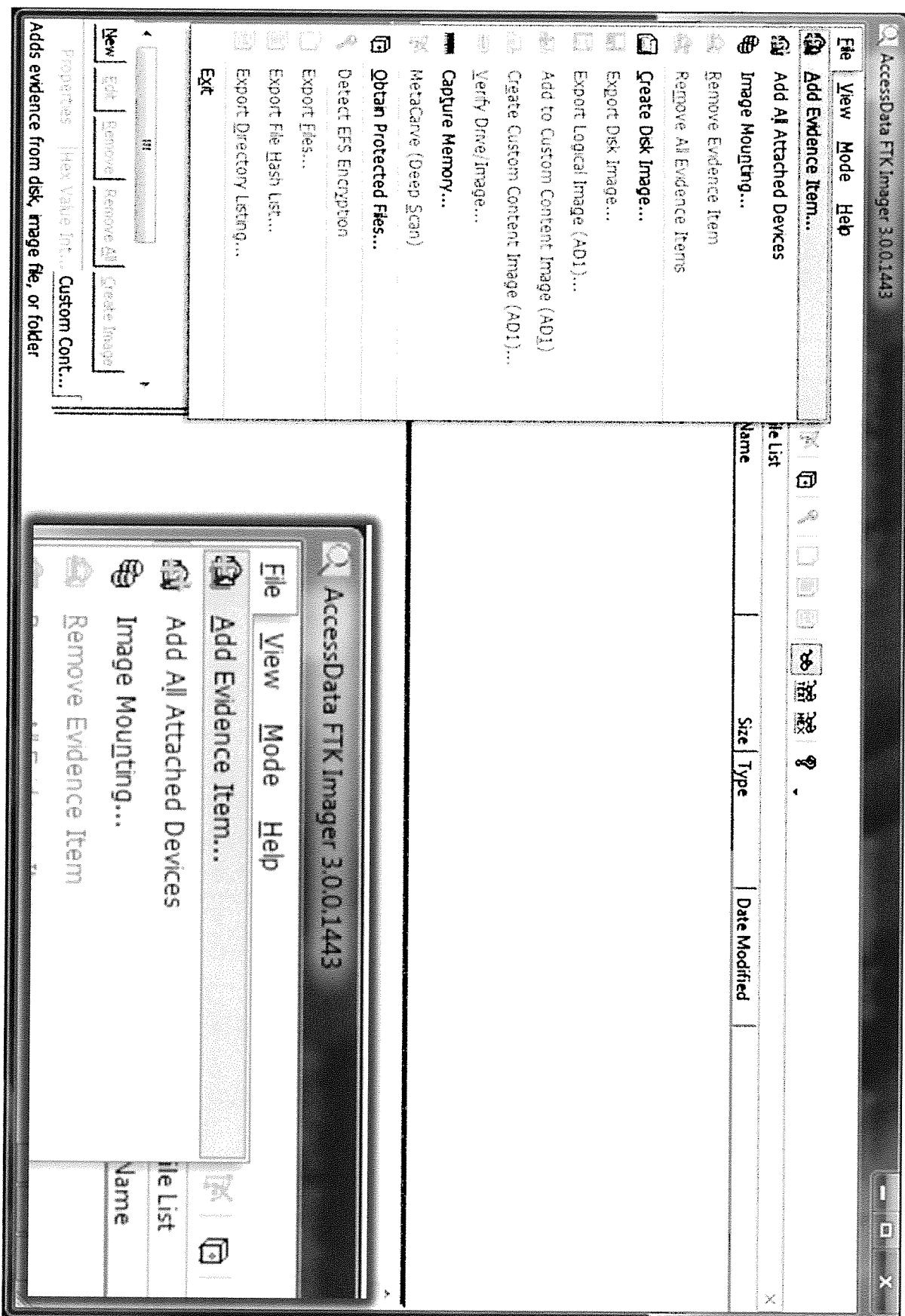


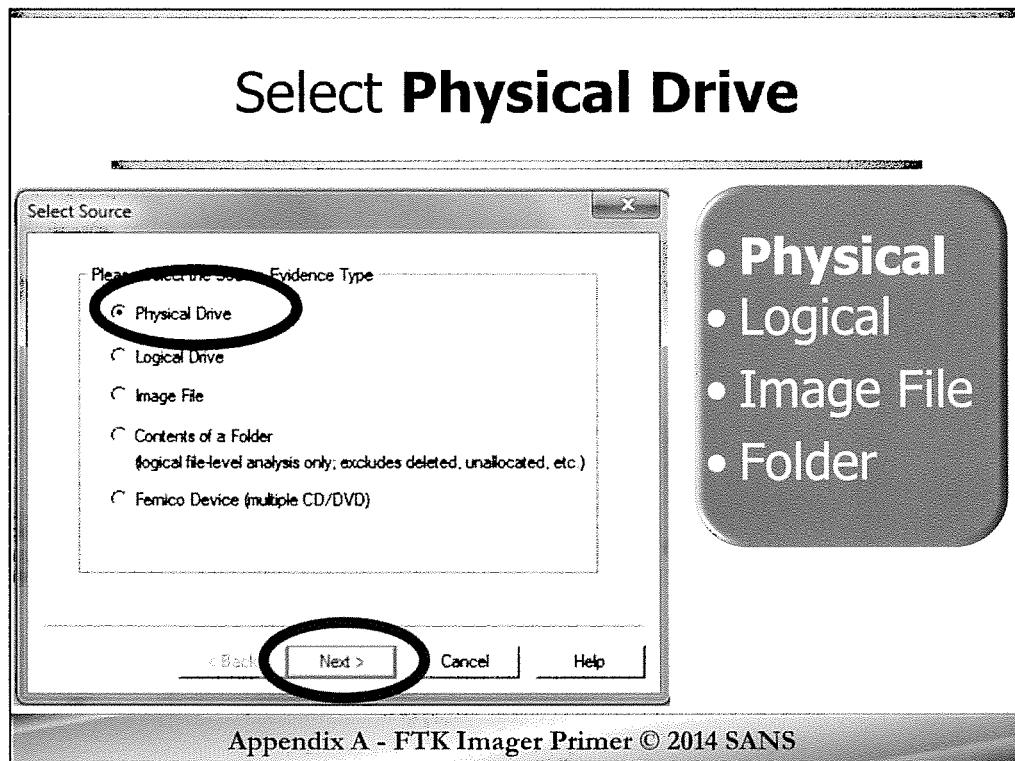
Appendix A - FTK Imager Primer © 2014 SANS

Start your virtual machine and launch FTK Imager from your DESKTOP.

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.

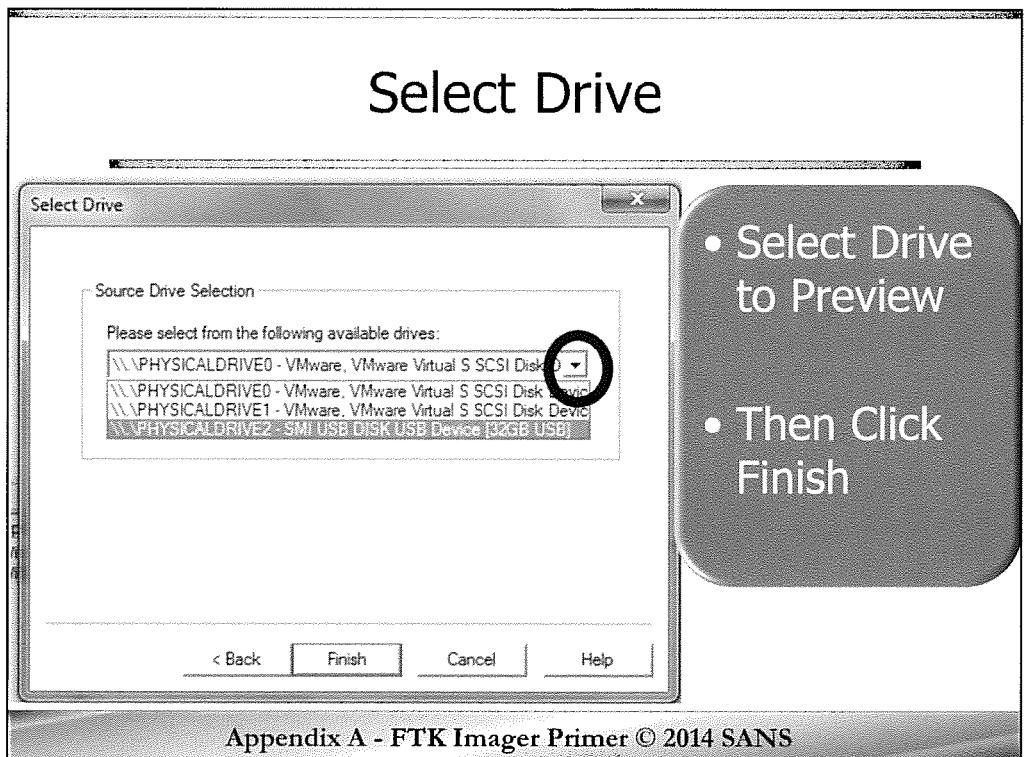
In the forensics world, since you typically want to see everything including the deleted files and unallocated space, you will almost always choose **PHYSICAL** drive. This will show you all the allocated and unallocated space, active and deleted files, etc.

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!

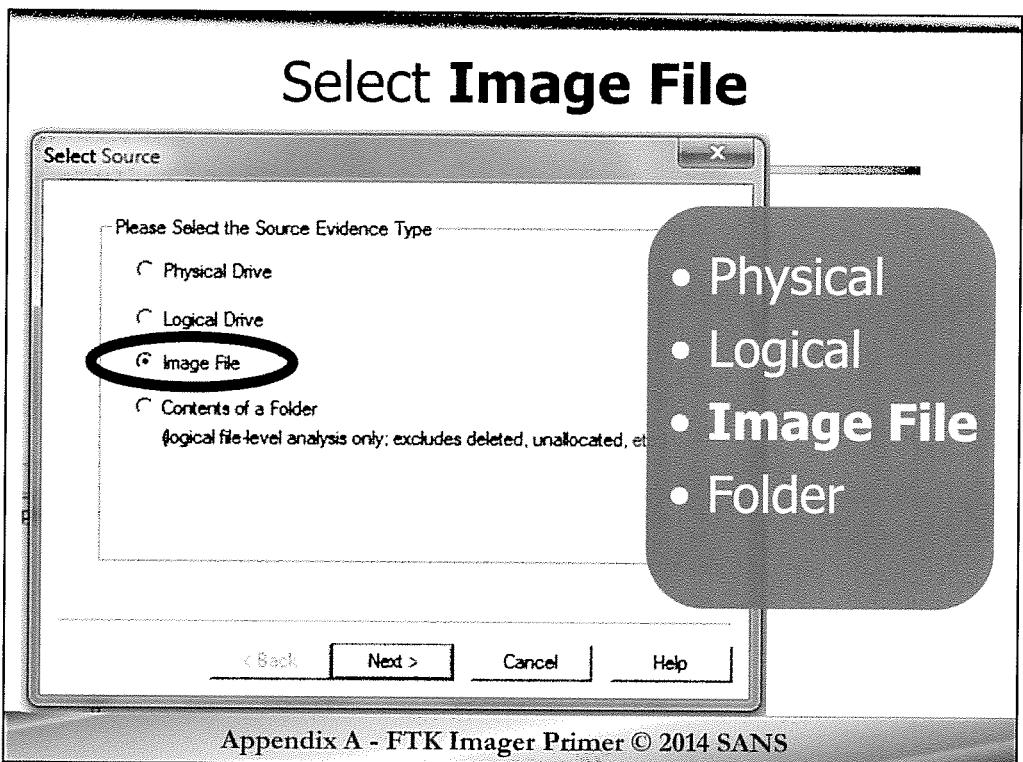
STOP AND LISTEN

- To “**Enhance Your User Experience**”, let's NOT select the hard drive
- We have already imaged a drive for you so we can all be looking at the same thing
- Select the “**BACK**” button and let's add an IMAGE

Appendix A - FTK Imager Primer © 2014 SANS

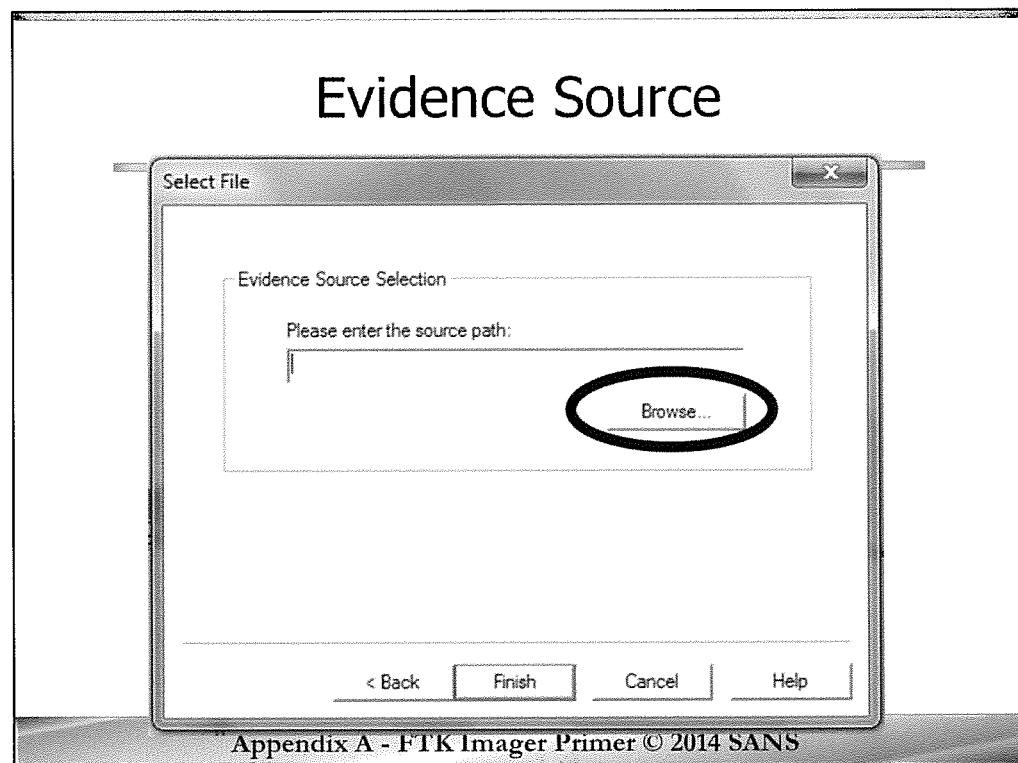
In order to better show you the Preview features as well as how you can use FTK Imager as a lightweight recovery tool, we have created an image file for you to use in this exercise. Do not click **Finish**. Instead, click the **BACK** button and let's go to the previous screen where it asked you what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

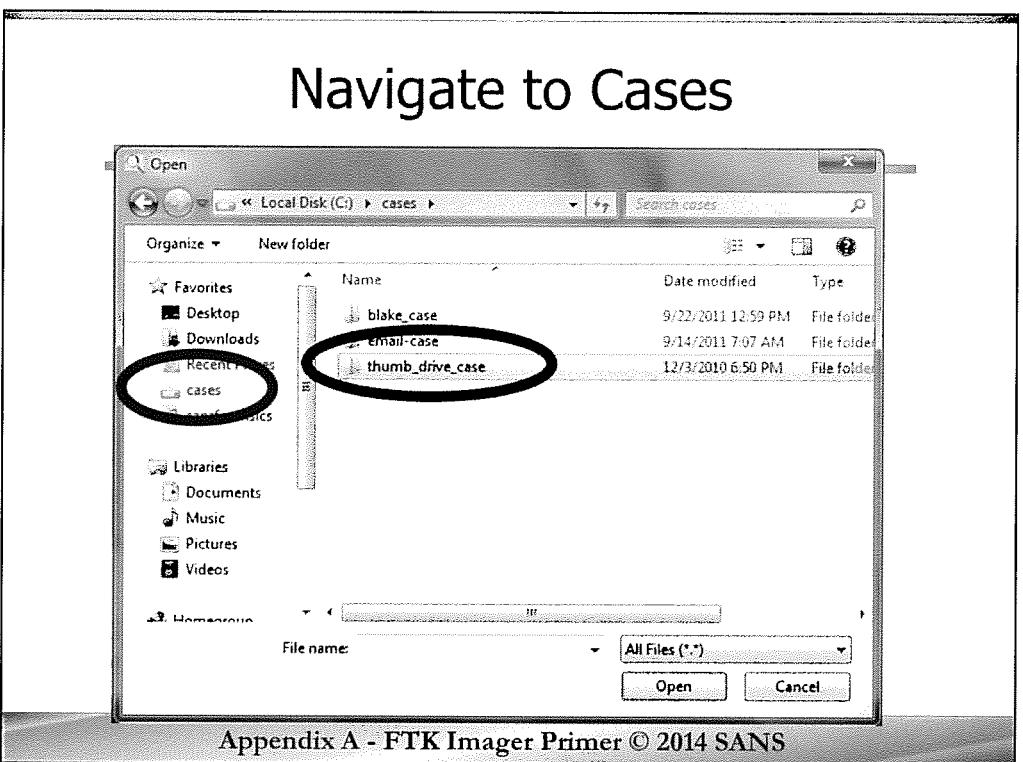


Because you said you wanted to load an image file, FTK Imager should now prompt you for the location of the image file you would like to preview.

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.

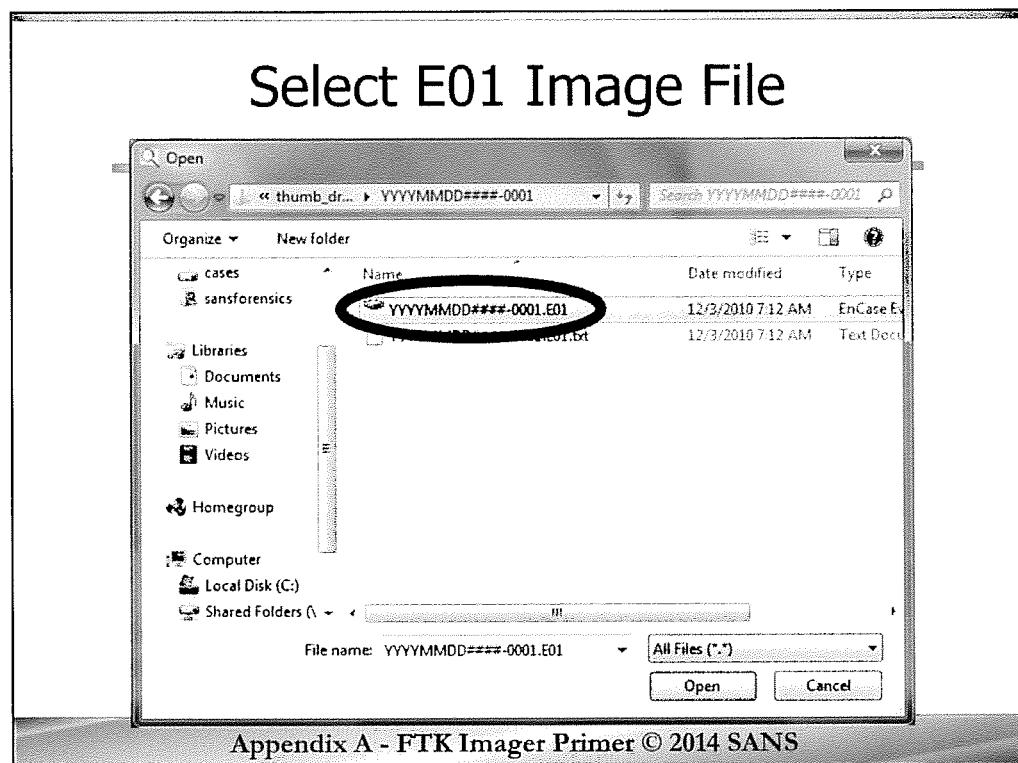
This is the same technique you would use back at the lab or even on-scene after you imaged a system and perhaps you need to quickly preview the device but don't want to have FTK go through the indexing and creation of a case file. I have used this technique to both preview as well as locate and extract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



Again, to keep us all on the same page, let's start by clicking on the cases icon on the left side of the screen. This will take you to the cases directory.

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

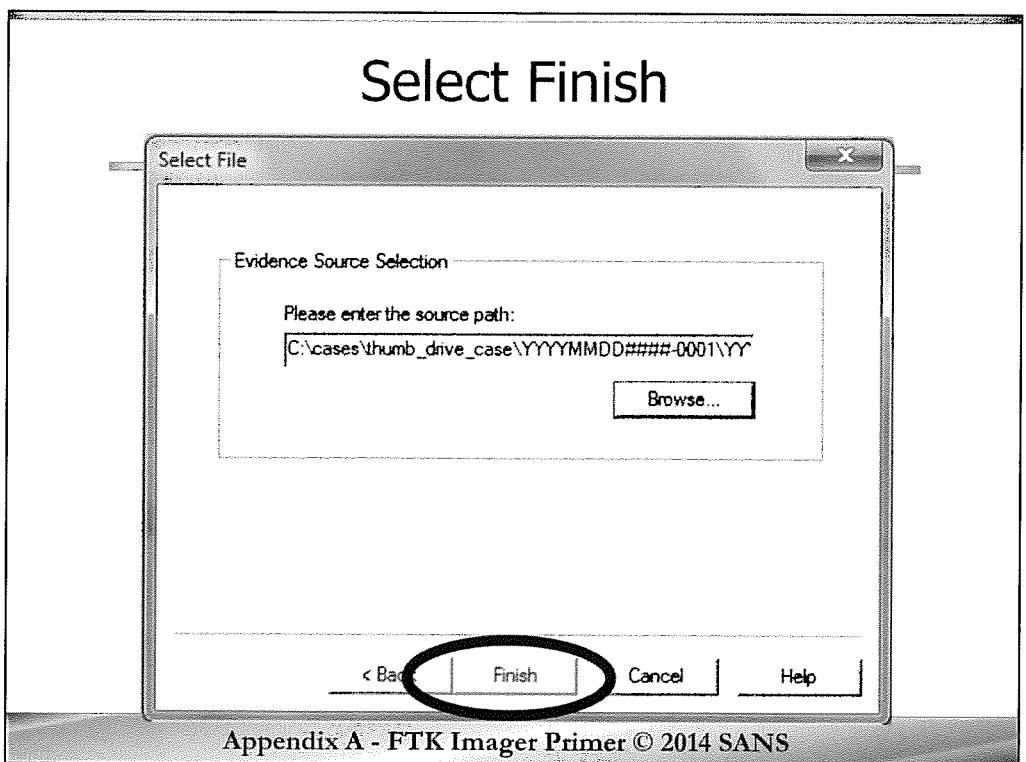
You can see how we have organized everything into a case folder. Because you will often have more than one piece of electronic evidence per case, we have also created sub-directories for each individual item. Find and double click on the directory folder labeled "**YYYYMMDD####-001**".



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.

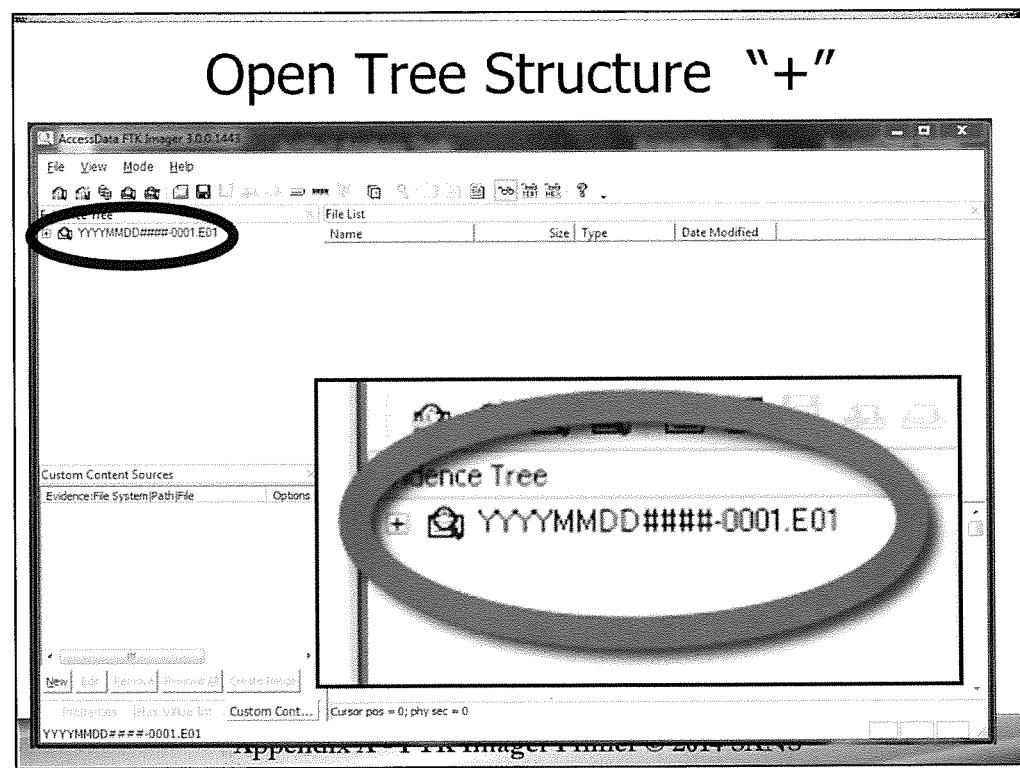
Find and double click on the top file labeled “**YYYYMMDD####-0001.E01**”.

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.

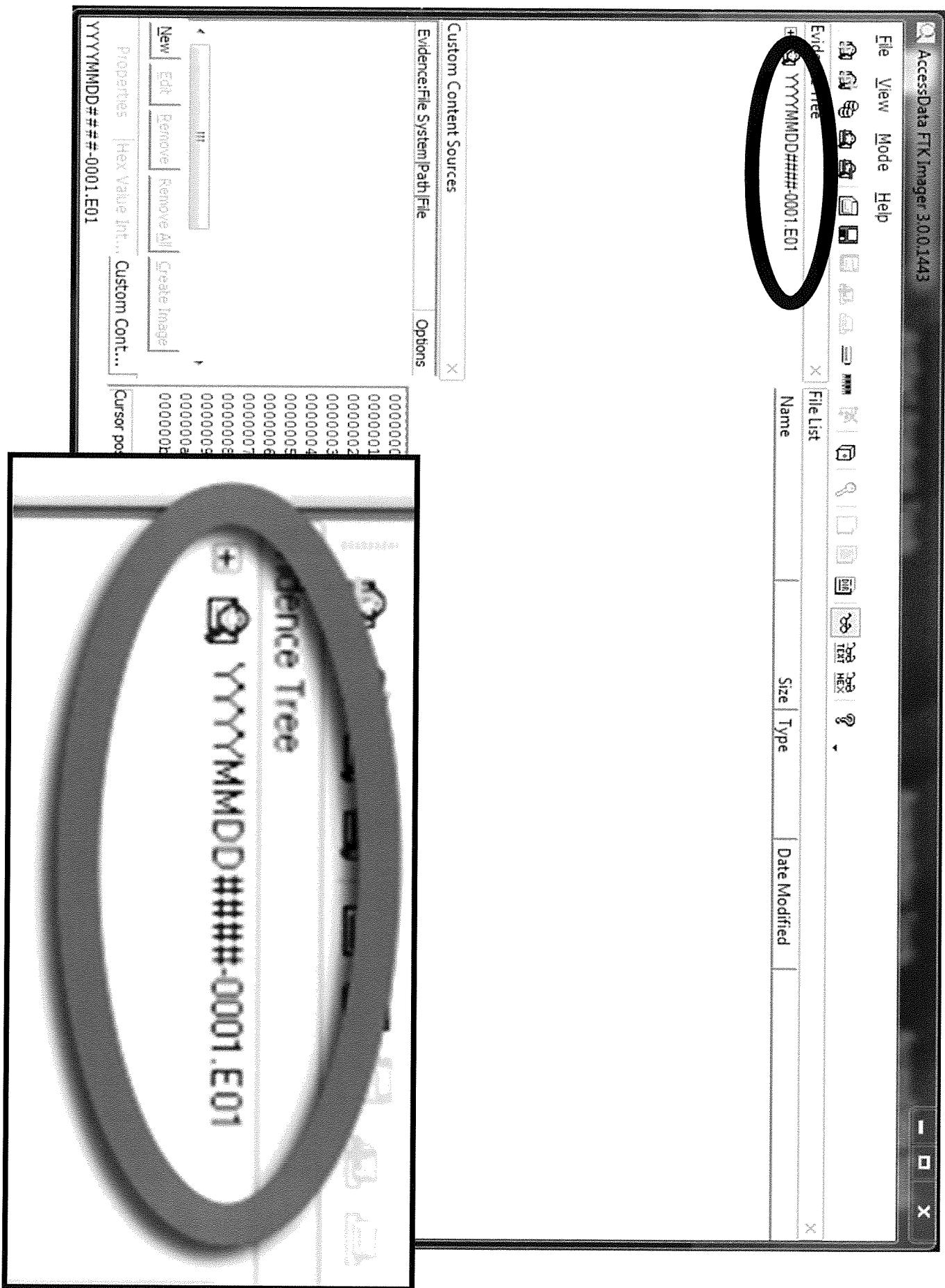


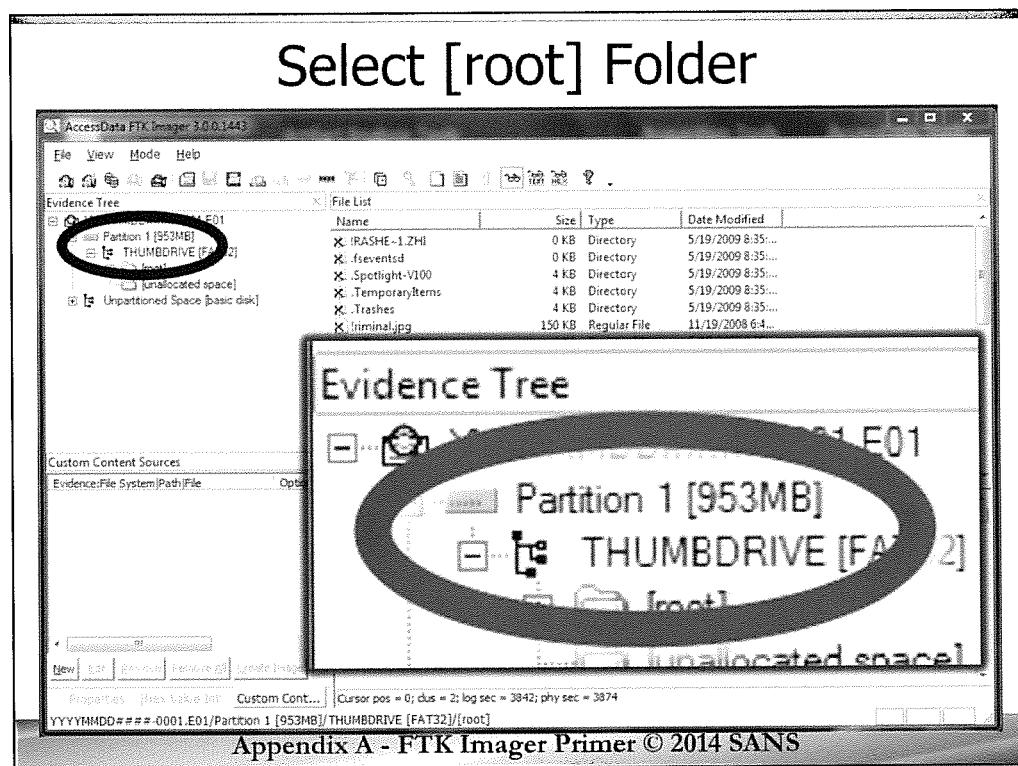
At the top left corner of the FTK Imager application, in the Evidence Tree window, you will see the image file/evidence you just added.

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, you'll reach 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].

AccessData FTK Imager 3.0.0.1443

File View Mode Help

Evidence Tree

File List

Name	Size	Type	Date Modified
IRASHE~1.ZHI	0 KB	Directory	5/19/2009 8:35...
feventsd	0 KB	Directory	5/19/2009 8:35...
.Spotlight-V100	4 KB	Directory	5/19/2009 8:35...
TemporaryItems	4 KB	Directory	5/19/2009 8:35...
.Trashes	4 KB	Directory	5/19/2009 8:35...
Immal.jpg	150 KB	Regular File	11/19/2008 6:4...
_TemporaryItems	4 KB	Regular File	5/19/2009 8:35...
_Trashes	4 KB	Regular File	5/19/2009 8:35...
anonymous comic.jpg	20 KB	Regular File	9/15/2008 4:03...
anonymouse	58 KB	Regular File	9/15/2008 4:03...

Custom Content Sources

Evidence:File System|Path|File Options

Evidence Tree

Partition 1 [953MB] E01

THUMBDRIVE [FAT32]

[root]

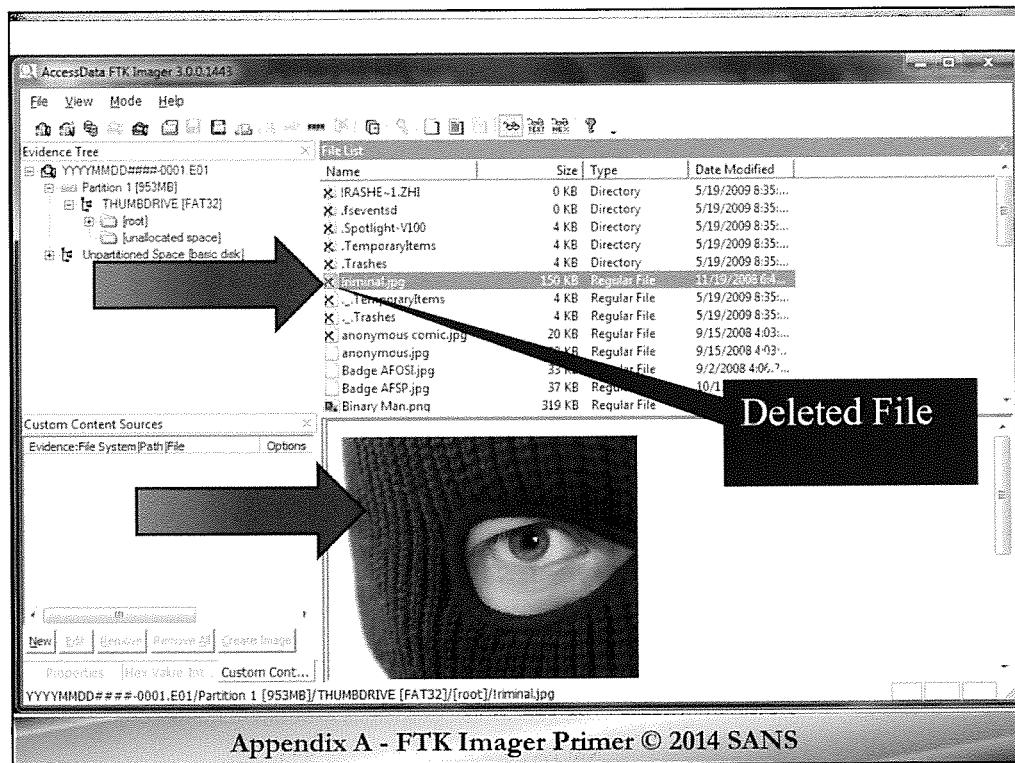
[unallocated space]

Unpartitioned Space [basic disk]

New Edit Remove Remove All Create Image

Properties Hex Value Int... Custom Cont

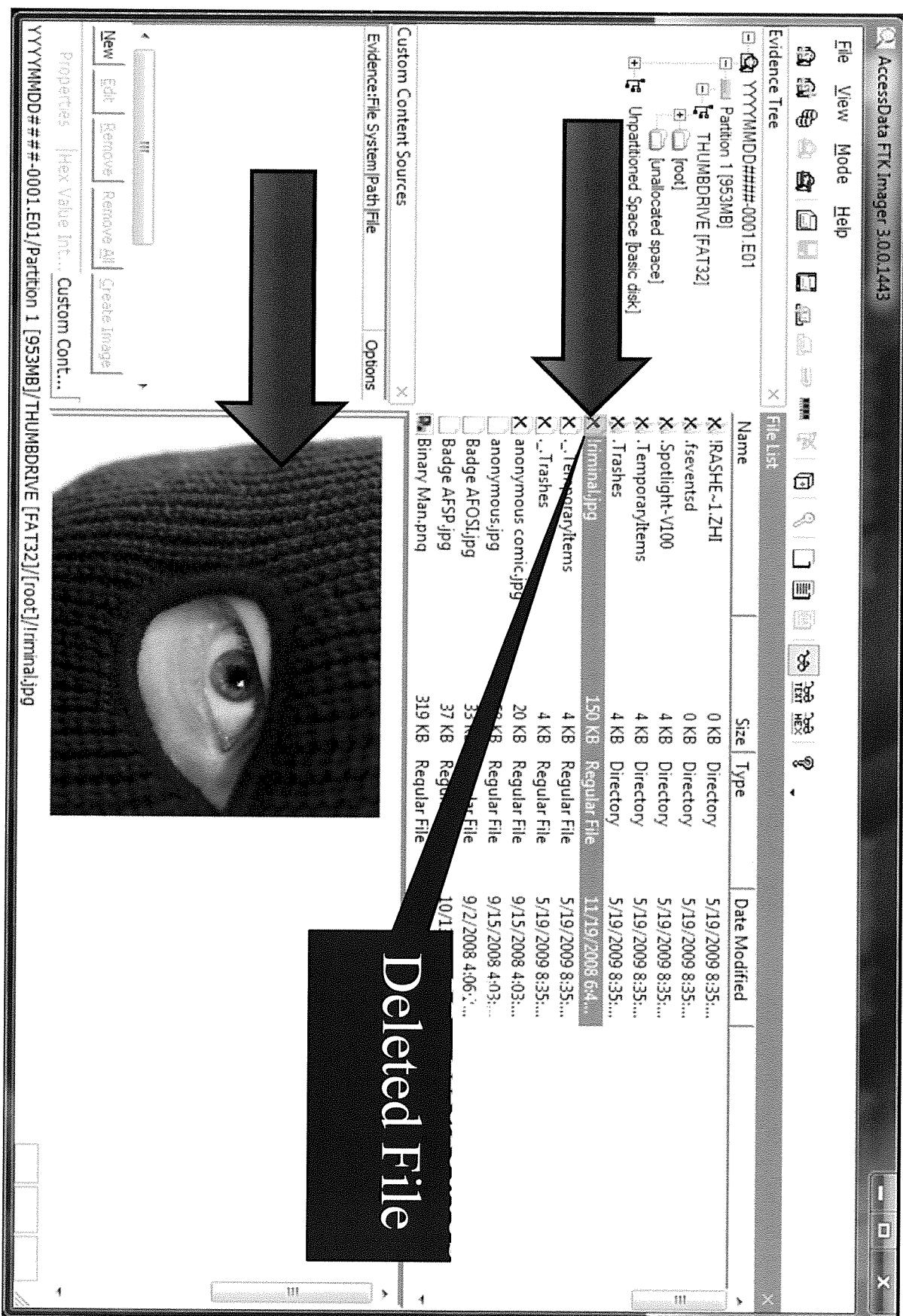
YYYYMMDD##-001.E01/Partition 1 [953M

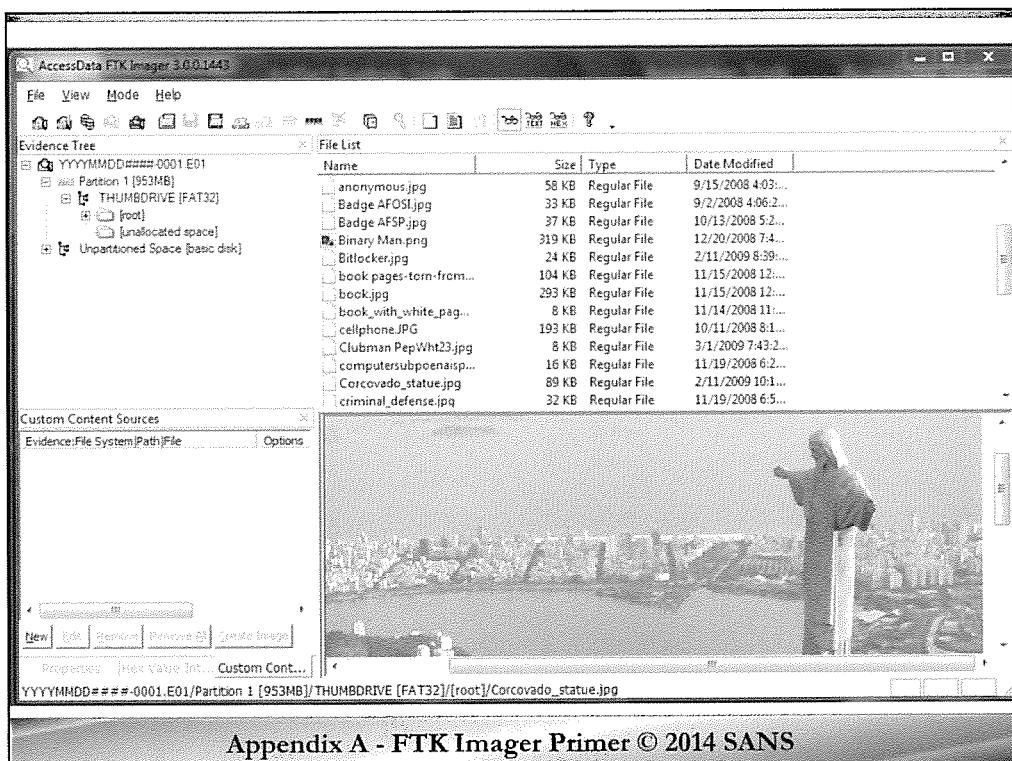


Now that you have selected the [root] directory in the Evidence Tree window, look to the window directly to the right of the Evidence Tree window we earlier identified as the File List window.

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.

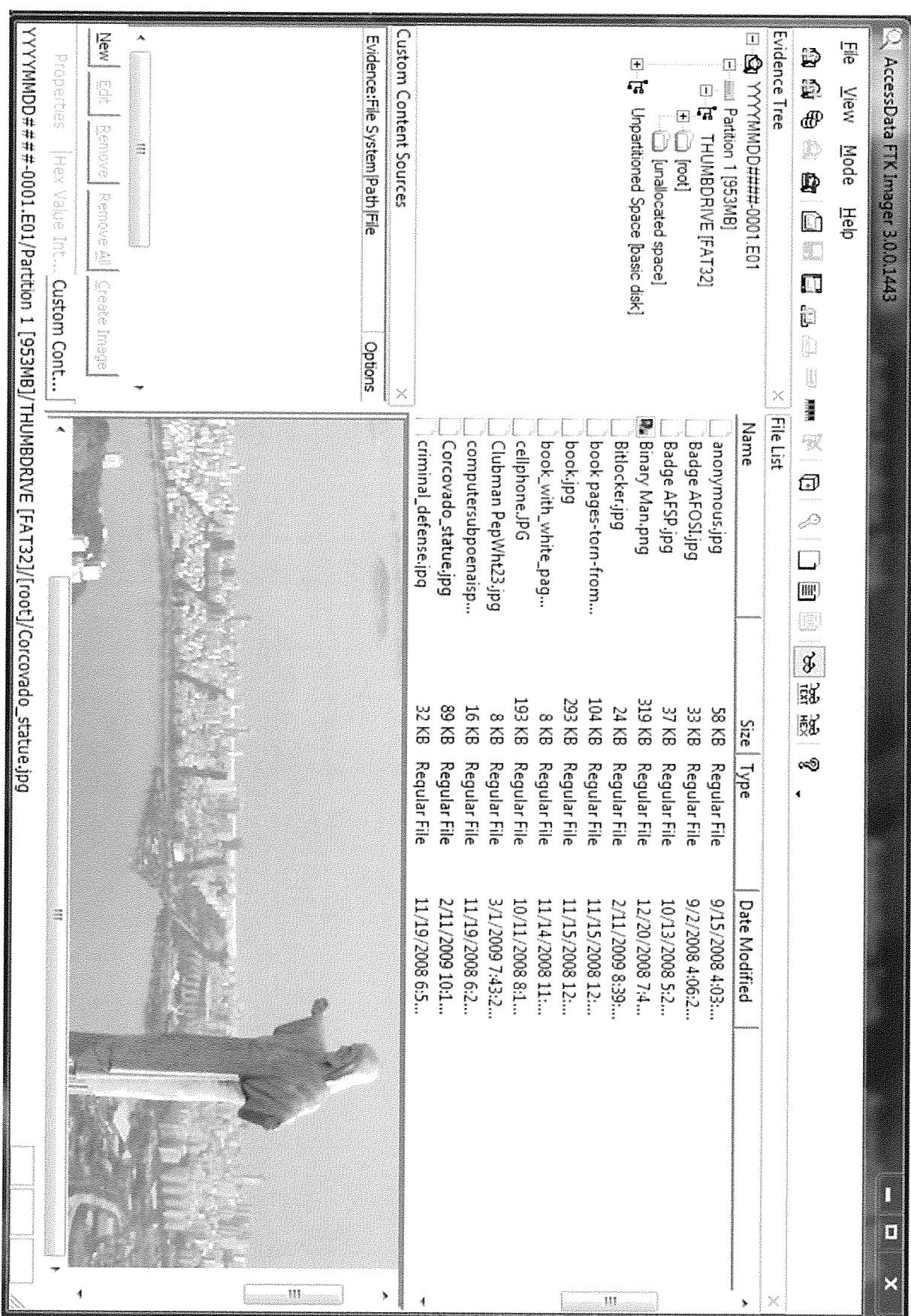
Find one of the deleted files and click on it. When you click on any of the files, the file or its contents are displayed in the viewer pane located directly below the File Viewer window.

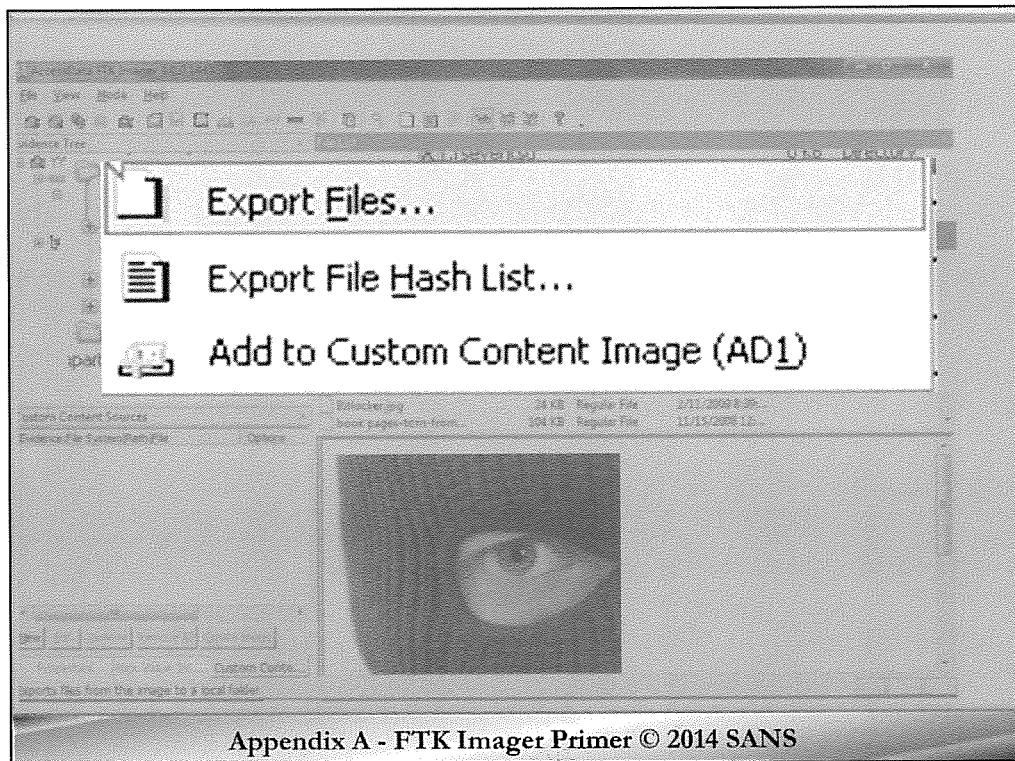




Appendix A - FTK Imager Primer © 2014 SANS

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 the exact files or information you need in your investigation, and either confront the subject, identify additional time critical evidence that requires additional investigative leads, etc. Imagine having this ability on-scene to give files to the investigators, all before they even leave the scene. I have also found sometimes that it is useful to bring the case agent over to my computer, so we can quickly poke through the system together.





Appendix A - FTK Imager Primer © 2014 SANS

Go ahead and find the file called “**!criminal.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.

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**

AccessData FTK Imager 3.00.1443

File View Mode Help

Evidence Tree

FileList

Name	Size	Type	Date Modified
!RASHE~1.ZHI	0 KB	Directory	5/19/2009 8:35...
.fsevents	0 KB	Directory	5/19/2009 8:35...
.Spotlight-V100	4 KB	Directory	5/19/2009 8:35...
.TemporaryItems	4 KB	Directory	5/19/2009 8:35...
.Trashes	4 KB	Directory	5/19/2009 8:35...
..Temporary			
..Trashes			
anonymous.c			
anonymous.j			
Badge AFOSI.jpg	33 KB	Regular File	5/2/2008 4:06:2...
Badge AFSP.jpg	37 KB	Regular File	10/13/2008 5:2...
Binary Man.png	319 KB	Regular File	12/20/2008 7:4...
Bitlocker.jpg	24 KB	Regular File	2/11/2009 8:39...
book pages-torn-from...	104 KB	Regular File	11/15/2008 12:...

