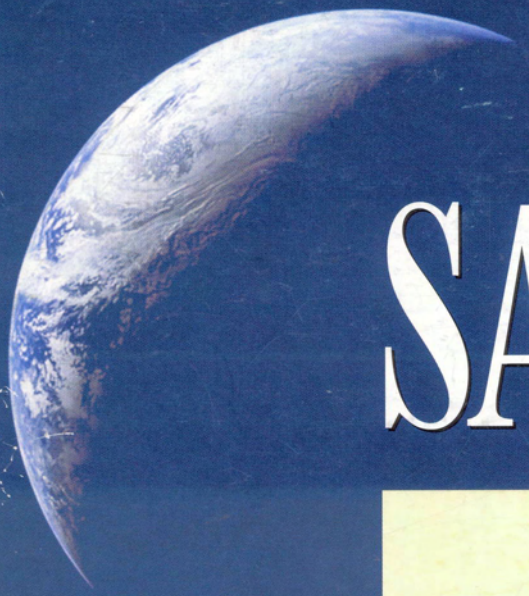


SANS

www.sans.org

FORENSICS 408

COMPUTER FORENSIC ESSENTIALS

408.1

Digital Forensics and E-Discovery Fundamentals

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

SANS

www.sans.org

FORENSICS 408

COMPUTER FORENSIC ESSENTIALS

408.1

Digital Forensics and E-Discovery Fundamentals

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

V2011_0228
Revision 1

Note to Students About SANS Institute Evaluations

SANS Institute works extremely hard to continuously improve both the quality of courseware and instruction. The evaluation forms that we provide daily are one of the most effective methods to help improve the course and to give feedback to the instructors. The numerical score helps us track trends, and the written comments give us the context to make immediate improvements. We truly appreciate the time you take to provide this feedback.

Some things to remember: 10 = very good, 1 = very bad!

Your scores and comments should be given based on your experience, the quality of the instruction, and the quality of the course material. Instructors should NOT be soliciting scores or in any way trying to influence your evaluations.

poor

1 2 3 4 5 6 7 8 9 10

Value of Course Content:

poor **excellent**

1 2 3 4 5 6 7 8 9 10

If you liked the course and wouldn't mind sharing your comments with others who might consider taking this course in the future, please write a sentence about why you felt this course was valuable.

Please make every effort to score each of these areas individually and write comments which you feel are relevant or important in the comments section. If a lab does not work on your computer system, please reflect that in the course content score, and please give us any information you have as to what went wrong so we make appropriate corrections to our courseware. Rest assured that all eval comments are read by the senior management at SANS. Evaluations are used to adapt the course and make it even better, so please do fill them in! If you have specific comments regarding the venue, snacks, etc., we have provided a separate evaluation specifically for those areas.

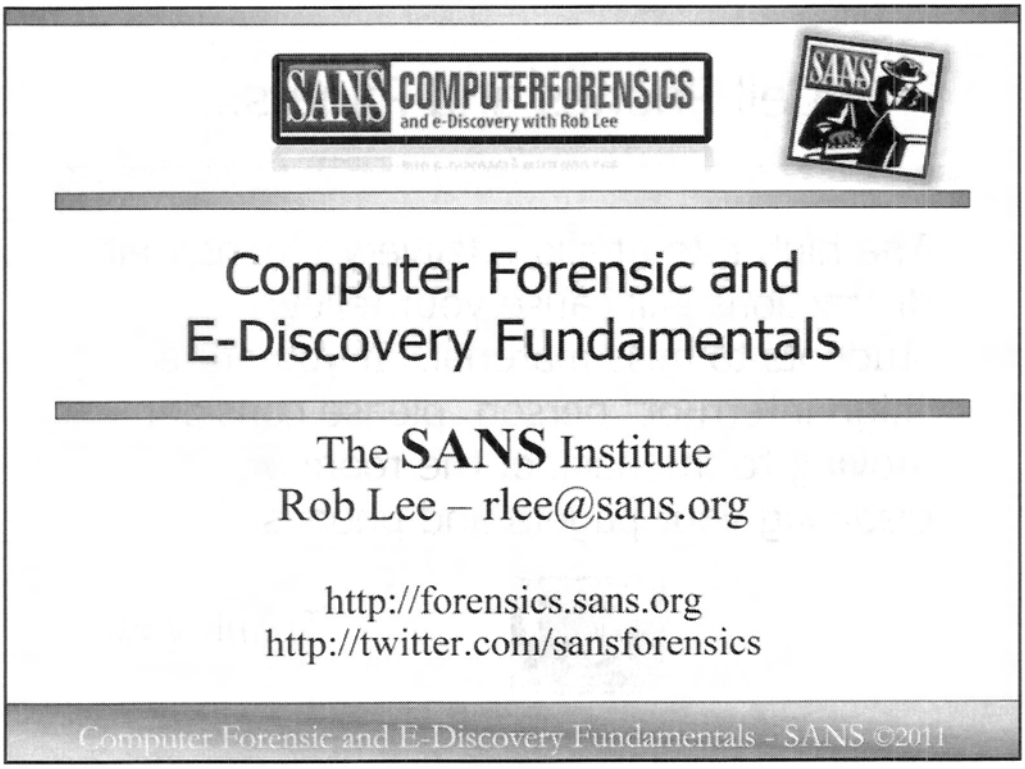
Some people do not believe in giving 10s, and that is fine. However, please keep in mind that delivering a course is a performance, and performers work harder when they are motivated. If and only if your course is on par with the best instruction you have ever received a 10 is appropriate.