Custom Content Sources

Evidence:File System|Path|File Options

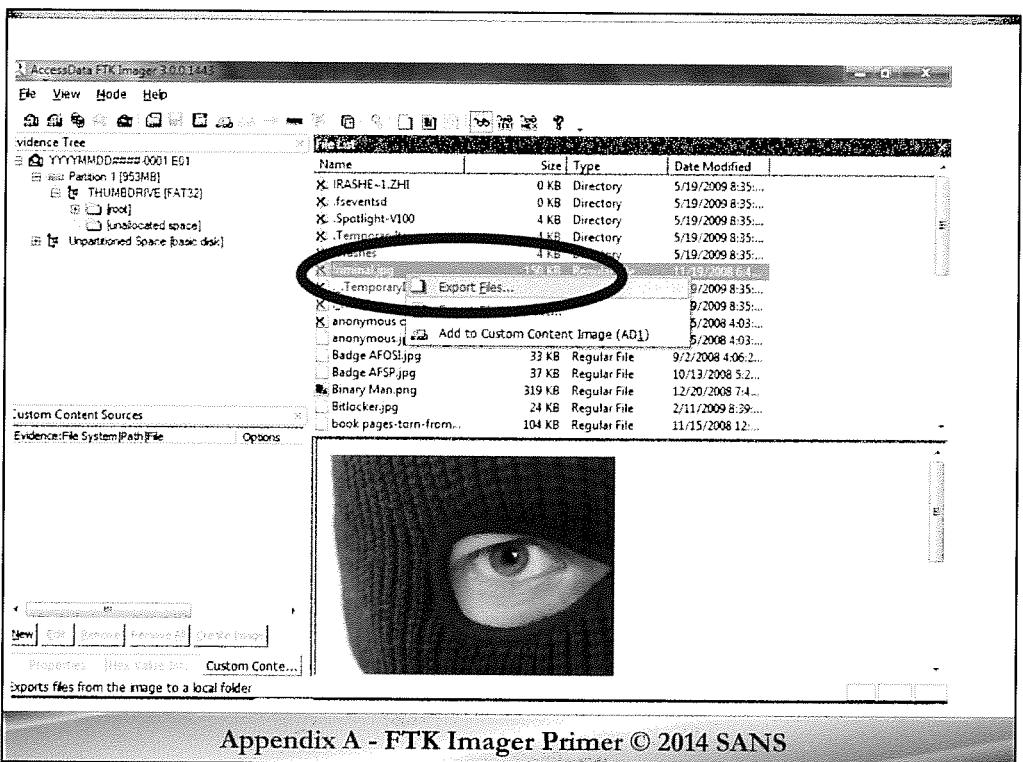
New Edit Remove As Create Image Properties Hex Value Int... Custom Conte...

Exports files from the image to a local folder

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.



Appendix A - FTK Imager Primer © 2014 SANS

To review, you should have right clicked on the file called “!criminal.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.

AccessData FTK Imager 3.0.0.1443

File View Mode Help

Evidence Tree

- Partition 1 [953MB]
 - THUMBDRIVE [FAT32]
 - [root]
 - [Unallocated space]
 - [Unpartitioned Space [Basic disk]]

File List

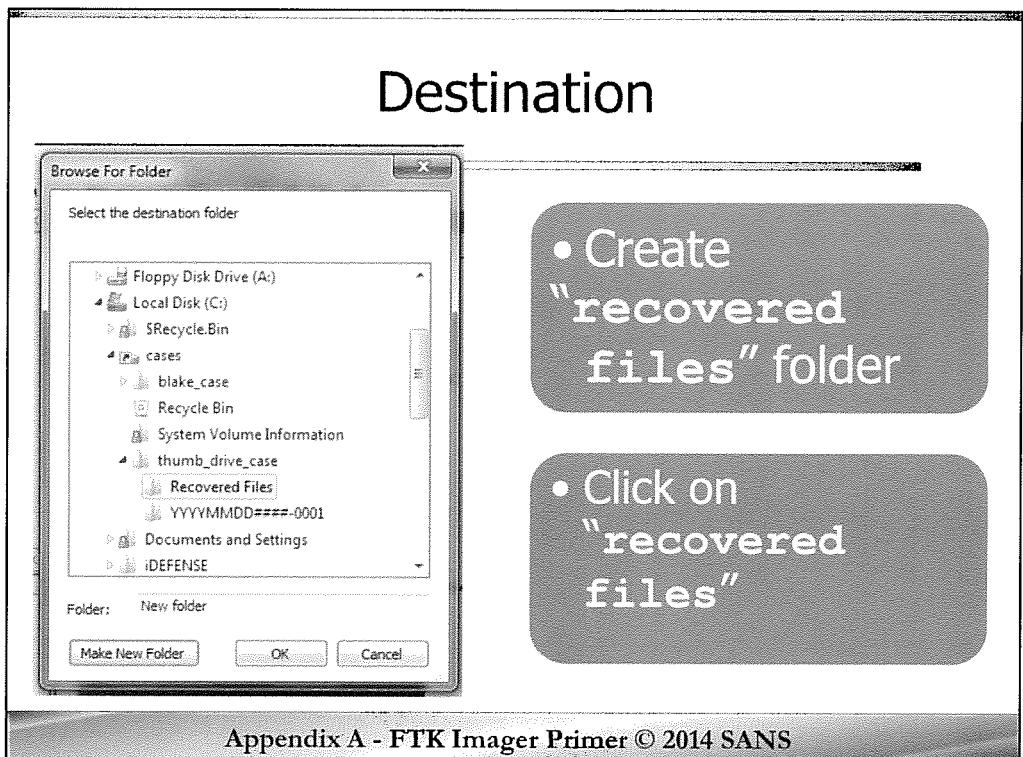
Name	Size	Type	Date Modified
X IRASHET~1.ZHI	0 KB	Directory	5/19/2009 8:35:....
X .sevents.d	0 KB	Directory	5/19/2009 8:35:....
X .Spotlight-V100	4 KB	Directory	5/19/2009 8:35:....
X .TemporaryItems	4 KB	Directory	5/19/2009 8:35:....
X .Trashes	4 KB	Directory	5/19/2009 8:35:....
X Immortal.jpg	150 KB	Bitmap File	11/19/2008 6:4:....
X .Temporary			9/2009 8:35:....
X .Trashes			9/2009 8:35:....
X anonymous.c			5/2008 4:03:....
X anonymous.jpg			5/2008 4:03:....
X Add to Custom Content Image (AD1)			
Badge AFOS.jpg	33 KB	Regular File	9/2/2008 4:06:2:....
Badge AFSP.jpg	37 KB	Regular File	10/13/2008 5:2:....
Binary Man.png	319 KB	Regular File	12/20/2008 7:4:....
Bitlocker.jpg	24 KB	Regular File	2/11/2009 8:39:....
book pages-torn-from...	104 KB	Regular File	11/15/2008 12:....

Custom Content Sources

Evidence File System Path File Options

New Edit Remove All Create Image Hex Value Editor Properties Custom Content..

Exports files from the image to a local folder

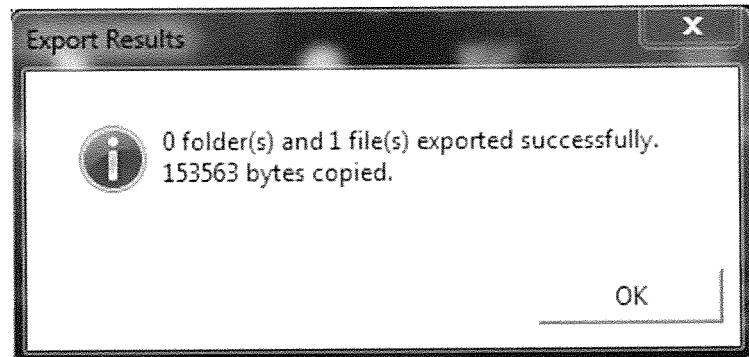


After selecting “**Export File...**”, you see a dialog box to select where you want to export your file(s). Remember, you will never export anything to the subject's drive, and since you have a write block attached to the device, you would not be able to anyway. But again, perhaps you just want to extract some files to the lead investigator's thumb drive. Create a new folder under C:\cases\thumb_drive_case called recovered files.

So we can easily find it, let's select the C:\cases\thumb_drive_case\recovered files folder then click “**OK**”.

Export Results

- If successful, you will receive this dialog box



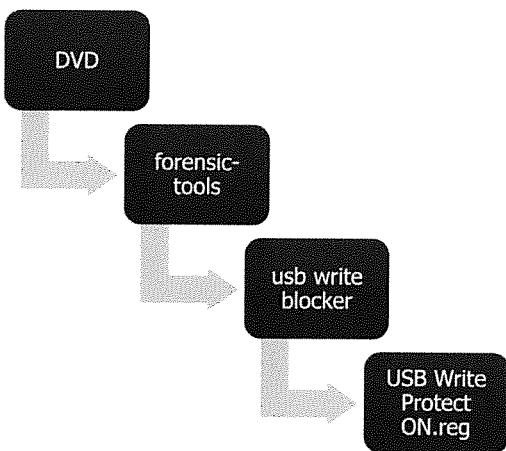
Appendix A - FTK Imager Primer © 2014 SANS

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

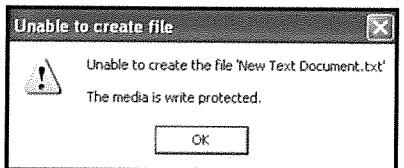
You can click "OK" to close the dialog box.

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

HANDS-ON: SET USB Write Protect



1. Execute "USB Write Protect ON.reg" from Desktop
2. Set USB Write Blocker to ON
3. Plug in your USB Thumb Drive



Appendix A - FTK Imager Primer © 2014 SANS

On your Course DVD, locate the "USB Write Protect ON.reg" and "USB Write Protect OFF.reg" files (Found in D:\forensic-tools\usb write blocker), and copy them to your host desktop.

1. Execute "USB Write Protect ON.reg" from your Host Machine
2. Set USB write blocker to ON
3. 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 WiebeTech USB Write Block or the Tableau T8 USB write block. With this device you are absolutely sure no writes will be made to the USB device.



Digital Forensics and Incident Response

CURRICULUM



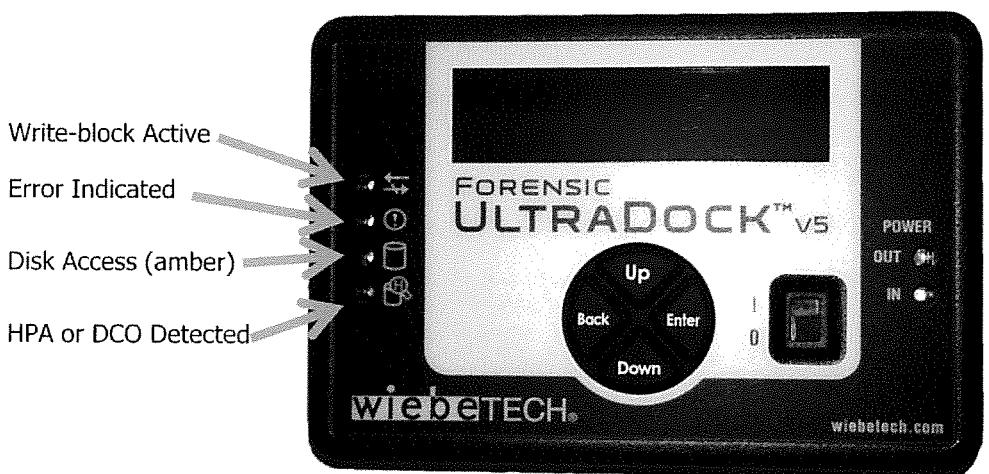
Hard Drive Acquisition

Working with the WiebeTech
UltraDock v5 Write Blocker Kit

Appendix B - Hard Drive Acquisition © 2014 SANS

This page intentionally left blank.

WiebeTech Forensic UltraDock v5



Appendix B - Hard Drive Acquisition © 2014 SANS

The WiebeTech Forensic UltraDock version 5 is WiebeTech's premium forensic write block device. The UltraDock is always write blocked so you don't have to worry about forgetting to flip a switch to protect your target media. The UltraDock provides the ability to image IDE devices (Parallel ATA hard disk devices with LBA (Logical Block Addressing)) or SATA 1 or SATA 2 hard disk devices.

The UltraDock device has a rugged aluminum enclosure and made to operate in weather conditions from Arizona to Louisiana and from Alaska to Baghdad – that is they can operate from 32-132 degrees Fahrenheit with NO airflow and up to 95% humidity. It comes with an international external power supply that accepts 100-240VAC and it can also be powered through a computer's SATA power supply.

The Forensic UltraDock has a benchmarked peak speed of 211.9 MB/s. Your imaging speed may vary depending on the slowest drive speed in the imaging process.

A series of LED indicators along the left side of the UltraDock provide feedback to the technician. The LED at the top left of the UltraDock will illuminate steady green to indicate the write block is working properly. The second LED will illuminate red if an error is detected. The third LED will flash green showing disk read activity and the last LED will illuminate green if a Host Protected Areas (HPA) or Disk Control Overlays (DCO) is detected. The technician will also be alerted through the LCD display screen. By default, the Forensic UltraDock will unlock any HPA making them available for imaging during the normal imaging process.

There is a four button navigation interface that will allow the technician to view either the target drive information or the UltraDock product information. When viewing the target drive information, the UltraDock will read and report Self Monitoring, Analysis and Reporting Technology (S.M.A.R.T.) if available information such as the following may be available:

Disk Temp - Temperature of the attached drive, measured in degrees Celsius.

Capacity (MB) - Capacity of the HDD, measured in megabytes.

Manufacturer - Manufacturing company name of the HDD.

Model number - Model number of the HDD.

Serial number - Serial number of the HDD.

Firmware Rev - Firmware revision number of the HDD .

HPA size (MB) - The size of the Host Protected Area of the HDD, measured in megabytes.

DCO size (MB) - The size of the Device Configuration Overlay of the HDD, measured in megabytes.

Disk health - Displays the S.M.A.R.T. health status of the drive.

Start/Stops - S.M.A.R.T. information on how many times the drive has spun up and spun down.

Power cycles - S.M.A.R.T. information on how many power on/off cycles the drive has underwent.

Bad sectors - Number of bad sectors reported by the drive.

Ref: S.M.A.R.T. - <http://en.wikipedia.org/wiki/S.M.A.R.T.>

WiebeTech UltraDock SATA/IDE Bridge

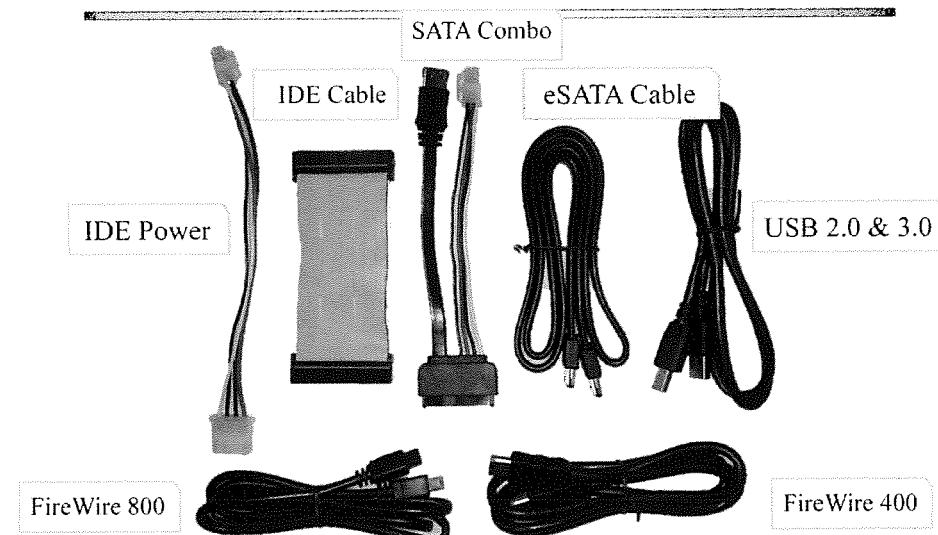


Appendix B - Hard Drive Acquisition © 2014 SANS

The UltraDock also provides two native 9-pin FireWire800 (1394B) and one native 6-pin FireWire400 (1394A) connection to your forensic system, as well as one USB 3.0 allowing USB 3.0 and 2.0 data transfer speeds and one eSATA.

On the left side of the UltraDock there is a USB 2.0 and 3.0 switch. For best you should always set this switch to the appropriate USB port you are connecting with.

Contents of Your UltraDock Kit



Appendix B - Hard Drive Acquisition © 2014 SANS

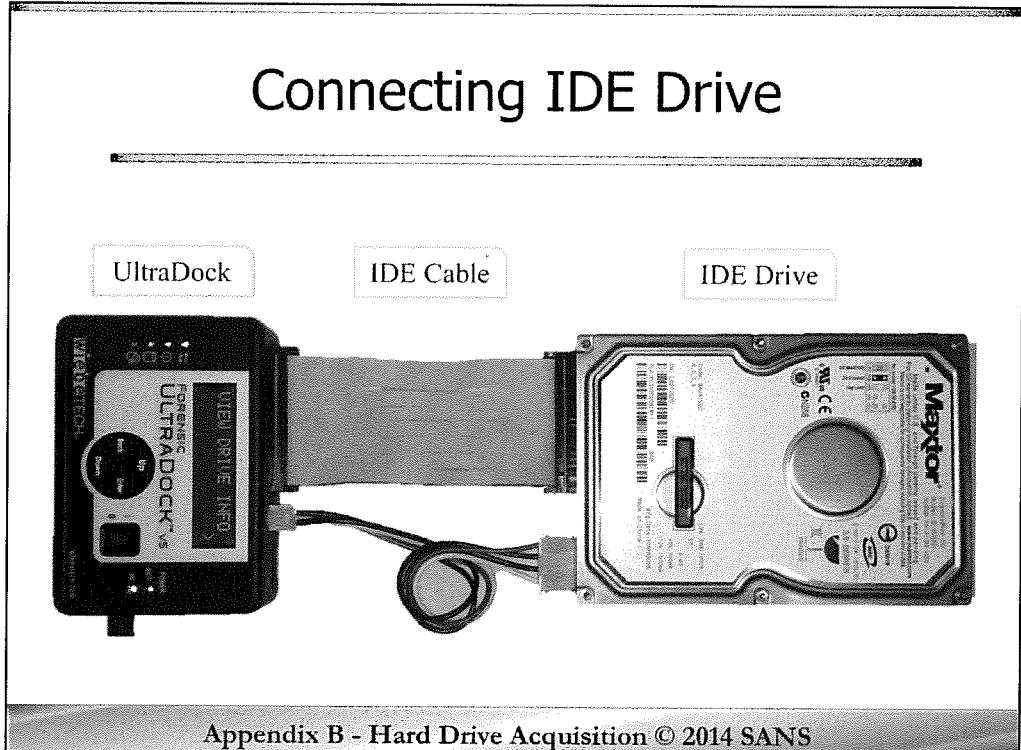
Pictured here are the primary items you will find in your Forensic UltraDock write block kit. It includes everything you need to image standard 3.5 inch IDE & SATA hard drives that you would typically find in desktop computer systems.

Starting from the left and going clockwise you have the IDE power cable, the IDE ribbon cable, a combo SATA cable and power connector, a SATA cable, a USB 3.0 or 2.0 cable, a 6-pin FireWire400 (1394A) cable and a 9-pin FireWire800 (1394B) cable.

WiebeTech also sells a number of adaptors for almost all other digital media that will interface with the Forensic UltraDock.

Ref: UltraDock Adaptors: http://www.wiebetech.com/products/v4_adapters.php

Connecting IDE Drive



Appendix B - Hard Drive Acquisition © 2014 SANS

In this slide we are showing you a typical connection to an IDE drive. Starting at the RIGHT of the screen you see the Subject drive or the drive you want to create an image of. In our picture here it is labeled as “IDE Drive”. Next, you see the IDE cable at the top connected from the drive to your UltraDock write block device.

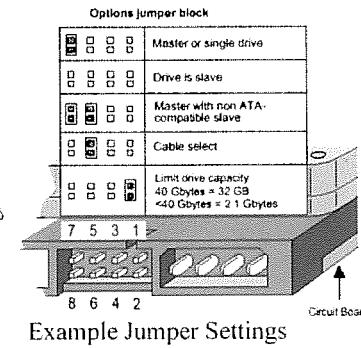
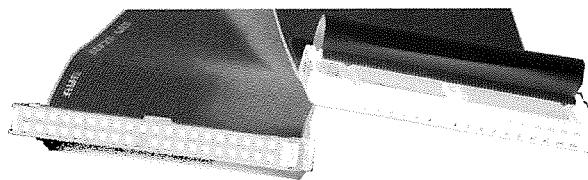
At the bottom of the screen you will see a blow up of the IDE connectors. You should notice a tab in the middle of each of the end connectors of the IDE cable. These tabs should correspond to the notch in the IDE connector of the drive. This helps you properly connect the ribbon cable to the drive without having to worry about where pin number one of the drive and cable is. When I started in forensics, not all drives had this and you had to look real close to the drive to identify where pin number 1 was, usually it is nearest the power plug but you could never assume. On the IDE ribbon cable you will see one side of the ribbon cable has a red line, this indicates it is pin number one on the cable. You should know this because you may come across a drive and cable without the tab and now you will know how to identify pin number one.

So now you have the IDE ribbon cable connecting the subject drive to the UltraDock write block device, next, just below the IDE cable in the photograph you will see the power cord. Your write block kit comes with two different power cords, one for IDE drives and another for SATA drives. On the opposite side from your IDE cable on your write block device you will attach the fastest data transfer cable your forensic system supports SATA, fire wire 800, firewire 400, or USB 3.0.

Hints for Success: Important Notes

- Drive Jumpers

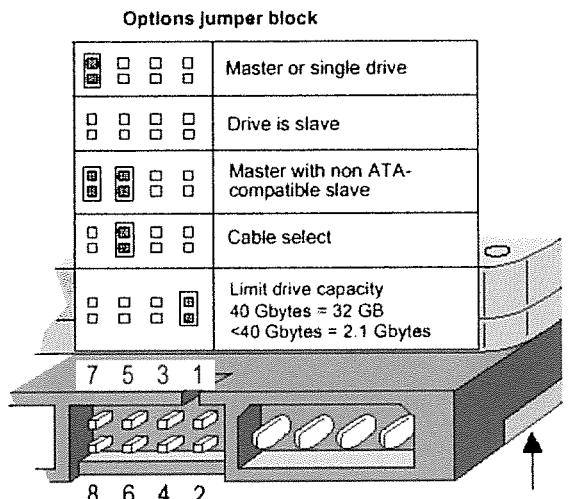
- The suspect IDE hard drive must be configured as a "Single Master Device"
- Not slave or cable select



Appendix B - Hard Drive Acquisition © 2014 SANS

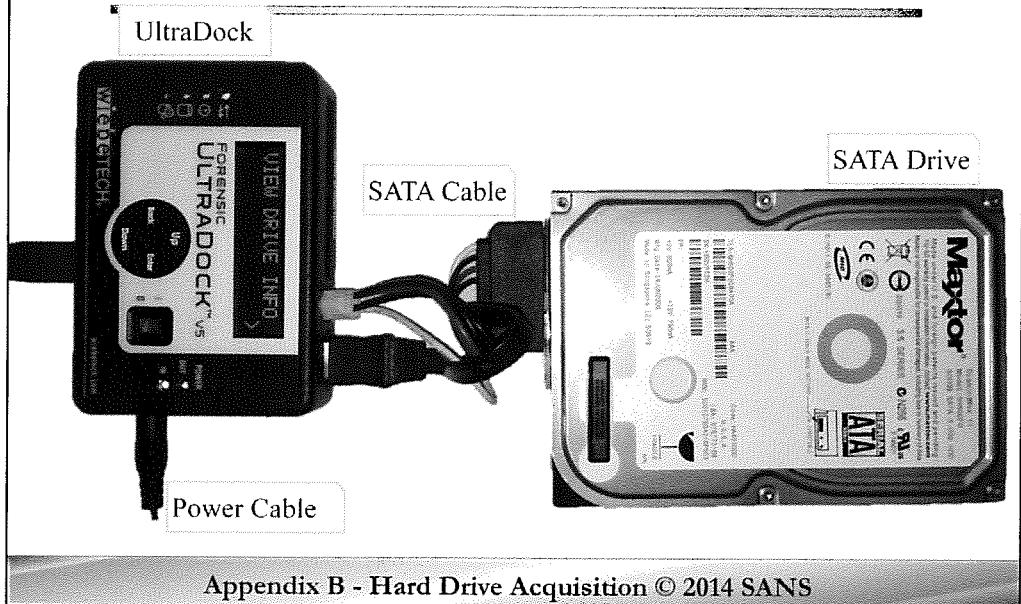
VERY IMPORTANT NOTES:

- *The suspect IDE hard drive must be configured as a "Single Master Device" (not slave or cable select).*



Example Jumper Settings

Connecting Serial ATA



Appendix B - Hard Drive Acquisition © 2014 SANS

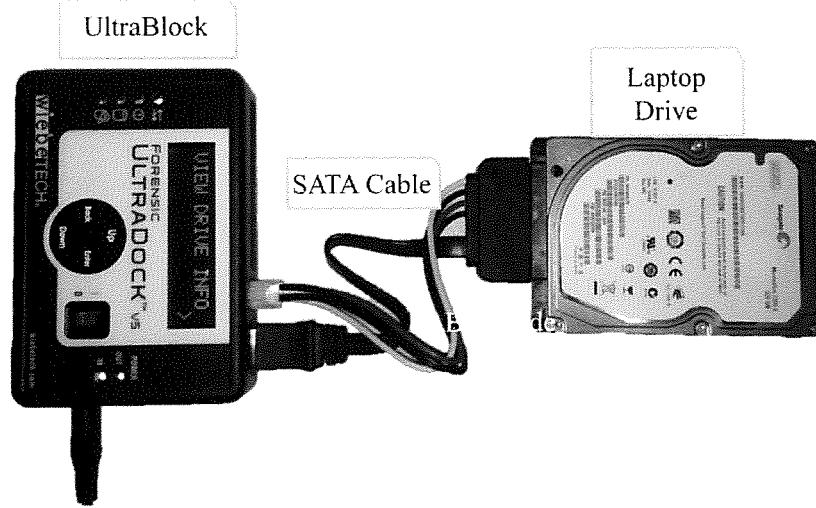
Now here in this slide we see the same kind of setup but this time with a Serial ATA drive. The only two things that are different are that the IDE cable has been replaced with the red SATA cable and we are now using the SATA power cable.

You will typically find that imaging a SATA drive takes a shorter time than imaging an IDE drive. The reason for that is the possible data read rates are higher, i.e. data can be read and moved off the target or subject drive faster than a typical IDE drive. Also, the thru-put on the SATA cable is faster.

Because imaging is such a time-intensive process, another thing to remember is you should always be looking to reduce bottle necks. What I mean by this is while you have no control over what your subject equipment is, the bottle-neck should never be on your end. You should always look to be imaging to the fastest drive you have available, using the fastest/best transfer medium (cable), etc.

You would not want to be imaging a subject's 10,000 RPM SCSI drive to your old 4200 RPM IDE drive over a USB cable.

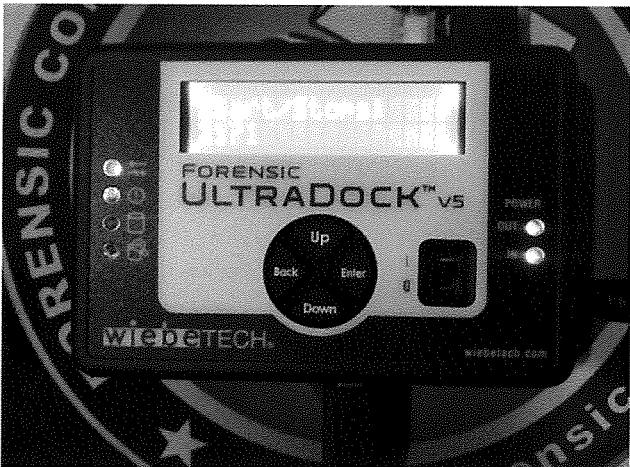
Connecting Laptop Drive



Appendix B - Hard Drive Acquisition © 2014 SANS

Now this slide shows the same set up but this time imaging a 2.5 inch laptop drive. In most cases, you will find it necessary to remove the drive from the component. While this seems logical when talking about a laptop, you may not have thought about it when imaging a portable USB drive. If you can take the drive out of the device, hook it directly to the write block device of yours, you will find you have the least problems.

Drive Info and S.M.A.R.T Data



- Disk Temp
- Drive Capacity
- Manufacturer
- Model Number
- Serial Number
- Firmware Revision
- HPA Size
- DCO Size
- Disk Health
- Start Stops
- Power Cycles
- Bad Sectors

Appendix B - Hard Drive Acquisition © 2014 SANS

S.M.A.R.T. stands for Self-Monitoring, Analysis, and Reporting Technology, and is a built-in feature of hard drive firmware that tries to predict upcoming drive failures. [1] A large amount of information is stored about the drive to assist with predictions.

Your Wiebetech Ultradock provides the option to “View Drive Info” when a drive is attached. Pressing “Enter” will show the following drive data and S.M.A.R.T. statistics:

- Disk Temp
- Drive Capacity
- Manufacturer
- Model Number
- Serial Number
- Firmware Revision
- HPA Size
- DCO Size
- Disk Health
- Start Stops
- Power Cycles
- Bad Sectors

The disk health and bad sector information is particularly helpful in situations when there are imaging or hash verification difficulties.

The Wiebetech unit does not have to be attached to a computer to provide this information.

[1] <http://en.wikipedia.org/wiki/S.M.A.R.T.>

Host Protected Area (HPA) and Disk Configuration Overlay (DCO) (1)

- Firmware based ATA disk commands that can be used to create hidden drive areas
- Not user accessible and will NOT be acquired by default
- Can be used to store system restore files, security software, or hidden data

Disk



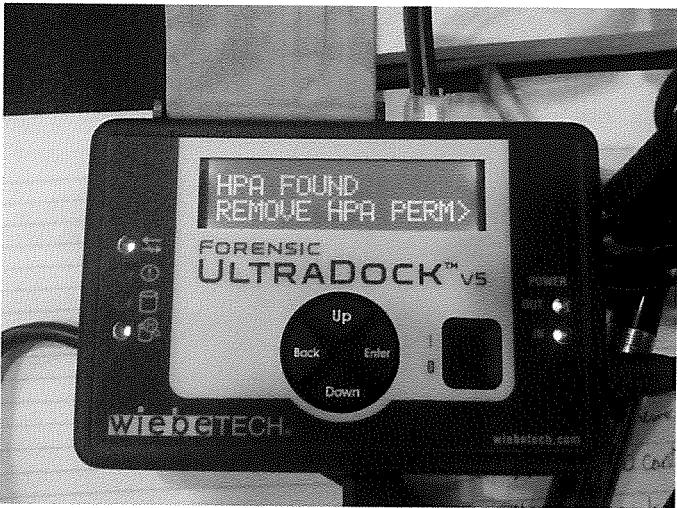
Appendix B - Hard Drive Acquisition © 2014 SANS

ATA disk standards provide standard mechanisms for reserving data at the end of the drive. The notion of a "Host Protected Area" was codified in the ATA-4 standard and a "Device Configuration Overlay" in the ATA-6 standard. [1,2] These mechanisms occur in the firmware of the drive and hence cannot be accessed by normal hardware/software commands (including forensic imaging software). A user cannot read or write to this area. Security software and computer manufacturers have been known to use HPA/DCOs to store restoration files and data so that the user cannot delete them. However, anyone can create one so the potential exists that interesting data may be present.

[1] http://en.wikipedia.org/wiki/Host_protected_area

[2] http://en.wikipedia.org/wiki/Device_Configuration_Overlay

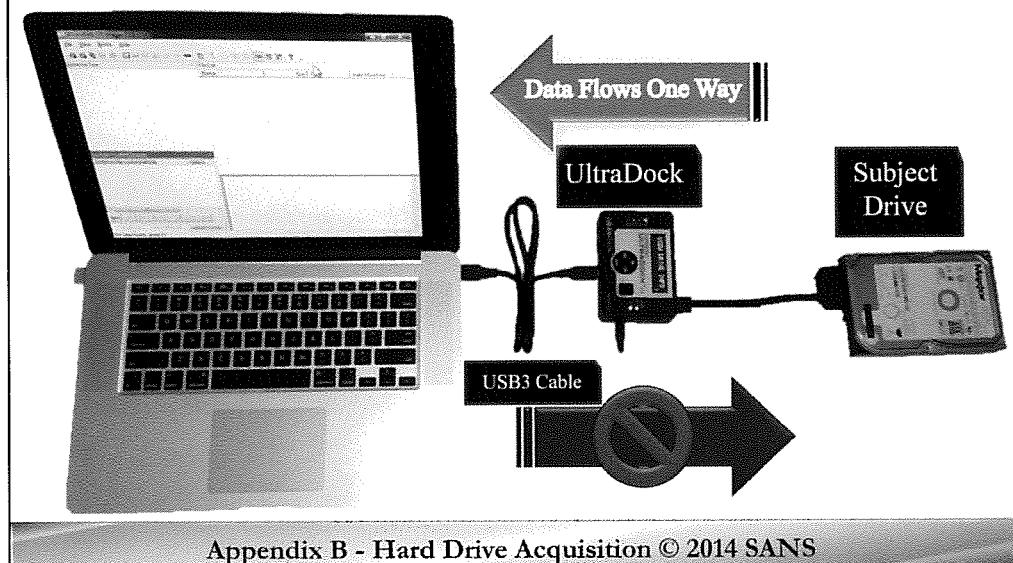
Host Protected Area (HPA) and Disk Configuration Overlay (DCO) (2)



Appendix B - Hard Drive Acquisition © 2014 SANS

When a HPA or DCO is detected, the Wiebetech UltraDock will provide the option to temporarily or permanently reset them, providing access to those locations. Since this results in a firmware change on the drive, doing so is not without risk, and has been known to result in an inoperable drive. When a HPA or DCO is encountered, the best practice is to first image the drive regularly without removing them. This gets you everything currently accessible by software. Once that is complete, you may remove the HPA or DCO and attempt to image the full drive. If the worst case happens and the drive become inoperable, you will still have your original image (minus the data in the HPA/DCO) to analyze.

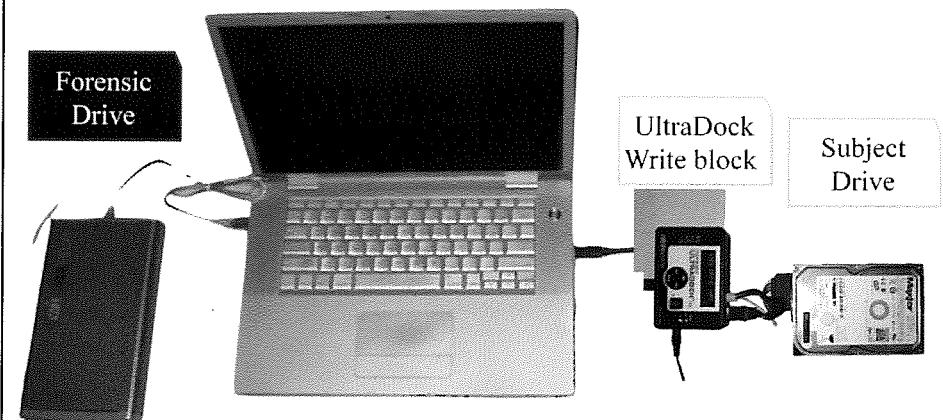
Connect the UltraDock to Forensic Machine



Once you have this all connected, you simply plug in the firewire cable as shown here into your forensic machine. In my experience, before you actually plug in the fire wire or USB device to your forensic machine, you should power up the entire device so that the drive gets to speed. If you don't do this you can sometimes have problems with your forensic machine recognizing your connected device.

(The actual power device for the UltraDock is not shown here to in an attempt to keep the example as visually clean as possible.)

Forensic Imaging Setup



Appendix B - Hard Drive Acquisition © 2014 SANS

The last image here shows the entire setup as it is most typically used in the field. You have the subject's drive on the right, then your UltraDock hardware write block, which is connected to your forensic machine where you are running your imaging software from, then your clean/prepared external capture drive. Again, you should look to make sure you do not have any bottlenecks in this process.

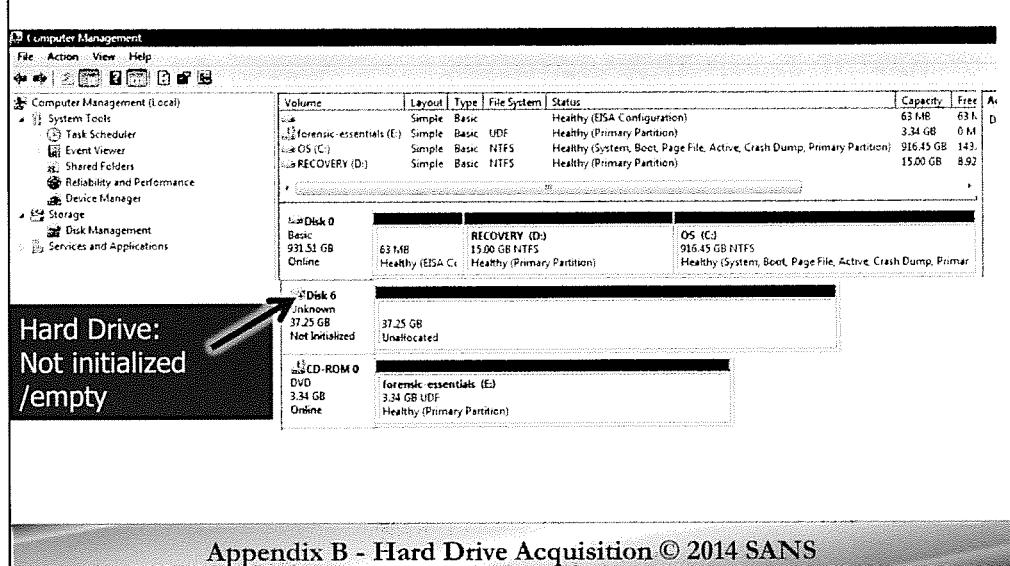
Also, while we have this screen up, it is the perfect time to remind you all that the forensic imaging machine you are using should be set up so that ALL the power saving features are turned off. You do not want a screen saver kicking in or worse, have it go into sleep or hibernation mode during the middle of your imaging. I know I have seen this happen on many occasions where the person creating the image for some reason was sitting at the system, doing something with the mouse that prevented it from going to sleep for about 5 hours, then for some reason, he did not touch the system for 30 minutes and it started trying to go into hibernation/sleep the last hour of the image, which completely screwed up the whole thing and he had to start the whole process again.

Also, while we're here that brings up another thing; you may want to consider bringing a UPS to make sure you have uninterrupted power during this whole process.

Lastly, if you have any issues with your WiebeTech Forensic UltraDock their technical support receives calls and answers email between **8:30 AM and 5:00 PM Central Time** Monday through Friday toll free 866.744.8722 (316.744.8722 Direct Line).

Write Blocker

Check if Drive is Attached to System



If the drive does not appear as a drive letter, it might not be currently formatted. If it does not show up as a drive it will show as uninitialized.

Check to see if the drive can be seen by windows via the GUI -

Click on:

Control Panel-> Administrative Tools -> Computer Management

Select Storage -> Disk Management

If the drive is uninitialized, then it still might contain data due to the fact it was formatted and the partitions cleared.

HANDS-ON: Write Blocker (1)

- Spend some time practicing connecting a hard drive through the write blocker to your forensic analysis machine
- If you would like to try a different type of hard drive, see your instructor

Appendix B - Hard Drive Acquisition © 2014 SANS

This page intentionally left blank.

HANDS-ON: Write Blocker (2)

1. Plug in Power Cord to Write Blocker
2. Plug drive into correct adapter
3. Power on Drive via UltraDock power switch
4. Plug USB into your computer

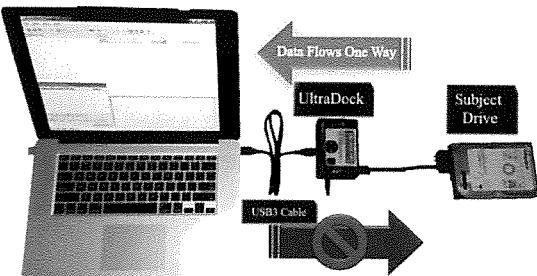
Appendix B - Hard Drive Acquisition © 2014 SANS

This page intentionally left blank.

Out-of-Class Exercise

HANDS-ON: Drive Acquisition

- What you need:
 - Practice Evidence Hard Drive (Used, Ebay, Instructor's Extra Drive)
 - External USB Drive (*Large capacity*) labeled "WORKING COPY"
 - UltraDock write blocker
- Use step-by-step on next slide
- Image your ORIGINAL Evidence hard drive to the large capacity "WORKING COPY" USB drive
- Fill out chain of custody form for the seizure



Appendix B - Hard Drive Acquisition © 2014 SANS

Out-of-Class Exercise: HANDS-ON: Drive Acquisition

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: Depending on the size of your subject drive, this exercise will take some time to complete. To ensure your system is available for other exercises, we recommend you practice this in your room tonight and bring any questions to class in the morning.

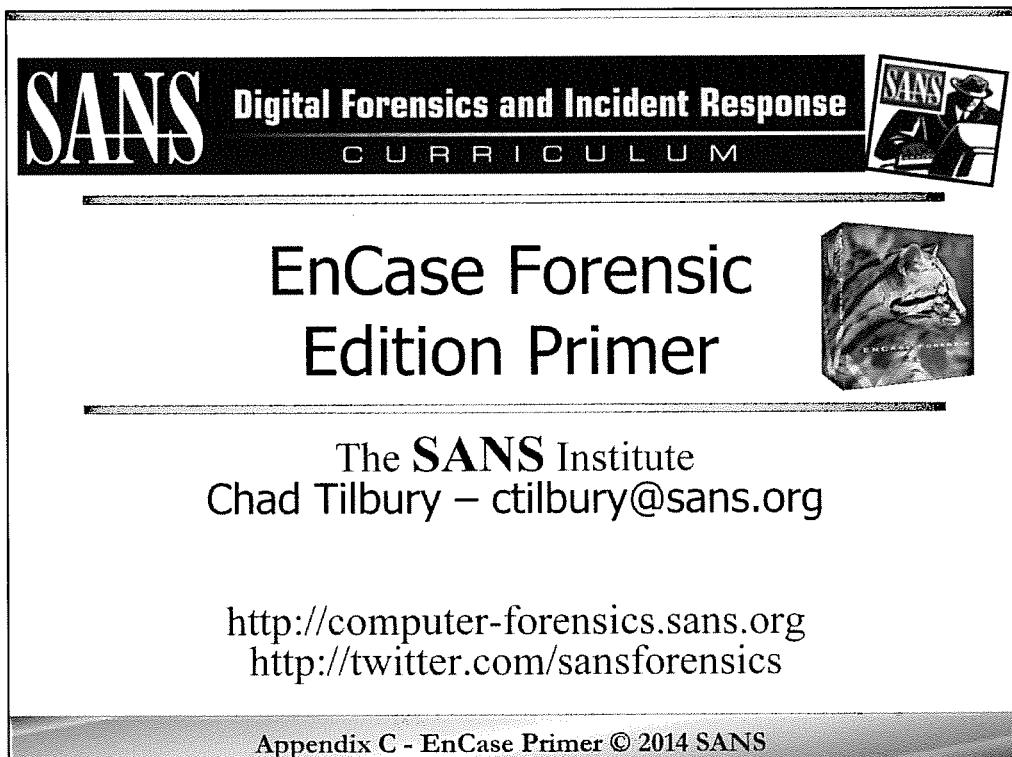
Step-by-Step: Acquisition

1. Find a used hard drive and fill out initial information on chain of custody form
2. Create a casename **YYYYMMDD#####-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 WiebeTech write blocker
 - Power on the UltraDock write blocker
 - Plug UltraDock write blocker into your laptop
7. Acquire the image "**ORIGINAL EVIDENCE**" using UltraDock and appropriate cables to the "**WORKING COPY**" USB drive
 - Use FTK Imager
8. Check Chain of Custody Form Once Complete

Appendix B - Hard Drive Acquisition © 2014 SANS

1. Find a used hard drive.
2. Create a casename **YYYYMMDD#####-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 UltraDock write blocker.
Power on the UltraDock write blocker.
Plug UltraDock write blocker into your laptop.
7. Acquire the image "**ORIGINAL EVIDENCE**" using the UltraDock 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.

This page intentionally left blank.



The slide is titled "EnCase Forensic Edition Primer". It features the SANS logo at the top left, followed by "Digital Forensics and Incident Response" and "CURRICULUM". To the right is a small graphic of a person wearing a mask. Below the title is a large image of an EnCase software box. The text "The SANS Institute" and "Chad Tilbury – ctisbury@sans.org" is centered. At the bottom, there are two URLs: <http://computer-forensics.sans.org> and <http://twitter.com/sansforensics>. A footer bar at the bottom contains the text "Appendix C - EnCase Primer © 2014 SANS".

Welcome to Core Windows Forensics.

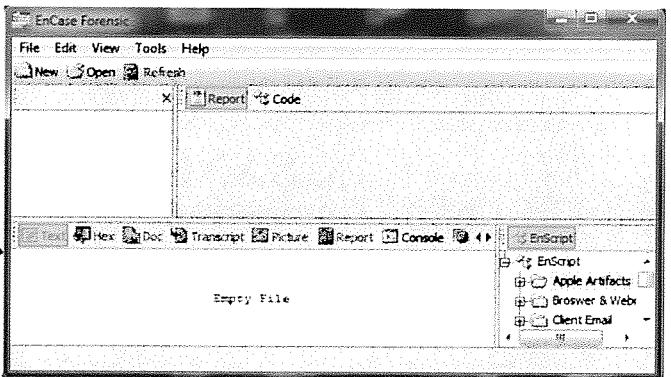
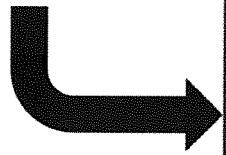
The SANS Institute
Chad Tilbury – ctisbury@sans.org

<http://computer-forensics.sans.org>
<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.

Launching EnCase

Guidance Software

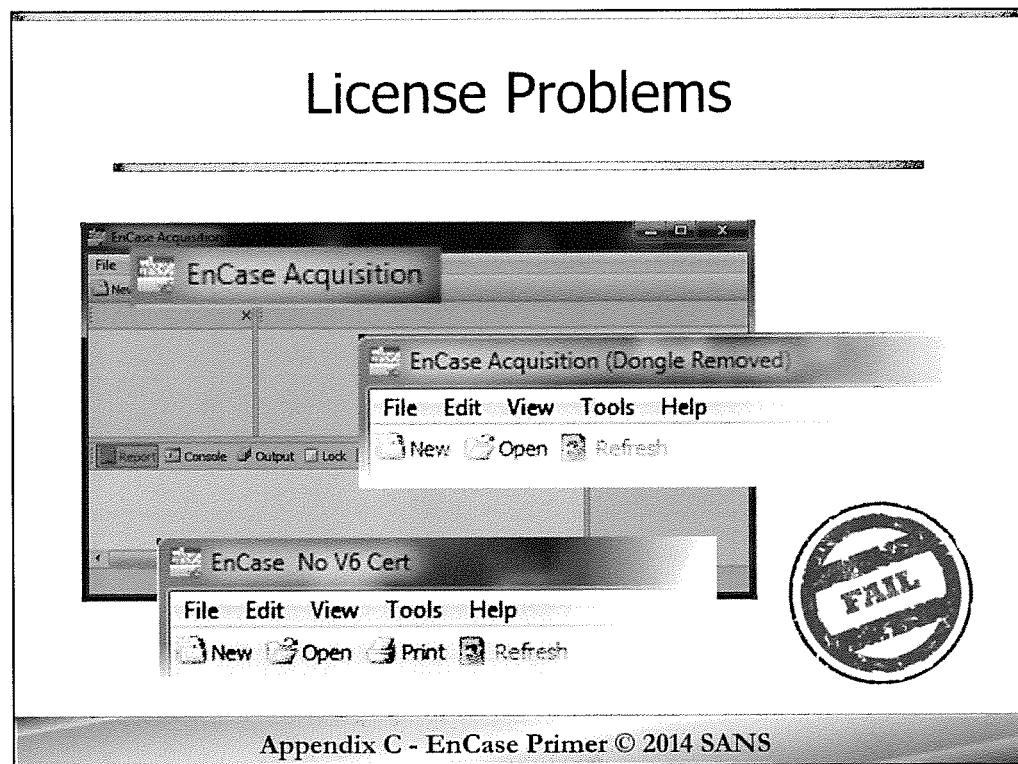


Appendix C - EnCase Primer © 2014 SANS

Launching EnCase on your Windows SIFT workstation is as simple as finding the Guidance Software menu on the desktop and clicking the EnCase shortcut. Be patient! It takes a while for the application to load and multiple clicks will load multiple instances. If you have given up all hope, check the Windows Task Manager to see if the EnCase.exe process is currently running.

EnCase uses dongle-based copy protection and thus a dongle/license key is required to run the software. There is no evaluation mode in the product. Your license will be provided via a Network Authentication Server located at the SANS operations center. To retrieve the license, you must have previously configured and be connected to the OpenVPN within the SIFT workstation. You will only have access to EnCase while connected to the VPN.

If the application loads and the title bar reads “EnCase Forensic”, you have successfully retrieved a valid license.



Appendix C - EnCase Primer © 2014 SANS

If you were not successful at retrieving a license from the Network Authentication Server (over the configured OpenVPN connection), EnCase will still load, but you will notice a slightly different interface. If no dongle is detected, EnCase loads an acquisition application, allowing forensic images to be created without a dongle. However, you will not be able to conduct any analysis of evidence.