If you give the overall course and/or course content a low score, please explain why in the comments field so we can adapt. You can also be assured if you explain your concerns to an event manager we will be discreet. If you are willing, please sign your name at the bottom of the evaluation. If you are having difficulties, SANS can quickly come to your aid if we know who you are. In addition, we also routinely use quotes from previous students in upcoming brochures. If you do not want to be quoted, please let us know.

Thank you for your thoughtful consideration,

Eric Bassel, Mason Brown, Stephen Northcutt, and Alan Paller

This page intentionally left blank.



Rob Lee

rlee@sans.org

http://twitter.com/robtlee

http://twitter.com/sansforensics

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

Special Thanks for Jenny Delucia for helping with slides for E-Discovery and Online Investigation Techniques Section.

Cell Phones and Pagers...

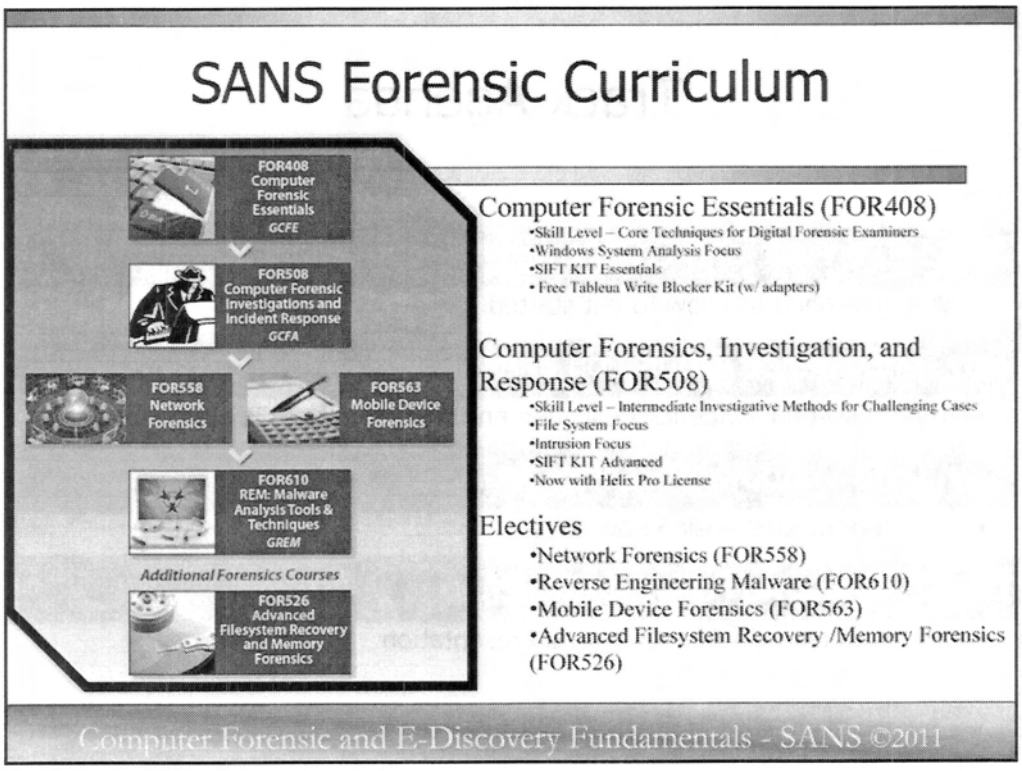
The high rate of slide delivery means that distractions will cause your fellow students to miss material. If you are a "high interrupt" person, please consider moving to the back of the room or disabling your pagers and phones.