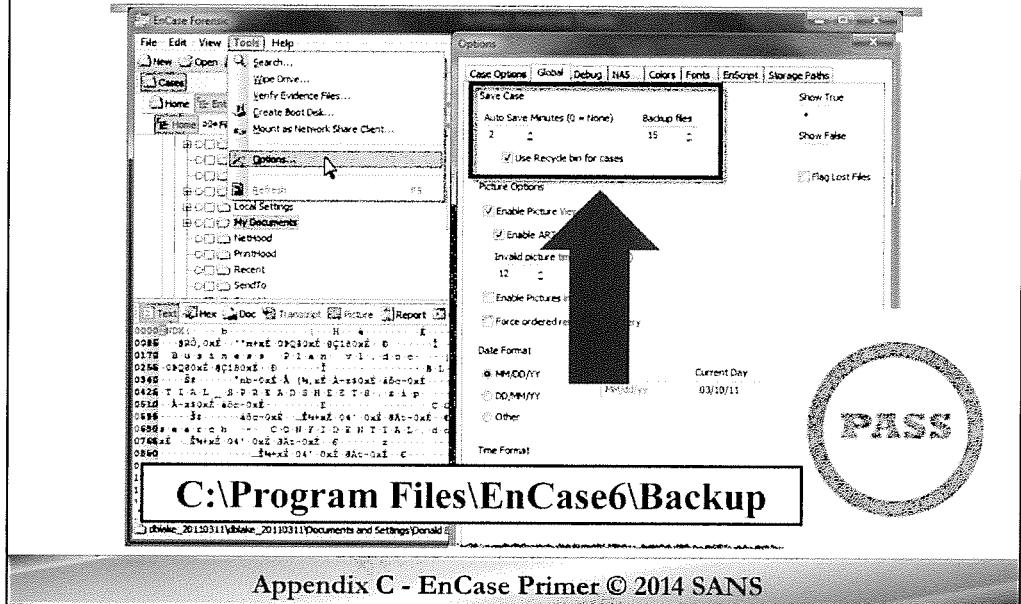
A similar process occurs if for some reason you lose your network-based license key. This most often occurs due to network problems. In most circumstances your previous work will be preserved. If your current EnCase session transitions from "EnCase Forensic" to "EnCase Acquisition" do the following:

1. **File → Save** (to save your current changes)
2. **File → Exit**
3. Reload EnCase
4. Confirm that EnCase Forensic has loaded
5. **File → Open** to reopen your Case File

If EnCase Forensic does not load during step 3, check your network and OpenVPN connectivity and wait a short while, then try again. You may need to reconnect your OpenVPN or restart your workstation in rare instances.

If it appears that you have lost some of your work, consider reverting to one of your Backup Case Files within the C:\Program Files\EnCase6\Backup folder using the **File → Open** command.

Automating Backups



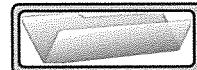
Appendix C - EnCase Primer © 2014 SANS

Strange things happen within an application suite as complicated as EnCase and thus you can never have too many backup files at your disposal. EnCase includes a handy Auto Save feature that we highly recommend you set up as soon as you start working with the application.

To set up Auto Save, go to the Tools menu and select Options. Within the Options dialog, select the Global tab and find the Save Case options. You have the ability to select how often you want backups to be created and how many backup files to keep. EnCase uses a First In First Out (FIFO) method for overwriting old backup files. Frequent Auto Saves may cause a minor performance drop, but for the purposes of this class it will be negligible.

By default, backup files are stored in the C:\Program Files\EnCase6\Backup folder. The files have an extension of ".cbak". This default location can be changed with **Tools → Options → Storage Paths**.

EnCase Overview



Creating a New Case



Using EnCase



EnScript Engine



Forensic Techniques



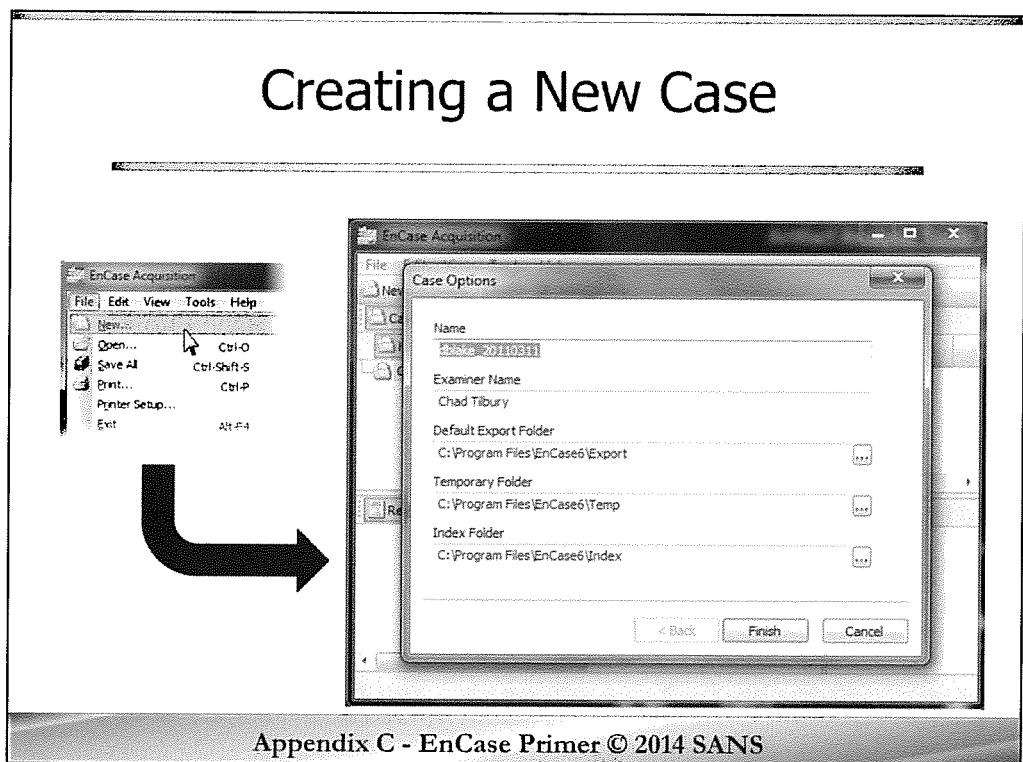
Application Parsing



Bookmarks and Reporting

Appendix C - EnCase Primer © 2014 SANS

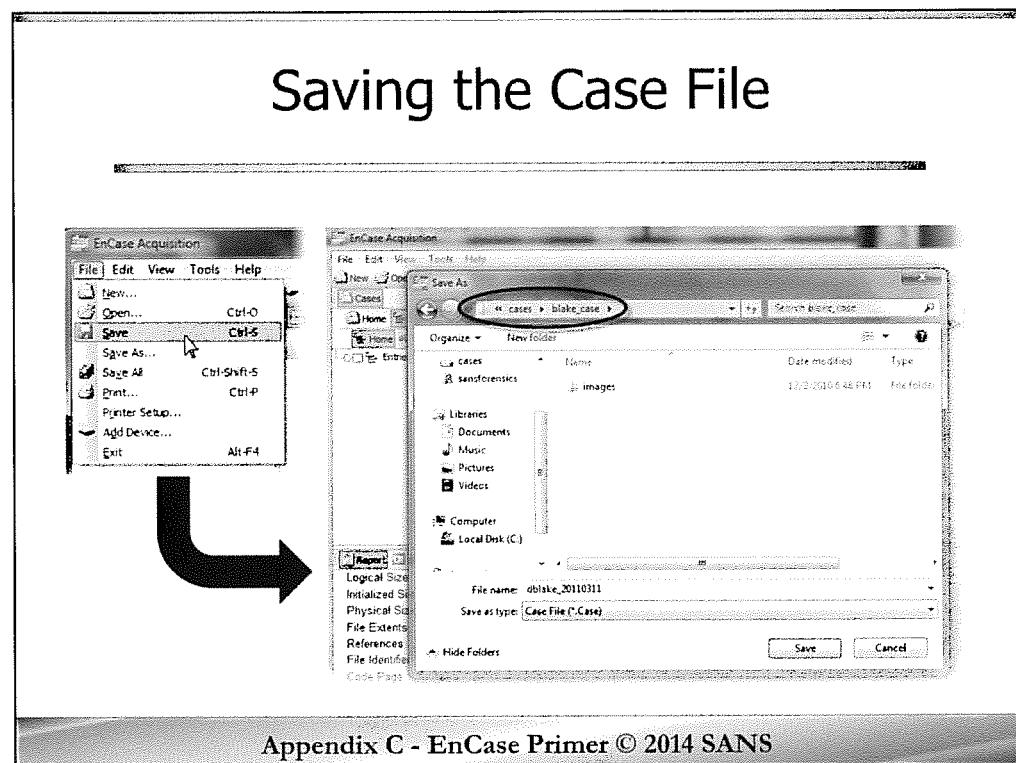
This page intentionally left blank.



Appendix C - EnCase Primer © 2014 SANS

The first step to using EnCase is to create a new case. Think of a case as your session within EnCase, incorporating all of your evidence, analysis, searches, and configuration information. A case must be created before evidence or image files can be added.

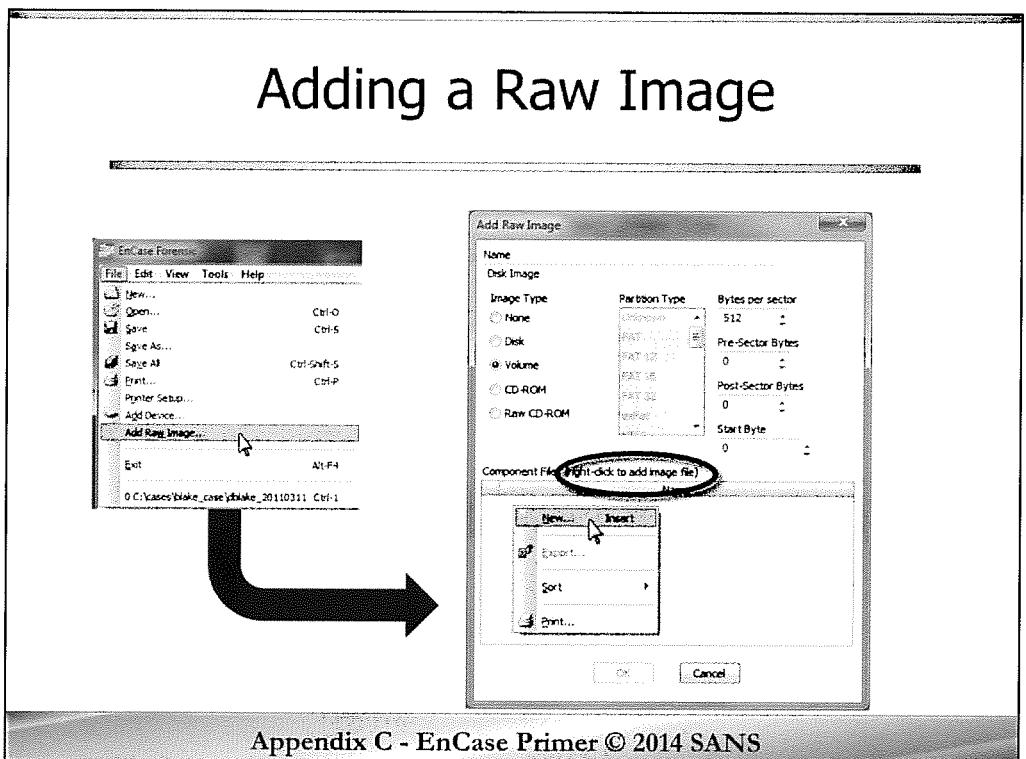
Setting up a new session is easy. Select **File** → **New** and the Case Options dialog will load. Simply provide a case name (consider using a descriptive, standard format) and your name as the examiner. A best practice is to change the default storage locations to unique folders under your cases folder. This is an easy way to keep data from multiple cases segregated.



Appendix C - EnCase Primer © 2014 SANS

Immediately after creating a case, you should save the case file. The action is **File → Save**. This creates the actual “.case” file and saves your settings. You will be prompted to browse to a save location. We recommend utilizing the existing “cases” directory on your SIFT workstation. It is easy to mix up old and new case files, often resulting in lost work. By using descriptive names for your cases and keeping them in a standard location, you can prevent confusion.

You should save your case often, particularly after any processing has finished or analysis milestones have been met. If a catastrophe occurs, you will still have your backup files, but it is best to not rely upon those unless you absolutely need them. Using the **File → Save All** command performs a more comprehensive save, similar to the one that occurs when exiting the application. The Save All command saves the case information AND the global application files containing preferences, conditions, and filters.



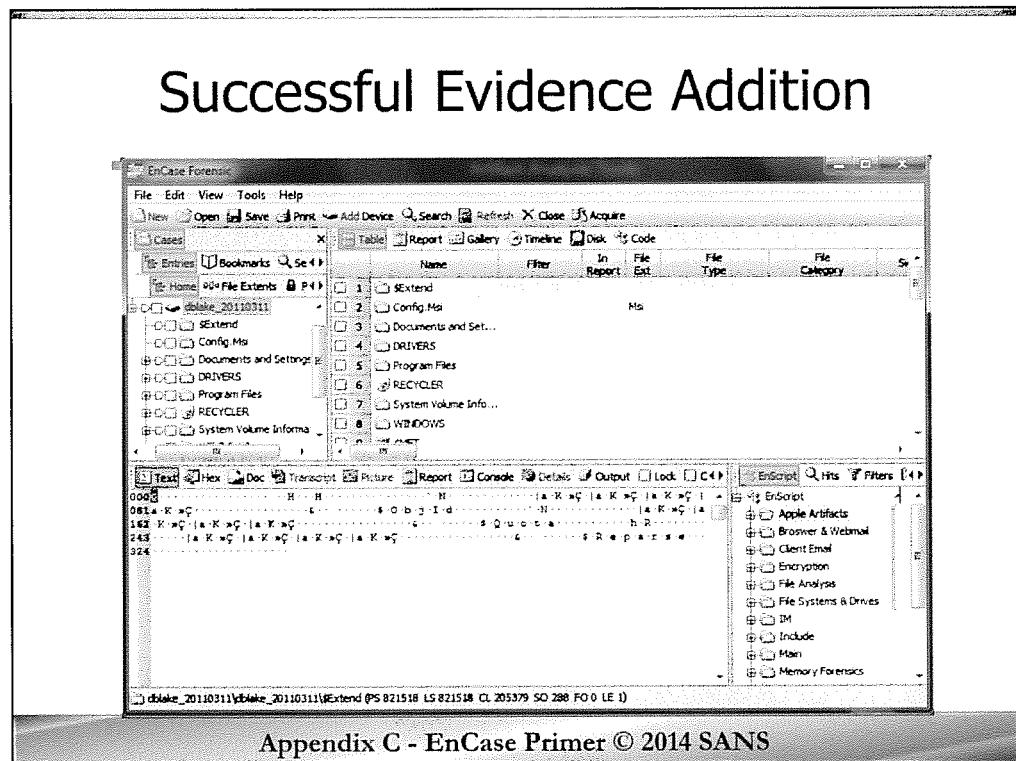
Appendix C - EnCase Primer © 2014 SANS

Once you have created a case, the next action is to add your evidence file(s) to that case. Using the Donald Blake exercise as an example, we would want to add a raw image to our case, because that evidence file was created in raw (dd) format.

Select **File → Add Raw Image**. This option will not be available if you do not have a case open.

You have the option to provide a label and provide information about the image being added. The **Image Type** radio button is important to get correct. If you select the wrong image type, EnCase may not display the existing data correctly. As an example, if you select “Disk” for the Donald Blake image file (which is actually a Volume), EnCase only shows the raw, binary data within the image and does not parse the file system artifacts. If you make a mistake and do not see what you were expecting, it is easy to remove the evidence from the case and re-add it using the correct settings. If you know the Partition Type and Byte information you can add those, but in most cases EnCase can determine these automatically.

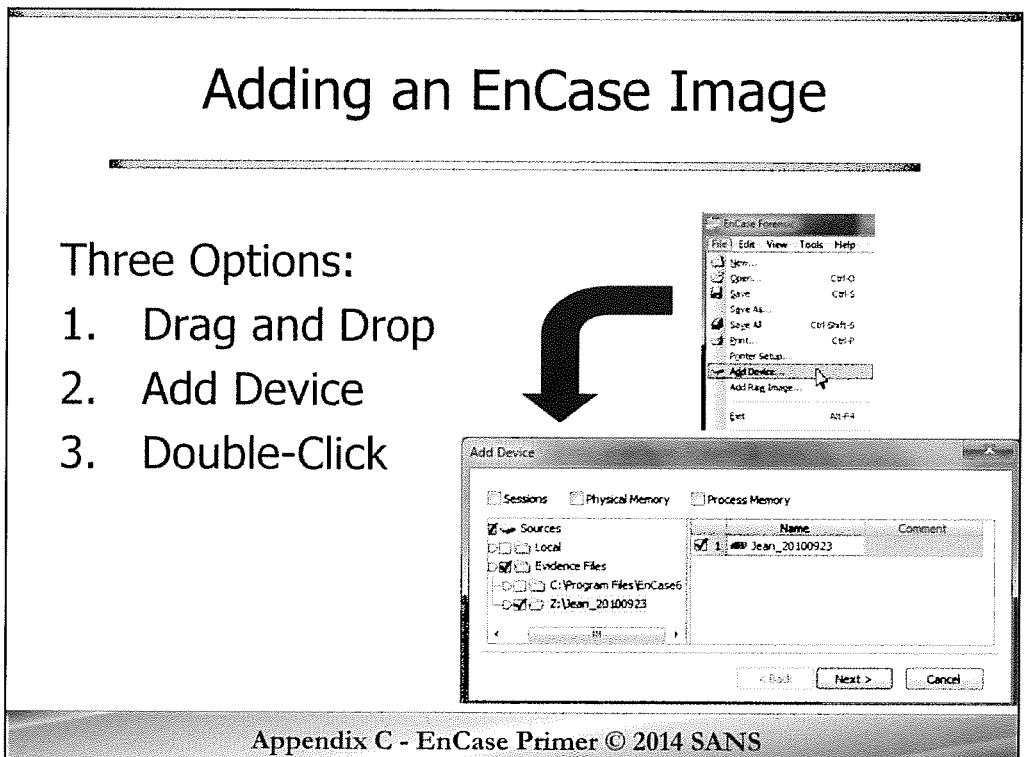
Once you have your settings in place, right click in the blank space and select **New**. This will allow you to browse to the location of your image file. Multiple images can be added using the same technique.



When you have successfully added an image file to your case, you should see the evidence listed within the **Cases | Entries | Home** tab within the Tree Pane (top left corner). In this example, we see a volume has been added named dblake_20110311 and has been expanded to view a NTFS file system. This is a good indication that the image was added successfully.

If a full disk image had been added, you would see a representation of the full disk along with any partitions and file systems that EnCase was able to identify and parse.

You are now ready to start your analysis!



If the evidence you are adding is stored in the Expert Witness Format (E01), you will use a different method to add it to your case. There are three methods for adding E01 files:

Drag and drop

- Drag the E01 file from Windows into EnCase

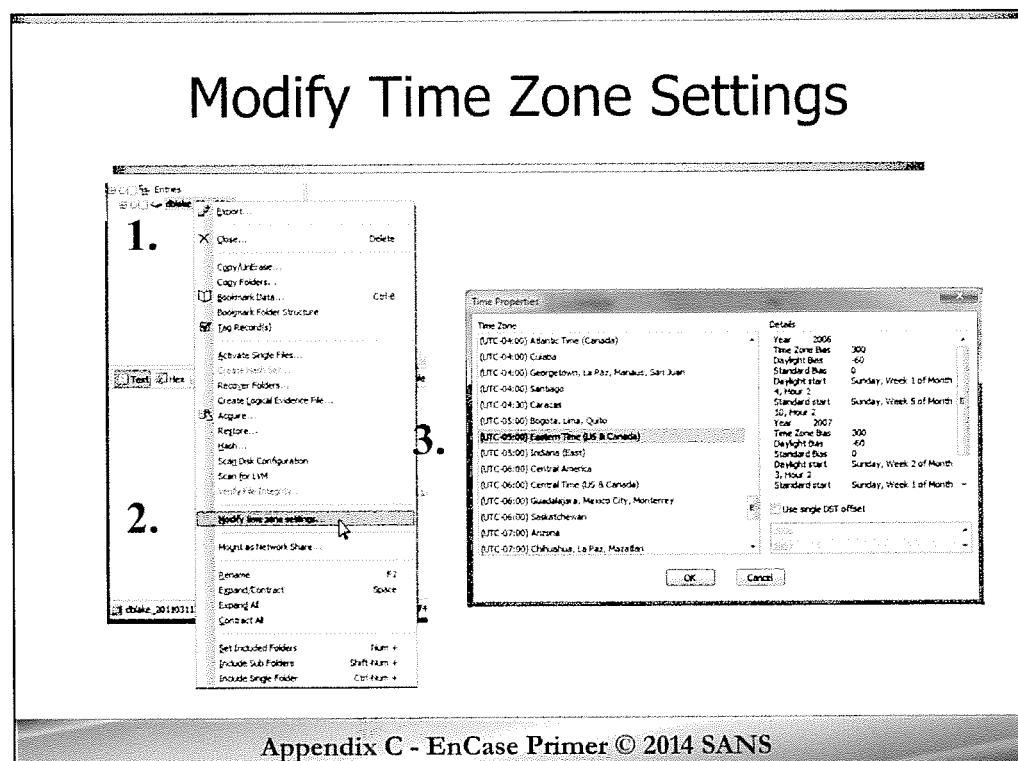
Double-click

- Double-click on the E01 file. A new instance of EnCase will be started, even if an existing process is currently running.

Add device

- **File → Add Device**
- Right Click on **Evidence Files**
- Select **New**
- Browse to folder holding E01 image(s)
- Ensure the evidence you wish to add is present and checked with a blue checkmark
- Click **Next**

Hash and CRC verification are automatically accomplished on any E01 images opened by EnCase. Keep in mind that this process can be lengthy on large image files.



Appendix C - EnCase Primer © 2014 SANS

Setting the proper time zone with EnCase is important to ensure forensic and network artifacts can be understood within the proper context. By default, all evidence is displayed using the examiner machine's time zone. Thus if you often work with UTC values, it is a good best practice to set your system time zone to UTC.

Alternatively, the time zone for a particular piece of evidence can be specifically set using the following process:

1. Right Click on the evidence
2. Select **Modify time zone settings**
3. Select the time zone that the evidence used (this information can be determined from the Registry on Windows systems) or via the Initialize module run from the Case Processor EnScript

The “Use single DST offset” is available for rare occasions when the default Daylight Savings Time system is not appropriate for a piece of evidence. A good example comes from the United States, which changed the dates of DST in 2007. Thus it is possible that an unpatched system could still be using the pre-2007 DST dates (perhaps it had not been connected to a network for updates). This option allows you to override the default settings to adjust for this situation.

Alternatively, the time zone can be set for the entire Case File, superseding any individual time zone information set. This is done by selecting **Cases | Home** within the Tree Pane, right clicking on the case and selecting **Modify time settings**.

EnCase Overview



Creating a New Case



Using EnCase



EnCase Engine



Forensic Techniques



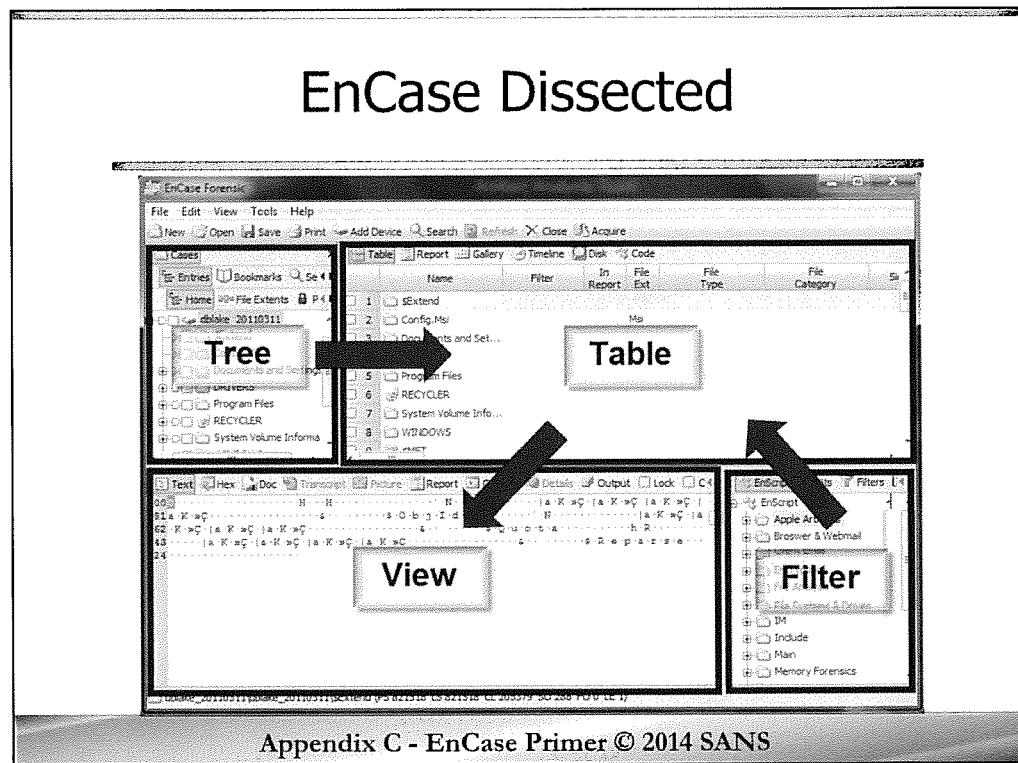
Application Parsing



Bookmarks and Reporting

Appendix C - EnCase Primer © 2014 SANS

This page intentionally left blank.



The EnCase suite can be broken into four primary areas:

Tree Pane

- Displays evidence contents using a hierarchical tree similar to Windows Explorer

Table Pane

- Shows identified evidence from the Tree Pane in a tabular form. Additional tabs provide different viewing options.

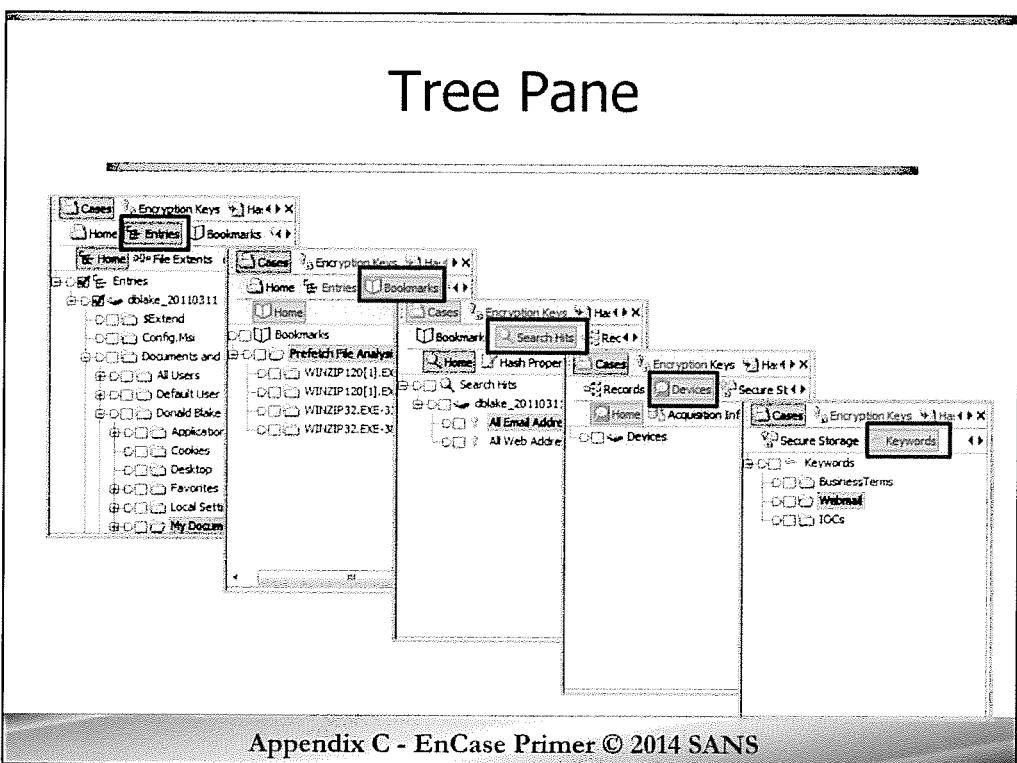
View Pane

- Displays marked items from the Table Pane in a variety of views

Filter Pane

- -EnScripts, filters, and queries used to filter results and perform analysis

Tree Pane

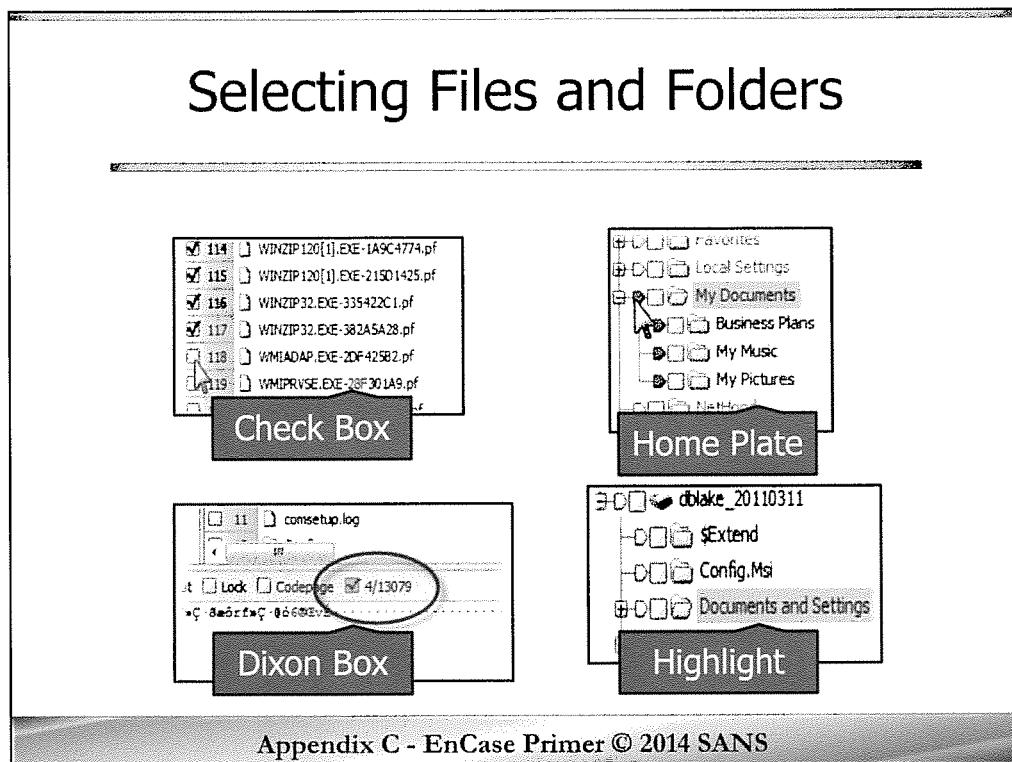


Appendix C - EnCase Primer © 2014 SANS

The Tree Pane allows interaction with a diverse number of case elements using a hierarchical tree structure. Descriptions of the most used configurations follow.

- In its most common configuration, the Tree view displays evidence contents similar to Windows Explorer. This is accomplished using **Cases | Entries**.
- Selecting **Cases | Bookmarks** displays all saved bookmarks
- **Cases | Search Hits** displays case-specific keyword search results
- The current physical devices associated with the case are shown in **Cases | Devices**
- All keywords are displayed in **Cases | Keywords**
- **Cases | Records** (not shown in this slide) holds results from a variety of actions such as e-mail archive parsing, webmail searches, and Internet address searches

Selecting Files and Folders



Selecting objects is a critical skill when using EnCase. Selected objects can be displayed or have actions performed on them, such as reporting, filtering, and hashing. Since evidence files often contain thousands of files, EnCase employs several methods for identifying which files the examiner wishes to act upon.

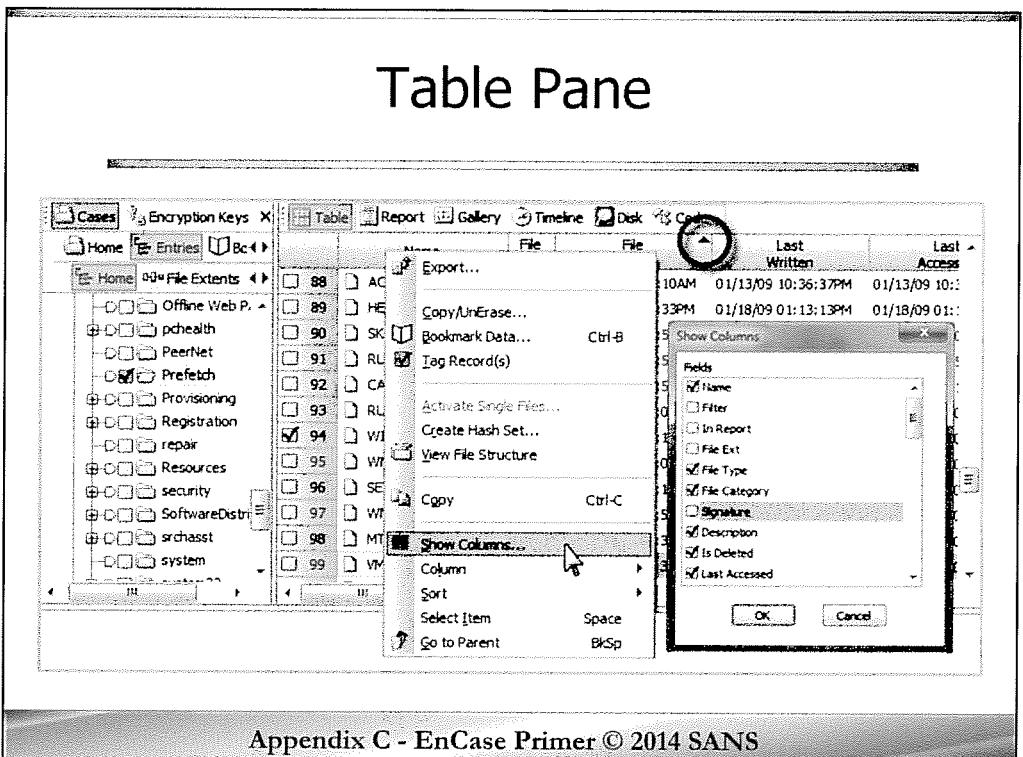
A Check Box *marks* a file for some later action. In the Tree Pane, a checked folder will select the folder contents and all of the contents of its subfolders. In the Table Pane, only the item checked will be selected.

The Dixon box displays the number of marked items out of the total number of items. You can mark or unmark all items in the case by clicking this control.

Highlighting *displays* the file or folder within the Table Pane, but does not include contents of subfolders (it displays only one level). Highlights are not persistent, meaning the selections are replaced with whatever is highlighted subsequently. Only one item can be highlighted at a time.

Home Plate, or Set Include, *displays* the contents of a folder and all of the contents of its subfolders within the Table Pane. Multiple sets can be chosen by holding down the control key while clicking the Home Plate icon.

A key distinction between the various options is whether the items are marked or just displayed. The former allows actions such as EnScripts to be performed on the marked files. The latter is used to identify which items should be displayed in the Table or View Pane.



Appendix C - EnCase Primer © 2014 SANS

The Table Pane shows highlighted items from the Tree Pane in a tabular form. It is most commonly used to display metadata associated with the currently highlighted or Set-Included (Home Plate) files.

By default, the Table Pane includes every possible column for displaying information. It is often worthwhile for the examiner to configure the columns and reduce their number to suit their analysis style. Columns can be hidden or shown using the **Show Columns** feature. Right click on the Table Pane and select **Show Columns**. The resulting dialog box allows viewable columns to be selected. Alternatively, columns can be hidden by selecting them and using Ctrl-H.

Columns can be moved by dragging their header fields to the desired location.

EnCase includes a powerful sorting capability. Simply double click a column heading to sort by that column. A small red triangle will be displayed in the sorted column. Double-click the column again to reverse the sort. A second sort can be accomplished by pressing Ctrl-Shift and selecting the second column header to sort by. Up to five complementary sorts can be done in this manner.

In this example, the \Windows\Prefetch folder has been highlighted and marked (blue-checked) in the Tree Pane, showing all files within that folder in the Table Pane. Further, the Show Columns action has been selected, allowing the visible columns to be chosen.

Table - Report View

The screenshot shows the EnCase Table pane with a report titled "Prefetch" for a file named "dblake_20110311WINDOWS!Prefetch". The report displays various metadata fields:

Name	DEFFRAG EXE-273F131E.pf
In Report	.
File Ext	.pf
Description	File, Archive, Not Indexed
Last Accessed	01/18/09 11 17 54PM
File Created	06/30/07 07 20 27PM
Last Written	01/18/09 11 17 54PM
Entry Modified	01/18/09 11 17 54PM
Logical Size	19,912
Initialized Size	19,912
Physical Size	20,480
Starting Extent	0dblake_20110311-C49514
File Extents	1
Permissions	.
References	0
Physical Location	101,404,672

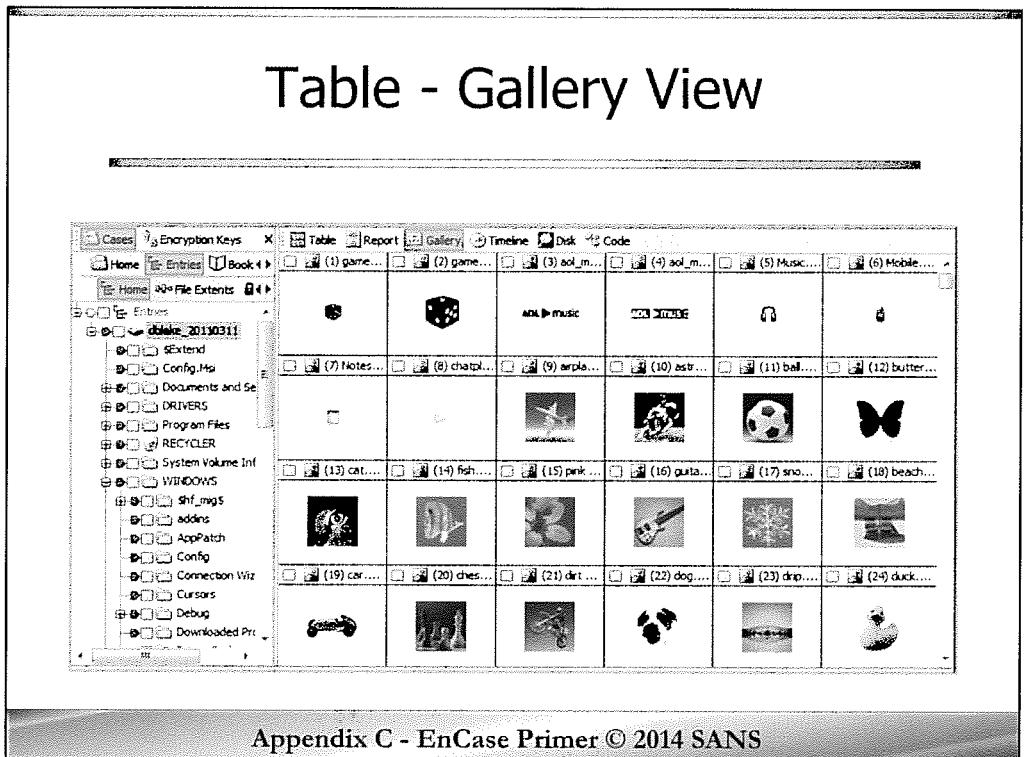
Appendix C - EnCase Primer © 2014 SANS

The Report View within the Table Pane can generate a text –based report for the highlighted or Set-Included (Home Plate) items. Items will not be included in the report unless they have been marked as **In Report**. To accomplish this, right click inside of the In Report column on the Table View and select **In Report**. Multiple items can be selected at once using the **In Report – Invert Selected Items action**.

Report View is used extensively to review bookmarks, including those created by running EnScript parsing modules. The final EnCase report will be shown and exported from this tab.

To export a report, Right Click on the report and click **Export**.

This example shows a report generated on a Prefetch file generated by the Defrag process. It is important to note that only the file system metadata will be displayed in the report. To parse the contents of the .pf file and identify the last time and number of times run, an EnScript would be required.



Appendix C - EnCase Primer © 2014 SANS

The Gallery tab provides an easy way to view selected images as thumbnails. Images are frequently relevant to forensic examinations and investigators may need to review tens of thousands of them. This view speeds that process, allowing examiners to focus only on images likely to be relevant to their investigation.

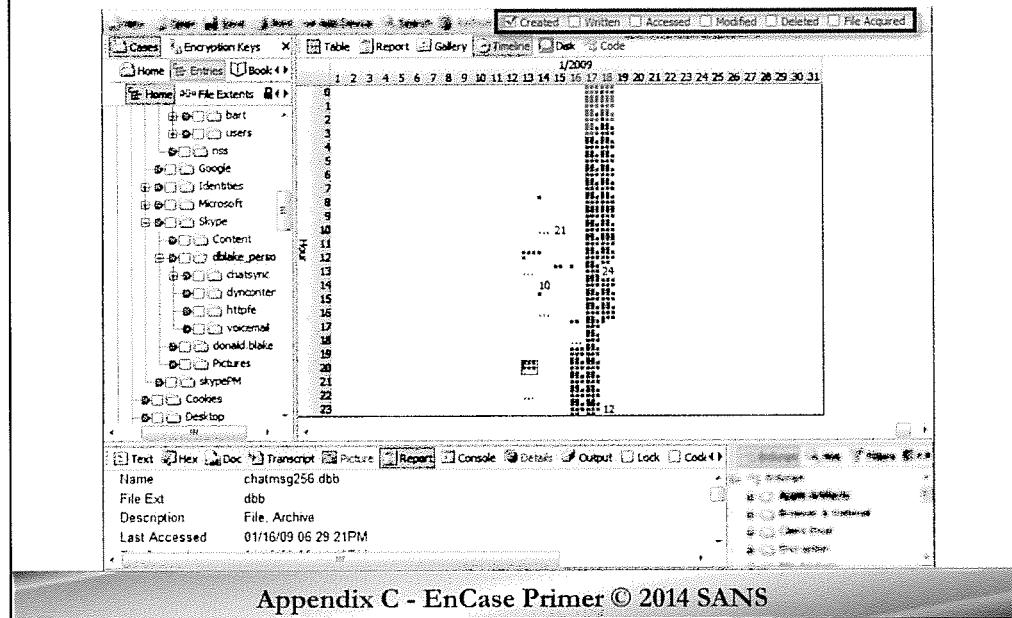
Remember that the Table Pane will only display files that have been highlighted or Set-Included in the Tree Pane. Thus to view all images from a piece of evidence, select the evidence item's Home Plate and then select the Gallery tab.

Thumbnail size can be controlled by selecting the number of columns and rows to display. This is accomplished by performing a right-click on the gallery and selecting either **More/Fewer Columns** or **More/Fewer Rows**.

Similar to the Table View, items of interest can be marked by checking the associated box.

It is important to note, that EnCase will only display images with well-known extensions (.jpg, .png, .gif, etc.) by default. To show all possible images in the evidence file, the File Signature Analysis tool must be run.

Table – Timeline View



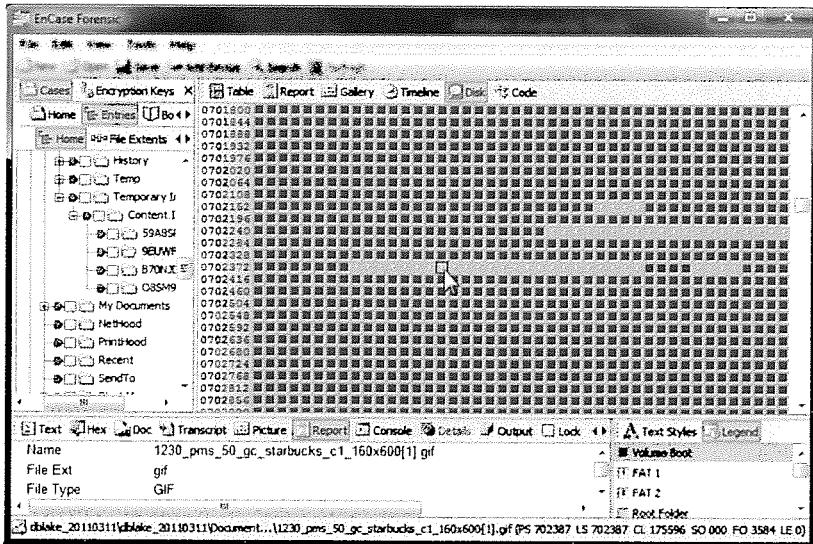
The EnCase Timeline View gives a quick means to visualize file system patterns based on timestamp information. The following timestamps can be plotted:

- Created
- Written (Data layer modified)
- Accessed
- Modified (Meta-data layer updated)
- Deleted (from Recycle Bin metadata in Windows)
- File Acquired (timestamp when evidence was imaged)

Timestamps will only be displayed for files that have been highlighted or Set-Included in the Tree Pane. Every dot on the timeline grid represents a file. A number represents a large number of file timestamps present during that interval. Clicking on a dot will display that file in the View Pane. Dots are arranged according to date (X-axis) and time (Y-axis). The date / time scale can be changed by zooming in and out on the grid (Double-click to zoom in, right-click and select **Lower-Resolution** to zoom out). Timestamps are color coded and the color key can be viewed and modified by right-clicking on the timeline and selecting **Options**.

This slide shows the analysis of a block of files created between 8 and 9 PM on 1/13/2009. One of the files created during that time is the chatmsg256.dbb database (described in the View Pane) located in a Skype profile folder (see Tree Pane). Depending on the circumstances of the case, this might indicate Skype usage at an anomalous time.

Table – Disk View



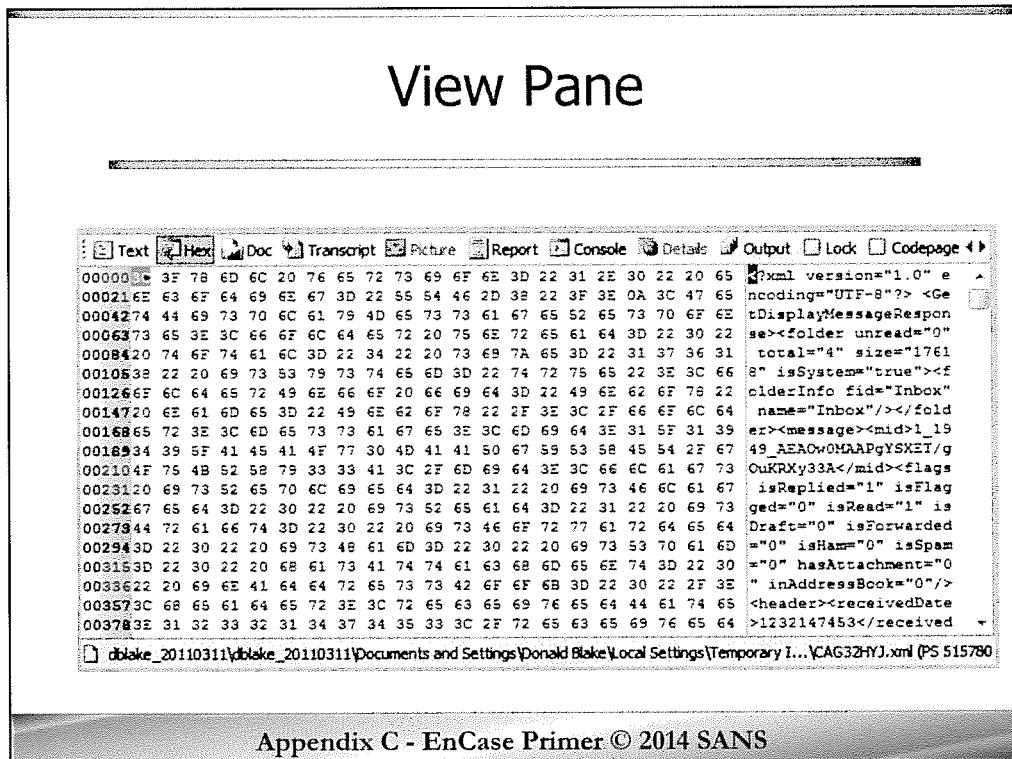
Appendix C - EnCase Primer © 2014 SANS

Disk View provides a novel means to view the status of sectors and clusters within an evidence file or target media. By default, each square represents a sector (512 bytes) of the evidence. This can be switched to represent clusters by right-clicking and selecting **View Clusters**.

Allocated sectors and clusters are represented as blue squares. Unallocated areas are shown in gray. In this example we also see four bad blocks represented with a circle-backslash, or “no” symbol. The legend for colors represented within Disk View is located on the lower right of the example, within the Filter Pane.

Each cluster (or sector) can be individually selected. The View Pane attempts to display the contents of that cluster. If metadata exists for the file that owns that cluster, the Tree Pane will show the folder it exists in. This information may even be available for items located in unallocated clusters.

If you are viewing a physical disk image, this view will also allow you to add and delete partitions. This functionality is typically only used in advanced circumstances when the partition table has been damaged or overwritten.

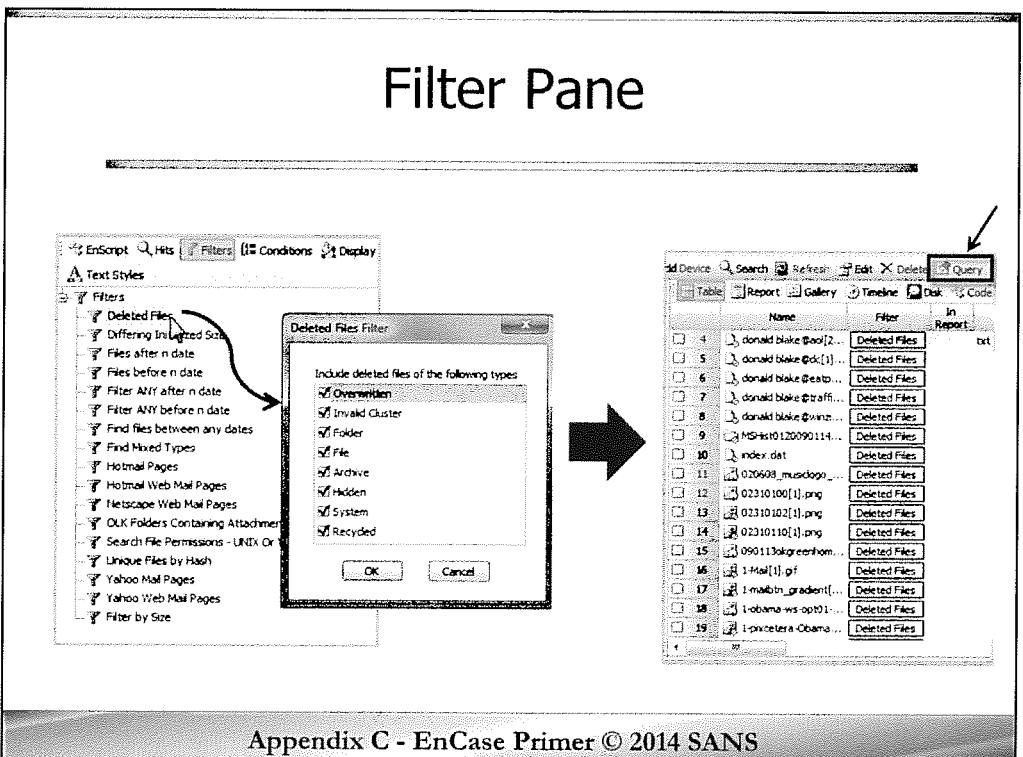


Appendix C - EnCase Primer © 2014 SANS

The View Pane displays information about the item currently highlighted in the Table Pane. The View Pane will attempt to display the item in its native form based on its file type. Alternatively, specific tabs can be selected by the examiner. The following views are possible:

- Text – Shows the item as ASCII or Unicode text, depending on the Text Style selected in the Filter Pane
- Hex – Standard hex editor view of hexadecimal values with ASCII representations (shown in this slide)
- Doc – Utilizes Outside In viewers to display the item in the native form of its application
- Transcript – Extracts text from a file containing more than text (uses same process to extract text as indexing engine)
- Picture – Default display for items identified as image files
- Report – Creates a comprehensive report of the item attributes
- Console – Used to display output messages from running EnScripts
- Details – Displays item information including location of file (sector, byte offset, cluster) and items like permissions and hash properties
- Output – The output of some EnScript programs will display in this tab (other utilize bookmarks for their output)

Tabs are disabled when they are not applicable to the item being displayed. Search results will be highlighted within the pane when they exist. The “Lock” checkbox will force an item to be displayed within a specific view.



The Filter Pane contains a wealth of functions to assist with forensic analysis. Most of the items within this pane are used to attain additional information (such as application specific metadata) or to filter the results within the Table pane according to some criteria. In the example presented here, the Deleted Files filter was invoked, limiting the view of the Table Pane (shown on the right of the slide) to only deleted items (seen in the Filter column). To turn off the filter, the examiner would click on the “+ Query” button identified on the top right of the image.

The filter pane contains several tabs:

- EnScripts – Provides list of available EnScripts and serves as their launching point
- Hits – Alternate location to view search hits for a file
- Filters – A collection of specialized EnScripts used to refine what is displayed in the Table Pane
- Conditions – Wizard-like interface for creating custom filters without need of EnScript coding expertise
- Queries – A query is a combination of two or more filters or conditions using Boolean operators
- Display – Identifies the currently active filters, conditions, and queries

EnCase Status Bar

□ dblake_20110311\blake_20110311\AUTOEXEC.BAT (PS 836344 LS 836344 CL 209086 SO 296 FO 0 LE 1)

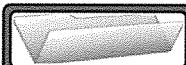
Navigation Fields	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td></td><td>File Type Icon</td></tr> <tr><td></td><td>Full Path of File</td></tr> <tr><td>PS</td><td>Physical Sector Location</td></tr> <tr><td>LS</td><td>Logical Sector Location (within volume)</td></tr> <tr><td>CL</td><td>Cluster Address</td></tr> <tr><td>SO</td><td>Offset within Sector</td></tr> <tr><td>FO</td><td>Offset within File</td></tr> <tr><td>LE</td><td>Length of Bytes Selected</td></tr> </table>		File Type Icon		Full Path of File	PS	Physical Sector Location	LS	Logical Sector Location (within volume)	CL	Cluster Address	SO	Offset within Sector	FO	Offset within File	LE	Length of Bytes Selected
	File Type Icon																
	Full Path of File																
PS	Physical Sector Location																
LS	Logical Sector Location (within volume)																
CL	Cluster Address																
SO	Offset within Sector																
FO	Offset within File																
LE	Length of Bytes Selected																

Appendix C - EnCase Primer © 2014 SANS

In a case with multiple pieces of evidence and hundreds of thousands of files, it is easy to forget what you are looking at and where it is from. At the bottom of the EnCase application is the navigation information for where you are currently looking within your evidence files. This can be used as a quick reminder of the full path of a file you are analyzing, or as specific data on where that file exists at the data layer. The data can be parsed as follows:

- File Type Icon
- Full Path of File
- PS – Physical sector location of file
- LS – Logical sector location of file (within the current volume)
- CL – Cluster address
- SO – Offset within current sector
- FO – Offset within file (most useful when viewing a search hit or a portion of a file that has been highlighted in the View Pane)
- LE – Length of bytes currently highlighted

EnCase Overview



Creating a New Case



Using EnCase



EnScript Engine



Forensic Techniques



Application Parsing



Bookmarks and Reporting

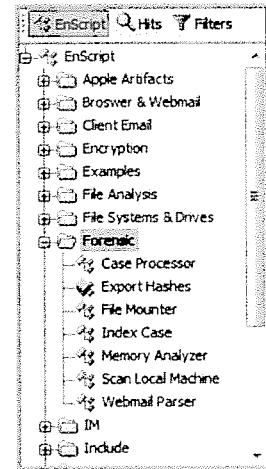
Appendix C - EnCase Primer © 2014 SANS

This page intentionally left blank.

What is an EnScript?

- Small programs used to automate forensic tasks
- Programming language and API
 - Object-oriented similar to C++
- Can be written by anyone

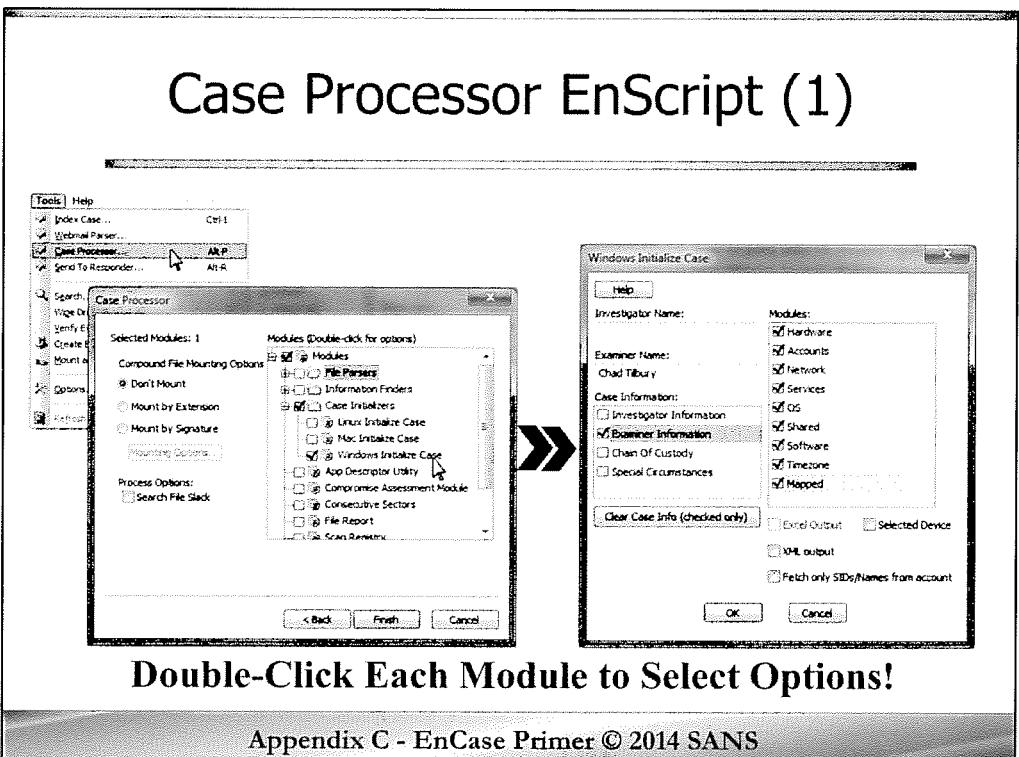
Disclaimer: The Win7 SIFT VM provides a large collection of third-party EnScripts to illustrate the full capabilities of the product. You MUST do your own testing and validation on anything you plan to use in a real case!



Appendix C - EnCase Primer © 2014 SANS

EnScripts have become a very important part of EnCase. You can think of EnScripts as small pieces of code that are used to accomplish forensic tasks. Through the years, the features of EnCase have been extended through a variety of different EnScripts. As an example, some of the menu items you select from the Tools menu are actually just links to specific EnScripts. In addition to providing a large selection of EnScripts, Guidance Software also made the decision to open up the interface to allow third-parties to create their own. This has led to many more EnScripts being written than Guidance alone could have supported. Like any software, there are good and bad EnScripts and thus caution should be exercised when employing a new script. Artifact features and locations change frequently and even good EnScripts eventually become obsolete. One advantage is that most EnScripts are written in plaintext and can be easily reviewed (the new EnPack format is the exception). We recommend personally testing and validating the results from EnScripts before using them on a real examination. The Win7 SIFT VM is perfect for this! Keep in mind that you may be called on to testify to the results that you gathered from your forensic tool, and you will be thankful for the testing and documentation you accomplished beforehand.

You will find the currently available EnScripts in the Filter Pane of EnCase, under the EnScripts tab. There you should find a folder structure organizing the various scripts. To run an EnScript, you simply double-click on it. EnScripts that require user input or preferences will then display a dialog box, otherwise they will run silently in the background. Output varies greatly with EnScripts, but most results can be found either in the Console (View Pane), Bookmarks (Tree Pane), or under the Records tab (Tree Pane).



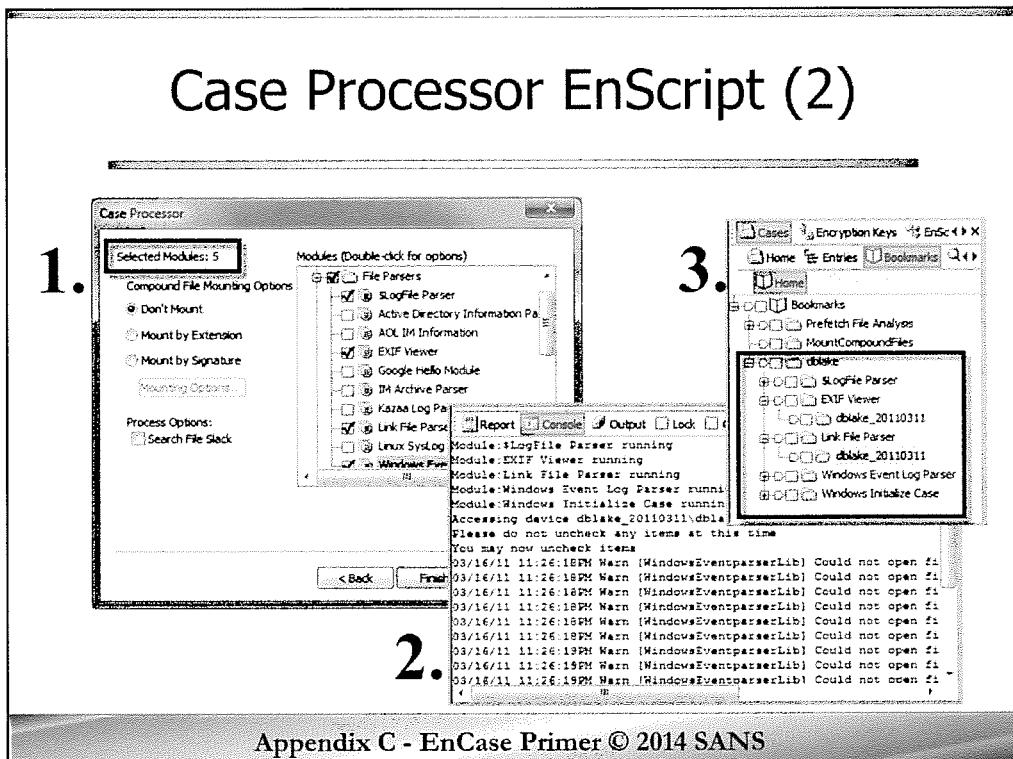
The Case Processor EnScript is a collection of the most frequently run scripts. It is usually one of the first things EnCase examiners run after adding (and verifying) their evidence. It has a large number of very powerful modules. In fact, a large amount of the forensic capability of EnCase is buried in this script. If you ever find yourself trying to remember how to perform a given forensic technique in EnCase, make sure to include the Case Processor in your list of areas to look!

Case Processor can be opened via the Filter Pane, or using the **Tools → Case Processor** menu item (shown here). A dialog will open and prompt for a Bookmark Folder Name (all results will be placed here), an optional Folder Comment, and the Export Path (the default is pre-populated). After clicking next, you will be shown the primary module menu. Mounting of compound files can be accomplished (see upcoming slide covering this topic), and a list of modules is available on the right. Each module selected MUST be double-clicked to select the relevant options. EnCase will usually remember module options you have set previously, so pay attention to what is already selected. Most modules also include a help button describing the tool, options, and limitations.

The Initialize Case modules (the Windows module is shown here) are an excellent way to collect information like OS, time zone, and user accounts that can be helpful at the beginning of an examination.

Don't feel like you only have one shot to select whatever processing you need for the case. The Case Processor can be run as many times as you like, just make sure to choose a new Bookmark Folder Name each time so you do not overwrite previous results. Examiners will often run the Windows Case Initialization first, and then return to the EnScript later in the investigation to parse items like EXIF, Link Files, and Event Logs.

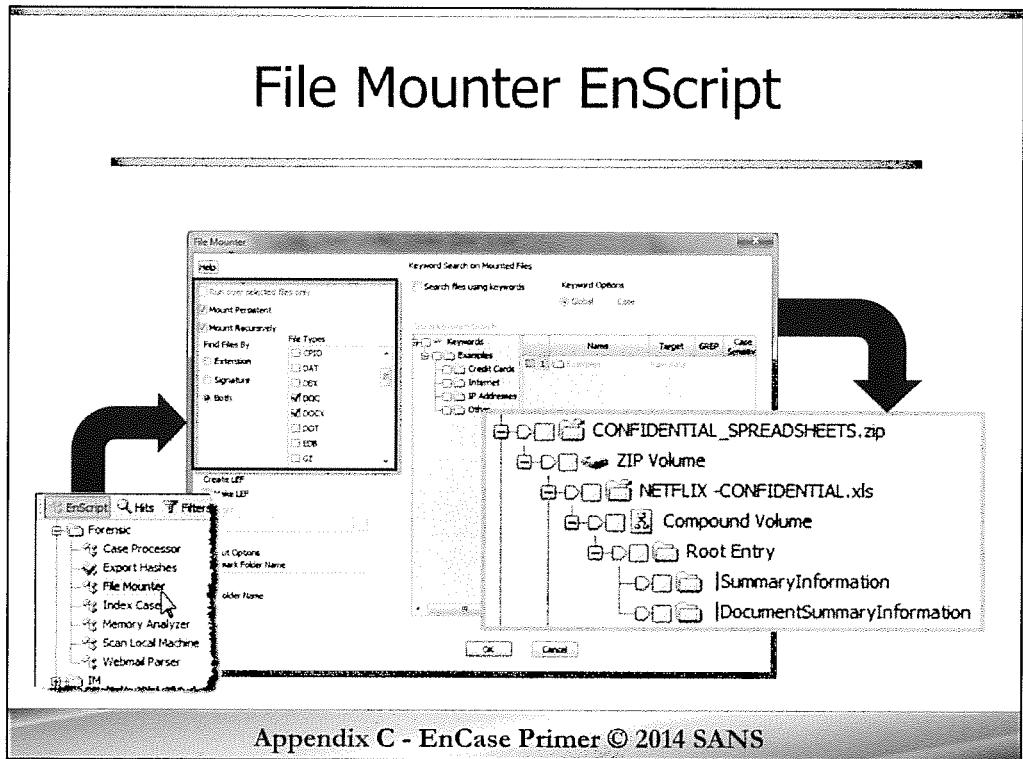
Case Processor EnScript (2)



After you have selected the modules you wish Case Processor to run (and double-clicked on each to set individual preferences), check the Selected Modules display in the upper-left of the dialog (see image 1 in slide). This allows you to easily identify how many modules you will be running. Some modules take a large amount of time (File Finder is a good example) and hence you may want to only run those overnight or during spare cycles.

Image 2 shows the Console output (View Pane) for the running EnScript. This is a great place to track what module is currently running and how many are left to be completed.

Finally, in image 3, we show the output location of the completed modules. These can be found in the Tree Pane under the **Cases | Bookmarks** tab. Each module will have its own folder structure organizing its results.



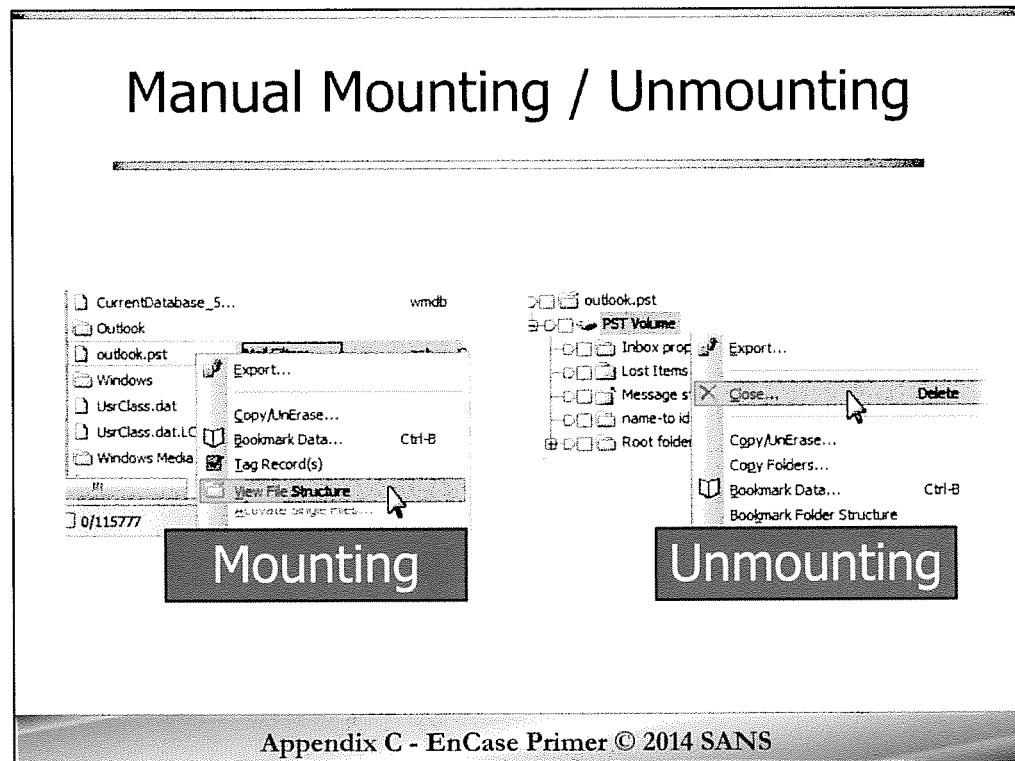
Many file types an examiner may encounter are compound files. The most well-known of these are compressed, or zipped, archives. There are a multitude of other compound files including Microsoft Office files (both the old OLE and the new XML based formats), E-mail archives, and system files like Windows Registry files and Thumbs.db. In order to view or search the contents of these files, they must first be “mounted” within EnCase. An EnScript has been created for this purpose.

In the Filter Pane, find the **File Mounter EnScript** under the Forensic folder. Double-clicking on the file will bring up the File Mounter dialog. This dialog facilitates the mounting of all compound file types that EnCase understands. Several useful features are included:

- Mount Persistent – Keeps files mounted even after EnScript is closed (use cautiously since large numbers of mounted files can sap available system memory)
- Mount Recursively – Mounts multiple levels of compound files. This slide shows an example of this with a Zip archive and its embedded XLS file both being mounted
- Create LEF – Creates a Logical Evidence File containing all selected compound file types
- Search files using keywords – Provides an easy way to mount and search compound files in one step. Files with keyword hits will be kept persistently mounted and all others will be unmounted (unless the persistent option is checked)

Working with compound files is a critical forensics skill. As an example, web content is being increasingly transferred in compressed format, leaving compressed archives within the browser cache. If those files are not mounted before string searches are run, valuable evidence may be missed.

Compound file mounting can also be accomplished via the Case Processor EnScript.



Appendix C - EnCase Primer © 2014 SANS

Compound files can also be mounted manually using the EnCase GUI. This is most commonly done when a file of interest is found while reviewing files in a particular folder. If you only need to review a few files, it is faster (and less memory intensive) to mount manually versus using the File Mounter EnScript.

To mount a file, highlight the file within the Table Pane and right-click. Select **View Folder Structure** to mount the file. If you do not see the **View Folder Structure** menu option, ensure that you have highlighted the correct file and that EnCase understands that type of compound file.

It is a good habit to unmount files when you are finished reviewing (or searching) them. This saves memory resources, particularly for very large files like Registry hives or e-mail archives. You will need to use the Tree Pane to unmount a file. Scroll the file location and look for the EnCase icon representing a mounted file (one example is shown in slide above). Right-click on the mounted file icon and select **Close**. You may be given a warning about removing the file from the case. This error is a little confusing and is telling you that the elements of the compound file will not be visible within the case (because the file will no longer be mounted).

EnCase Overview



Creating a New Case



Using EnCase



EnScript Engine



Forensic Techniques



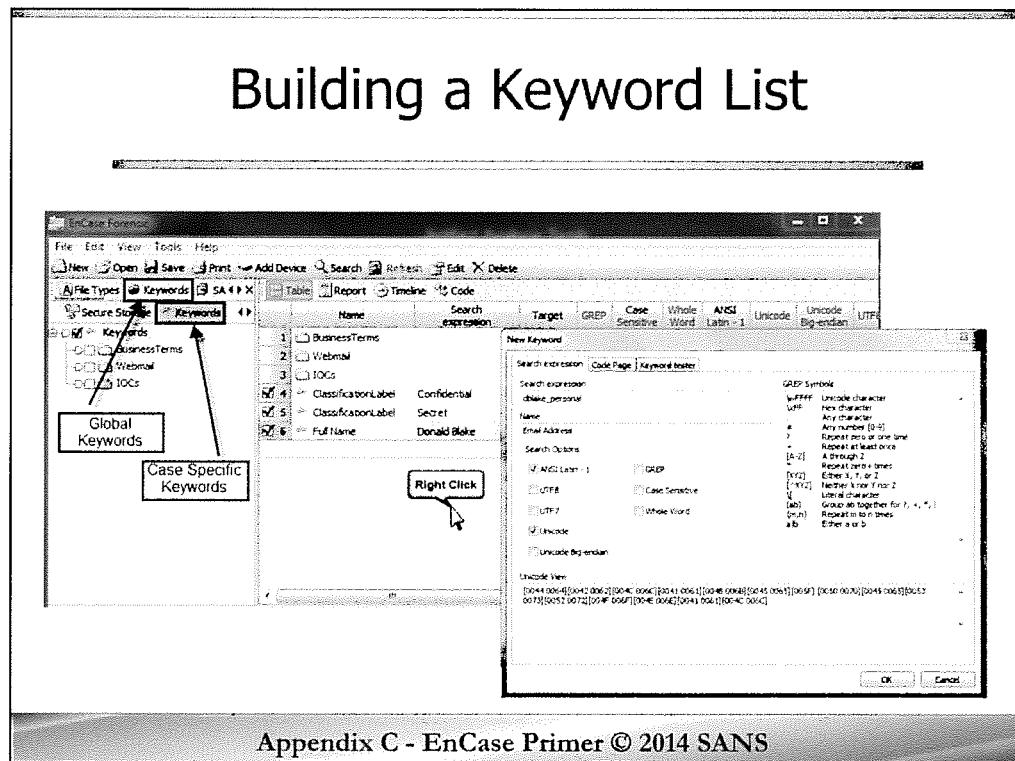
Application Parsing



Bookmarks and Reporting

Appendix C - EnCase Primer © 2014 SANS

This page intentionally left blank.

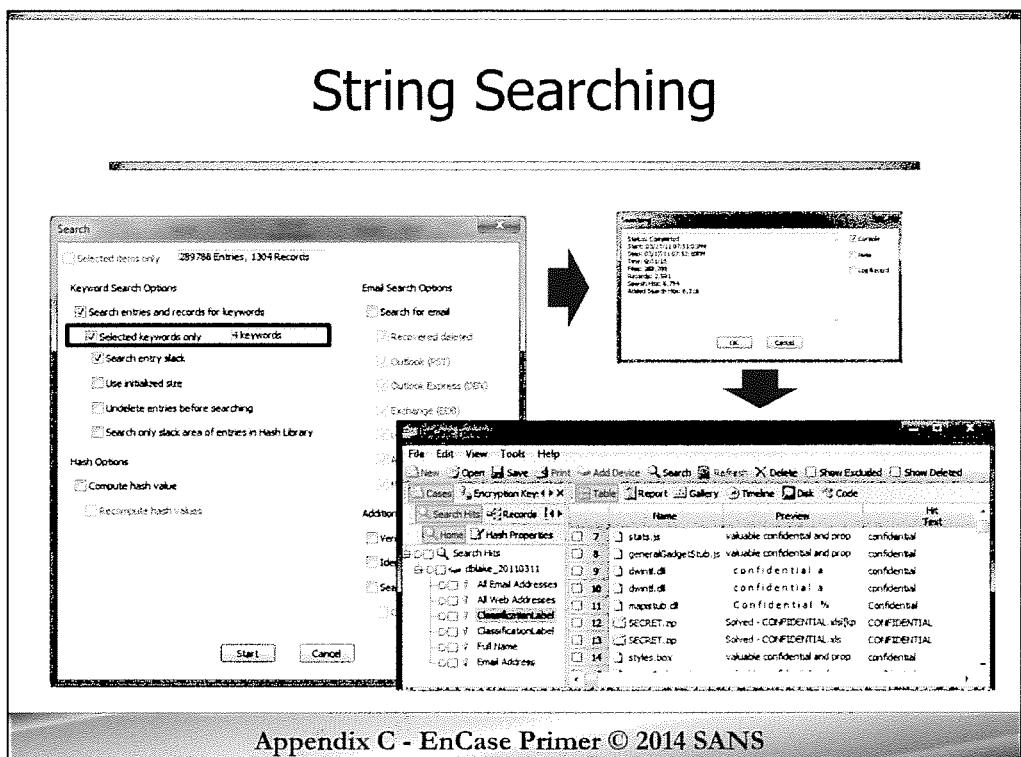


Appendix C - EnCase Primer © 2014 SANS

EnCase ships with a robust keyword search capability. There are two locations to store and view keywords. Global keywords exist as a tab on the top tier of the Tree Pane. Looking carefully, you should see an icon of a globe and a key. As their name implies, these keywords are available globally for all cases examined using the software. Several built-in keywords exist here, including regular expressions for web and Internet addresses, IP addresses, and credit cards. If you use the menu option **Tools → Keywords**, it will take you to the global keyword list. Keywords created here are saved to the EnCase settings files.

Many keywords are only relevant to a given case and would not be particularly useful to have available for other investigations. The case specific keyword list was built for this purpose. Any keywords created here are only available to the current open case. This list is saved in the case file.

To add to the keyword lists, simply right-click in the **Keywords | Table** view and select **New**. This will open up the New Keyword dialog box. Similarly, the **Edit** command will open a dialog for an existing keyword. The string to search for is placed in the Search Expression field and the Name field is a descriptive name that will be displayed when a hit is found. Several search options are available including Unicode searching, GREP (regular expression) searching, and a toggle for case sensitivity. A handy regular expression reference is located on the right side of the dialog, and the Keyword Tester tab allows you to double-check those regular expressions before letting them loose. The Code Page tab allows searching in a vast number of different character sets such as the Arabic, Chinese, and Cyrillic alphabets. Clicking **OK** saves your new keyword in the list.



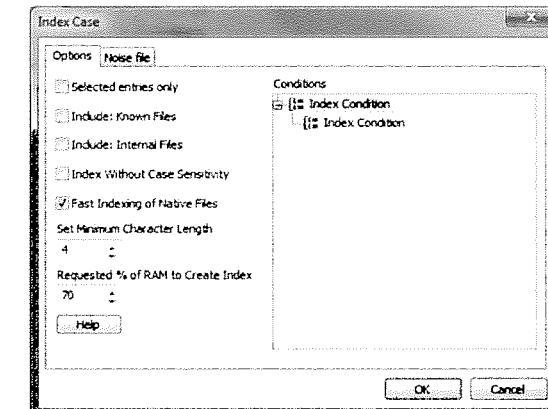
Appendix C - EnCase Primer © 2014 SANS

To search your evidence using your keyword list, use the **Tools → Search** application. On the left-hand side of the Search dialog you should see the Keyword Search Options. An important option to understand is the **Selected keywords only** option. By default, EnCase will search using every keyword in both the Global and Case keyword lists. This is rarely wanted, so by selecting this option you can limit your search to only those keywords you have previously check marked within the Keywords tab. Options are also available to search slack space and only use the initialized file size (some NTFS files only use a portion of their allocated space and this is called the initialized size). Finally, you have the option to undelete any unallocated files before searching to ensure hits are not missed due to fragmentation and an option to only search the slack space of files that were previously identified in your “known goods” hash list. Once your options are set, click **Start** and review your hits within the **Cases | Search Hits** tab (shown here).

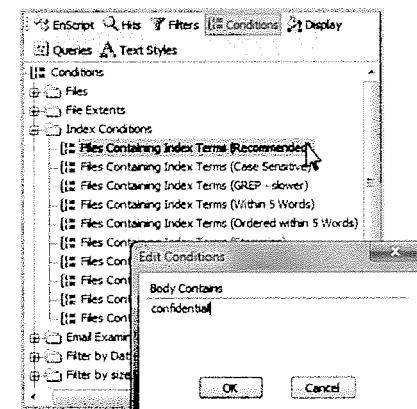
There are several other option categories within this dialog that pertain to completely different searches. Most of these will be covered in other slides.

Indexed Searching

Tools → Index Case



Searching the Index



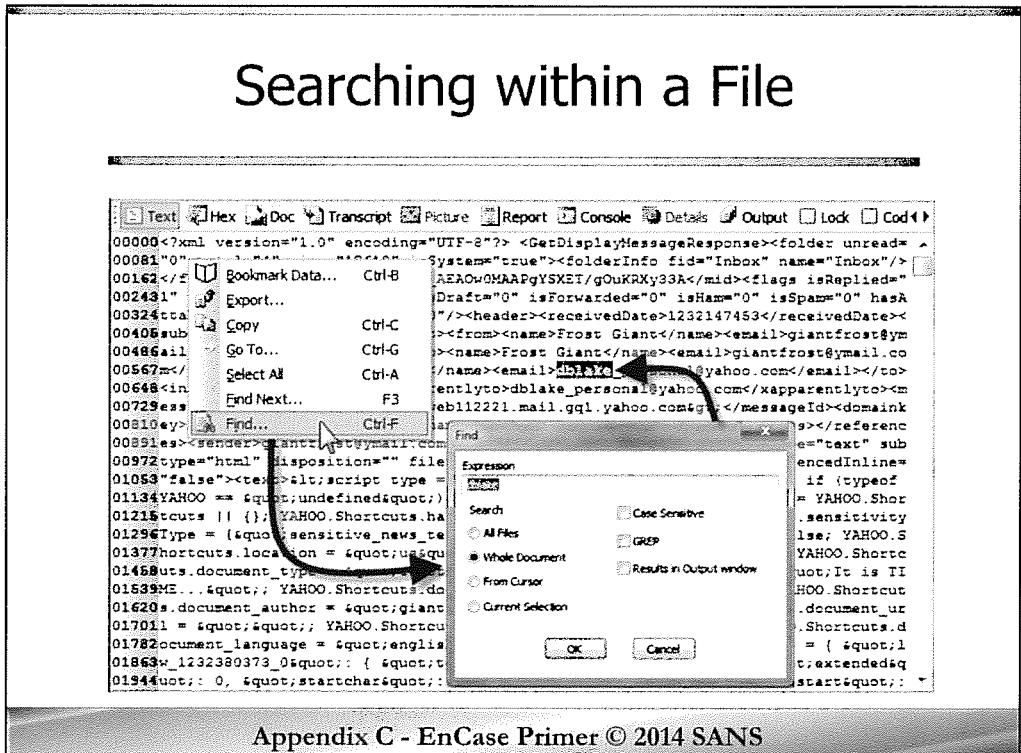
Appendix C - EnCase Primer © 2014 SANS

Indexed searching is a relatively new addition to EnCase. It is accessed via the menu item **Tools → Index Case**. Indexing gives examiners the choice to spend some processing time upfront to build an index of (nearly) all available strings within the evidence files and then reap the benefits with very fast searches. EnCase documentation warns that indexes may take a very long time to create, proportional to the size of your evidence files. Keep in mind that smaller indexes can be created by selecting the files of interest (with check boxes in Tree/Table Pane) and running the tool using the **Selected entries only** option. This might be useful if you are focusing your string searches on something like IIS logs. By default, known files from a hash analysis are excluded. The Fast Indexing option uses the built-in EnCase parsing functions when applicable as opposed to the beefier OutsideIn parsers.

Once started, the Indexing progress can be seen in the lower right corner of the EnCase GUI.

Searching using an index is accomplished through the use of filters. Within the Filter Pane and Conditions tab you will find a folder named, **Index Conditions**. These provide many customizable options for identifying and viewing files containing specific search terms.

Searching within a File

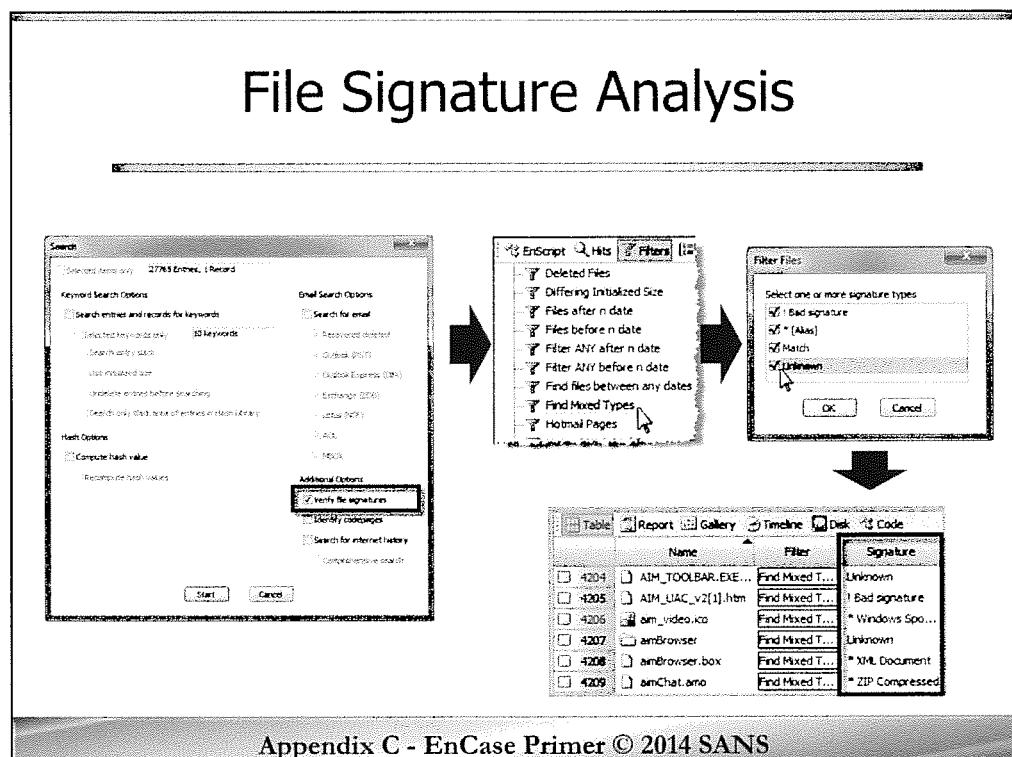


Appendix C - EnCase Primer © 2014 SANS

To search within a file, use the **Find** command. This is accessed from the View Pane, within the Text or Hex tab. Right-click in the View Pane and select **Find**. A dialog box will emerge and you can select a simple text pattern or a GREP style regular expression. Case sensitivity can also be toggled. The first available hit will be highlighted within the View Pane. To see additional hits, right-click and select **Find Next** (or press F3).

If you are looking for something at a particular offset, you can right-click and choose the **Go To** menu option. This is particularly helpful when using Hex view.

Arbitrary data can be highlighted and either **exported** as text or binary, **copied** to be pasted elsewhere, or **bookmarked** within the case file.



Appendix C - EnCase Primer © 2014 SANS

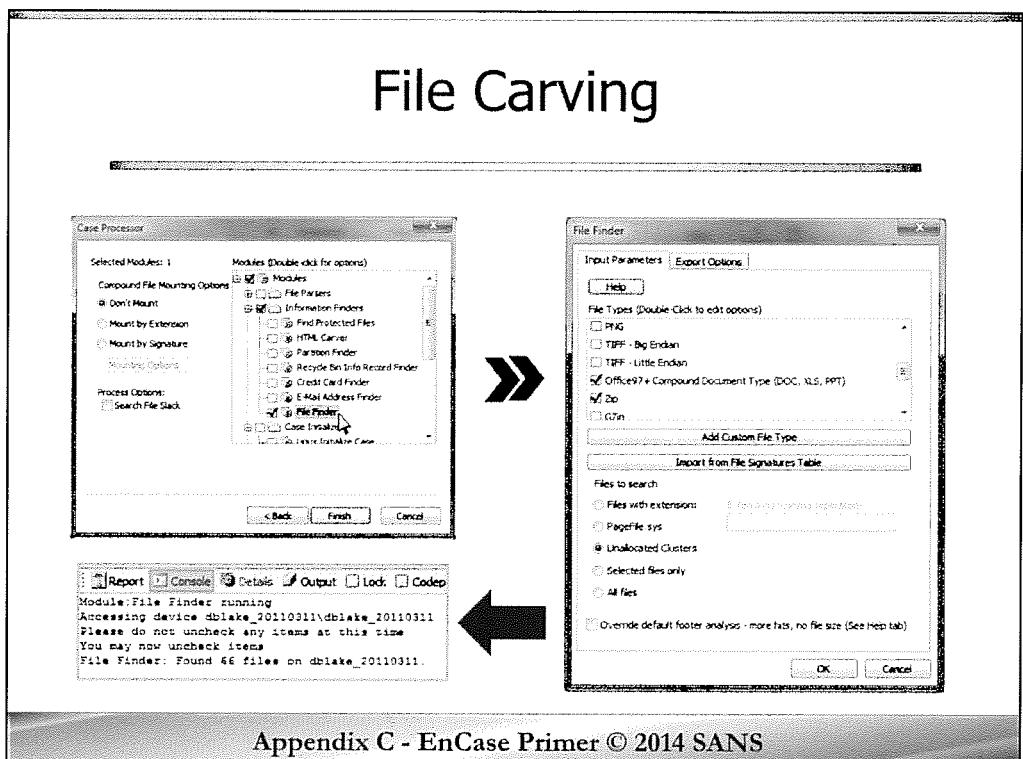
File signature analysis is a very important tool within EnCase. Nearly every file type has an associated header value. Many file types also have an associated footer value. Together these values can be used as a file signature. File signatures are not visible within the operating system (except perhaps by a hex editor) and are not affected by changing the file extension. EnCase has a built in database of known files signatures matched with their common file extensions. You can view and update this database using the command **View → File Signatures**.

When conducting a file signature analysis you are asking EnCase to extract the header, footer, and extension from every file and compare them to the File Signatures Database. The comparison will give one of four results:

- **!Bad signature** – The file signature is unknown and does not match what is expected for the given file extension.
- *<true file type> – The file signature is of type <true file type> and the file extension is missing or does not match. Reported as a signature mismatch in other forensic tools
- **Match** – The file signature and extension match a database record
- **Unknown** – The file signature AND file extension could not be found in the database

This slide shows the file signature analysis process. From the Tools menu, select **Tools → Search**. Check **Verify File Signatures** and click **Start**. To view the results, a filter can be employed, **Filters → Find Mixed Types**. This filter will provide a dialog to select one or all of the four comparison results. Finally, the Table Pane will be populated with the filtered results for easy review.

Performing a file signature analysis is often one of the first things you will want to do when starting a new examination. Many EnCase features can use this data once it has been added to the case. Some examples of this are smarter mounting of compound files to ensure proper searching and choosing the proper viewer for a previously unknown file type.



Appendix C - EnCase Primer © 2014 SANS

File carving is accomplished in EnCase via the **File Finder** module of the **Case Processor** EnScript. It is a little buried, but you can find it in the **Information Finders** folder. File carving utilizes known file signatures to identify files at the data layer. It is an extremely powerful forensic technique that can often resurrect long forgotten files from the depths of unallocated space. That being said, it is a dumb tool, assuming all files are contiguous. This can lead to many false positives depending on the uniqueness of the file signature used.

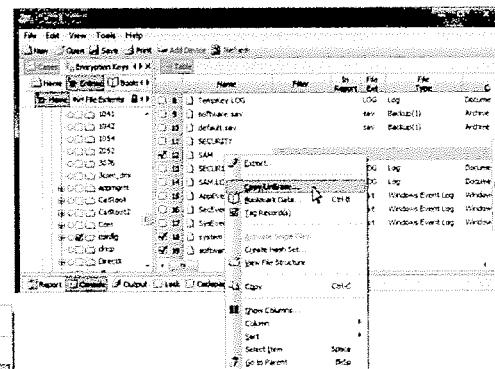
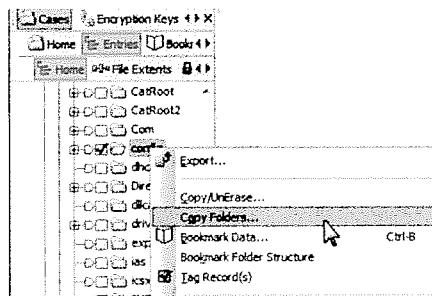
When File Finder is opened (by double-clicking the module within the Case Processor), it provides a default list of common files to search for. This is a very limited set and it is important to note that additional types can be imported from the EnCase File Signatures Database (see File Signature Analysis for a more in depth discussion of this database). Custom file signatures can also be searched for using the Add Custom File Type option, or by adding them to the File Signatures table. This gives the flexibility to search for nearly any type of file.

Once the file signatures to search for are selected you must then decide what files in your case to search. Several options are presented, but file carving is most often performed on Unallocated Clusters. The PageFile.sys option may also be interesting as it gives the opportunity to recover files that once existed in memory.

The tab Export Options allow recovered files to be automatically exported to a location of your choosing. Exporting your results can be a big timesaver, allowing you to quickly review the contents of your export folder instead of individually reviewing results within the EnCase Bookmarks tab. Additional parameters can be set to limit file sizes and the max number of files exported. These can be helpful considering the large number of files and false positives that file carving can create.

Exporting Data

Exporting a Folder



Exporting a File

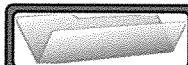
Appendix C - EnCase Primer © 2014 SANS

Every tool has its strengths and weaknesses and even a forensic suite as powerful as EnCase will often need to be supplemented by other tools. Thus it is important to understand how to export files out of EnCase. Once the files are exported in their native form, third-party tools such as Regripper or Event Log Explorer can be easily utilized.

There are a couple of gotchas when exporting files from EnCase. The first is that the **Export** menu option does not actually export files. Instead, it saves a text report of marked items from the Table Pane. To export the actual files, you will need to use the **Copy/UnErase** option. This option opens a dialog that steps the user through several steps, identifying which files to export (a single highlighted file or all marked), parts of the files to export (logical, physical, or slack), and where to save the files. As always, double-check the Dixon Box to make sure you have the correct number of files marked. It is easy to make a mistake and export thousands of unwanted files.

If you wish to export an entire folder (including subfolders), you will want to use the **Copy Folders** menu option. Using the **Copy/UnErase** option will copy just the folder file itself, which is rarely what is intended. **Copy Folders** provides a simpler dialog, confirming the folder and contents to copy as well as the export directory. In both cases, a status box is displayed, showing how many files and total bytes were exported.

EnCase Overview



Creating a New Case



Using EnCase



EnCase Engine



Forensic Techniques



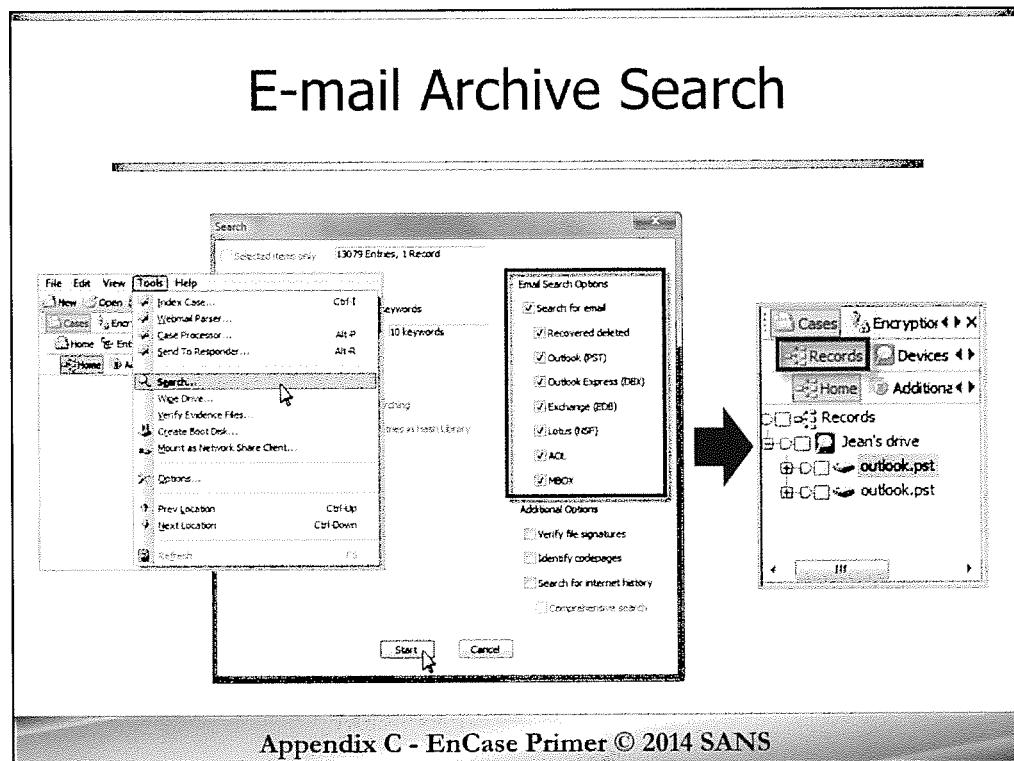
Application Parsing



Bookmarks and Reporting

Appendix C - EnCase Primer © 2014 SANS

This page intentionally left blank.



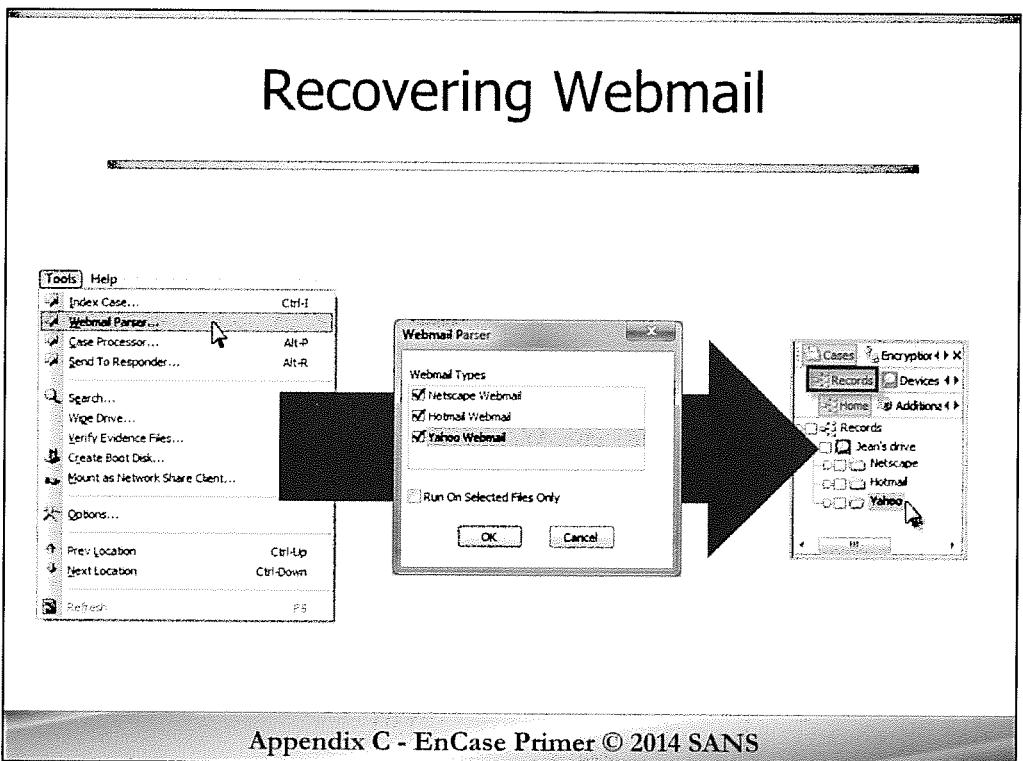
Appendix C - EnCase Primer © 2014 SANS

Owing to the large importance of e-mail in many investigations, EnCase provides a robust feature for finding and parsing several of the most popular e-mail client formats. This capability is reached via the **Tools → Search** menu. Within the search dialog box you will find a section labeled **E-mail Search Options**. Most of the options are self-explanatory, telling the tool to look for particular types of archives. One option to pay attention to is named **Recovered deleted**. This option will attempt to recover any soft deleted messages that remain in the archives that are found. If such information is within the scope of your investigation, it can provide valuable insight into e-mail marked as deleted, but still resident in the archive.

E-mail search will be conducted on every file in the case (including the unallocated space file) unless it is overridden with the **Selected Items only** option at the top of the Search dialog. This option allows the examiner to have a fine grained control over what is searched, for instance selecting only the files within a particular user's folder and focusing the search there.