Thank you.

Computer Forensic and E-Discovery Fundamentals - SANS ©2011

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

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



Computer Forensic Essentials (SEC408)

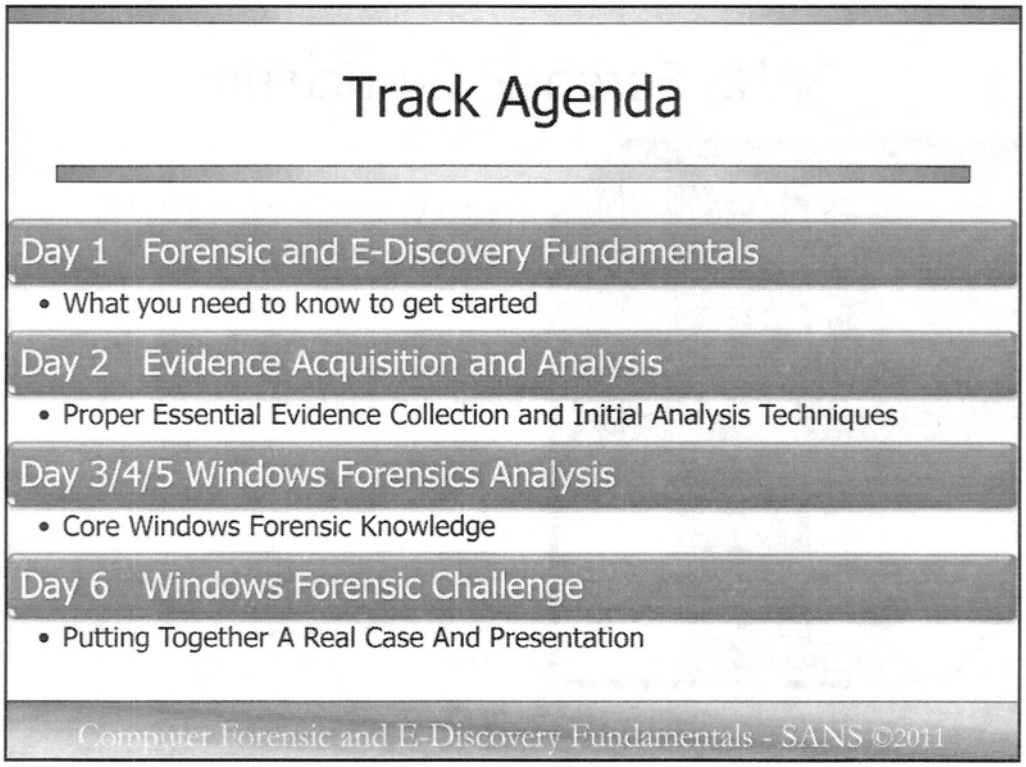
- Skill Level – Core Techniques for Digital Forensic Examiners
- Windows System Analysis Focus
- SIFT KIT Essentials
- Free Tableua Write Blocker Kit (w/ adapters)

Computer Forensics, Investigation, and Response (FOR508)

- Skill Level – Intermediate Investigative Methods for Challenging Cases
- File System Focus
- Intrusion Focus
- SIFT KIT Advanced
- Now with Helix Pro License