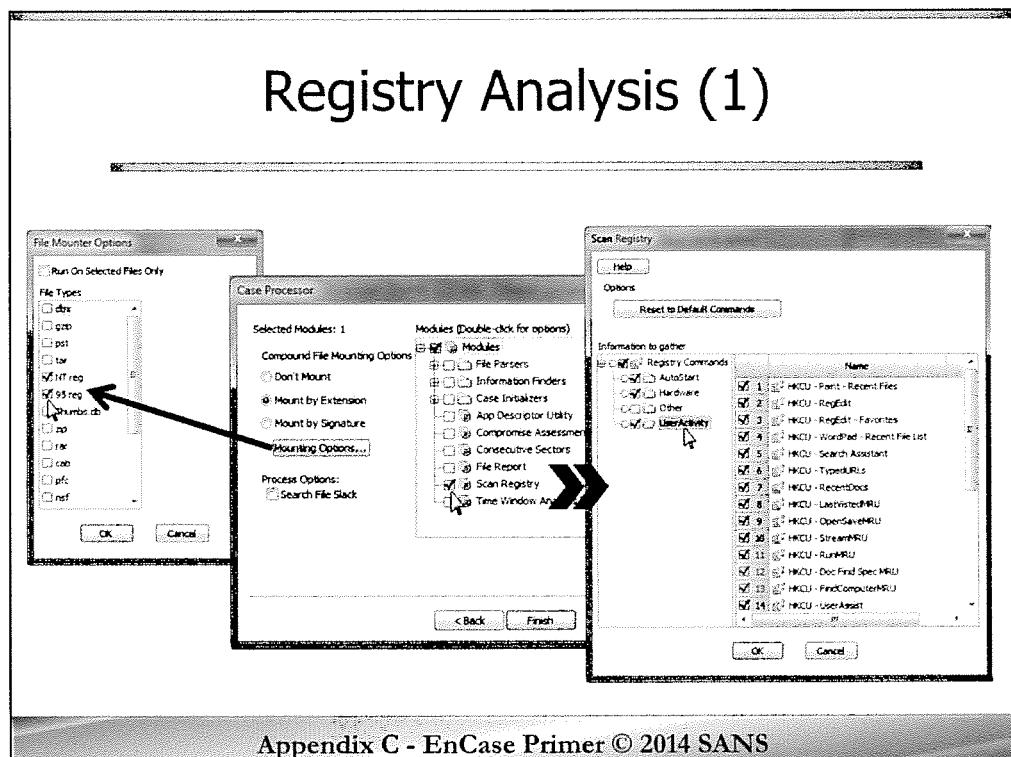
Not shown here, there is a built-in condition within the Filters Pane for scanning the file system for e-mail archives. It can be found in **Conditions → Email Examinations → Mail Finder → Mail Filters – comprehensive**. Keep in mind that this condition only identifies archives. It would then be up to the examiner to manually mount those archives and perform their review.

Recovering Webmail



Appendix C - EnCase Primer © 2014 SANS

A simple webmail search tool is built into EnCase. It is reached through the **Tools → Webmail Parser** menu item and executes a built-in EnScript. The tool searches either all files in the case or just marked files for fragments that appear to contain webmail from Netscape, Hotmail, and Yahoo!. Any output it finds will be placed within the Records tab within the Tree Pane and will be labeled accordingly (as shown in the slide). Webmail can be a big part of many investigations and can be frustratingly hard to find. This is particularly true with newer systems because as webmail has moved to the Web 2.0 Dynamic HTML model, there are less and less artifacts to be found. Keep this in mind when running this tool. It is only really effective at discovering e-mail from the “Classic” versions of these services. Thus it should not be your only search for webmail fragments. While keyword searching can be more effective at finding a larger pool of e-mail (including fragments from the new dynamic versions of webmail), the Webmail Parser does not require a list of keywords. Leveraging both types of searches is often the key to conducting a complete examination.



Appendix C - EnCase Primer © 2014 SANS

EnCase has a powerful built-in means to scan the Windows Registry and extract well-known keys for review. The interface is not particularly intuitive, but once you learn the process, it can be a valuable means for quickly getting information from the registry without exporting the hives and running third-party tools.

The **Scan Registry** module is located in the **Case Processor** EnScript, so open that first and create a unique name for the resulting bookmark. Since Registry hives are considered compound files, we will need to direct the EnScript to mount the hives. Select **Mounting Options** and click the checkboxes for **NT reg** and **95 reg** (the latter can be ignored for post Win95 systems, but can be included for the sake of completeness).

After setting up your File Mounter Options, double-click on the **Scan Registry** module and select the categories and/or individual keys that you wish EnCase to extract and parse. Click **Ok** and then **Finish** to start the Registry scan.

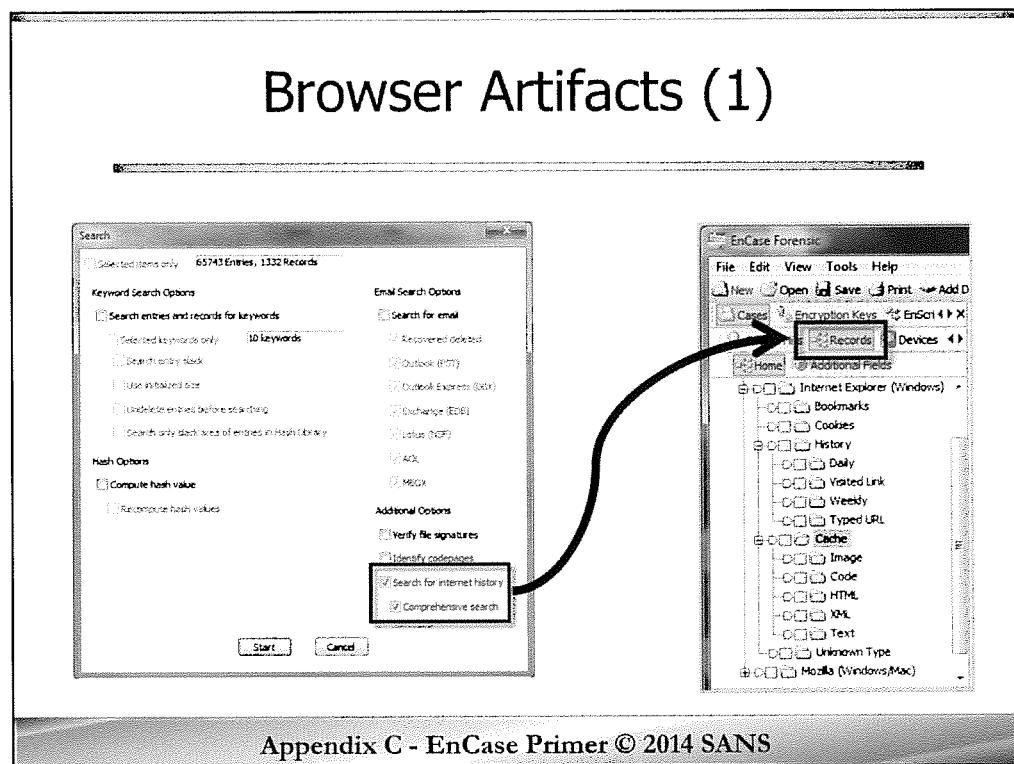
Registry Analysis (2)

The screenshot shows the EnCase Forensic interface. On the left, the Tree Pane displays various analysis modules like Encryption Keys, Prefetch File Analysis, and Registry Analysis. A callout arrow points from the 'Scan Registry' option in the Registry Analysis section to the 'Scan Registry' tab in the Bookmarks section of the main pane. The main pane shows the 'Entries' tab selected, displaying a list of registry keys under 'UserActivity'. A second callout arrow points from the 'Scan Registry' tab in the Bookmarks pane to the 'Registry Values' tab in the main pane, which is currently selected and shows a table of registry values. The table has columns for Name, Value, Type, and Last Written. The data in the table is as follows:

Name	Value	Type	Last Written
url1	http://www.winamp.com/	String	
url2	http://www.color.adobepass.com/	String	
url3	http://www.craiglist.com/	String	
url4	http://mail.yahoo.com/	String	
url5	http://www.weather.com/	String	
url6	http://www.opentable.com/	String	
url7	http://www.espn.com/	String	
url8	http://www.cnn.com/	String	
url9	http://www.facebook.com/	String	
url10	http://www.twitter.com/	String	
url11	http://www.am.com/	String	
url12	http://www.skype.com/	String	
url13	http://windowsupdate.microsoft...	String	
url14	windowupdate.com	String	

Appendix C - EnCase Primer © 2014 SANS

After the Scan Registry script has run, you should see your new bookmark within the **Cases | Bookmarks** tab in the Tree Pane. This bookmark will contain a seemingly empty folder named, **Scan Registry**. By highlighting that folder, a new sub-tab will appear in the Tree Pane under the Bookmarks tab. It will be called **Registry Values** and will contain the results of your Scan Registry process. Keys can be viewed within the Tree Pane and Registry Values within the Table Pane. You can bookmark data within the Table Pane and/or export it out to a file for further analysis.



Appendix C - EnCase Primer © 2014 SANS

EnCase includes a built-in script for identifying and parsing browser artifacts. It recognizes artifacts from Internet Explorer, Safari, Firefox (pre and post-version 3), and Opera. You can find this feature on the Search menu, reached through the **Tools → Search** menu. On the lower right corner you will find **Search for internet history**. Checking this box will cause EnCase to search through the list of known files looking for any browser databases it can find. Results are parsed and placed in the **Cases | Records** tab on the Tree Pane. EnCase does an excellent job of categorizing its findings, even breaking up the IE History index.dat files into daily or weekly versions, and organizing cache files by file type. In the example shown here, artifacts were found for both Internet Explorer and Mozilla Firefox.

The **Comprehensive search** option within the Search dialog box asks EnCase to go a step further and search unallocated and slack space for deleted browser files. If it finds any, they will be parsed and placed in the Records tab.

Browser Artifacts (2)

The screenshot shows the EnCase Forensic interface. The left pane displays a tree view of evidence files, with one entry for 'dblade_20110311' expanded to show sub-folders like 'Records', 'USB Device History', and 'Internet Explorer (Windows)'. The 'Internet Explorer (Windows)' folder is further expanded to show 'Bookmarks', 'Cookies', 'History', 'Daily', 'Visited Link', and 'Weedy'. The right pane is a 'Table' view showing browser artifacts. The columns are 'Name', 'URL', 'Start Date', and 'Last Accessed'. The data includes:

Name	URL	Start Date	Last Accessed
1. Unallocated Clusters	http://us.mg-t-mail.yahoo.com/dc/a...	01/15/09 07:00:00PM	01/16/09 06:10:57PM
2. Unallocated Clusters	us.mg-t-mail.yahoo.com	01/15/09 07:00:00PM	01/16/09 06:10:57PM
3. Unallocated Clusters	file:///falconi/Users/dblade/Documen...	01/15/09 07:00:00PM	01/16/09 06:13:45PM
4. Unallocated Clusters	falconi	01/15/09 07:00:00PM	01/16/09 06:13:45PM
5. Unallocated Clusters	file:///falconi/Users/dblade/Documen...	01/15/09 07:00:00PM	01/16/09 06:13:50PM
6. Unallocated Clusters	file:///C:/Documents%20and%20S...	01/15/09 07:00:00PM	01/16/09 06:13:58PM
7. Unallocated Clusters	My Computer	01/15/09 07:00:00PM	01/16/09 06:13:58PM
8. Unallocated Clusters	file:///falconi/Users/dblade/Documen...	01/15/09 07:00:00PM	01/16/09 06:14:01PM
9. Unallocated Clusters	file:///C:/Documents%20and%20S...	01/15/09 07:00:00PM	01/16/09 06:14:45PM
10. Unallocated Clusters	file:///C:/Documents%20and%20S...	01/15/09 07:00:00PM	01/16/09 06:14:52PM

Appendix C - EnCase Primer © 2014 SANS

This slide provides a more comprehensive view of how browser artifact results are displayed within EnCase. Note that we are in the **Case | Records** tab within the Tree Pane and have highlighted the Daily History results within Internet Explorer. The results displayed in the Table Pane were sources from unallocated space using the **Comprehensive search** option. The location of each browser artifact file is noted by EnCase, easily allowing the examiner to determine where it was found. Similar to other views utilizing the Table Pane, columns can be hidden, sorted, and moved to aid review.

EnCase Overview



Creating a New Case



Using EnCase



EnScript Engine



Forensic Techniques



Application Parsing



Bookmarks and Reporting

Appendix C - EnCase Primer © 2014 SANS

This page intentionally left blank.

Bookmarks

Bookmarks allow files, folders, metadata, and data to be saved and packaged for reference and reporting

- User Generated
 - Text Fragment / Data
 - Notable File
 - File Groups
 - Folder Structure
 - Notes
 - System Snapshots
- System Generated
 - Evidence verification
 - Searching
 - File Signature Analysis
 - Hashing
 - Exporting
 - EnScript output

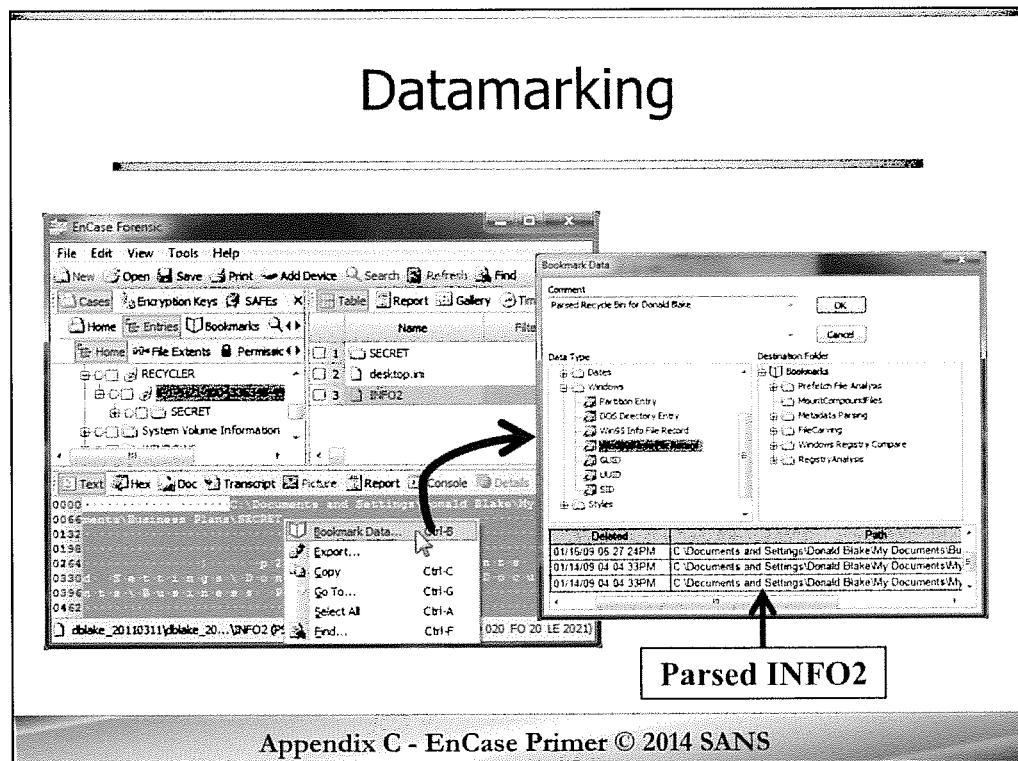
Appendix C - EnCase Primer © 2014 SANS

Before we can discuss reporting, we must first talk about bookmarking. EnCase reports are generated from an examiner's bookmarks, so the better the bookmarks, the better the report. Bookmarks can be created anywhere you interact with data within EnCase. Evidence files are often incredibly large and a good examiner will utilize bookmarks to document critical findings as they are found. Here are several different types of bookmarks available.

User generated bookmarks:

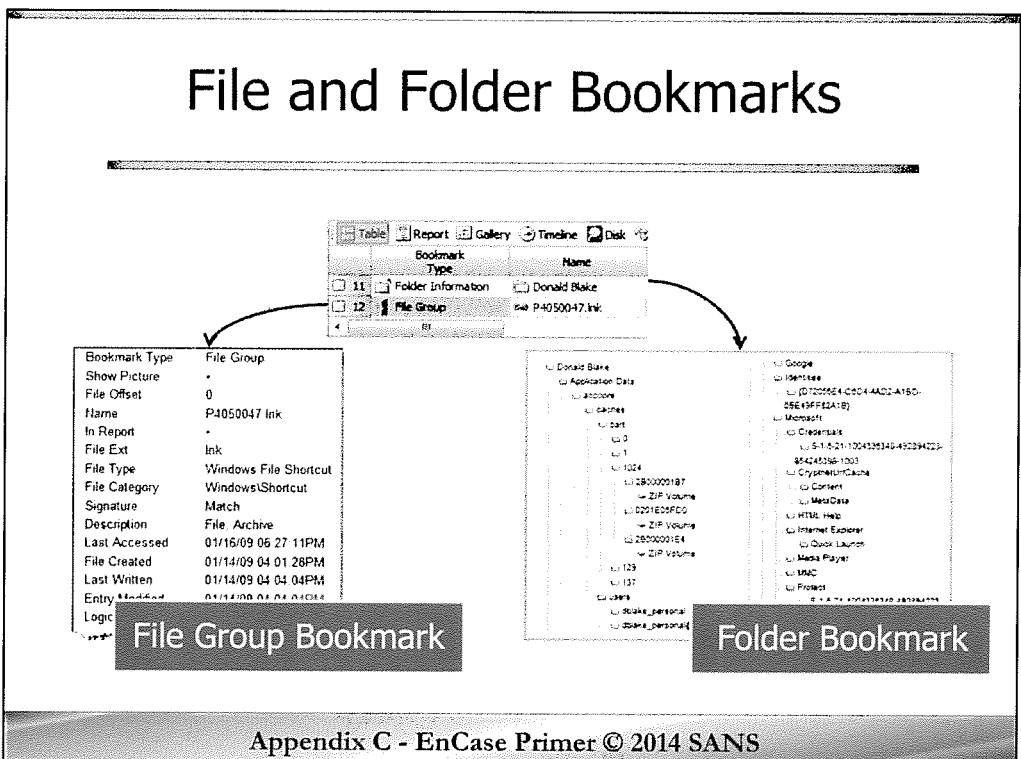
- Text Fragment / Data – Created from highlighted data in the View Pane.
- Notable File – Bookmarked files from the Table Pane. The file name and its associated metadata are bookmarked.
- File Groups – Similar to notable file, but consists of a group of marked files
- Folder Structure – Bookmarked from the Tree Pane, this records the directory structure of a folder and its children.
- Notes – Freeform notes can be created anywhere and allow the examiner to add comments or thoughts that can give context to reported results.
- System Snapshots – Used to record live response data collected via **Tools → Scan Local Machine**

System generated bookmarks result from variety of different programs and actions within EnCase. These programs store their output as bookmarks. These results can then be further bookmarked to pull out relevant details.



Data bookmarks are an incredibly powerful and often underestimated feature of EnCase. In their simplest form, they allow text fragments to be copied out of the View Pane (from the Text, Hex, Transcript and Doc tabs) and placed into a bookmark. This is done by highlighting (sweeping) the data of interest and then right-clicking and selecting **Bookmark Data**. A dialog box will appear allowing you to add an optional comment providing context for the bookmark and choose the bookmark folder in which to save the data. The most important part of the data bookmark dialog is the ability to choose the data type. This option is used for much more than just display. If the data is part of a known forensic artifact and the proper data type is set, EnCase will attempt to parse that artifact and save the parsed output. Thus if you bookmark the start of an INFO2 record, and choose INFO2 from the data type list, EnCase will parse all of the deleted file metadata for that file and save it accordingly. This trick works for myriad different artifacts such as timestamps, partition tables, ROT 13 encoding, etc. It is truly one of the great “hidden” features of the suite, but takes practice to use effectively.

File and Folder Bookmarks



Bookmarking files and folders is relatively straightforward once you consider what you are actually bookmarking. Unlike bookmarking raw data, you will instead be marking the file metadata (Table Pane) or folder hierarchy (Tree Pane). Many users new to EnCase create all of their bookmarks in the Table Pane and expect each file's data to also be included. A good way to keep things straight is to imagine you are bookmarking whatever that particular view can show you. All of that being said, when it comes time to generate your report, you will have the ability to export whatever files or folders have been bookmarked and to hyperlink those files to be viewed in their original forms.

File bookmarks are created in the Table Pane and hence record filenames and associated metadata. Either highlight (for one file) or check the boxes of the files you wish to mark and right-click within the table. Select **Bookmark Data** to bookmark the files. A dialog box will emerge allowing you to select an existing Bookmark folder or create a new bookmark folder. If multiple files were marked, each will be saved as an individual bookmark. There is no mechanism for adding a comment along with the bookmark. To accomplish this, you would want to perform a second step, right-clicking and selecting **Add Note**.

Folder bookmarks are created in the Tree Pane. Right-click the folder or device and select **Bookmark Data**. You can then select the bookmark folder for the results and choose how many columns of information to display for the folder structure. The columns value determines how the information is displayed within the bookmark. A value of "0" saves the information as text only. Values of 1-3 display the folder contents using that number of columns.

System Generated Bookmarks

The screenshot shows the EnCase Forensic software interface. The left pane displays a tree view of analysis results under 'Entries' and 'Bookmarks'. The 'Bookmarks' section contains several entries, including 'Prefetch File Analysis', 'MountCompoundFiles', 'Metadata Parsing', 'FileCarving', 'File Finder', 'dblake_20110311', 'EMF', 'Office97+ Compound Document', 'Zip', and 'Windows Registry Compare'. The right pane shows a table titled 'Bookmarks' with columns for 'Bookmark Type', 'Preview', and 'Comment'. The table lists 14 entries, all of which are 'Highlighted Data' type. Each entry has a preview of the data and a comment indicating it is 'Zip: Unallocated Clusters File offset'. The table rows are numbered 1 through 14.

Bookmark Type	Preview	Comment
1 Highlighted Data	PK t CEU "yyYSv\p\Eds+YY	Zip: Unallocated Clusters File offset
2 Highlighted Data	PK "9~Y/ 'u	Zip: Unallocated Clusters File offset
3 Highlighted Data	I Z8 fb à	Zip: Unallocated Clusters File offset
4 Highlighted Data	PK u eayyé- þeK u éþbyY	Zip: Unallocated Clusters File offset
5 Highlighted Data	PK uG E - fè M %>J EOPyù è>	Zip: Unallocated Clusters File offset
6 Highlighted Data	PK tzf)ò t =PK tmf)ò t =PK	Zip: Unallocated Clusters File offset
7 Highlighted Data	PK L=PK _wyÿùPK tPK	Zip: Unallocated Clusters File offset
8 Highlighted Data	PK Wézyf/A Áš F) PWé	Zip: Unallocated Clusters File offset
9 Highlighted Data	PK tsDAMöd% Y_~[M483é	Zip: Unallocated Clusters File offset
10 Highlighted Data	PK FT8O?]: a	Zip: Unallocated Clusters File offset
11 Highlighted Data	PK "9F A8* 2t	Zip: Unallocated Clusters File offset
12 Highlighted Data	I Z8 fb à	Zip: Unallocated Clusters File offset
13 Highlighted Data	PK .exe .z	Zip: Unallocated Clusters File offset
14 Highlighted Data	#iv+ù;ÀñPK "9[3	Zip: Unallocated Clusters File offset

Appendix C - EnCase Primer © 2014 SANS

A large number of actions within EnCase result in a bookmark being created. In fact, new EnScript users will often assume that the script failed due to a lack of any confirmation only to find the results neatly tucked into a bookmark. You should frequently check the bookmarks tab, use descriptive comments when prompted, and organize as you go. This way when new data suddenly shows up as a bookmark, it is easy to spot and review its contents. This is particularly true for large cases. If you don't keep up with them, you may forget exactly why something was bookmarked to begin with. In addition to EnScripts, other common actions that store results within bookmarks include:

- Evidence verification
- Searching
- File Signature Analysis
- Hashing
- Exporting
- EnScript output

Within the Bookmarks tab you can move, delete, rename, exclude, and create new folders by using the right-click menu.

Creating the Final Report

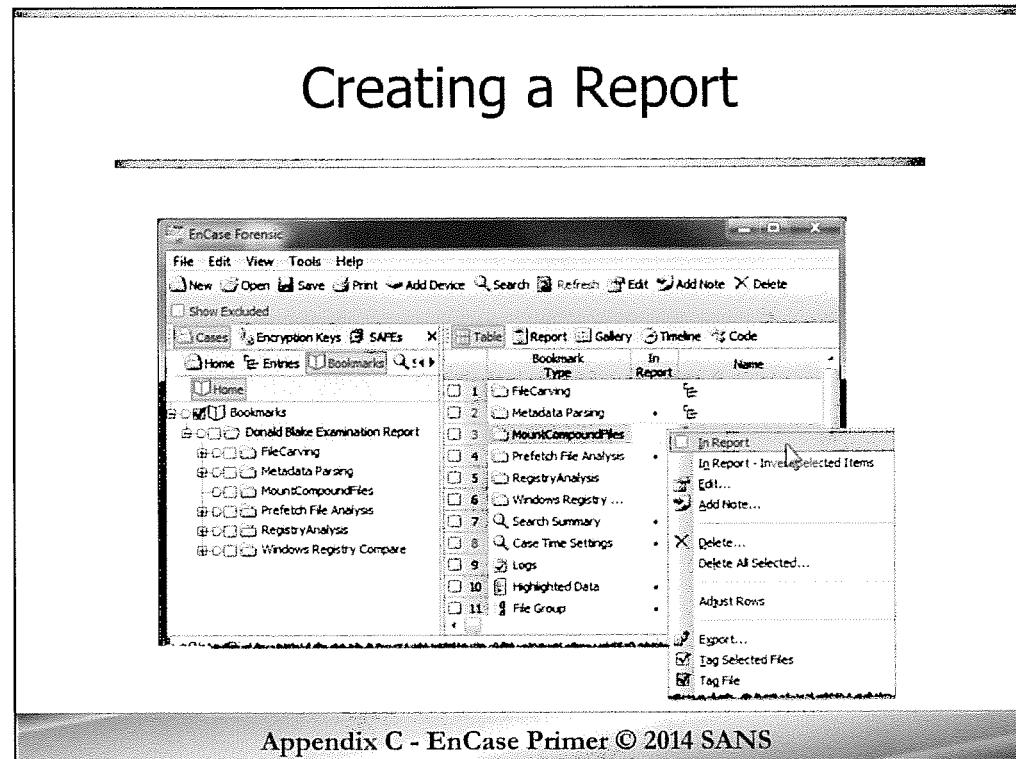
1. Bookmark all relevant files and results
2. Navigate to the Bookmarks tab
3. Choose items to include in report 
4. Select the "Home Plate" on bookmark folders
5. Switch to the Report tab (in Table Pane)
6. Review output
7. Export the report
 - Save as HTML

Appendix C - EnCase Primer © 2014 SANS

The Report tab on the Table Pane is used to create a summary report of your findings. This tab is different than the Report tab within the View Pane as the latter is used to create a report on a single item in the case (for instance, a highlighted file within the Table Pane). The Report tab in the Table Pane can generate a report on artifacts of interest throughout your case. The process is (relatively) straightforward:

1. Navigate throughout your case and bookmark any files, folders, search results, e-mails, etc. It is a good habit to do this while you are doing the examination instead of all at once.
2. Switch to the Bookmarks tab to review your final set of bookmarks
3. Review each bookmark and select or de-select **In Report**. Don't assume that children within a bookmark will inherit their parent's **In Report** selection! You may need to do this for each individual bookmarked entry. Use **In Report – Invert Selected Items** within the Table Pane to select or de-select multiple files.
4. Select the Set Included trigger (Home Plate) within the Tree Pane for each bookmark folder you wish to be included in the report. This feels redundant since you have already explicitly selected bookmarks for inclusion, but it is a necessary step.
5. Switch to the Report tab within the Table Pane.
6. Review your output. Whatever is shown in this view will ultimately end up in your report.
7. Right-click within the Table Pane and select Export. The HTML version of the report is excellent and creates a nice hyperlinked report.

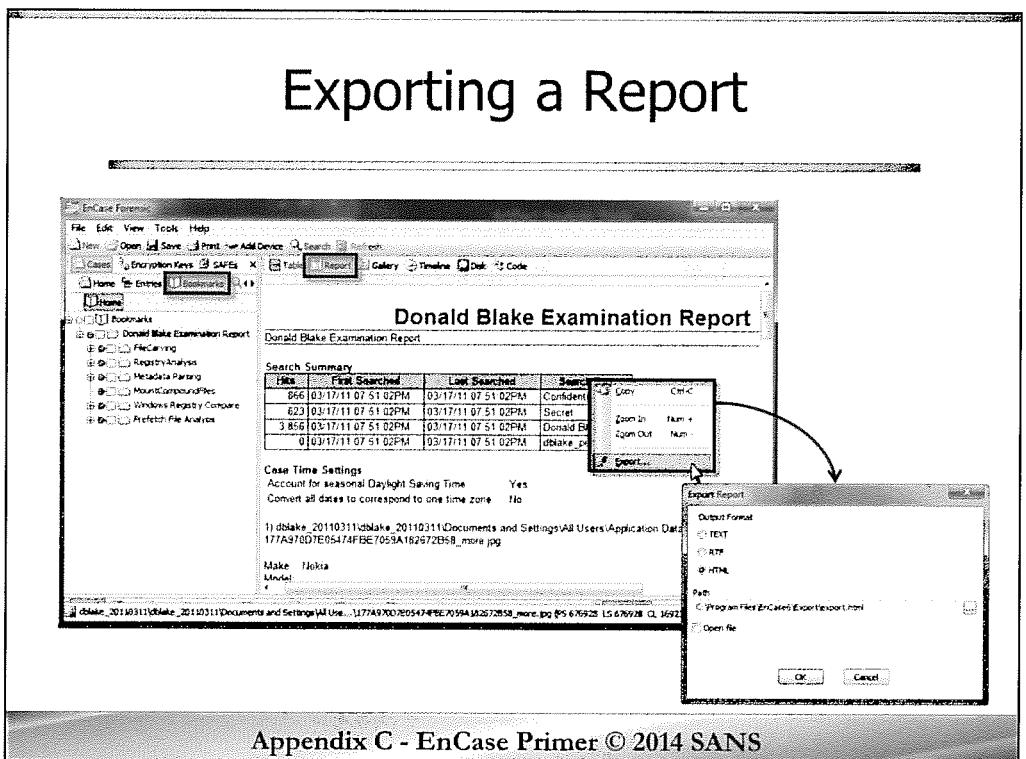
Creating a Report



Appendix C - EnCase Primer © 2014 SANS

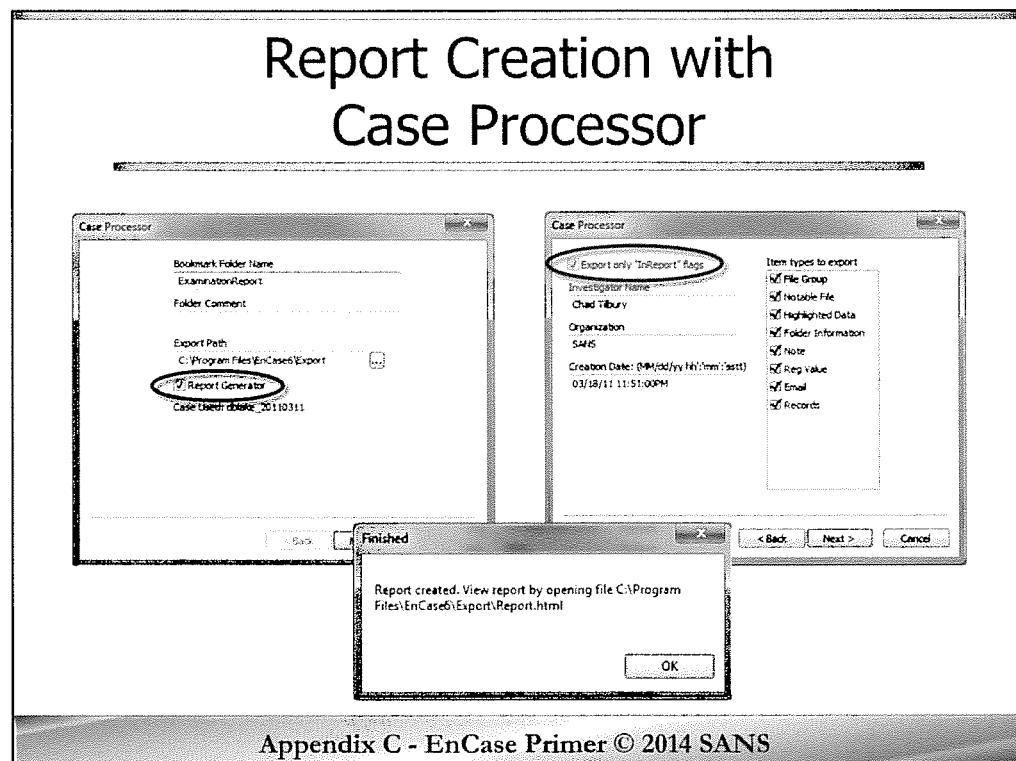
This slide shows the process of reviewing individual bookmarks and selecting or de-selecting them to be **In Report**. The process is easy, but can become tedious. For large numbers of items, select via the check boxes within the Tree Pane and utilize the **In Report – Invert selected items** option to operate on them all at once.

Exporting a Report



Appendix C - EnCase Primer © 2014 SANS

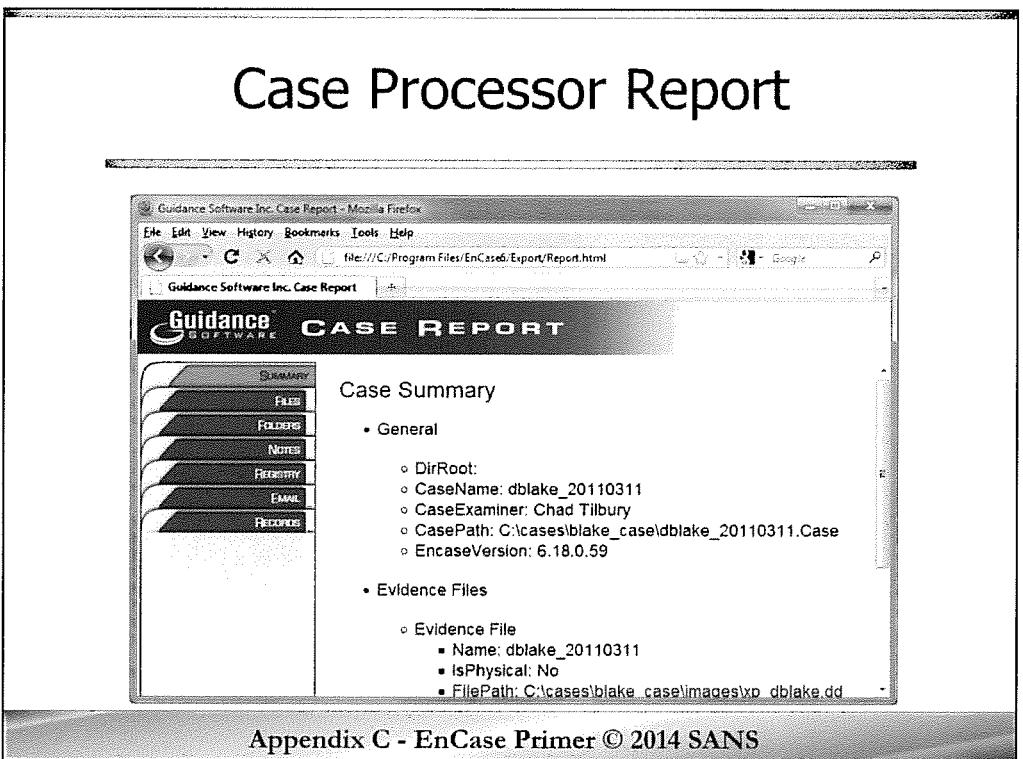
This slide graphically shows the export report process. Notice that it shows the Bookmarks view within the Tree Pane and the Report view within the Table Pane. The “home plates” for the bookmarks of interest have been set within Tree Pane and you can see what the report will look like within the Table Pane. Once you are satisfied with the report, right-click within the Table Pane and select **Export**. In this example, we have selected an HTML report and left the export path as the default.



Appendix C - EnCase Primer © 2014 SANS

The Case Processor script now includes a means to auto-generate a web-based report. The process and results are very different than the traditional export report method. Nevertheless, the process is relatively simple:

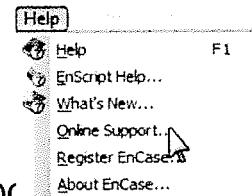
1. Select **Tools → Case Processor**
2. Input a unique bookmark folder name and select **Report Generator**. Click **Next**.
3. Select which items to export and input examination metadata. Be very careful with how much data you are exporting! There can be thousands of files referenced in your bookmarks, e-mail and records tabs. It is a good best practice to check the **Export only “InReport” flags** and manually select which items you wish to be in the report via the EnCase GUI. Click **Next**.
4. The final dialog in Case Processor asks which files you wish to Mount and which modules you wish to run. De-select all options since you want to just create a report. (This step is not shown on this slide as we have seen the dialog in a previous slide). Click **Next**.
5. Navigate to your Export Path (C:\Program Files\EnCase6\Export is shown on this slide). You will see multiple HTML files and folders representing all of the data exported and linked by the Case Processor. Open **Report.html** with your favorite browser.



While not likely to be the final report you hand in, the Case Processor module does provide a good head start. It has a nice HTML based report structure with each type of data in its own tab and the exported files all hyperlinked. Since it is HTML based, you can add additional findings outside of EnCase rather easily. Keep in mind that getting the report you desire will likely take some work. Very often you will review the report and be disappointed to find some of your key findings missing. Then you must go back into EnCase and ensure that those findings (and more commonly the children of those findings) are marked as "In Report" and generate the report again. In my experience, it usually takes a few tries to correctly produce my report using this tool.

Resources

- EnCase Forensic User's Guide
 - On Course DVD
- EnCase Help Menu
- Online Resources
 - <http://www.forensicfocus.com>
 - <http://www.forensickb.com>
- EnCE Study Guide by Steve Bunting



Appendix C - EnCase Primer © 2014 SANS

While this primer touches on the features most critical to getting started with EnCase, you certainly recognize by now that it is an enormously complicated application. The best way to learn is by doing and as you spend more time with EnCase you will undoubtedly uncover new shortcuts and features. EnCase ships with a very robust user manual weighing in at 627 pages at last count. This is an excellent starting point and a great reference to have nearby while using the tool. The help menu within EnCase has greatly improved from older versions and is robust in its own right. There are also a large number of blogs and forums covering tools, techniques, new EnScripts, and discussions of problems encountered. Forensic Focus and ForensicKB are two excellent sites to start with, but there are countless others to explore. Finally, Steve Bunting wrote an excellent study guide for the EnCase certification, EnCE, that covers most of the fundamentals.

This page intentionally left blank.



Digital Forensics and Incident Response

C U R R I C U L U M



FTK Primer

The SANS Institute

Ovie Carroll – oviecarroll@gmail.com

Rob Lee – rlee@sans.org



@sansforensics

<http://computer-forensics.sans.org>

Appendix D FTK Primer © 2014 SANS

Authors:

Ovie Carroll – oviecarroll@gmail.com

Rob Lee – rlee@sans.org

<http://twitter.com/robtee>

<http://twitter.com/sansforensics>

Special Thanks to Chad Tilbury, Ovie Carroll, and Jenny Delucia. Your thoughts, opinions, research, and insight were invaluable to the creation of the course.

Ready to Go

- Launch FTK
- On Your Desktop



Appendix D FTK Primer © 2014 SANS

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.

FTK Splash Screen

- First you will see
FTK Splash Screen

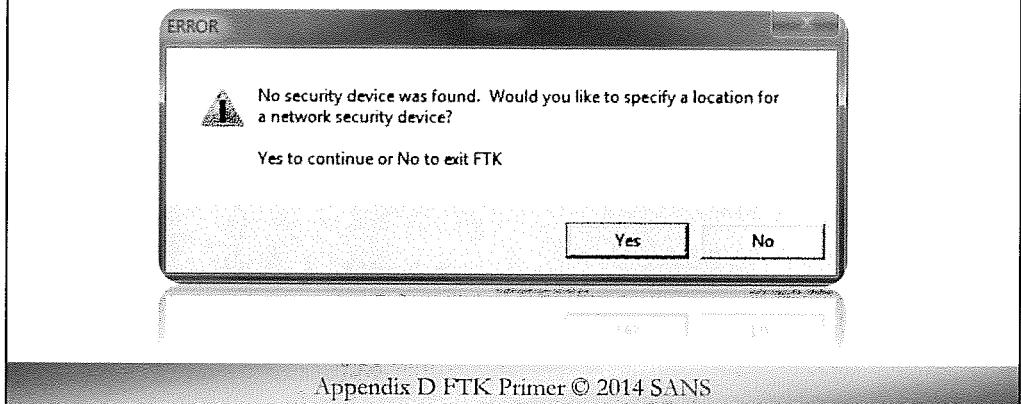


Appendix D FTK Primer © 2014 SANS

After launching FTK, you should get the FTK splash screen – hang on ... depending on the speed of your machine, this will go away in 10-20 seconds after FTK initializes. The version we are using in class is the FTK 4.1.0.502, 32-bit version . FTK has both a 32-bit and 64-bit version. Because hard drives and the data sets digital investigative analyst are seeing now have become so large, you want to use the most powerful system you can with as much RAM as possible. It is also recommended all forensic workstations use 64-bit operating system so they can take advantage of large amounts of RAM.

Oops!

- If you see this – your computer cannot see the license hub/dongle



Now did anyone receive this warning dialog box?

If you did, one of five 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.
5. You are not connected to the instructor license server.

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 during the installation process.

If you are using the SANS VPN or connecting to the instructors license server 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.

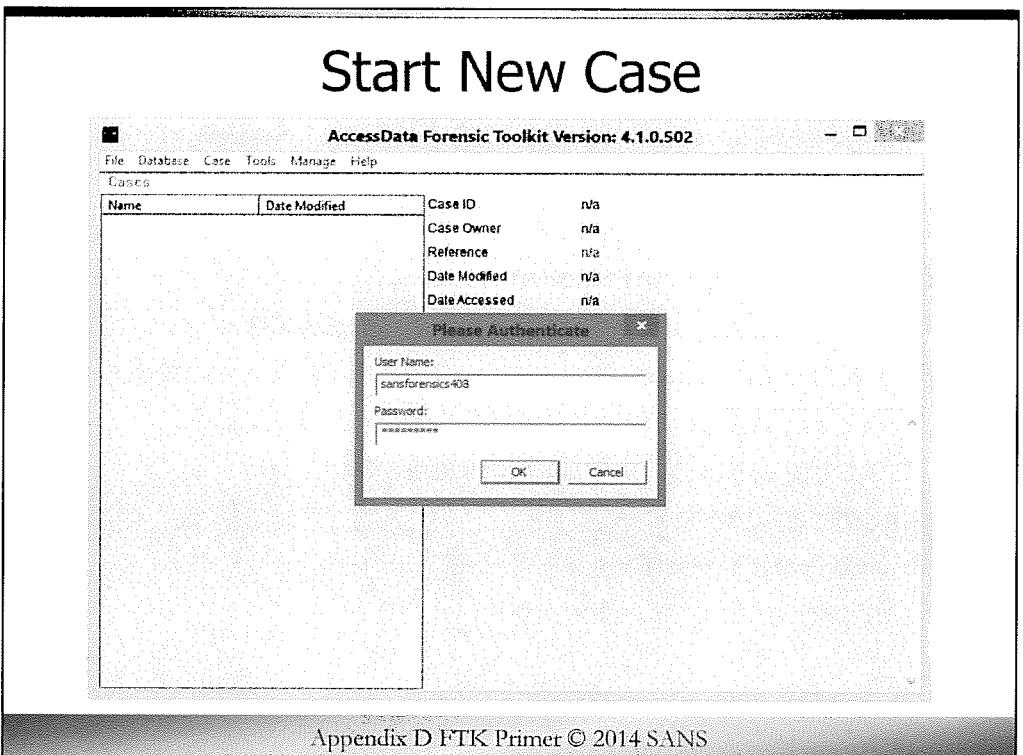
Steps for Case Setup

- Log in to the FTK application
- Enter basic case information
- Check what you want included in the case log
- Check the processes that you want run on the evidence
- Select the criteria for adding evidence to the case
- Select the criteria for creating the index
- Add the evidence
- Review your selections
- Start processing of evidence

Appendix D FTK Primer © 2014 SANS

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 already has been 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.



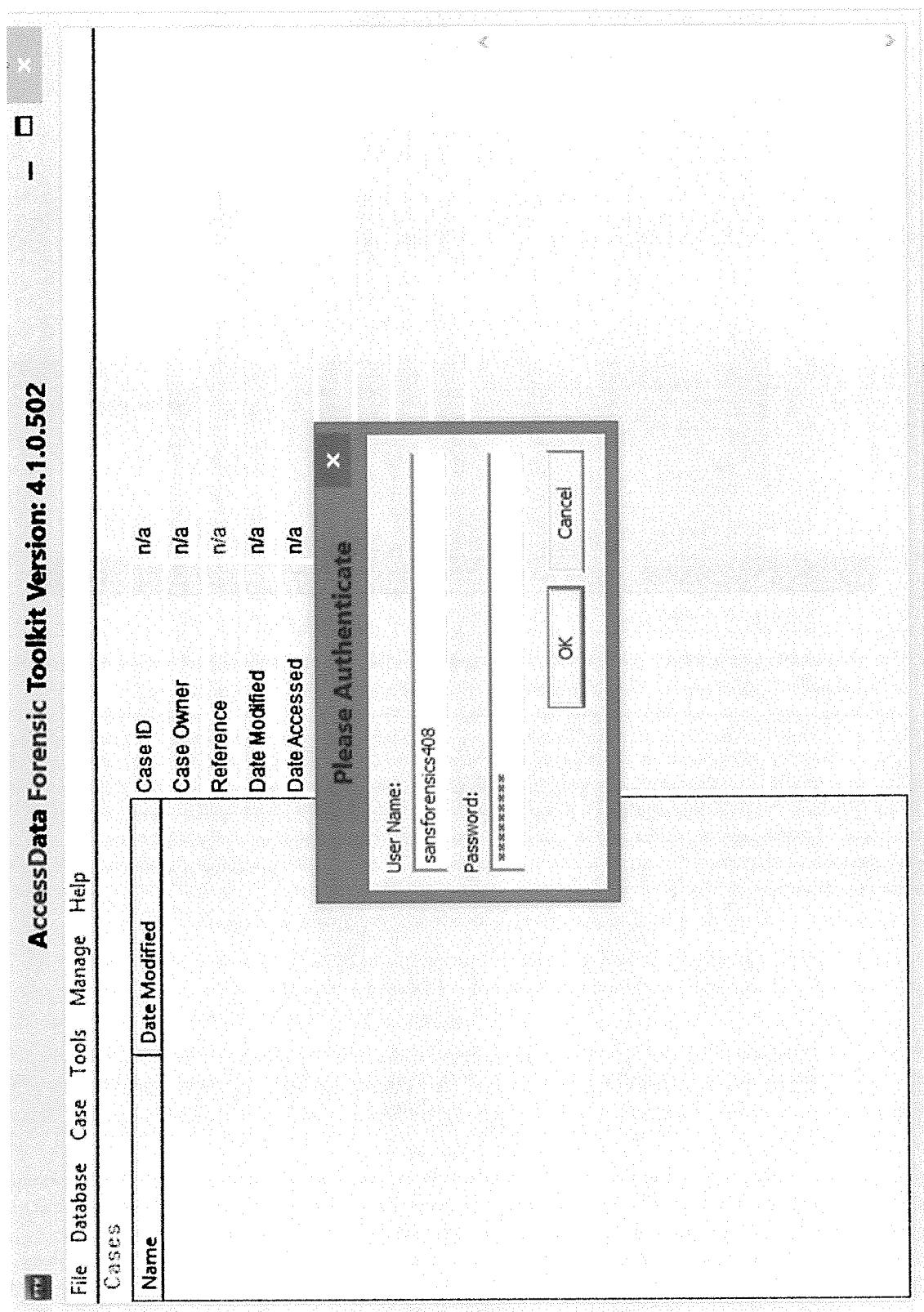
Appendix D FTK Primer © 2014 SANS

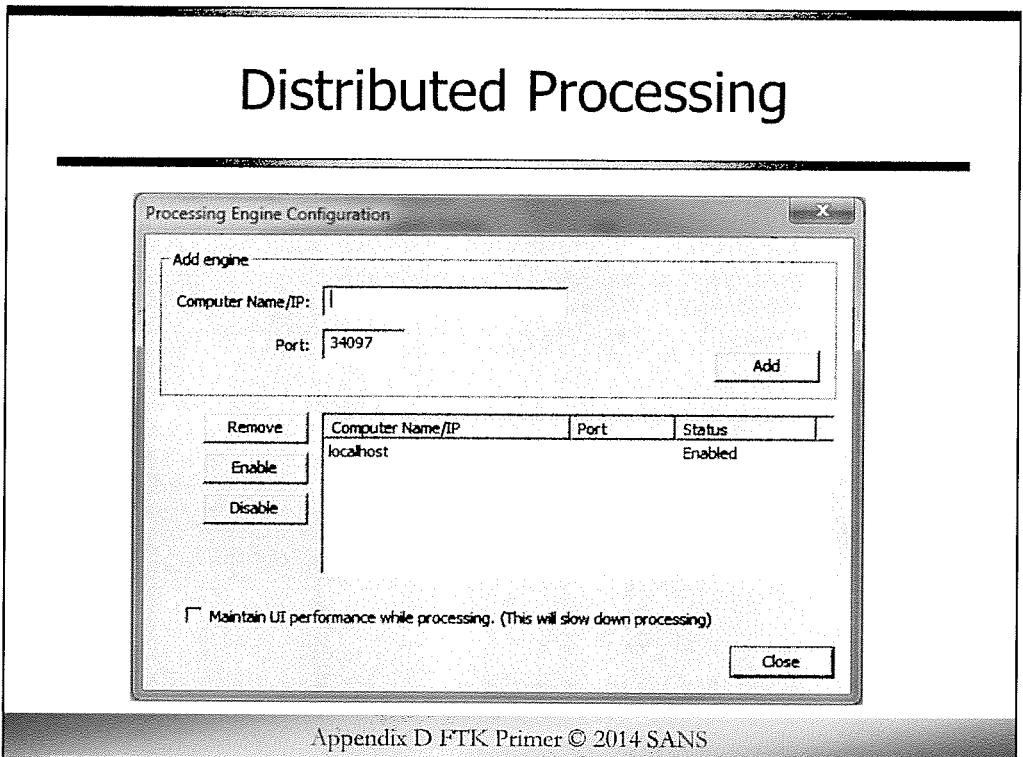
When you launch FTK, the first thing you should see is the AccessData FTK Case Manager interface and an authentication dialog box. We will log in with the application administrator account. This account allows you to administer the FTK application and create user accounts. The application administrator account has full rights to access every case, can create new users, change passwords for users (they do not have to know the users old password to change it) and assign rights at the global level.

When setting up your FTK environment at your workplace you should strongly consider establishing individual accounts for each examiner. Additionally, you can set up accounts with review only privileges that will allow an individual the ability to review a case but not add additional evidence, manage KFF, export items from the case, etc.

We will be using the application administrator account during class. Let's go ahead and log into the FTK case manager interface.

The application administrator username is “sansforensics408” and the password is “forensics”.





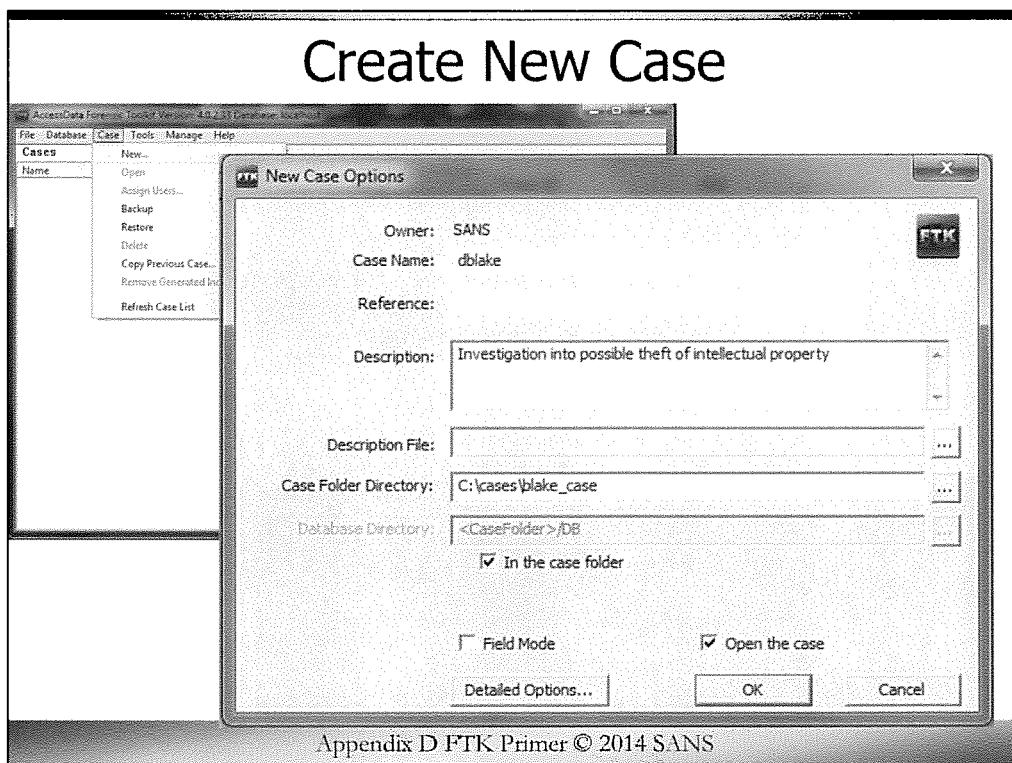
Starting with the stand-alone version of FTK 3, you can add three additional computers to be used as distributed processing engines. This can significantly speed up the initial case processing.

To use additional computers as additional processing engines, the additional computers can NOT have the full version of FTK installed, they can only have the processing engine installed. The processing engine can be found on the FTK install disk. One option for being able to set up your lab environment to take advantage of distributed processing, you can setup each forensic workstation with a dual boot configuration. The primary partition would be setup normally as your forensic analysis machine and the second partition would only have the processing engine installed.

On the menu bar, select Tools; Processing Engine Config..., and enter the IP Address of the remote computer then add the computer to the list of available processing engines.

When you want to use distributed processing to process a case, simply reboot your additional machines into the distributed processing partition then launch FTK from your primary machine. It will then be able to see and use the processing power of the additional machines.

When initially processing a case, FTK will use as much RAM and processor power as possible. This can leave your computer and your FTK user interface relatively sluggish or unresponsive. An interesting option under this configuration utility is a check box that gives you the ability to maintain the user interface performance while processing cases. This option does slow down the processing of your case but makes your FTK user interface much more responsive while the case is being indexed.



Appendix D FTK Primer © 2014 SANS

To start a new case select “Case”, then “New...” from the menu bar of the Case Manager interface.

The New Case Options dialog box will open and type “dblake” in the “Case Name” field.

Next is the “Reference” field. You can add a reference such as a case number or work load tracking number.

The next field is “Description” where you can type 512 characters describing the case. For cases where the description requires an extensive explanation, the “Description File” field allows you to attach a file such as a text or word document describing the case.

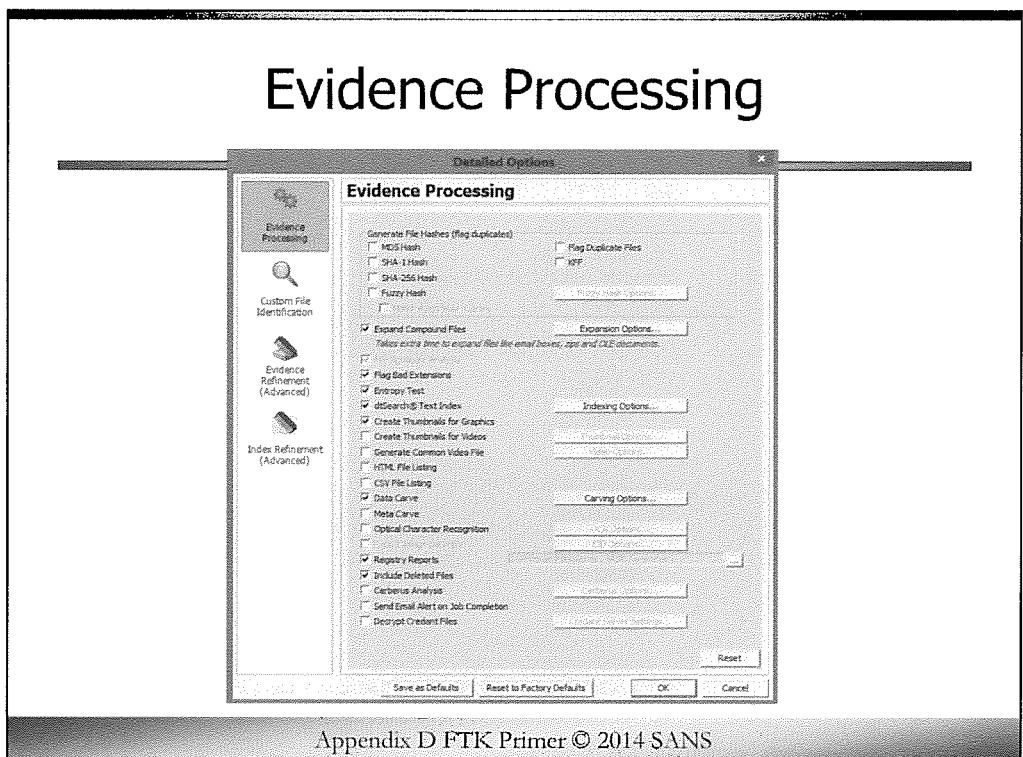
Next is the “Case Folder Directory”. Select the “...” navigation button to navigate to the directory where your case will be stored.

To optimize your forensic workstation, the case folder should be on a separate drive from the forensic images. The next field is the “Database Directory” and it should also be on a separate drive from the case folder and the images.

Since this is a small case, we are going to leave it in the same directory as the case folder so select the check box next to “In the case folder”. This will also make it easier to move your case from one machine to another if needed.

At the bottom of the New Case Options dialog box there is a “Field Mode” checkbox. If you would like to immediately start looking at your case and start conducting triage you can select this box and all processing and indexing will be postponed. Field Mode does no processing of any kind, including file signature analysis. The case evidence tree will be shown as soon as the case is open and files will be listed in the overview tab based on file extension only.

The last item we need to look at before moving on is the “Detailed Options...” button. Select “Detailed Options...” and we will take a look at processing options.



Appendix D FTK Primer © 2014 SANS

The Detailed Options Evidence Processing tab may be familiar to those who used previous versions of FTK with some improvements.

At the top of the Evidence Processing dialog box you will find all of your hashing functions. You have the option to create MD5, SHA-1, SHA-256 and Fuzzy hashes. You can save some time by only using the MD5 hash. If you want to use the known file filters (KFF) feature of FTK, MD5 is the hash value that KFF signatures use and must be enabled. Additionally, FTK automatically adds the SHA-1 hash when using the KFF feature.

The Fuzzy Hashing function is also known as contextual piecewise hashing. Fuzzy hashing looks for homologous files, not exact matches. This feature is very helpful with intellectual property cases or other situations where you need to find similar files. Warning, enabling fuzzy hashing adds considerably to the time it takes to initially process the case.

The “Flag Duplicate Files” will identify files based on hash and flag them as primary and secondary. The primary flag has no significance other than it was the first file found during case processing.

Expanding compound files can be time intensive but depending on the case type you are analyzing can be very helpful. You can reduce the number of files to expand if you know some file types are not significant to your analysis.

Entropy Test will run against unknown file types to test if the file is encrypted or compressed. If a unknown file is encrypted or compressed, it will not be indexed. Since the likelihood of indexing any of these files is remote, this can save you time in the initial processing of your case.

FTK uses the DTSearc indexing engine to index your case. This will make all indexed search result instantaneous. When you process a case you will almost always want to enable this feature. FTK requires space equal to 50% of the evidence files to initially index the case. Once the case is created, it will shrink back to approximately 25% the size of the case but it needs that extra space for working room during the initial indexing.

Data Carve - Data carving looks for data that was lost or deleted from the file system and is predominantly done by identifying file headers and/or footers, and then “carving out” the blocks between these two boundaries. Data carving is a time intensive process and generally it is best to do data carving as a secondary step after the case has been indexed. This can easily be accomplished by selecting the “Evidence” then “Additional Analysis...” options from the menu bar of FTK. By default data carving will look for AOL bag files, BMP, EMF, GIF, HTML, JPEG, LNK, OLE (MS Office), PDF, and PNG files but you also have the option of creating your own custom data carvers to meet your specific needs.

Meta Carve – Meta carve searches volume free space for deleted directories that have been orphaned. Orphaned directories are directories whose parent directory has been deleted or overwritten.

OCR - converts text in graphic files to text. A new file containing the OCR`ed text will be created and is named the same as the parent graphic, [graphic.ext], but with the .OCR extension, (e.g. IncomingFax.jpg.ocr) FTK can use 2 OCR engines, Tesseract (default and included with FTK), and GypReader (which requires separate licensing).

Evidence refinement - if you exclude a file type they can never be brought back into this case, a new case would have to be created.

Ref:

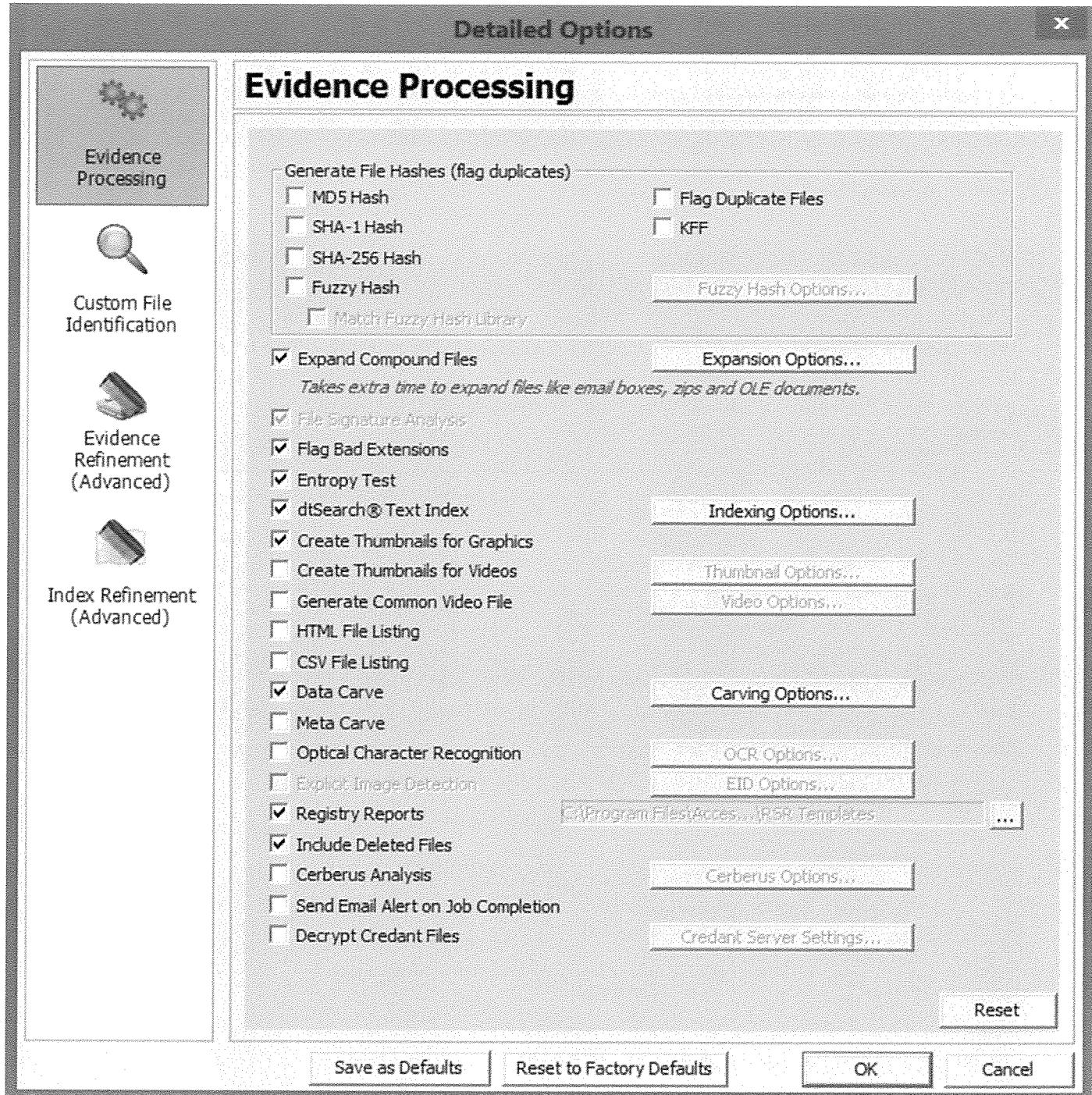
MD5 Hash - <http://www.loc.gov/standards/premis/pif-presentations/rebecca-SKOS/cryptographicHashFunctions-MD5.html>

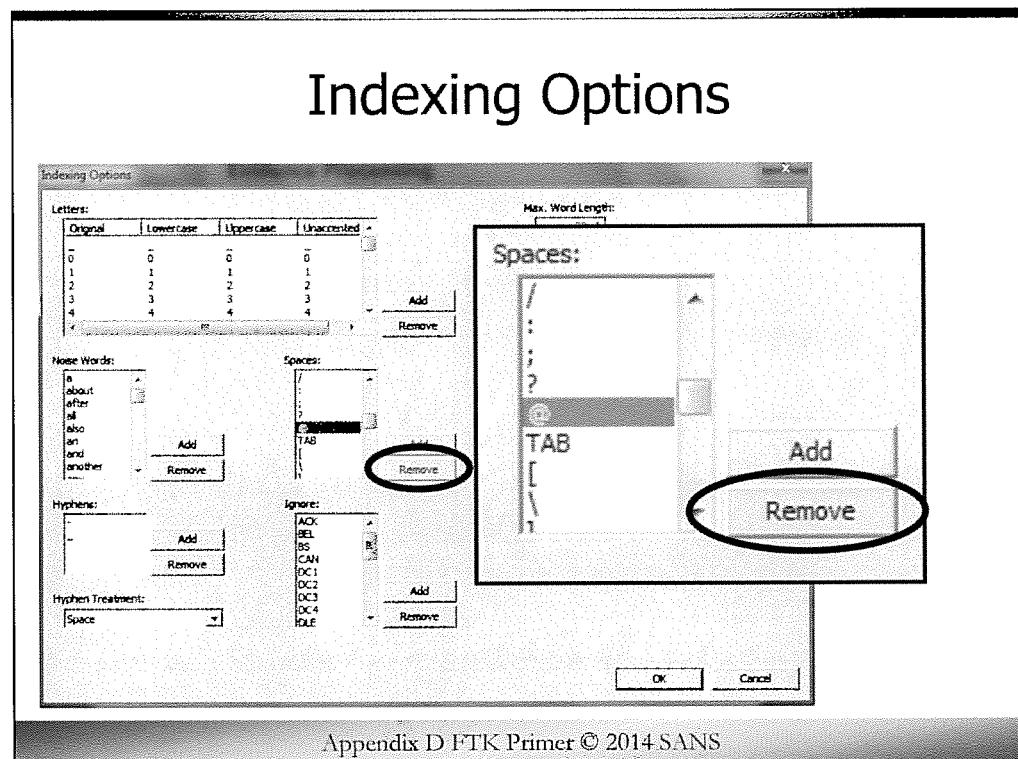
SHA-1 & 256 - http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf

Fuzzy Hashing - http://accessdata.com/downloads/media/Fuzzy_Hashing_for_Investigators.pdf

Tesseract - <http://code.google.com/p/tesseract-ocr/>

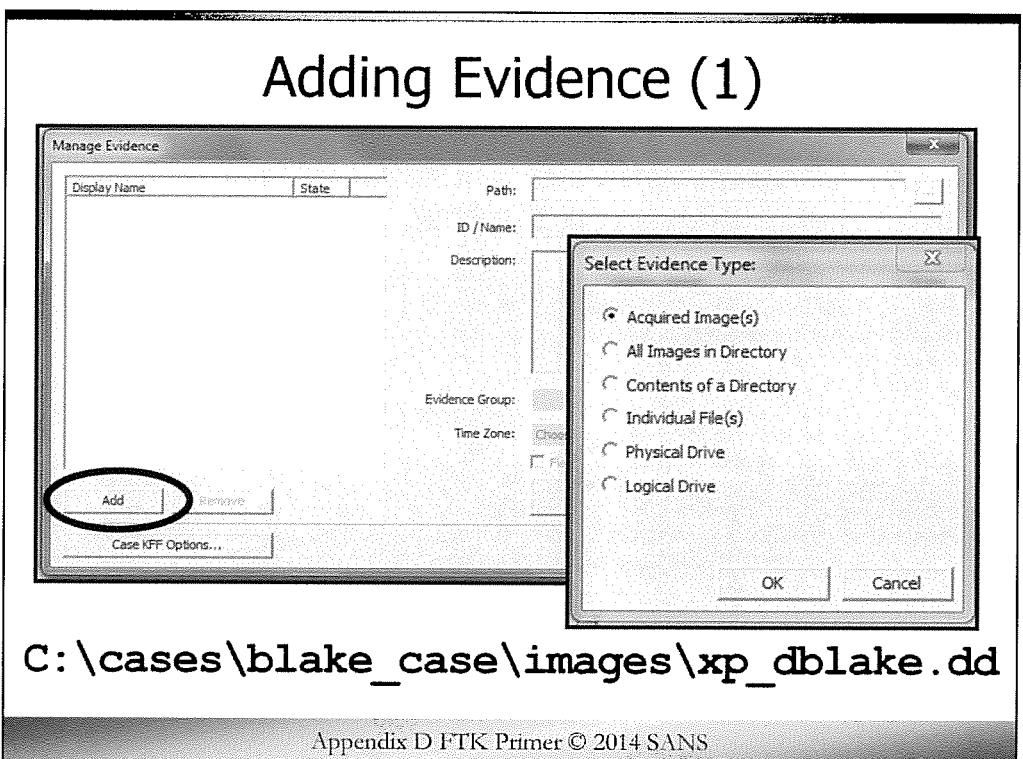
Glyphreader OCR - <http://www.atalasoft.com/products/dotimage/ocr/glyphreader/>





Appendix D FTK Primer © 2014 SANS

By default, FTK's indexing options interpret 35 special characters such as / : ; ? @ as a space. You can specially configure the indexing options to allow any or all of these characters to be indexed as they are. As an example, if you think it would be valuable to be able to search for full e-mail addresses you can select the @ symbol from the list of characters listed in the "Spaces:" box, then select "Remove". The @ symbol will now be indexed as itself and you can conduct indexed searches for full e-mail addresses such as "rob@sans".

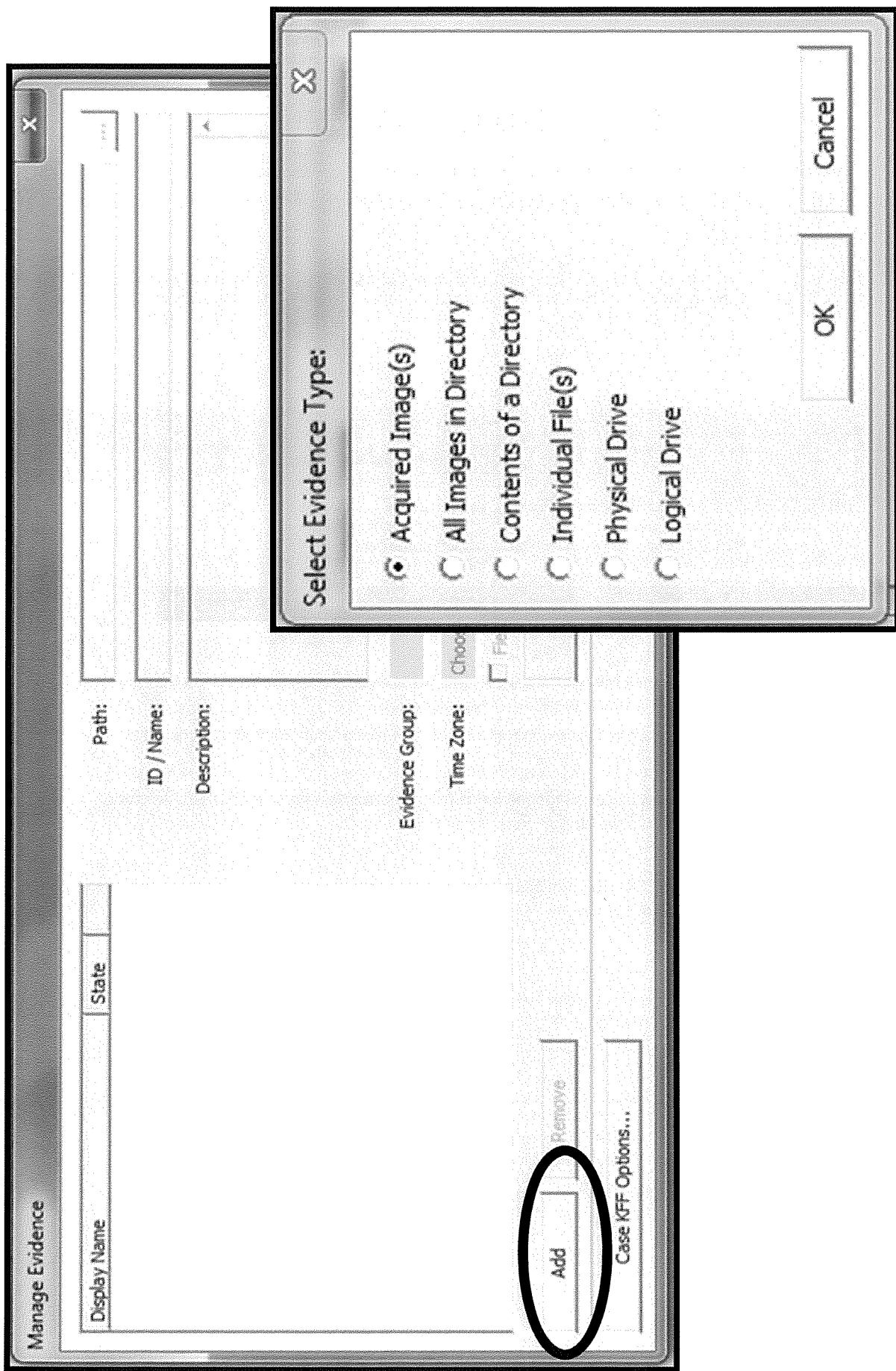


Now it is time to Add Evidence to your case. To do this, simply click on the “Add” button at the bottom left of the Manage Evidence dialog box.

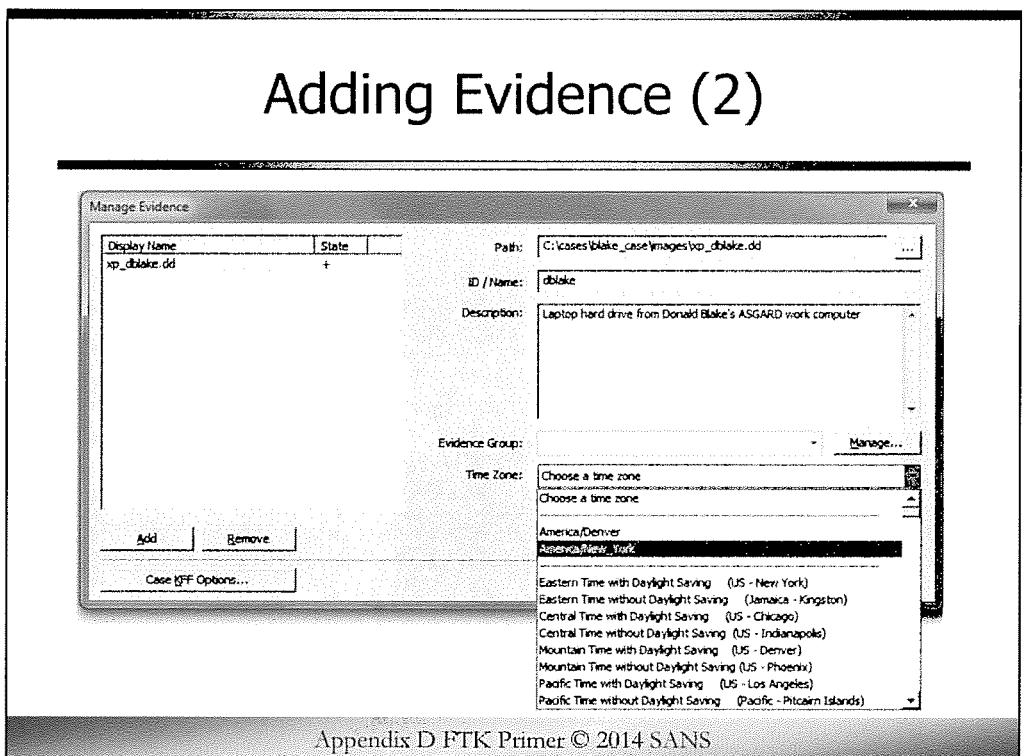
Once you click the add button you will have the option to choose what type of evidence you are adding to your case. Typically it is going to be an “**Acquired Image(s)**” or in large cases where you have several images in a directory, you have the option to select “All Images in Directory”. You could also add the “Contents of a Directory”, Individual File(s)”, or even a physical or logical drive (with a write block of course).

Select “Acquired Image(s)”, then click “OK” and navigate to the location where your image file is located.

C:\cases\blake_case\images\xp_db1ake.dd



Adding Evidence (2)



Appendix D FTK Primer © 2014 SANS

Once you have selected the evidence to be added and verified the path to the evidence in the “Path” field, you should give each item of evidence an ID or name in the ID/Name field.

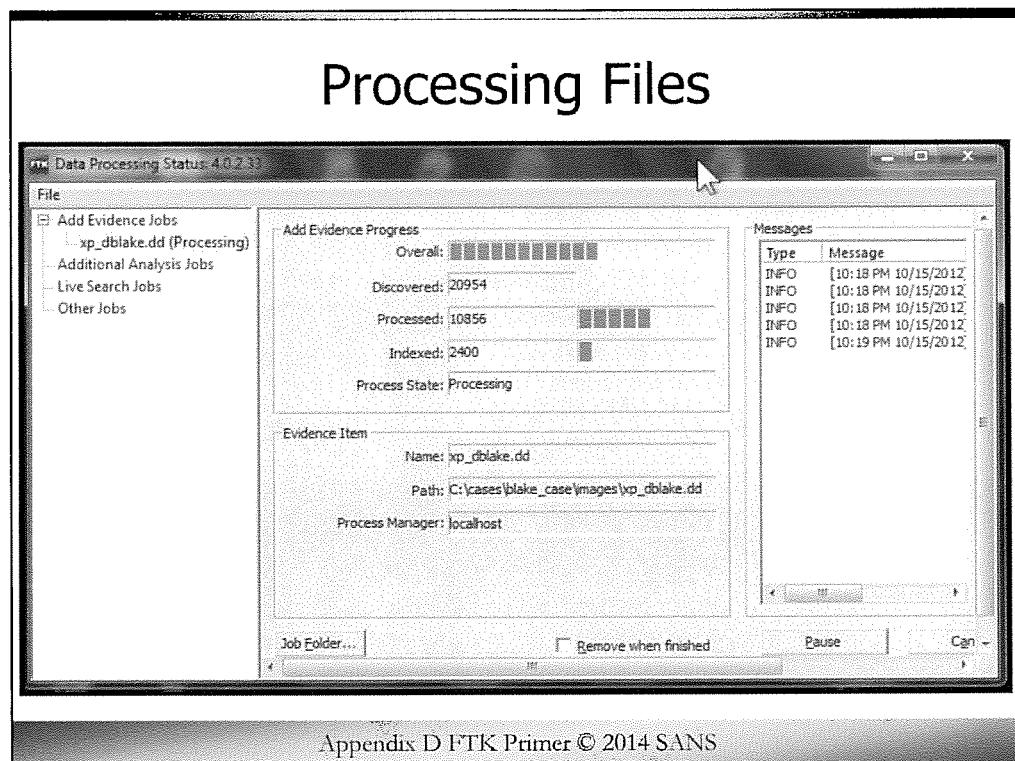
You can also add a description for each item of evidence that will be included in any FTK report generated.

With the Evidence Group feature, you can assign evidence items to different groups and share them between cases. We will not be assigning an evidence group for our purposes here.

The next step is to identify the time zone for each evidence item. This must be done with all evidence items and allows FTK to normalize all data in the index.

If you have multiple evidence items, you should consider selecting the Merge Index option. This will put all indexed evidence items in the same database. The only disadvantage to doing this is if you later decide to remove an evidence item from your case, the indexed database will still contain entries for items that were removed. If you conduct an index search after removing an evidence item you will get hits on items that were in the removed evidence item.

You also have the ability to configure KFF options for each item of evidence. By selecting “Case KFF Options...” we will be able to select only the KFF sets to run against each evidence item.

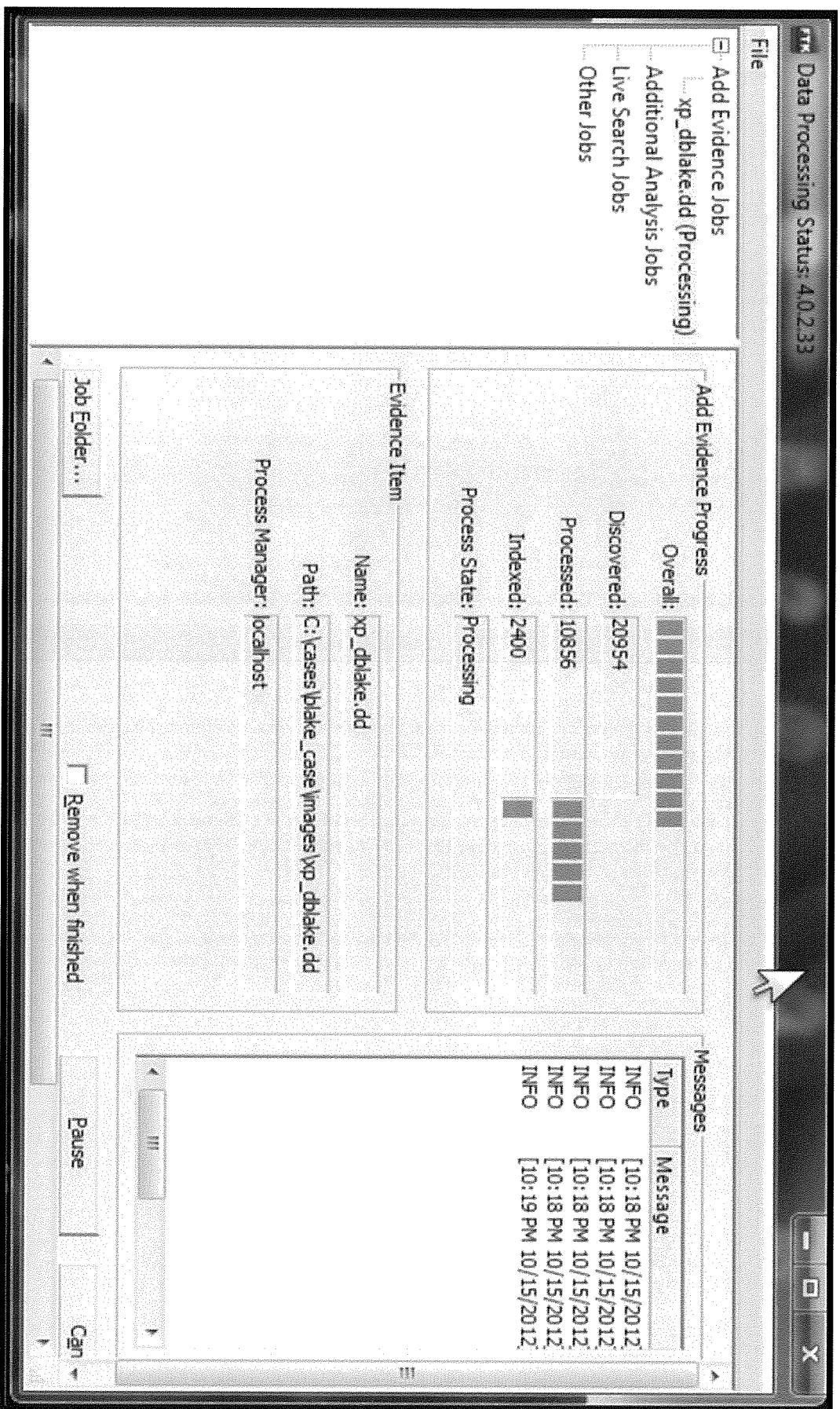


Appendix D FTK Primer © 2014 SANS

Get used to looking at this screen since it will be there for hours or even days depending on the size of your case and what processing options you selected.

With previous versions of FTK if something bad happened while a case was indexing you would typically have to start this whole indexing process over again. Current versions of FTK can pick back up where it left off if you have a crash or power failure.

Author note: Although FTK has improved the way it handles system crashes, etc., I still recommend reprocessing the entire case because there is just no assurance that a single file was not missed.



FTK Overview

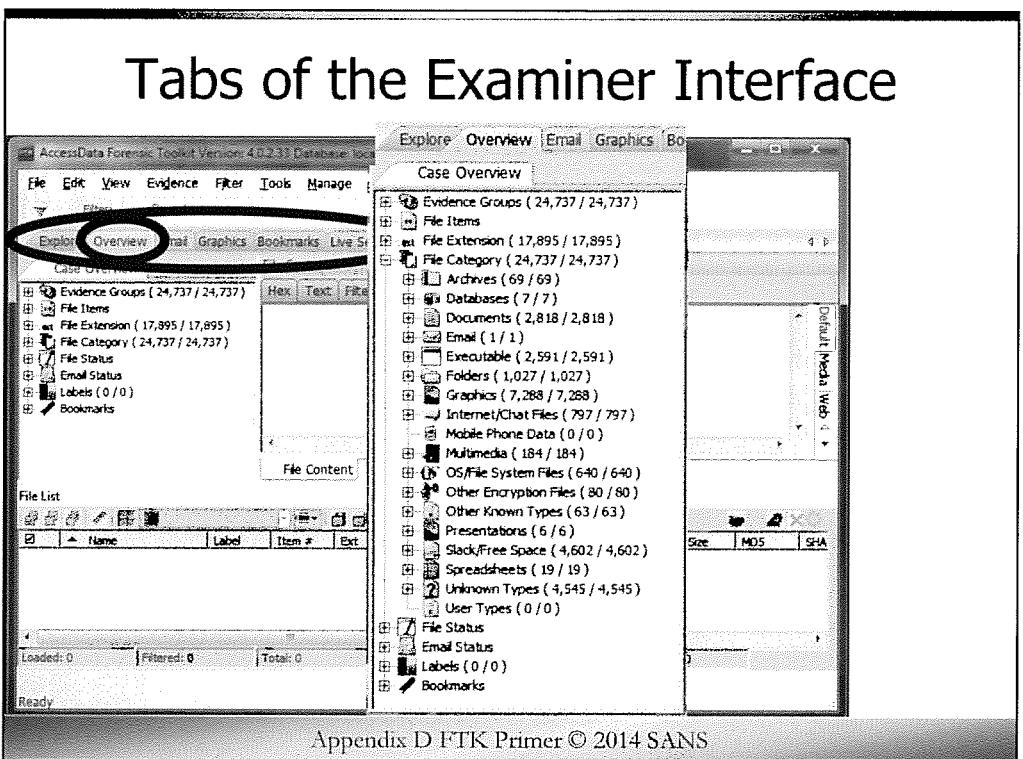
Case Setup

Features



Appendix D FTK Primer © 2014 SANS

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 (8) EIGHT tabs. We will be discussing each of these tabs briefly because you will be navigating through your analysis 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 (8) eight basic areas:

- Evidence Groups
- File Items
- File Extension
- File Category
- File Status
- E-mail Status
- Labels
- Bookmarks

AccessData Forensic Toolkit Version: 4.0.233 Database: localhost Case: Blake

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered -

File Content Properties Hex Interpretation

File List

<input checked="" type="checkbox"/>	Name	Label	Item #	Ext	Path
					Normal

Total: 0 Highlighted: 0 Checked: 0

Ready

Overview Tab Filter:

Evidence Groups (24,737 / 24,737)

File Items

.ext File Extension (17,895 / 17,895)

File Category (24,737 / 24,737)

Archives (69 / 69)

Databases (7 / 7)

Documents (2,818 / 2,818)

Email (1 / 1)

Executable (2,591 / 2,591)

Folders (1,027 / 1,027)

Graphics (7,288 / 7,288)

Internet/Chat Files (797 / 797)

Mobile Phone Data (0 / 0)

Multimedia (184 / 184)

OS/File System Files (540 / 540)

Other Encryption Files (80 / 80)

Other Known Types (63 / 63)

Presentations (6 / 6)

Slack/Free Space (4,602 / 4,602)

Spreadsheets (19 / 19)

Unknown Types (4,545 / 4,545)

User Types (0 / 0)

File Status

Email Status

Labels (0 / 0)

Bookmarks

Case Overview

File Manager...

Hex Text Filtered Natural

Evidence Groups (24,737 / 24,737)

File Items

.ext File Extension (17,895 / 17,895)

File Category (24,737 / 24,737)

Labels (0 / 0)

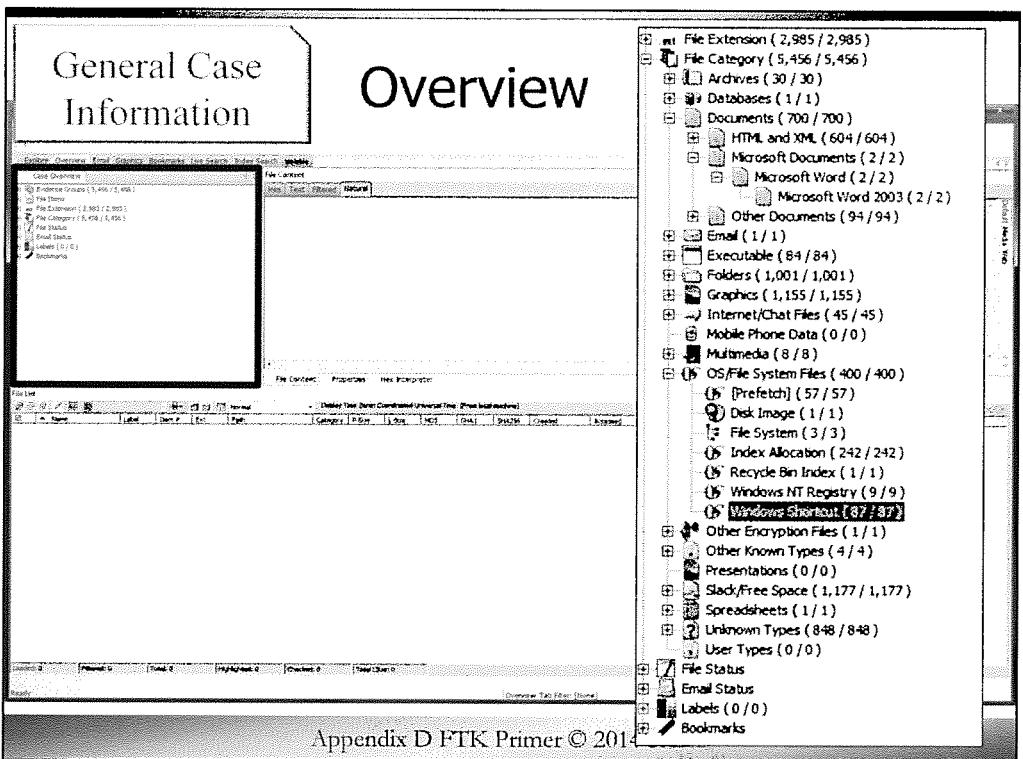
Bookmarks

File Status

Email Status

Labels (0 / 0)

Bookmarks



In the Overview Tab you will find your case organized in several different ways to help you quickly locate certain file types. It also shows you some basic information about your case. To name a few, it shows you:

The File Items lists the number of evidence items and files by whether they have been checked.

The File Extension list itemizes files by their extensions. The total number of files listed in this list will not equal the total number of items in the case as it does not include items such as file folders do not have extensions and are not listed here.

The File Category list organizes files by type, such as graphics, e-mail, documents, etc. and lists them in a tree view. You can create your own custom file categories and have them show up under this list by adding the file header and selecting the file category you want it to be listed under. You can create your custom file carver by selecting “Manage”, then “Carvers”, then “Manage Carvers...” from the menu bar of the FTK examiner interface.

The E-mail Status list organizes e-mail items by status such as E-mail Attachments, E-mail Reply, Forwarded E-mail and From E-mail (all items from an e-mail source, i.e., e-mail related)

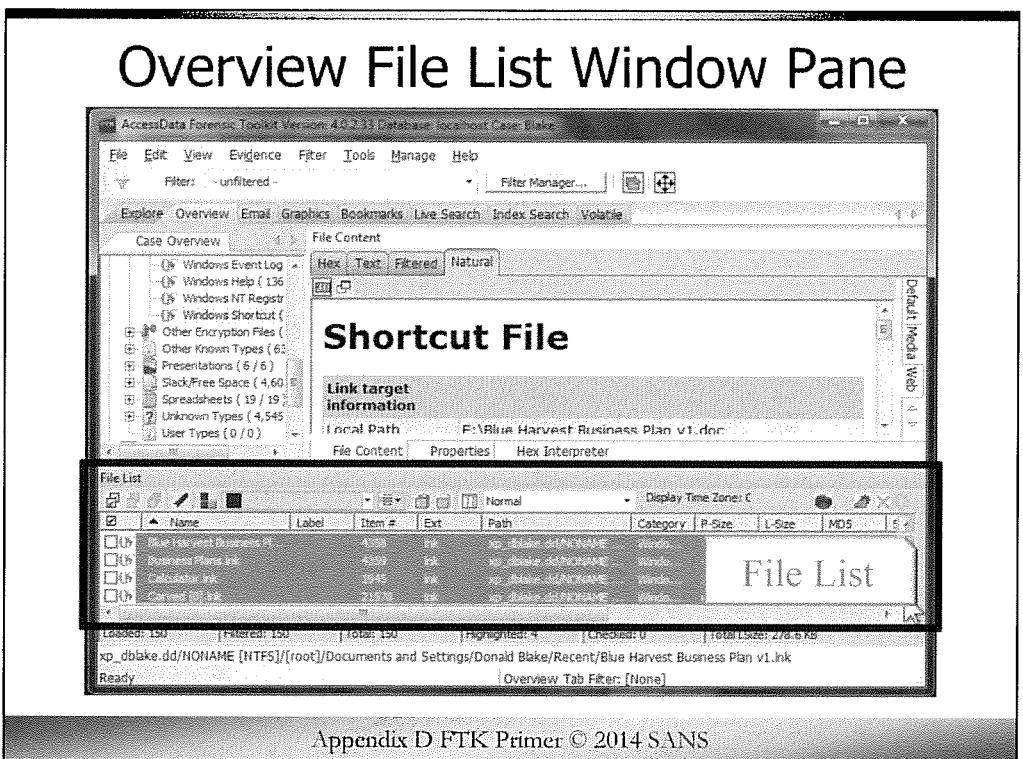
The Labels list shows all labels that have been applied to the evidence. You can create your own custom labels.

The Bookmarks container lists bookmarks as they are nested in the shared and the user-defined folders. Bookmarks are defined by the investigator as the case is being investigated and analyzed. Bookmarks are viewed from the Bookmarks Tab.

.ext File Extension (2,985 / 2,985)
.File Category (5,456 / 5,456)
Archives (30 / 30)
Databases (1 / 1)
Documents (700 / 700)
HTML and XML (604 / 604)
Microsoft Documents (2 / 2)
Microsoft Word (2 / 2)
Microsoft Word 2003 (2 / 2)
Other Documents (94 / 94)
Email (1 / 1)
Executable (84 / 84)
Folders (1,001 / 1,001)
Graphics (1,155 / 1,155)
Internet/Chat Files (45 / 45)
Mobile Phone Data (0 / 0)
Multimedia (8 / 8)
OS/File System Files (400 / 400)
[Prefetch] (57 / 57)
Disk Image (1 / 1)
File System (3 / 3)
Index Allocation (242 / 242)
Recycle Bin Index (1 / 1)
Windows NT Registry (9 / 9)
Windows Shortcut (87 / 87)
Other Encryption Files (1 / 1)
Other Known Types (4 / 4)
Presentations (0 / 0)
Slack/Free Space (1,177 / 1,177)
Spreadsheets (1 / 1)
Unknown Types (848 / 848)
User Types (0 / 0)
File Status
Email Status
Labels (0 / 0)
Bookmarks

The screenshot shows the Case Overview page with the following sections:

- Evidence Groups (5,456 / 5,456)**
 - File Items
 - File Extension (2,985 / 2,985)
 - File Category (5,456 / 5,456)
 - Archives (30 / 30)
 - Databases (1 / 1)
 - Documents (700 / 700)
 - Email (1 / 1)
 - Executable (84 / 84)
 - Folders (1,001 / 1,001)
 - Graphics (1,155 / 1,155)
 - Internet/Chat Files (45 / 45)
 - Mobile Phone Data (0 / 0)
 - Multimedia (8 / 8)
 - OS/File System Files (400 / 400)
 - Other Encryption Files (1 / 1)
 - Other Known Types (4 / 4)
 - Presentations (0 / 0)
 - Slack/Free Space (1,177 / 1,177)
 - Spreadsheets (1 / 1)
 - Unknown Types (848 / 848)
 - User Types (0 / 0)
- File Sets**
- Email Status**
- Labels (0 / 0)**
- Bookmarks**



Across the bottom of the Overview tab window you will find the File List area.

If you click on any of the file lists in the above Case Overview section, all files of that particular list will be listed here. You can scroll through, review, bookmark, or export these items quickly and easily.

By clicking on the “File Category”, then “OS / File System Files”, then “Windows Shortcut”, all Windows Link Files would be displayed in the File List section.

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

AccessData Forensic Toolkit Version: 4.0.2.33 Database: local\host Case: Blake

File Edit View Evidence Filter Tools Manage Help

Filter: - unfiltered - Filter Manager...

Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile

Case Overview

- Windows Event Log (136)
- Windows Help (136)
- Windows NT Registry (136)
- Windows Shortcut (136)
- Other Encryption Files (6)
- Presentations (6 / 6)
- Slack/Free Space (4,60)
- Spreadsheets (19 / 19)
- Unknown Types (4,545)
- User Types (0 / 0)

Shortcut File

Link target information

Local Path F:\Blue Harvest Business Plan v1.doc

File Content Properties Hex Interpreter

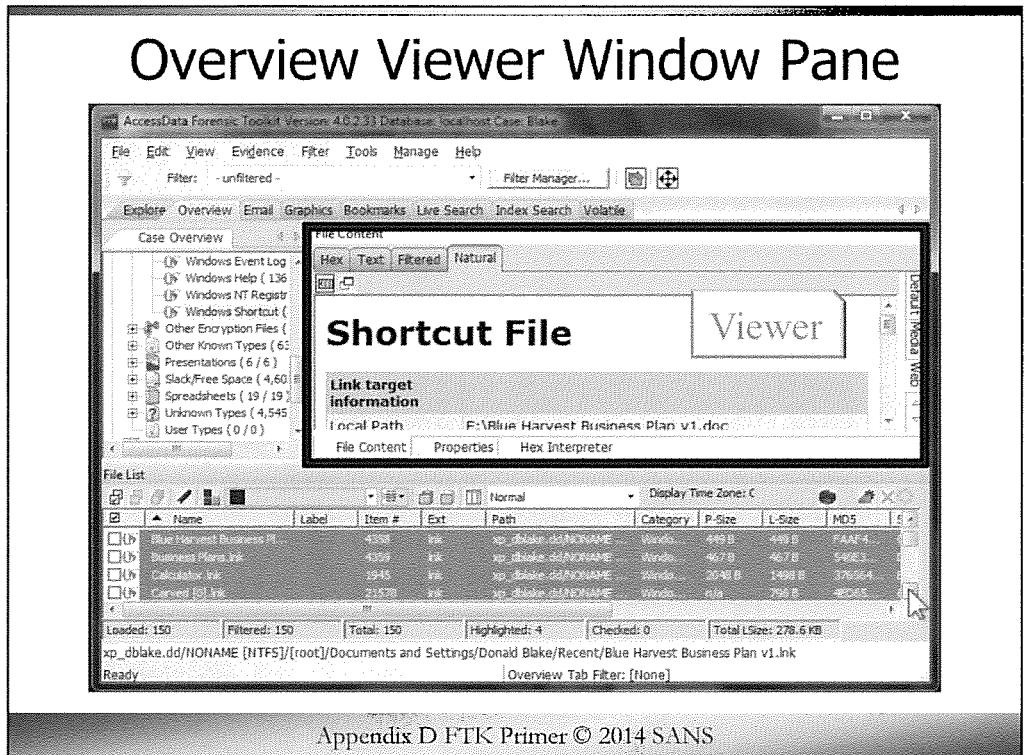
Display Time Zone: C

Selected	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	S...
<input checked="" type="checkbox"/>	Blue Harvest Business Pl...		4353	lnk	xp_dblake.dd/NONAME...	Windo...	449 B	449 B	FAAF4...	
<input checked="" type="checkbox"/>	Business Plans.lnk		4359	lnk	xp_dblake.dd/NONAME...	Windo...	467 B	467 B	546E3...	
<input checked="" type="checkbox"/>	Calculator.lnk		1945	lnk	xp_dblake.dd/NONAME...	Windo...	2048 B	1498 B	376564...	
<input checked="" type="checkbox"/>	Carved [0].lnk		21573	lnk	xp_dblake.dd/NONAME...	Windo...	n/a	796 B	4ED65...	