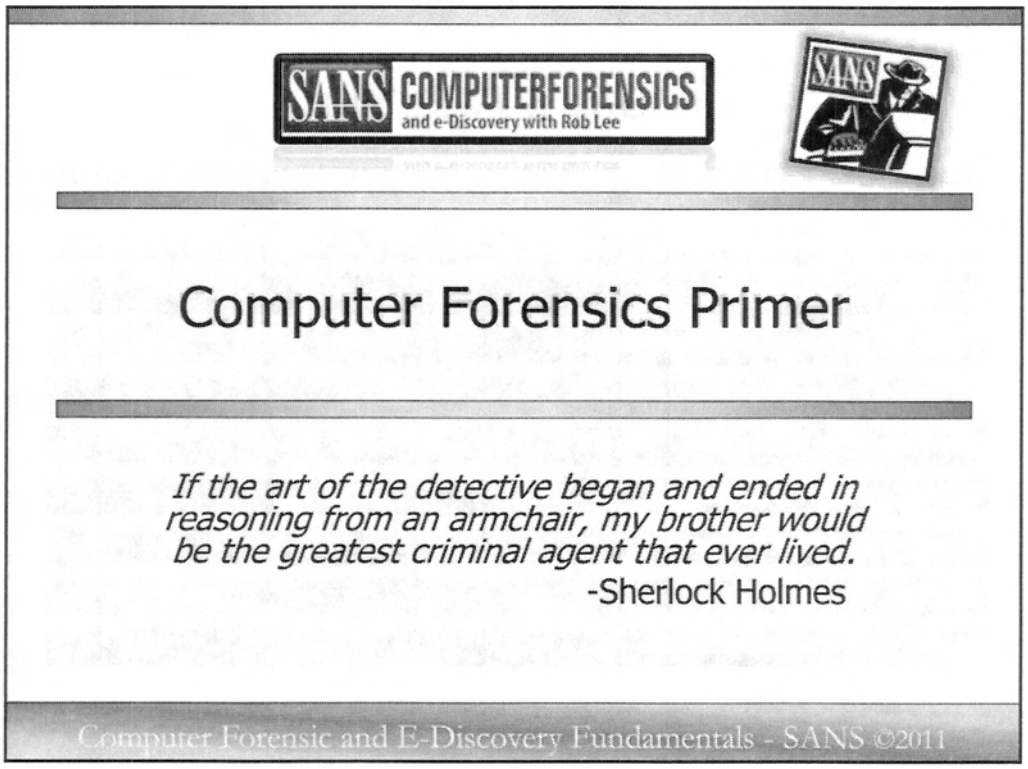
Electives

- Network Forensics (FOR558)
- Reverse Engineering Malware (FOR610)
- Mobile Device Forensics (FOR563)
- Advanced Filesystem Recovery /Memory Forensics (FOR526)
- Drive and Data Recovery Forensics (SEC606)