Loaded: 150 Filtered: 150 Total: 150 Highlighted: 4 Checked: 0 Total LSize: 278.6 KB

xp_dblake.dd/NONAME [NTFS]\[root]\Documents and Settings\Donald Blake\Recent\Blue Harvest Business Plan v1.lnk

Ready Overview Tab Filter: [None]



Appendix D FTK Primer © 2014 SANS

At the top right of your screen you will find the Viewer Window. FTK uses Stellent Outside In technology (now owned by Oracle) or Internet Explorer as the viewing engines 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.

Ref:

<http://www.oracle.com/us/technologies/embedded/025613.htm>

AccessData Forensic Toolkit Version: 4.0.2.33 Database: localhost Case: Blake

File Edit View Evidence Filter Tools Manage Help

Filter: - unfiltered -

File Content

Case Overview

- Windows Event Log (136)
- Windows Help (136)
- Windows NT Registry (136)
- Windows Shortcut (136)
- Other Encryption Files (6)
- Presentations (6 / 6)
- Slack/Free Space (4,60)
- Spreadsheets (19 / 19)
- Unknown Types (4,545)
- User Types (0 / 0)

Shortcut File

Viewer

Link target information

Local Path: F:\R\H\ Blue Harvest Business Plan v1.doc

File Content Properties Hex Interpreter

Display Time Zone: C

File List

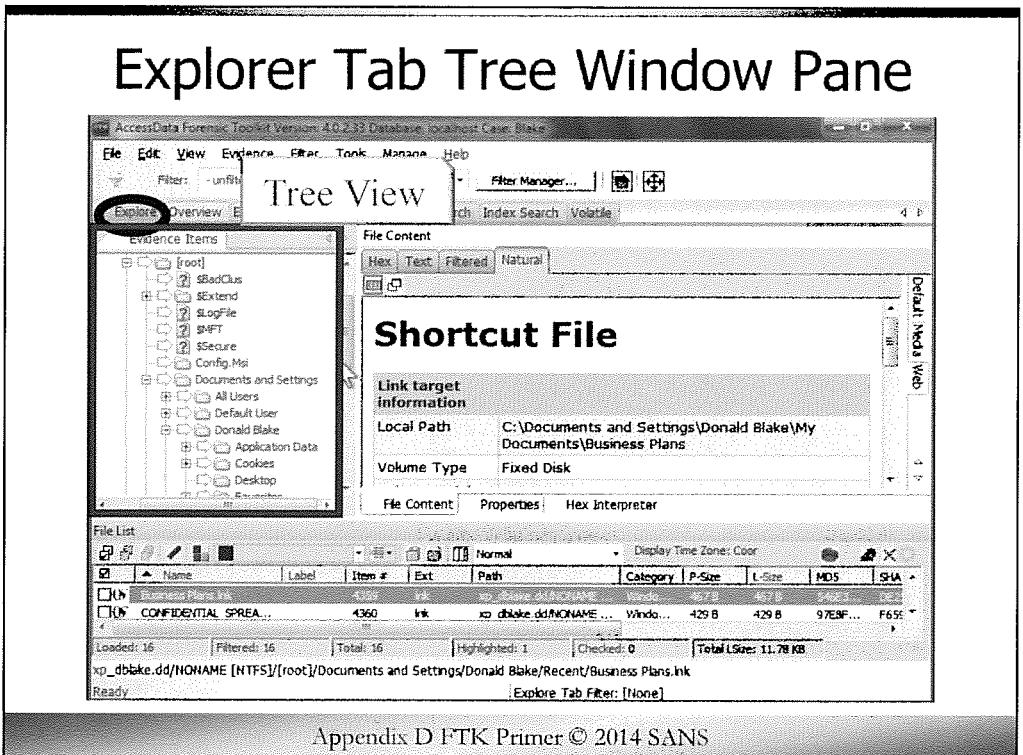
Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1
Blue Harvest Business Pl...	4358	ink	xp_dblake.dd/NONAME...	Window...	449 B	449 B	F4AFA4...	0
Business Plans.ink	4359	ink	xp_dblake.dd/NONAME...	Window...	467 B	467 B	546E3...	1
Calculator.ink	1945	ink	xp_dblake.dd/NONAME...	Window...	2048 B	1498 B	376564...	2
Carved [0].ink	21578	ink	xp_dblake.dd/NONAME...	Window...	n/a	796 B	4E065...	3

Loaded: 150 Filtered: 150 Total: 150 Checked: 0 Total LSize: 278.6 KB

xp_dblake.dd/NONAME [NTFS]/[root]/Documents and Settings/Donald Blake/Recent/Blue Harvest Business Plan v1.ink

Ready

Overview Tab Filter: [None]



Next, let's click on the Explorer Tab found across the top of FTK to the left 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 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 arrow adjacent to the directory. This arrow is called the “quick picks” icon and is a type of filter that allows the selection of multiple directories so you can focus your analysis of specific content.

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 your quick picks settings.

AccessData Forensic Toolkit Version: 4.0.2.33 Database: localhost Case: Blake

File Edit View Evidence Filter Tools Manage Help

Filter: -unfilter

Tree

Evidence Items

Explore Overview E

[root] \$BadClus \$Extend \$LogFile \$MFT \$Secure Config.Msi Documents and Settings All Users Default User Donald Blake Application Data Cookies Desktop Environment

File Content Filtered Natural

Default Media Web

File Content Index Search Volatile

Shortcut File

Link target information

Local Path C:\Documents and Settings\Donald Blake\My Documents\Business Plans

Volume Type Fixed Disk

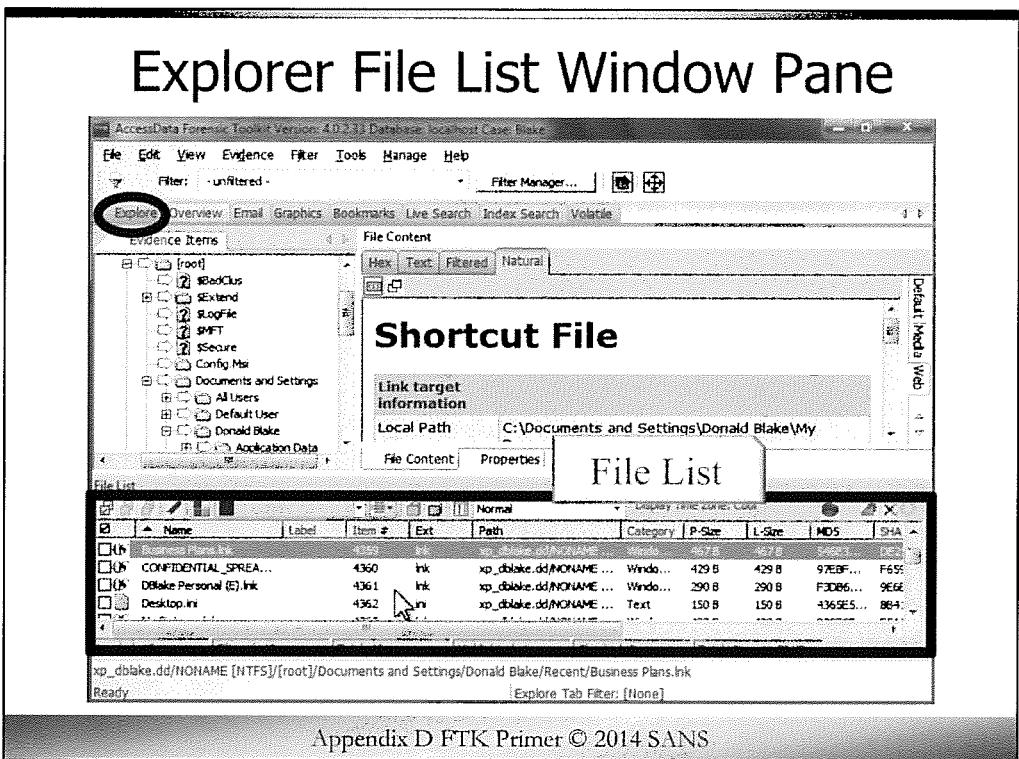
File Content Properties Hex Interpreter

File List

	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA
<input checked="" type="checkbox"/>	BusinessPlans.lnk		4359	Ink	xp_dblake.dd/NONAME...\\Windows\\457B	Windows	457B	457B	SAGE3...	DE2...
<input checked="" type="checkbox"/>	CONFIDENTIAL SPREA...		4360	Ink	xp_dblake.dd/NONAME...\\Windows\\429B	Windows	429B	429B	97E8F...	F65...
										Loaded: 16 Filtered: 1 Total: 16 Checked: 0 Total LSize: 11.78 KB

xp_dblake.dd/NONAME [NTFS]/[root]/Documents and Settings/Donald Blake/Recent/Business Plans.lnk

Ready Explore Tab Filter: [None]



Appendix D FTK Primer © 2014 SANS

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 if the “**quick picks**” arrow is selected its subdirectories 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.

AccessData Forensic Toolkit Version: 4.0.233 Database: localhost Case: Blake

File Edit View Evidence Filter Tools Manage Help

Filter: - unfiltered - Filter Manager...

Evidence Items

File Content

Hex Text Filtered Natural

File List

Shortcut File

Link target information

Local Path C:\Documents and Settings\Donald Blake\My

Properties

File Content

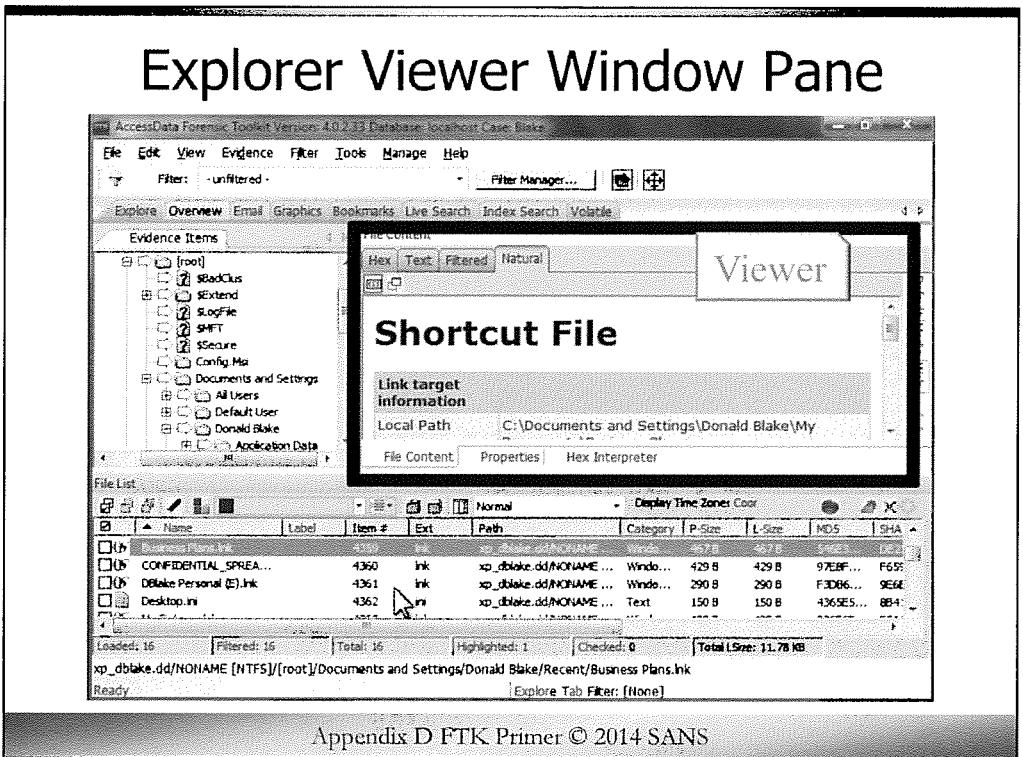
File List

	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA
<input checked="" type="checkbox"/>	Business Plans.lnk		4359	lnk	XP_DBLAKE\NONAME\...	Word...	457B	457B	54533...	D32...
<input type="checkbox"/>	CONFIDENTIAL_SPREA...		4360	lnk	XP_DBLAKE\dd\NONAME...	Window...	429B	429B	97E8F...	F65C
<input type="checkbox"/>	DBlake Personal (E).lnk		4361	lnk	XP_DBLAKE\dd\NONAME...	Window...	290B	290B	F3DB6...	9E6E
<input type="checkbox"/>	Desktop.ini		4362	ini	XP_DBLAKE\dd\NONAME...	Text	150B	150B	4365E5...	884...

xp_dblake.dd/NONAME [NTFS]/[root]/Documents and Settings/Donald Blake/Recent/Business Plans.lnk

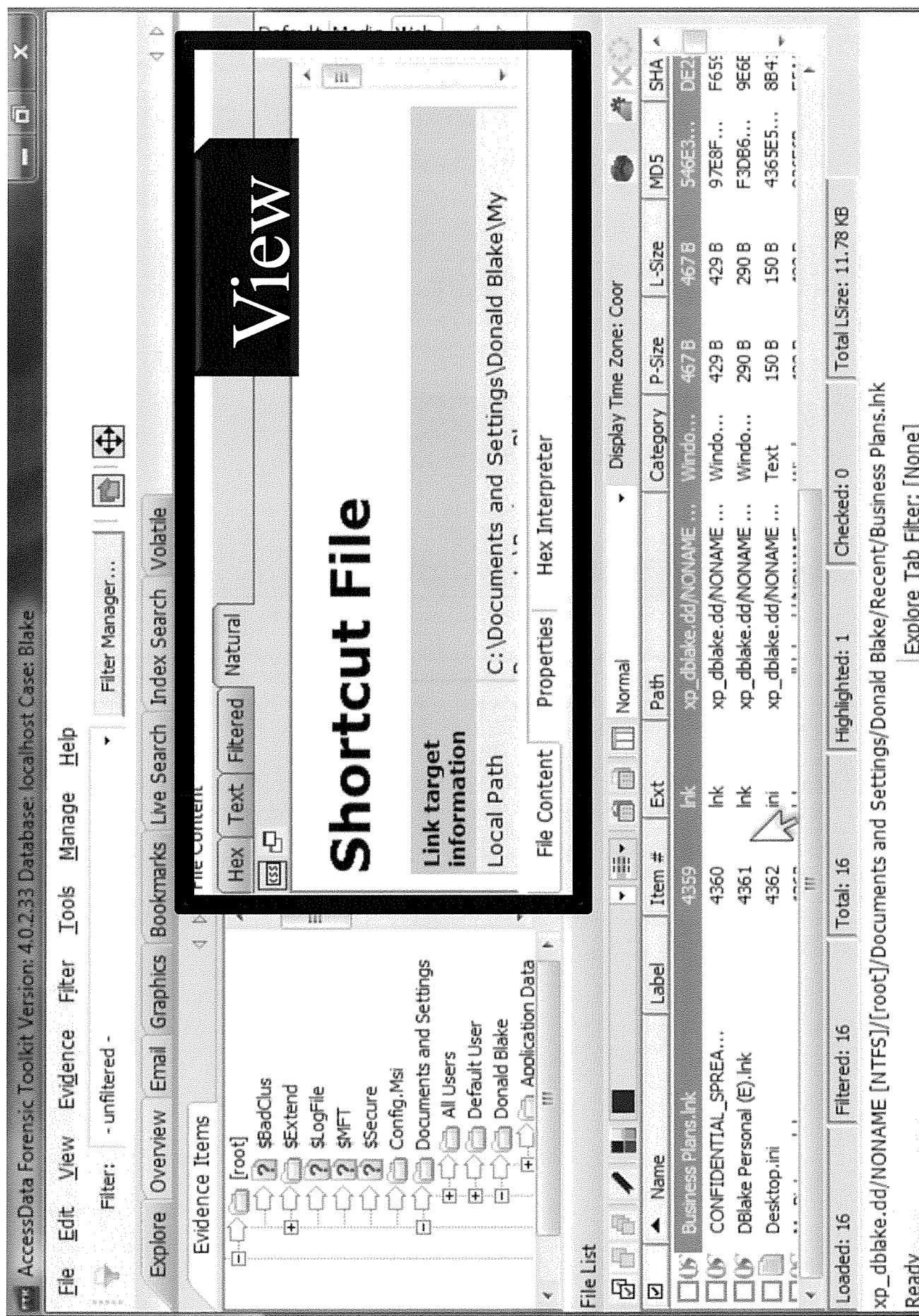
Explore Tab Filter: [None]

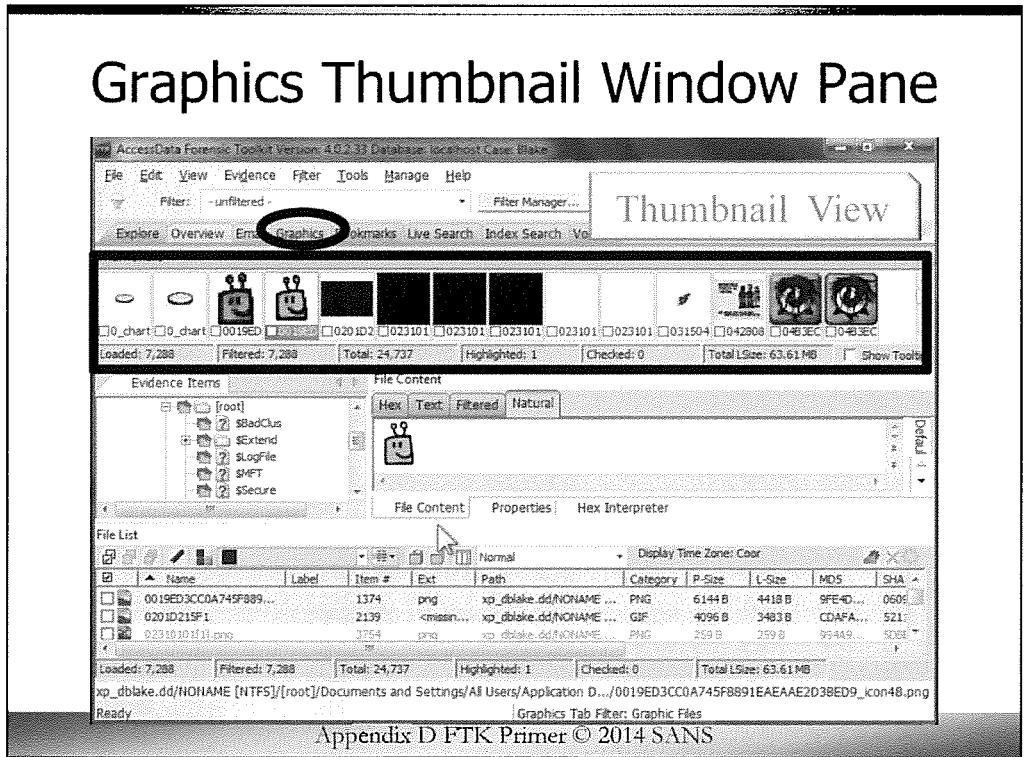
Ready



Appendix D FTK Primer © 2014 SANS

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, 100 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. You can even completely detach each viewer pane from FTK by clicking and dragging the area above each window pane. If you are like me, when you have to review a lot of graphics, you spread the thumbnail pane across multiple large monitors so you can quickly triage or review them. By detaching each window pane you can arrange each tab in a way that best suits you. The window pane placement is specific to each tab so when you move back to the explorer tab, it will look just like it did when it was last active. To reset all your window panes back to their default location, from the menu bar select “View”, then “Tab Layout”, then “Reset to Default”.

AccessData Forensic Toolkit Version: 4.0.2.33 Database: localhost Case: Blake

File Edit View Evidence Filter Tools Manage Help

Filter: - unfiltered -

Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile

0_chart 0_chart 0019ED 0201D2 023101 023101 023101 023101 023101 023101 Total: 24,737 Checked: 0

Loaded: 7,288 Filtered: 7,288

Evidence Items [root] 2 \$BadClus 2 \$Extend 2 \$LogFile 2 \$MFT 2 \$Secure

File Content Hex Text Filtered Natural

File List

	Name	Label	Item #	Ext	Path	Category	F-Size	L-Size	MD5	SHA
<input checked="" type="checkbox"/>	0019ED3CC0A745F889...		1374	png	xp_dblake.dd\nONAME...	PNG	6144B	4418B	9FE4D...	060c...
<input type="checkbox"/>	0201D215F1		2139	<missin...	xp_dblake.dd\nONAME...	GIF	4096B	3483B	CDAFA...	5211...
<input type="checkbox"/>	02310101[1].png		3754	png	xp_dblake.dd\nONAME...	PNG	259B	259B	994A9...	5C1E...

Total L-Size: 63.61 MB

Checked: 0

xp_dblake.dd\nONAME [NTFS]/[root]/Documents and Settings/All Users/Application D.../0019ED3CC0A745F8891EAEEAE2D3BED9_Icon48.png

Graphics Tab Filter: Graphic Files

Ready

Thumbnails

--	--	--	--	--	--	--	--	--	--	--	--

Loaded: 7,288 Filtered: 7,288 Total: 24,737 Highlighted: 1 Checked: 0 Total LSize: 63.61 MB Show Tooltip

File List

<input type="checkbox"/>	Name	Item #	Ext	Path
<input type="checkbox"/>	HelpCenter.bmp	10187	bmp	xp_dilate.dd/NONAME
<input type="checkbox"/>	HelpCenter.gif	10188	gif	xp_dilate.dd/NONAME
<input type="checkbox"/>	helpdoc.gif	10101	gif	xp_dilate.dd/NONAME
<input type="checkbox"/>	HelpSee_line.gif	10211	gif	xp_dilate.dd/NONAME
<input type="checkbox"/>	hero-work_20090101...png	4240	png	xp_dilate.dd/NONAME
<input type="checkbox"/>	hero-waiting200901...png	3784	png	xp_dilate.dd/NONAME
<input type="checkbox"/>	hero-waiting200901...png	16070	png	xp_dilate.dd/NONAME
<input type="checkbox"/>	hero-secondkey11.jpg	16059	jpg	xp_dilate.dd/NONAME
<input type="checkbox"/>	hbeam.cur	6900	cur	xp_dilate.dd/NONAME
<input type="checkbox"/>	hide.chat.gif	10189	gif	xp_dilate.dd/NONAME
<input type="checkbox"/>	hidr.cur	4066	cur	xp_dilate.dd/NONAME

Loaded: 7,288 Filtered: 7,288 Total: 24,737 Highlighted: 1 Checked: 0 Total Size: 63.61 MB

RECYCLER

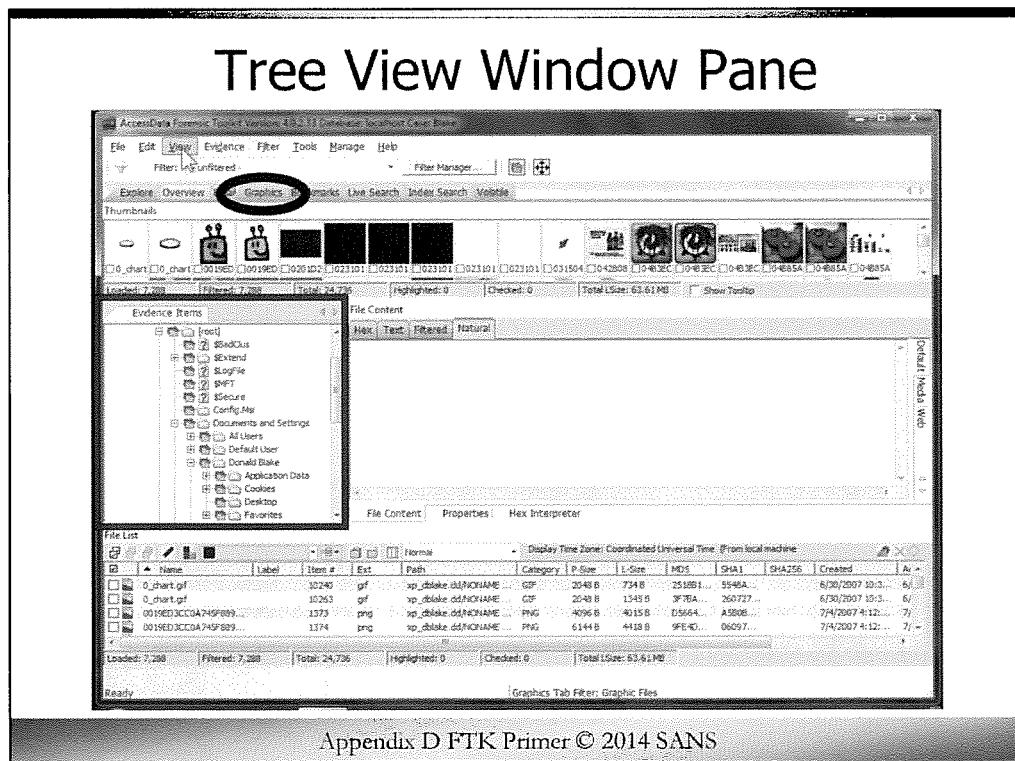
System Volume Information

WINDOWS

File Content

Default Media Web

File Content Properties Hex Interpreter



Appendix D FTK Primer © 2014 SANS

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 quick picks icon on that directory.

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 quick picks icon.

AccessData Forensic Toolkit Version 4.0.233 Database: localhost Case: Blake

File Edit View Evidence Filter Tools Manage Help

Filter: A unfiltered - Filter Manager...  

Explore Overview Real Graphics Bookmarks Live Search Index Search Volatile

thumbnails

Loaded: 7.288 Filtered: 7.288 Total: 24.736 Highlighted: 0 Checked: 0 Total LSize: 63.61MB Show Tooltip

Evidence Items

[root]                     

File Content Hex Text Filtered Natural

File List

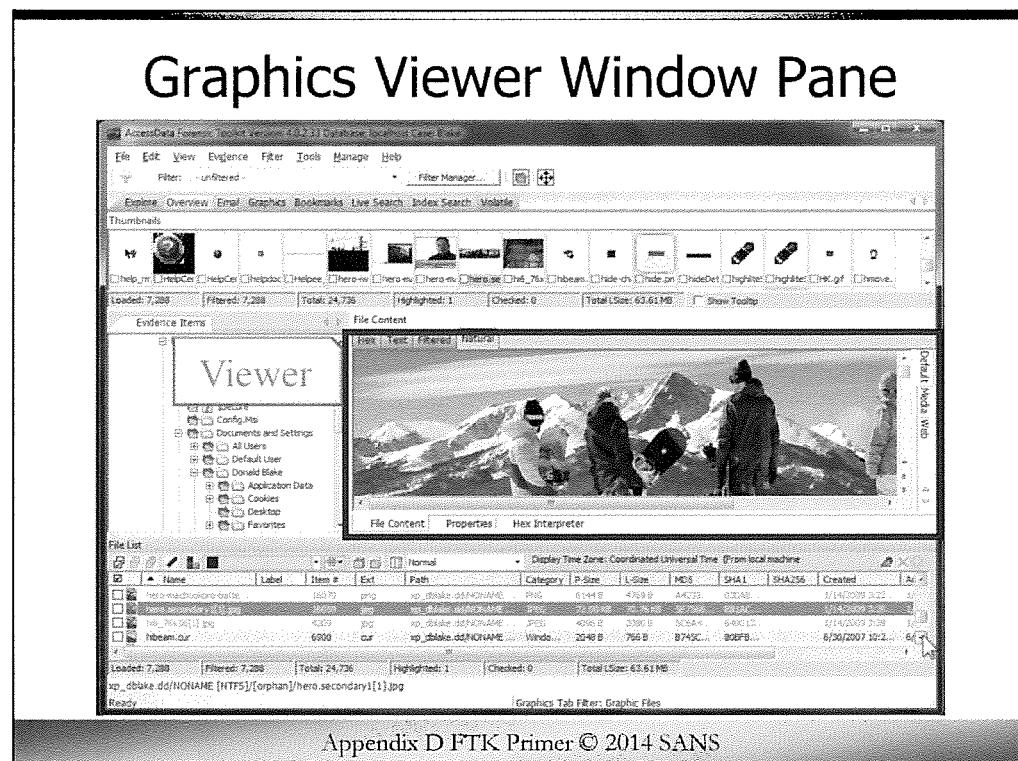
Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	At
0_chart.gif		10240	gif	xp_ddisk.dd/NONAME...	GIF	2048 B	734 B	251081...	5548A...	6130/2007 10:3...	6/	
0_chart.gif		10283	gif	xp_ddisk.dd/NONAME...	GIF	2048 B	1345 B	3F78A...	260727...	6/30/2007 10:3...	6/	
0019ED3CC0A745F899...		1373	png	xp_ddisk.dd/NONAME...	PNG	4096 B	4015 B	D564...	A3B0B...	7/4/2007 4:12...	7/	
0019ED3CC0A745F899...		1374	png	xp_ddisk.dd/NONAME...	PNG	6144 B	4418 B	9FE4D...	06097...	7/4/2007 4:12...	7/	

Default Media Web

Loaded: 7.288 Filtered: 7.288 Total: 24.736 Highlighted: 0 Checked: 0 Total LSize: 63.61MB

Graphics Tab Filter: Graphic Files

Ready



Appendix D FTK Primer © 2014 SANS

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.

AccessData Forensic Toolkit Version 4.0.2.33 Database:localhost Case: Blake

File Edit View Evidence Filter Tools Manage Help

Filter: - unfiltered - Filter Manager...

Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile

Thumbnails

Loaded: 7,288 Filtered: 7,288 Total: 24,736 Highlighted: 1 Checked: 0 Total LSize: 63.61MB Show Tooltip

Evidence Items

Viewer

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	I-Size	MD5	SHA1	SHA256	Created	Al.
hero-macbookpro-batt...		16070	png	xp_dblake.dd[NONAME...]	PNG	6144B	4769B	A4235...	03043...		1/14/2009 3:22...	1
herosecondary1.jpg		16059	JPG	xp_dblake.dd[NONAME...]	JPEG	72.00K	72.00K	SE7556...	2814C...		1/14/2009 3:20...	1
hero_7656[1].jpg		4209	JPG	xp_dblake.dd[NONAME...]	JPEG	4956B	2080B	SC6A4...	649013...		1/14/2009 3:39...	1
hibeam.cur		6900	cur	xp_dblake.dd[NONAME...]	Windo...	2048B	766B	B745C...	808FB...		6/30/2007 10:2...	6

Loaded: 7,288 Filtered: 7,288 Total: 24,736 Highlighted: 1 Checked: 0 Total LSize: 63.61MB

xp_dblake.dd/NONAME [NTFS]/orphan]/hero.secondary1.jpg

Ready

Graphics Tab Filter: Graphic Files



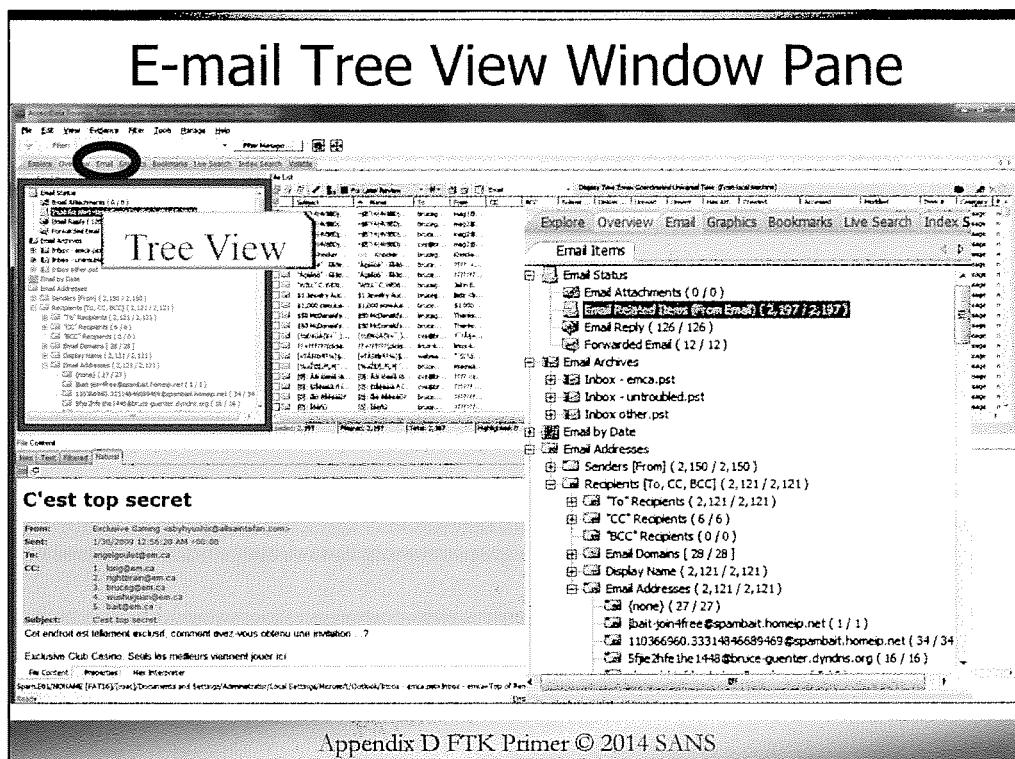
At the very bottom you will find the **File List** window.

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).

The screenshot shows the AccessData Forensic Toolkit interface. The top menu bar includes File, Edit, View, Evidence, Filter, Tools, Manage, Help, Filter Manager..., and several icons. The left sidebar has tabs for Explore, Overview, Email, Graphics, Bookmarks, Live Search, Index Search, and Volatile. The main area has tabs for Thumbnails, Evidence Items, and File Content. The Evidence Items tab is active, displaying a tree view of file system contents under 'root'. The File Content tab shows a large preview image of a person in a dynamic pose, with tabs for Hex, Text, Filtered, and Natural. The bottom section is titled 'File List' and contains a table of file details:

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	At
hero-macbookpro-batt...		16070	png	xp_dblake dd NONAME ...	PIK	61448	4789 B	A44235...	030AB...	11142009 3:22...	1/14/2009 3:22...	1
herosecondary1[1].jpg		16058	jpg	xp_dblake dd NONAME ...	JPG	72,00 KB	70,76 KB	37356...	E81AC...	11142009 3:22...	1/14/2009 3:22...	1
hbeam.jpg		4209	jpg	xp_dblake dd NONAME ...	JPEG	4096 B	2030 B	5C6A4...	649013...	11142009 3:30...	1/14/2009 3:30...	1
hbeam.cur		6900	cur	xp_dblake dd NONAME ...	Windo...	2048 B	766 B	8745C...	808E6...	11142009 3:30...	1/14/2009 3:30...	1

The bottom navigation bar includes Default, Media, and Web.



Appendix D FTK Primer © 2014 SANS

Go to the top again and click on the **E-MAIL** tab.

When you talk to people who do a lot of computer forensics, almost everyone will agree that FTK processes and displays e-mail better than most of the other forensic programs. The E-mail tab displays e-mail messages and attachments in a coded HyperText Markup Language (HTML) format.

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

The E-mail tree lists message counts, AOL, PST, NSF, MBOX, and several other archive formats.

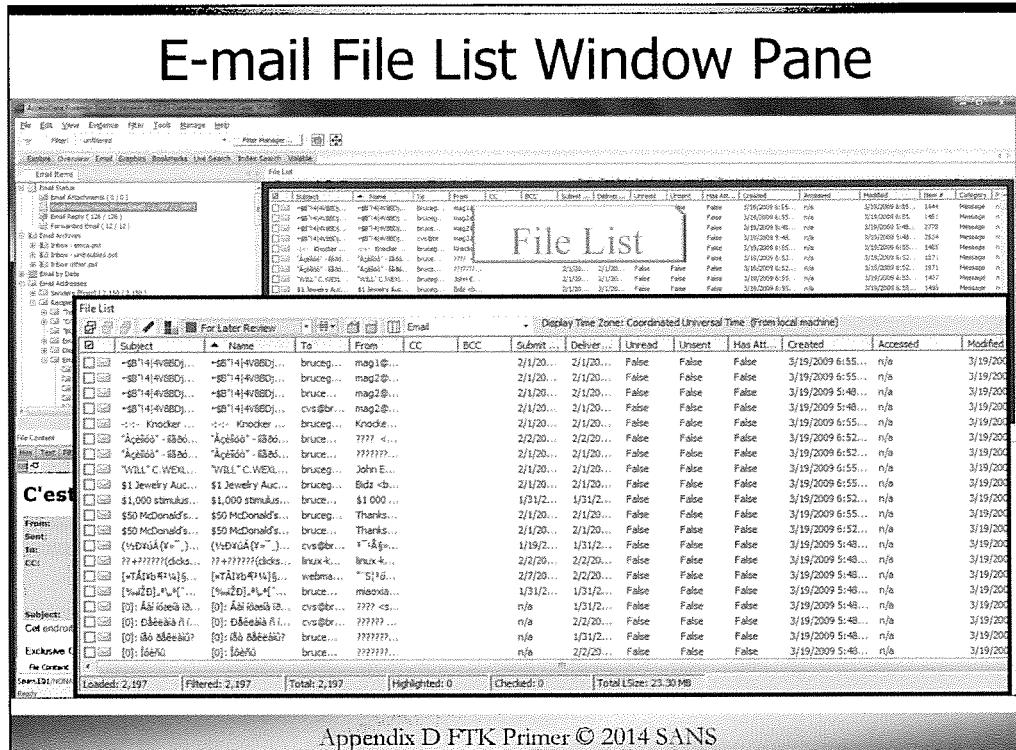
With FTK 4, e-mail items tree view contains two new groups: E-mail By Date (organized by year, month, then date, for both submitted and delivered); and E-mail Addresses (organized by senders, recipients, e-mail domain, display name, and e-mail addresses). This is a great way to quickly look for all e-mails from a particular domain or specific e-mail address contained in an e-mail archive.

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

- [Explore](#)
- [Overview](#)
- [Email](#)
- [Graphics](#)
- [Bookmarks](#)
- [Live Search](#)
- [Index S](#)

Email Items

- [Email Status](#)
- [Email Attachments \(0 / 0\)](#)
- [Email Related Items \(From Email\) \(2,197 / 2,197\)](#)
- [Email Reply \(126 / 126 \)](#)
- [Forwarded Email \(12 / 12 \)](#)
- [Email Archives](#)
- [Inbox - emca.pst](#)
- [Inbox - untroubled.pst](#)
- [Inbox other.pst](#)
- [Email by Date](#)
- [Email Addresses](#)
- [Senders \[From\] \(2,150 / 2,150 \)](#)
- [Recipients \[To, CC, BCC\] \(2,121 / 2,121 \)](#)
- ["To" Recipients \(2,121 / 2,121 \)](#)
- ["CC" Recipients \(6 / 6 \)](#)
- ["BCC" Recipients \(0 / 0 \)](#)
- [Email Domains \(28 / 28 \)](#)
- [Display Name \(2,121 / 2,121 \)](#)
- [Email Addresses \(2,121 / 2,121 \)](#)
- [{none} \(27 / 27 \)](#)
- [lball-join4free@spambait.homeip.net \(1 / 1 \)](#)
- [110366950.33314846689469@spambait.homeip.net \(34 / 34 \)](#)
- [5fjeZhfeIhe1448@bruce-guentner.dyndns.org \(16 / 16 \)](#)

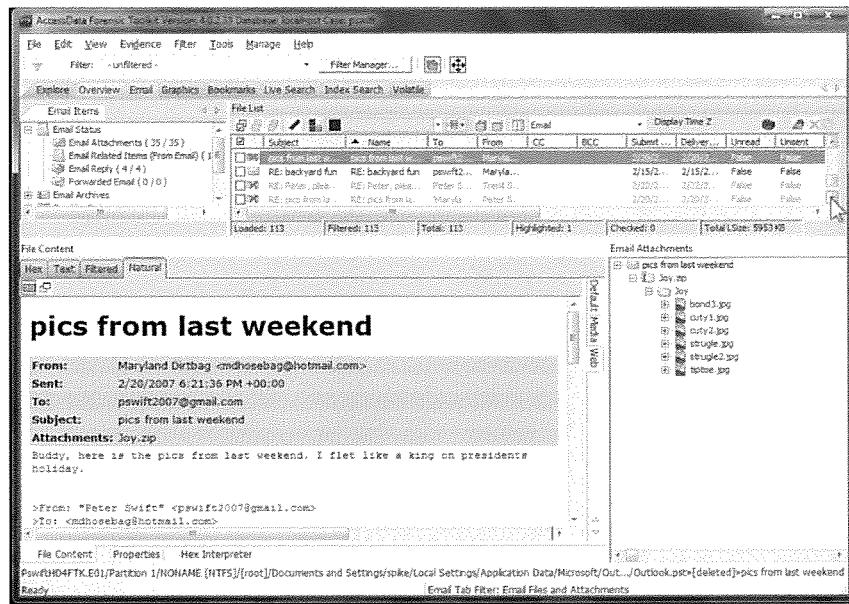


To the right of the Tree View is where you will find all the messages for the selected list in the tree view.

You will notice that the column headings are different in the e-mail tab. By default in the file list window you will see the subject line of the e-mail; the name; To, From, CC, and BCC e-mail fields; submitted date; delivered date; current status of the unread and unsent flags and if the message has an attachment. Several additional fields are also available and can be configured to display in the file view pane in any order the examiner desires.

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

E-mail Viewer Window Pane

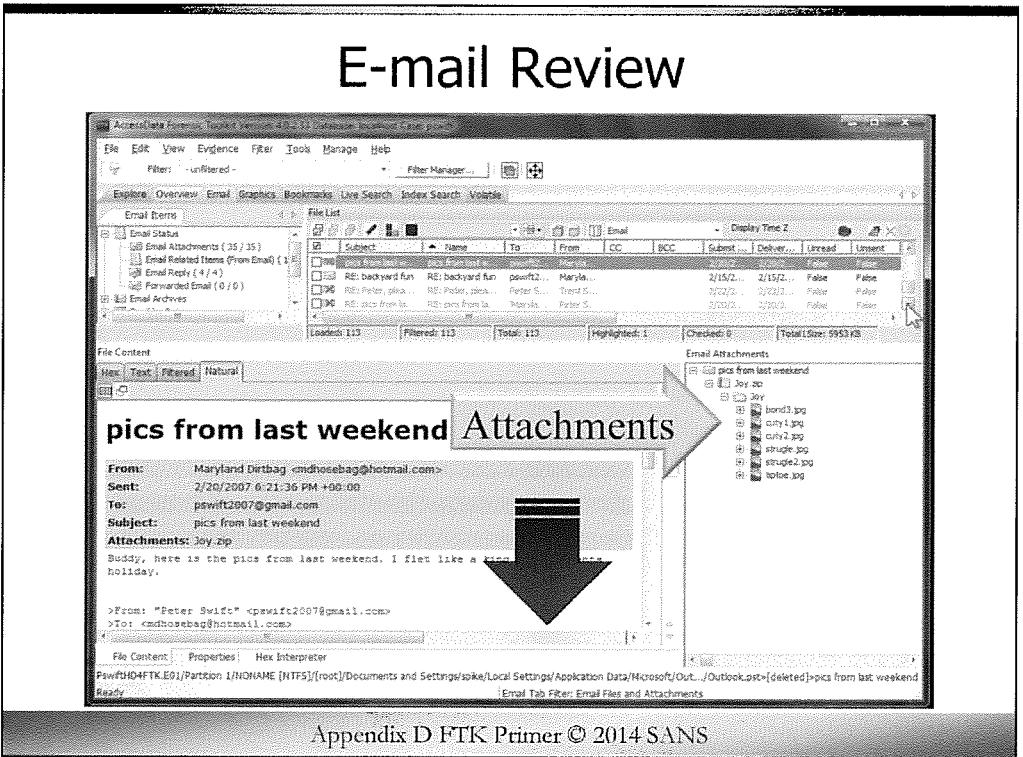


Appendix D FTK Primer © 2014 SANS

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 ...



Appendix D FTK Primer © 2014 SANS

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.

AccessData Forensic Toolkit Version: 4.0.2.33 Database: localhost\Case1.pnw4

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered - Filter Manager...

Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile

Email Items

Email Status

File List

#	Subject	Name	To	From	CC	BCC	Submit...	Delivery...	Unread	Unsent
1	pics from last weekend	pswift2...	Maryla...					2/20/2...	2/20/2...	False
2	RE: backyard fun	pswift2...	Maryla...					2/15/2...	2/15/2...	False
3	RE: Peter, please...	Peter S...	Trent S...					2/22/2...	2/22/2...	False
4	RE: pics from la...	Maryla...	Peter S...					2/20/2...	2/20/2...	False

Loaded: 113 Filtered: 113 Total: 113 Highlighted: 1 Checked: 0 Total Size: 5953KB

Email Attachments

- pics from last weekend
- Joy.zip
- Joy
- bond3.jpg
- cute1.jpg
- cute2.jpg
- striggle.jpg
- striggle2.jpg
- tiptoe.jpg

File Content

Hex Text Filtered Natural

pics from last weekend

Attachments

From: Maryland Dirtbag <mdhosebag@hotmail.com>
Sent: 2/20/2007 6:21:36 PM +00:00
To: pswift2007@gmail.com
Subject: pics from last weekend
Attachments: Joy.zip

Buddy, here is the pics from last weekend. I file like a ~~king~~ holiday.

>From: "Peter Swift" <pswift2007@gmail.com>
>To: <mdhosebag@hotmail.com>

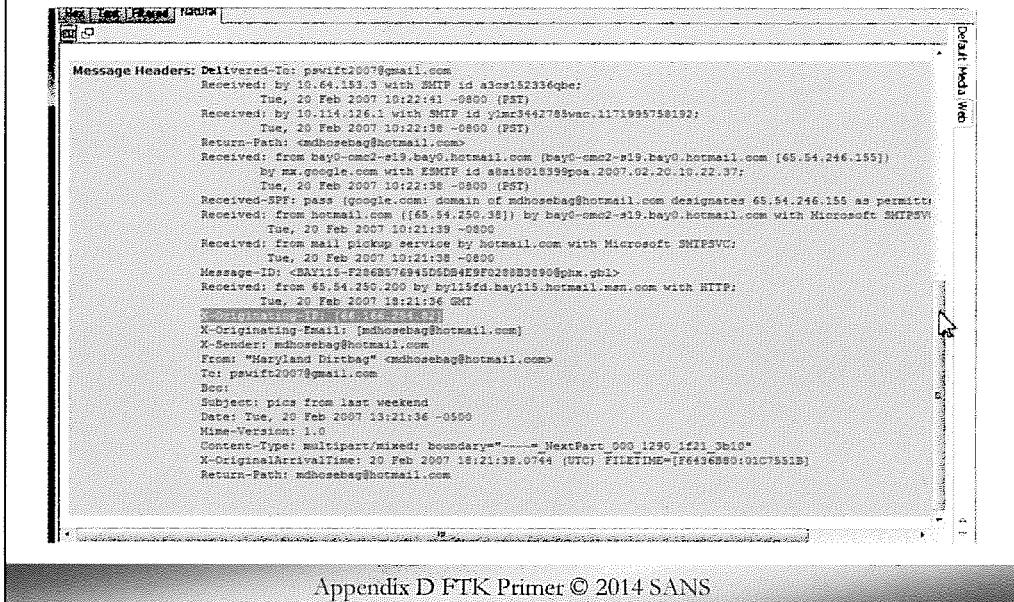
File Content Properties Hex Interpreter

PswiftHD4FTK:E01/Partition 1/NONAME [NTFS]/[root]/Documents and Settings/spike/Local Settings/Application Data/Microsoft/Outlook/Outlook.pst|[deleted]>pics from last weekend

Email Tab Filter: Email Files and Attachments

Ready

Scroll to Bottom for Headers



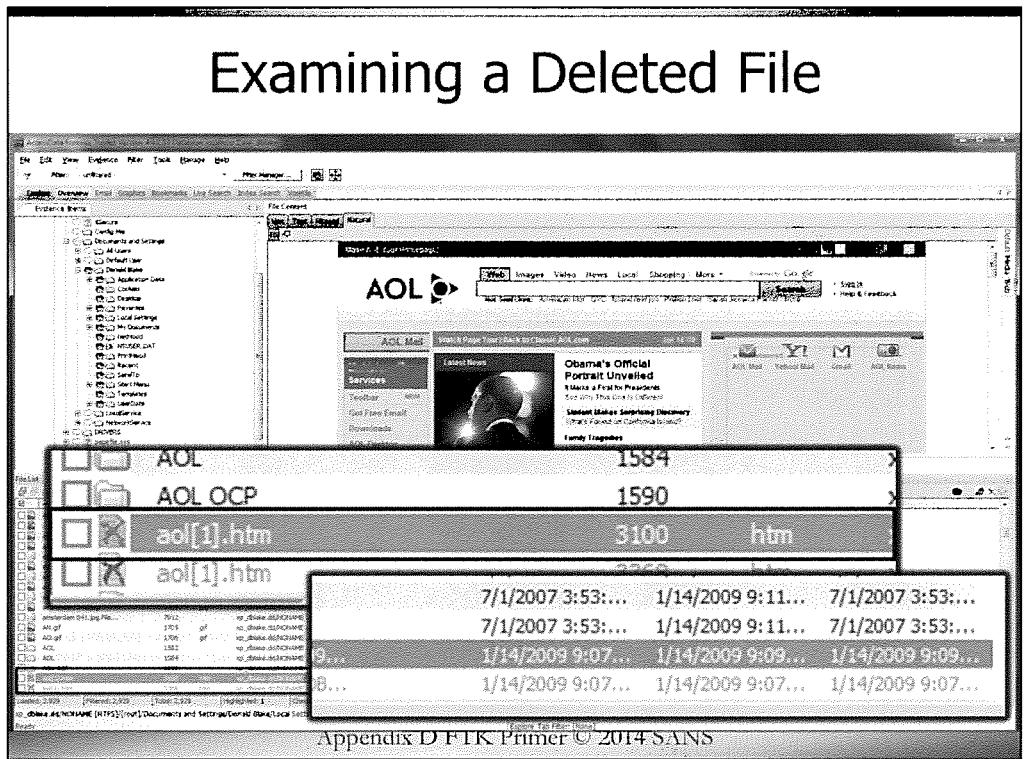
Appendix D FTK Primer © 2014 SANS

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.

Hex Text Filtered Natural

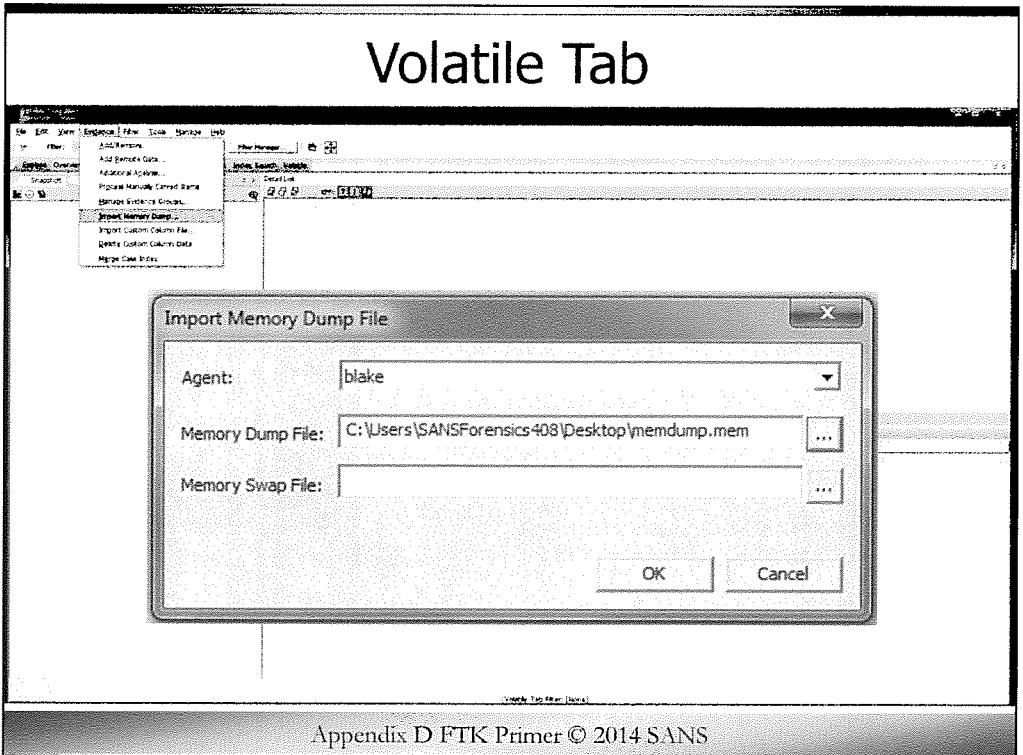


Message Headers: Delivered-To: pswift2007@gmail.com
 Received: by 10.64.153.3 with SMTP id a3c8152336qbe;
 Tue, 20 Feb 2007 10:22:41 -0800 (PST)
 Received: by 10.114.126.1 with SMTP id Yimr3442785wac.1171995758192;
 Tue, 20 Feb 2007 10:22:38 -0800 (PST)
 Return-Patch: <mdhosebag@hotmail.com>
 Received: from bay0-omc2-s19.bay0.hotmail.com (bay0-omc2-s19.bay0.hotmail.com [65.54.246.155])
 by mx.google.com with ESMTP id a8s18018399poa.2007.02.20.10.22.37;
 Tue, 20 Feb 2007 10:22:38 -0800 (PST)
 Received-SPE: pass (google.com: domain of mdhosebag@hotmail.com designates 65.54.246.155 as permitted by mx.google.com ([65.54.250.38]) by bay0-omc2-s19.bay0.hotmail.com with Microsoft SMTPSVC (Tue, 20 Feb 2007 10:21:39 -0800)
 Received: from mail pickup service by hotmail.com with Microsoft SMTPSVC;
 Tue, 20 Feb 2007 10:21:38 -0800
 Message-ID: <BAV115-E286B576945D5DE4E9F0288B3890@phx.gbl>
 Received: from 65.54.250.200 by by115fd.bay115.hotmail.msn.com with HTTP;
 Tue, 20 Feb 2007 18:21:36 GMT
 X-Originating-IP: [66.166.254.82]
 X-Originating-Email: [mdhosebag@hotmail.com]
 X-Sender: mdhosebag@hotmail.com
 From: "Maryland Dirtbag" <mdhosebag@hotmail.com>
 To: pswift2007@gmail.com
 Bcc:
 Subject: Pics from last weekend
 Date: Tue, 20 Feb 2007 13:21:36 -0500
 Mime-Version: 1.0
 Content-Type: multipart/mixed; boundary="-----NextPart_000_1290_1f21_3b10"
 X-OriginalArrivalTime: 20 Feb 2007 18:21:38.0744 (UTC) FILETIME=[F6436B80:01C7551B]
 Return-Patch: mdhosebag@hotmail.com



This is an example of utilizing the framework of FTK to view a deleted file. The deleted files are marked with a red X on the file icon and the file details in the file viewer pane are slightly grayed out 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.

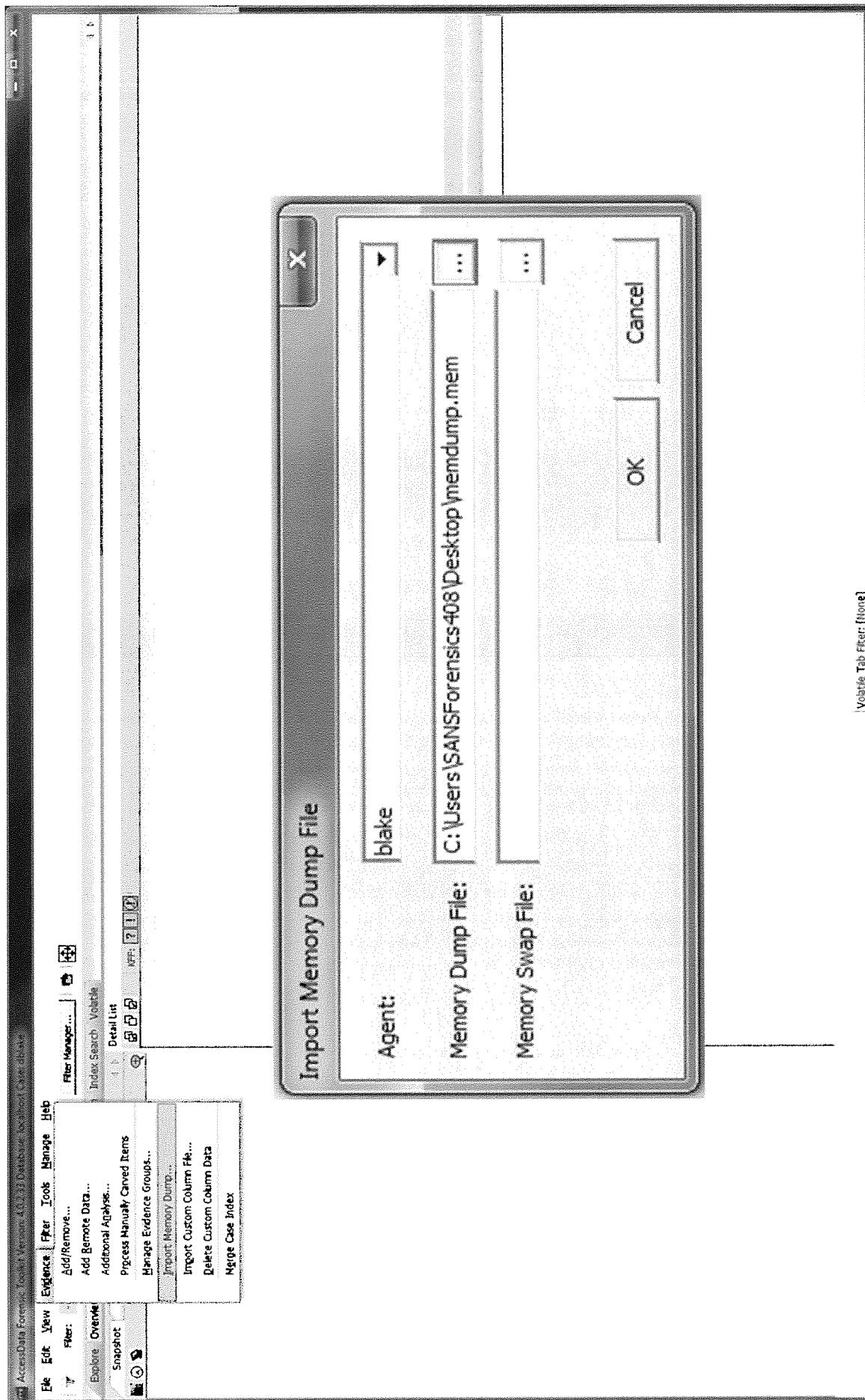


Appendix D FTK Primer © 2014 SANS

FTK also allows you to capture RAM from a remote computer on your network by pushing an agent to that machine, then acquiring RAM across the network. You will need to have administrative privileges on the remote machine to do this. FTK can also allow you to import images of RAM previously imaged for viewing.

You can import a memory dump file by selecting “Evidence”, then “Import Memory Dump...”, from the menu bar.

From the Import Memory Dump File dialog box, you will need to add a name to the “Agent” field. This name is only used to title the memory dump file you are importing. Next, browse to and select the memory dump file in the “Memory Dump File” field, then select “OK”. FTK will then begin the import process of the memory dump file.



FTK Memory Analysis

AccessData Forensic Toolkit Version: 4.0.0.35129 Database: localhost Case: Zeus Memory Test

File Edit View Evidence Filter Tools Manage Help

Filter Manager... Filter

Explore Overview Email Graphics Bookmarks Live Search Index Search Visible

Snapshot Find pin ↻ FPF: 7 | 1 | P

Name	Path	Start Time	Command Line	PPID	Parent PID
System		Invalid Date/Time (J)		4	0
svhost.exe	C:\Windows\System32\svhost.exe	4/11/2010 6:06:21...	C:\Windows\System32\svhost.exe	544	4
winlogon.exe	C:\Windows\System32\winlogon.exe	4/11/2010 6:06:23...	winlogon.exe	622	544
ksvc.exe	C:\Windows\System32\ksvc.exe	4/11/2010 6:06:24...	C:\Windows\System32\ksvc.exe	688	622
services.exe	C:\Windows\System32\services.exe	4/11/2010 6:06:24...	C:\Windows\System32\services.exe	676	622
orchestr.exe	C:\Windows\System32\orchestr.exe	4/11/2010 6:06:25...	C:\Windows\System32\orchestr.exe + Netw...	1008	676
vmacthlp.exe	C:\Program Files\VMware\Tools\vmacthlp...	4/11/2010 6:06:24...	C:\Program Files\VMware\Tools\vmacthlp...	844	676
orchestr.exe	C:\Windows\System32\orchestr.exe	4/11/2010 6:06:24...	C:\Windows\System32\orchestr.exe + pcas...	936	676
orchestr.exe	C:\Windows\System32\orchestr.exe	4/11/2010 6:06:26...	C:\Windows\System32\orchestr.exe + local5...	1148	676
VMwareRelEd...	C:\Program Files\VMware\Tools\VMUpgra...	4/11/2010 6:06:38...	C:\Program Files\VMware\Tools\VMUpgra...	1784	676
spooler.exe	C:\Windows\System32\spooler.exe	4/11/2010 6:06:28...	C:\Windows\System32\spooler.exe	1422	676
vmballoon.exe	C:\Program Files\VMware\Tools\vmballo...	4/11/2010 6:06:35...	C:\Program Files\VMware\Tools\vmballo...	1668	676
endnode.exe	C:\Windows\System32\endnode.exe	4/11/2010 6:06:24...	C:\Windows\System32\endnode.exe + network...	2228	676
identity.exe	C:\Windows\System32\identity.exe	4/11/2010 6:06:49...	C:\Windows\System32\identity.exe	848	1028
win32k.exe	C:\Windows\System32\win32k.exe	4/11/2010 6:07:44...	C:\Windows\System32\win32k.exe + RunSL...	1732	1028
win32k.exe	C:\Windows\System32\win32k.exe	4/11/2010 6:07:37...	C:\Windows\System32\win32k.exe*	468	1028
TPAutConn...	C:\Windows\System32\tpautconn.exe	4/11/2010 6:06:24...	C:\Windows\System32\tpautconn.exe	876	676
TPAutConn...	C:\Program Files\VMware\Tools\TPAut...	4/11/2010 6:06:39...	C:\Program Files\VMware\Tools\TPAut...	2968	676

Total: 24 | Highlighted: 1 | Checked: 0 | FPF: Unlisted, Important, Unimportant

DLLs TOP/IP Handles Fuzzy Hash Search Hits SOT VAD

Port	Protocol	Local Address	Remote Address	Remote Port	Status	Process Name	PPID	Machine	Agent OS	Acquisition T
29220	TCP	0.0.0.0	0	Unknown	svchost.exe	856	Zeus	?	\$/15/2010 3	
1054	TCP	172.16.176.143	193.104.41.75	80	Unknown	svchost.exe	856	Zeus	?	\$/15/2010 3
1056	TCP	0.0.0.0	193.104.41.75	80	Unknown	svchost.exe	856	Zeus	?	\$/15/2010 3

Volatile Tab Filter: (None)

Appendix D FTK Primer © 2014 SANS

FTK will sort all the running processes, DLLs, Sockets, Drivers, Open Handles, Processors, System Descriptor Tables and Devices in the tree window pane of the Volatile Tab.

You can right click on any dump file in the Snapshot view and create custom filters for memory objects.

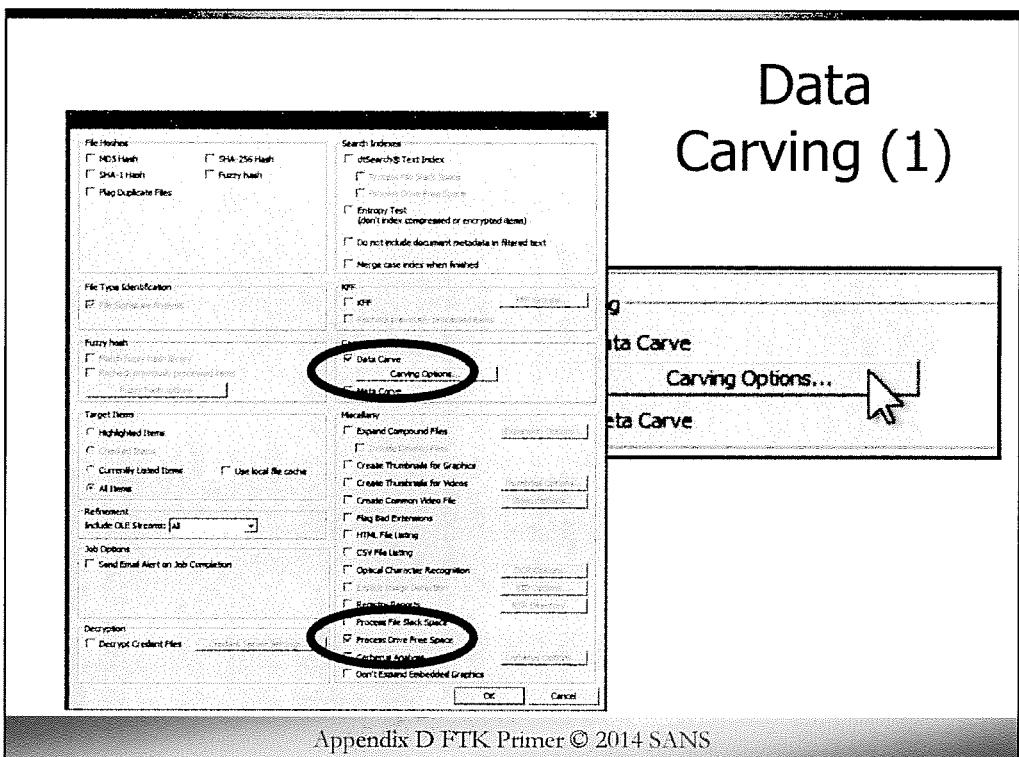
For each process in the Process List, further information can be found in the Detailed Information pane at the bottom. Analyzing imported DLLs, network sockets and connections, process handles, and the virtual address descriptor (VAD) tree can help identify suspicious processes. In this example, a svchost.exe process is communicating with an external IP address over port 80. This is commonly seen in bots when they communicate with their command and control server. A web search for the IP address 193.104.41.75 shows it as a blacklisted IP associated with Zeus malware.

There is a lot of analysis that can be done to memory but that is another course.

The screenshot shows the AccessData Forensic Toolkit interface. The top menu bar includes File, Edit, View, Evidence, Filter, Tools, Manage, Help, and a Filter Manager button. The left sidebar has tabs for Snapshot, Find, Diff, and a search bar with filters for NPF, ? (highlighted), and X (checked). The main window displays a 'Process List' with columns for Name, Path, Start Time, and Command Line. A table below lists DLLs, TCP/IP connections, and network traffic. A status bar at the bottom indicates 'Total: 24' processes, 'Highlighted: 1', 'Checked: 0', and 'ICFF: Unlisted, Incomplete, Unimportant'.

DLL	TCP/IP	Handles	Fuzzy Hash	Search Hits	SDT	VAD				
29220	TCP	0.0.0.0		0	Unknown	svchost.exe	856	Zeus	?	8/15/2010 3
1054	TCP	172.16.176.143	193.104.41.75	90	Unknown	svchost.exe	856	Zeus	?	8/15/2010 3
1056	TCP	0.0.0.0	193.104.41.75	80	Unknown	svchost.exe	856	Zeus	?	8/15/2010 3

Data Carving (1)



Appendix D FTK Primer © 2014 SANS

One of the advanced features I love about FTK 4 is the additional data carving feature. How many times have you found a file significant to the investigation but suspect there are more, only they have not automatically been carved from unallocated space. Perhaps you suspect they have been deleted and partially overwritten. You can setup custom data carvers for specific file types either at the start of your case or at any point throughout your analysis. If your case has already been indexed and processed, simply select from the menu bar Evidence then Additional Analysis.

Under the Carving, select “Data Carve”, then select the “Carving Options...” button.

Additional Analysis

File Hashes

MD5 Hash SHA-256 Hash
 SHA-1 Hash Fuzzy hash
 Flag Duplicate Files

Search Indexes

dtSearch® Text Index
 Process File Slack Space
 Process Drive Free Space
 Entropy Test
 (don't index compressed or encrypted items)
 Do not include document metadata in filtered text
 Merge case index when finished

File Type Identification

File Signature Analysis

KFF

KFF KFF Groups...
 Recheck previously processed items

Fuzzy hash

Match fuzzy hash library
 Recheck previously processed items
Fuzzy hash options

Carving

Data Carve Carving Options...
 Meta Carve

Target Items

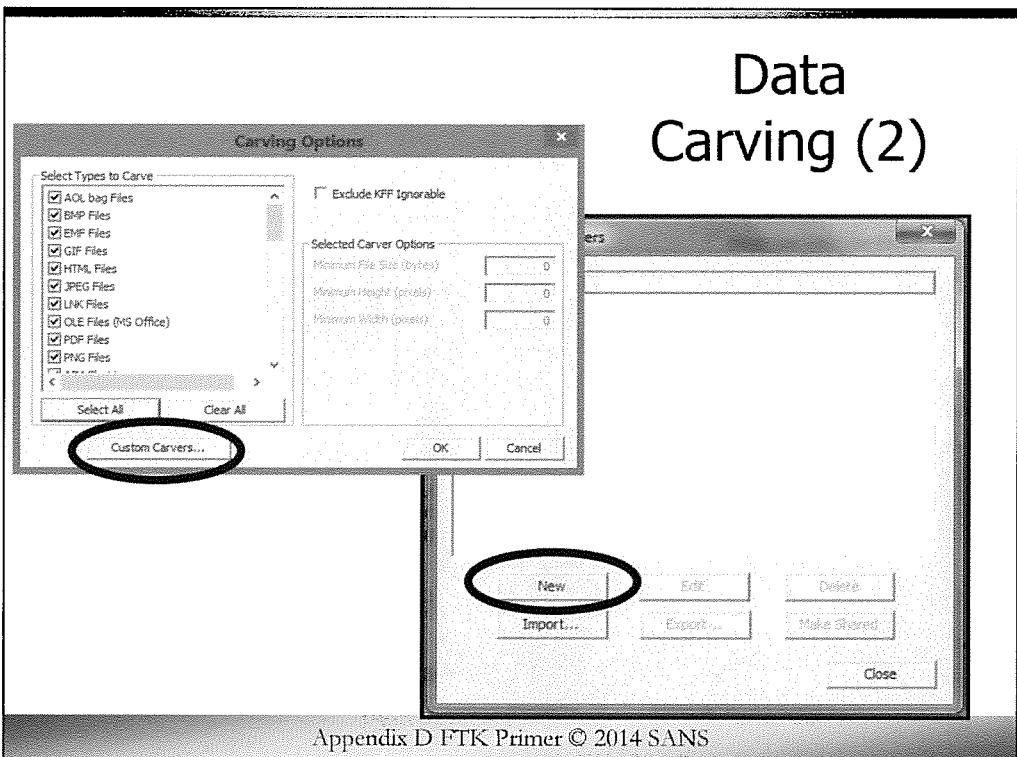
Highlighted Items
 Checked Items
 Currently Listed Items Use local file cache
 All Items

Miscellany

Expand Compound Files Expansion Options...
 Include Deleted Files
 Create Thumbnails for Graphics Thumbnail Options...
 Create Thumbnails for Videos Video Options...
 Create Common Video File
 Flag Bad Extensions
 HTML File Listing
 CSV File Listing
 Optical Character Recognition OCR Options...
 Explicit Image Detection EID Options...
 Registry Reports RSR Directory...
 Process File Slack Space
 Process Drive Free Space
 Cerberus Analysis Cerberus Options...
 Don't Expand Embedded Graphics

OK
Cancel

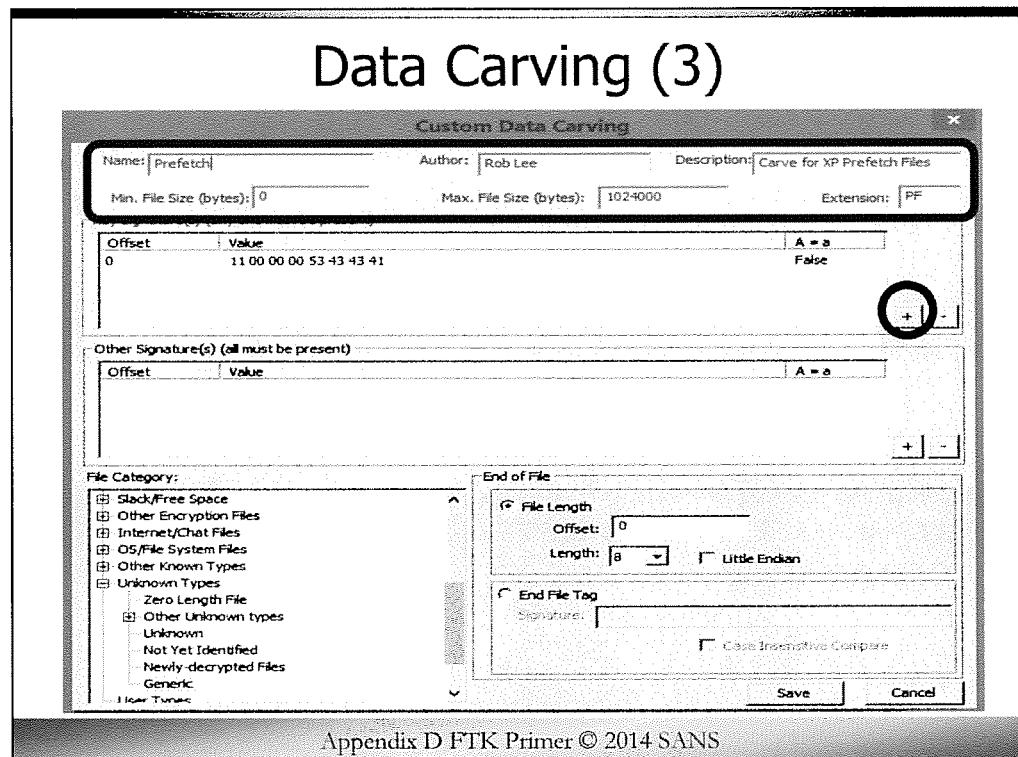
Data Carving (2)



Appendix D FTK Primer © 2014 SANS

Next, select the “**Custom Carvers...**” button then select the “**New**” button to create your new custom carver.

For adding more custom carvers you can download more AD carvers from
<http://www.accessdata.com/support/technical-customer-support/custom-carvers>.



Appendix D FTK Primer © 2014 SANS

Now give your new custom carver a name, annotate the author's name who created the carver and provide a brief description of what the carver does. Over time, you can develop a library in your lab of custom carvers that can be shared and imported into any case you or your colleagues are working.

In this example, we are using a prefetch file signature. We will examine and discuss windows prefetch files in section 4 of this course.

There are two dialogue boxes you can add signatures. In the top dialogue box you can enter one or multiple signatures that are in the file you are looking for. Click the plus "+" and add the file signature in Hex and offset where the signature starts. If your file signature is not case sensitive then uncheck the "Signature is case sensitive" box then click "OK". Files will be carved if they have any of the signatures in this top dialogue box.

If you place any signatures into the second dialogue box, only files with ALL signatures entered into the second dialogue box will be carved. Unless you are looking for a very specific file that must have both signatures, you may want to leave this blank.

Custom Data Carving

Name: <input type="text" value="Prefetchl"/>	Author: <input type="text" value="Rob Lee"/>	Description: <input type="text" value="Carve for XP Prefetch Files"/>
Min. File Size (bytes): <input type="text" value="0"/>	Max. File Size (bytes): <input type="text" value="1024000"/>	Extension: <input type="text" value="PF"/>

Offset	Value	A = a
0	11 00 00 00 53 43 43 41	False

+ (highlighted with a circle)

Other Signature(s) (all must be present)

Offset	Value	A = a

+ -

File Category:

- + Slack/Free Space
- + Other Encryption Files
- + Internet/Chat Files
- + OS/File System Files
- + Other Known Types
- Unknown Types
 - Zero Length File
 - + Other Unknown types
 - Unknown
 - Not Yet Identified
 - Newly-decrypted Files
 - Generic
- Other Types

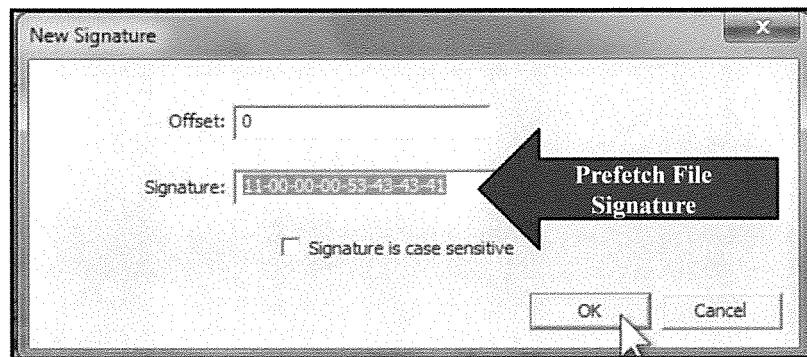
End of File

File Length
 Offset:
 Length: Little Endian

End File Tag
 Signature:
 Case Insensitive Compare

Save Cancel

Add Prefetch Signature



Appendix D FTK Primer © 2014 SANS

This page intentionally left blank.

New Signature

X

Offset: 0

Signature:

11-00-00-00-53-43-43-41

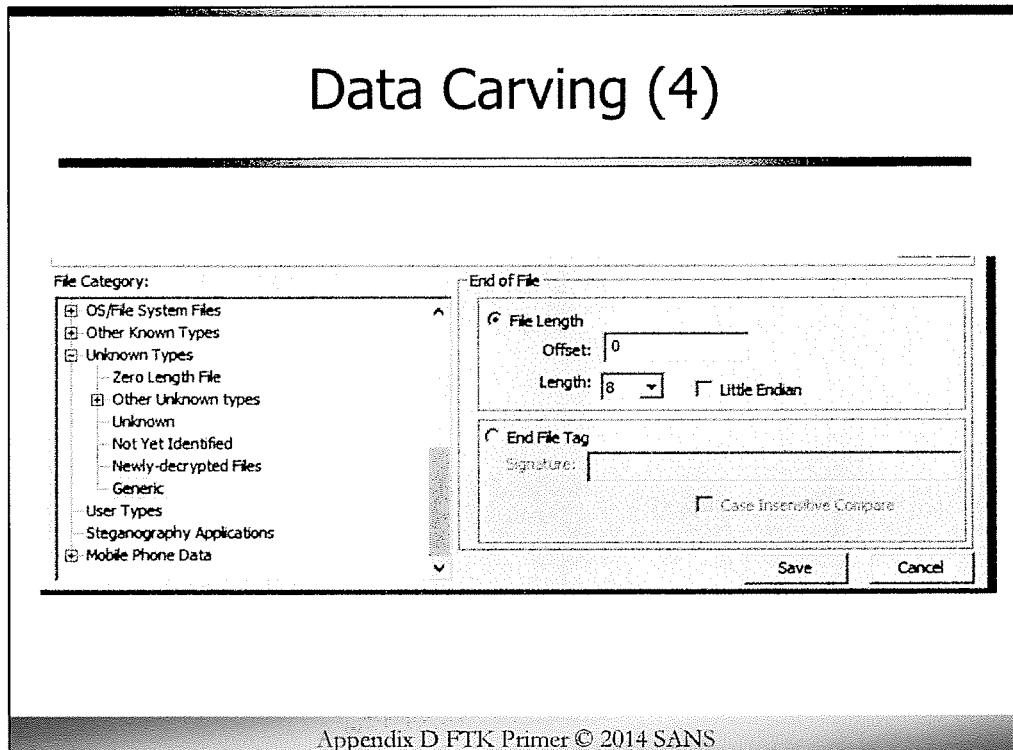
Signature is case sensitive

Prefetch File
Signature

OK

Cancel

Data Carving (4)



Appendix D FTK Primer © 2014 SANS

At the bottom left of the Custom Data Carving screen, select a file category to place your carved files, then you can add End of File information such as the hex for the End File Tag. This End of File information is not necessary.

Once you have entered your new file carving information select save then close your Manage Custom Carvers dialogue box. Make sure only the carvers you would like to search for are selected in the Carving Options dialogue box then select OK to both the Carving Options and Additional Analysis dialogue boxes.

File Category:

- [+] OS/File System Files
- [+] Other Known Types
- [=] Unknown Types
 - [...] Zero Length File
 - [+] Other Unknown types
 - [...] Unknown
 - [...] Not Yet Identified
 - [...] Newly-decrypted Files
 - [...] Generic
 - [...] User Types
 - [...] Steganography Applications
 - [+] Mobile Phone Data

End of File

File Length

Offset:

Length: ▾

Little Endian

End File Tag

Signature:

Case Insensitive Compare

Save

Cancel

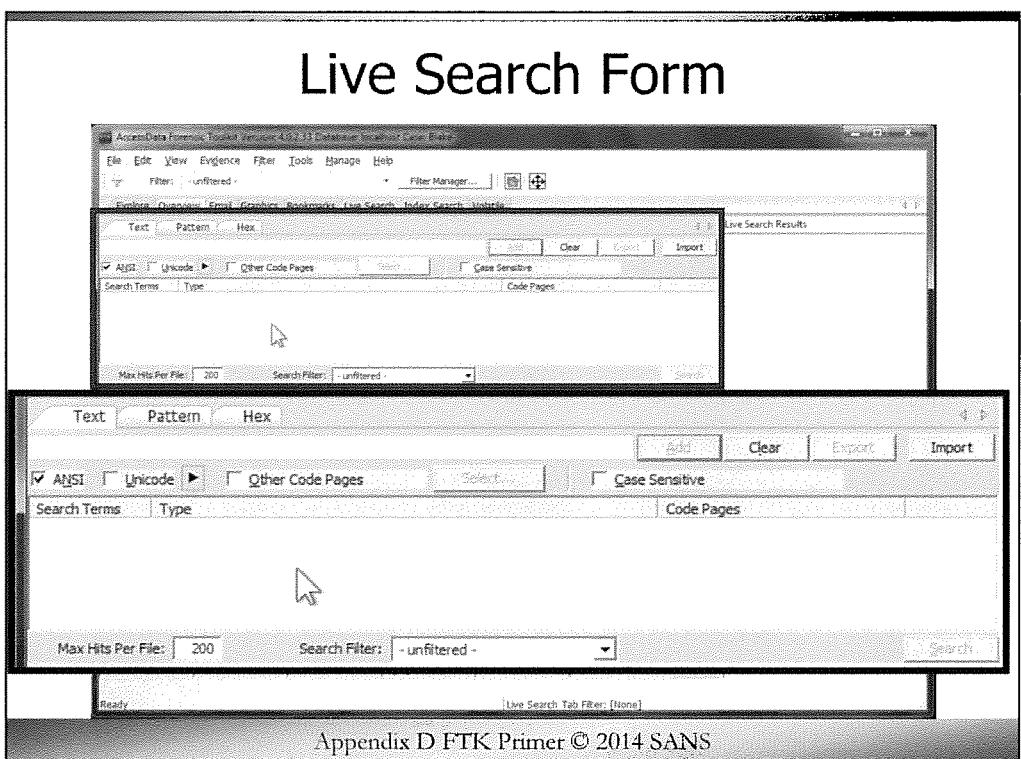
Data Carving (5)

The screenshot shows the FTK Forensic Toolkit interface. The top menu bar includes File, Edit, View, Evidence, Filter, Tools, Manage, and Help. The Evidence tab is selected, showing a tree view of file types: Graphics (3,392 / 3,392), Internet/Chat Files (793 / 793), Mobile Phone Data (0 / 0), Multimedia (184 / 184), OS/File System Files (506 / 606), Other Encryption Files (86 / 86), Other Known Types (1,457 / 1,457), Other Known Types (9 / 9), Solid/Free Space (4,832 / 4,832), Spreadsheets (21 / 21), Unknown Types (4,420 / 4,420), Generic (34 / 34), Other Unknown types (1 / 1), Unknown (4,272 / 4,272), and Zero Length File (113 / 113). The main pane displays a "Windows Prefetch File" with properties: File Path (\DEVICE\HARDISK\VOLUME1\PROGRAM FILES\WINDOWS NT\ACCESSORIES\WORDPAD.EXE), Times Run 5, and Last Time Run 1/16/2009 11:18:29 PM +00:00. Below this are tabs for File Content, Properties, and Hex Interpreter. The bottom section shows a "File List" table with columns: Name, Label, Item #, Ext, Path, Category, P.Size, L.Size, MD5, SHA1, SHA256, and Created. The table lists several entries, all labeled "Carved [0].PF" and "xp_dblaze.dd\NONAME...".

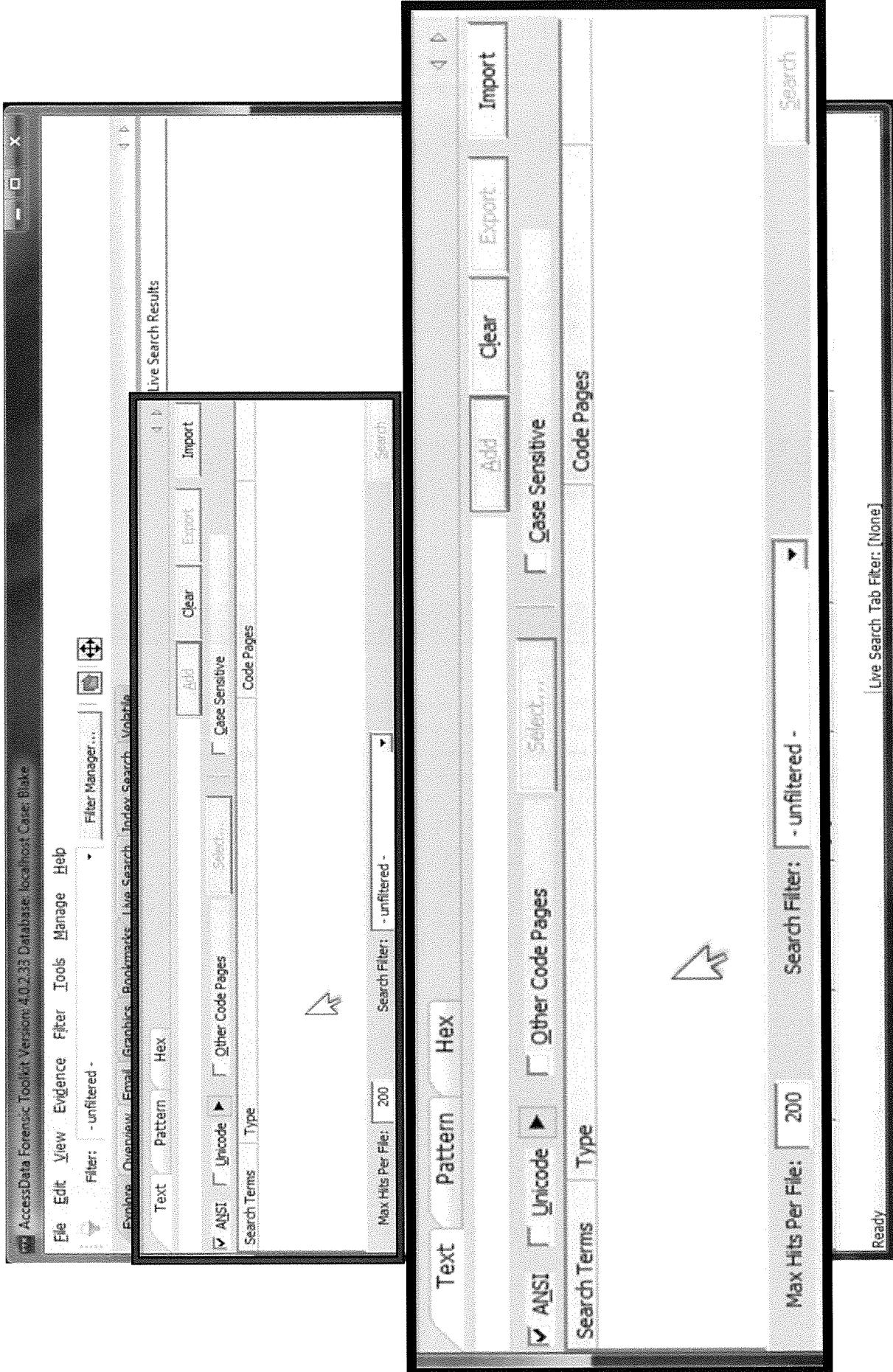
Name	Label	Item #	Ext	Path	Category	P.Size	L.Size	MD5	SHA1	SHA256	Created
Carved [0].PF		24002	pf	xp_dblaze.dd\NONAME...	Generic	n/a	126.0 KB	n/a	n/a	n/a	
Carved [0].PF		24003	pf	xp_dblaze.dd\NONAME...	Generic	n/a	162.0 KB	n/a	n/a	n/a	
Carved [0].PF		24004	pf	xp_dblaze.dd\NONAME...	Generic	n/a	18.00 KB	n/a	n/a	n/a	
Carved [0].PF		24005	pf	xp_dblaze.dd\NONAME...	Generic	n/a	4096 B	n/a	n/a	n/a	
Carved [0].PF		24006	pf	xp_dblaze.dd\NONAME...	Generic	n/a	20.00 KB	n/a	n/a	n/a	
Carved [0].PF		24007	pf	xp_dblaze.dd\NONAME...	Generic	n/a	36.00 KB	n/a	n/a	n/a	
Carved [0].PF		24008	pf	xp_dblaze.dd\NONAME...	Generic	n/a	8192 B	n/a	n/a	n/a	
Carved [0].PF		24009	pf	xp_dblaze.dd\NONAME...	Generic	n/a	8192 B	n/a	n/a	n/a	

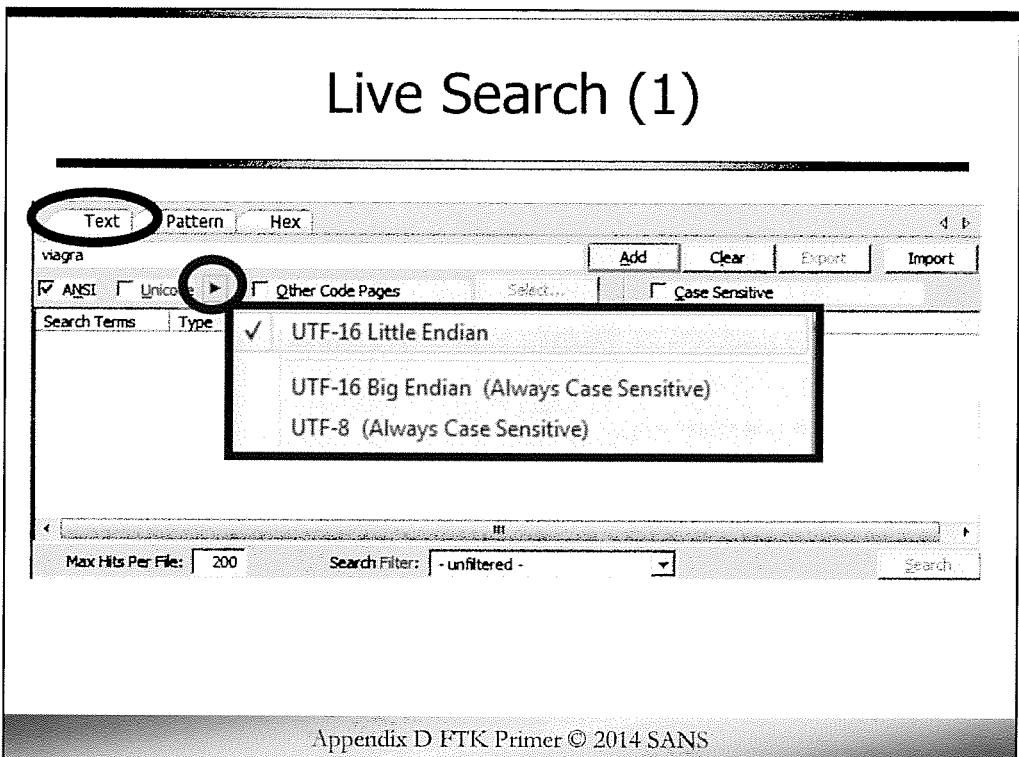
Appendix D FTK Primer © 2014 SANS

To find your newly carved files go to the Overview tab and select the file category you selected for your custom carved file. We will discuss Prefetch files in-depth later in the course, but recovering deleted ones is very important and will help your overall analysis.



While an Indexed Search gives instantaneous results, a live search includes options such as text, pattern and hexadecimal searching. You can view search results from the File List and File Contents views of the Search tab. The Live Search is accomplished by a bit-by-bit comparison of the entire evidence set with the search term or pattern.





Appendix D FTK Primer © 2014 SANS

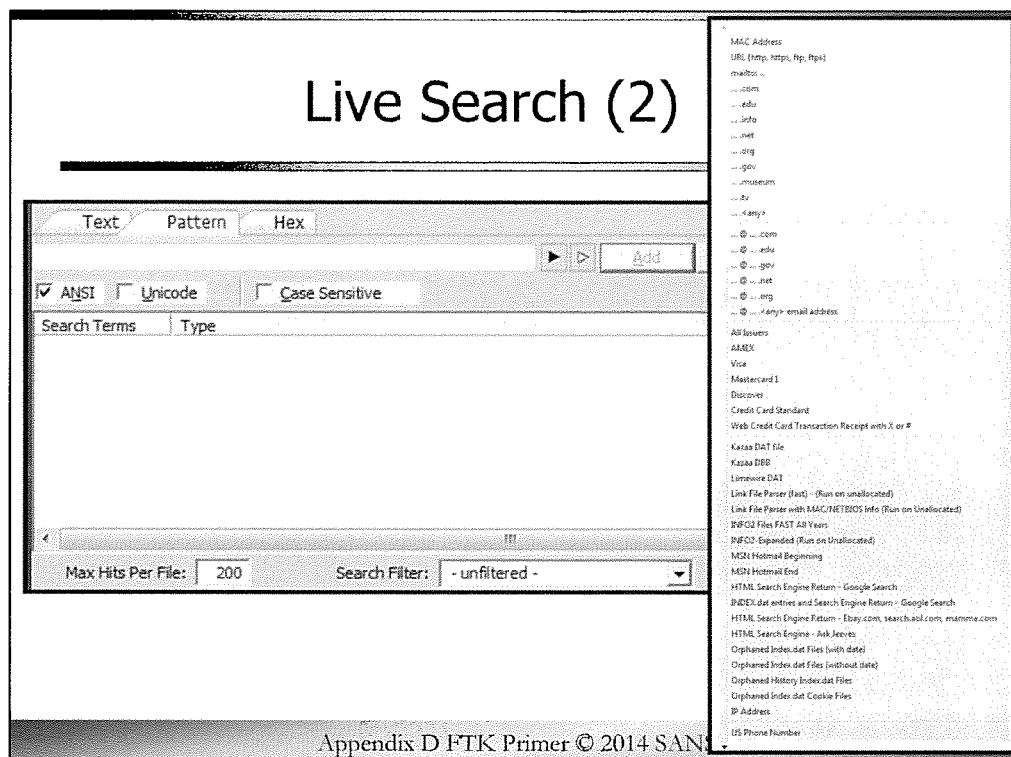
The second way you can do searches in FTK is through the **Live Search** function. Live search can be used to search for special characters, case sensitive words, Hexadecimal or Regular Expressions. Live Search should be used judiciously since it is a time intensive process that involves an item-by-item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

With the Text tab selected you can search for text strings in ANSI, Unicode with UTF-16 Little Endian, UTF-16 Big Endian, and UTF-8. Selecting the black arrow under the text search entry field to quickly switch between UTF-16 Little Endian, UTF-16 Big Endian, and UTF-8.

You can choose to make your searches case sensitive (except for UTF-16 Big Endian and UTF-8 which are always case sensitive). You can also choose from a list of other code pages to apply to your search by checking the "Other Code Pages" box then click on the "Select..." button.

References:

- Forms of Unicode - http://www.icu-project.org/docs/papers/forms_of_unicode
- <http://www.utf8-chartable.de>
- http://unicode.org/faq/utf_bom.html

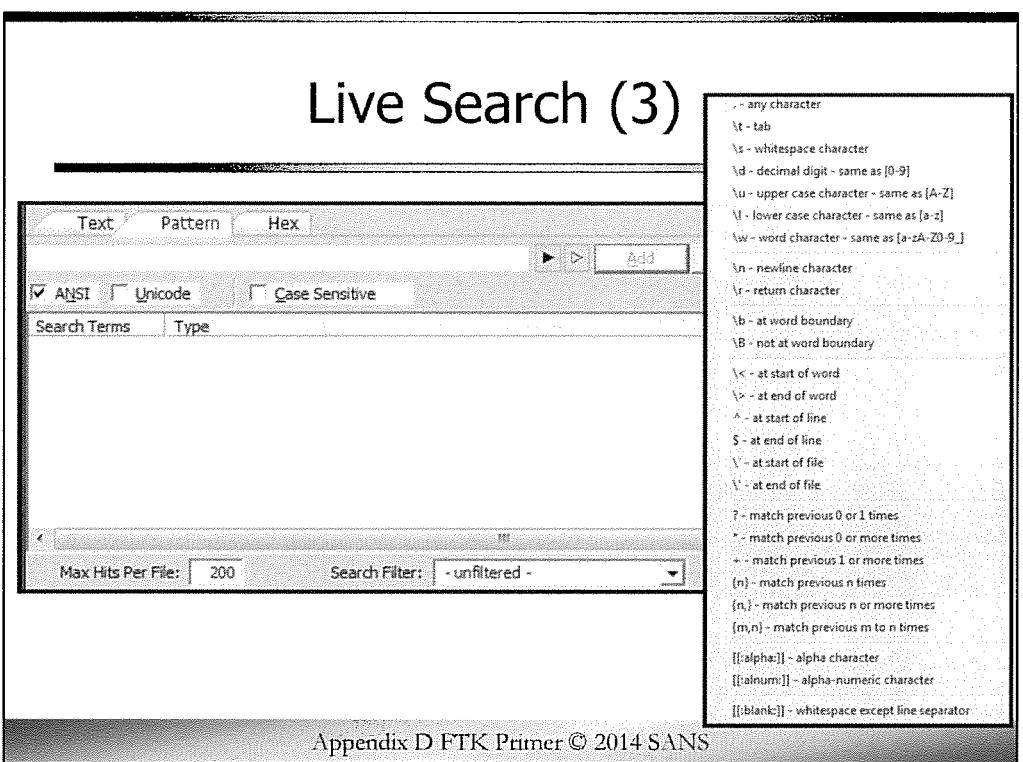


Under the Pattern search tab you can search for precise character strings that describe a data pattern such as a credit card or social security number.

Click on the white arrow to the right of the search term entry field and you will see a menu where you can select several common patterns that have been preloaded.

You can edit this list and add your own that will show up here by scrolling to the bottom of this list and selecting “edit expressions...”.

Live Search (3)



You can also click on the black arrow to the right of the search term field and you will see a menu where you can select from a number of common operators to help you build your own complex expressions.

Core Windows Forensics Agenda



Part 1 String Searching/Data Carving



Part 2 Registry Forensics



Part 3 E-mail Forensics



Part 4 Windows Artifact Analysis



Part 5 Log File Analysis



Part 6 Browser Forensics

Appendix D FTK Primer © 2014 SANS

This page intentionally left blank.