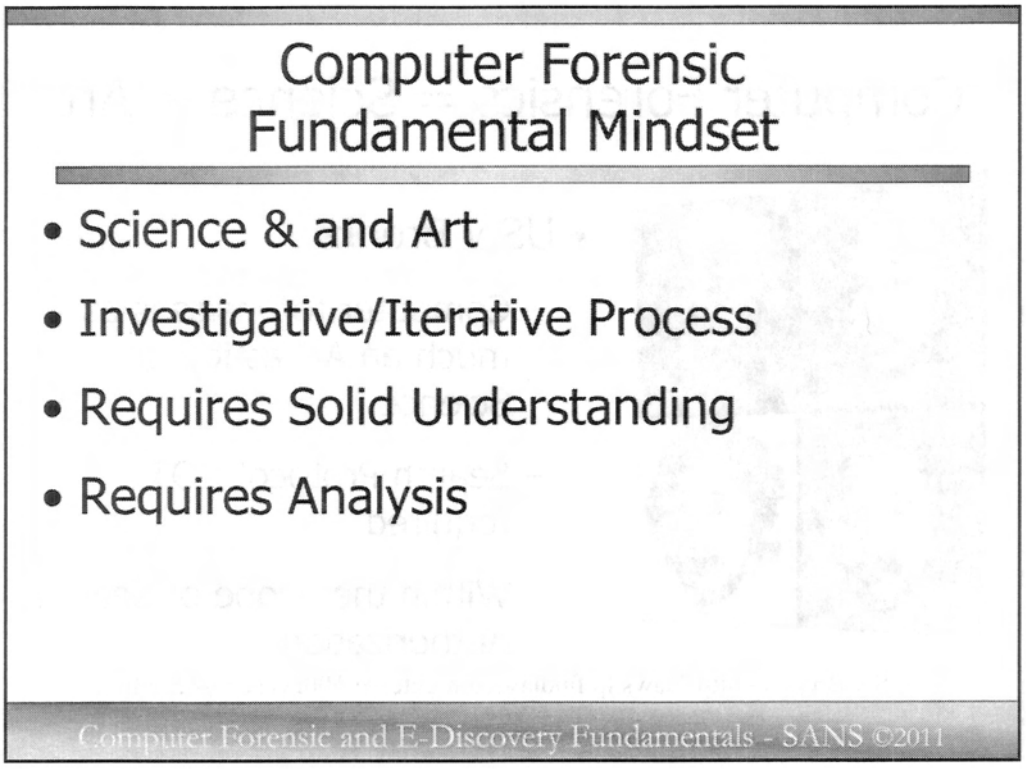


This page intentionally left blank.

This page intentionally left blank.

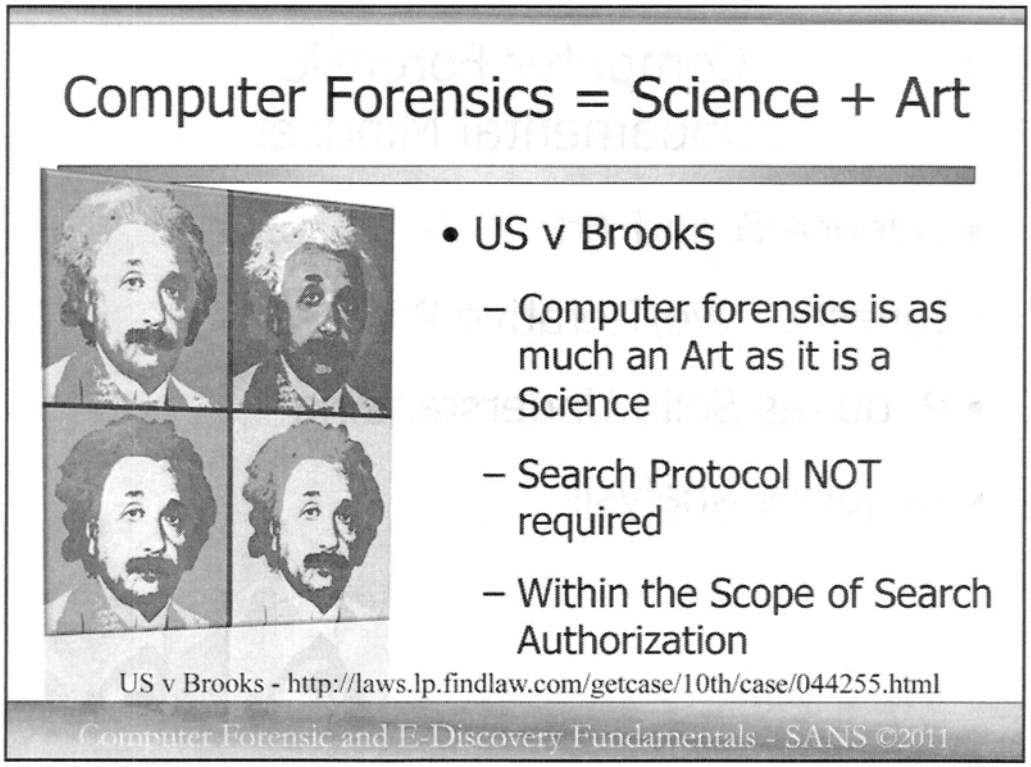


This page intentionally left blank.



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 important to know that it 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 Brook. In this decision, the courts concluded that "Given the numerous ways information is stored on a computer, [both] openly and surreptiously, 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 subjects 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 **images 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 SURREPTIOUSLY and that a search methodology or protocol need NOT be stipulated or detailed in the search authorization.

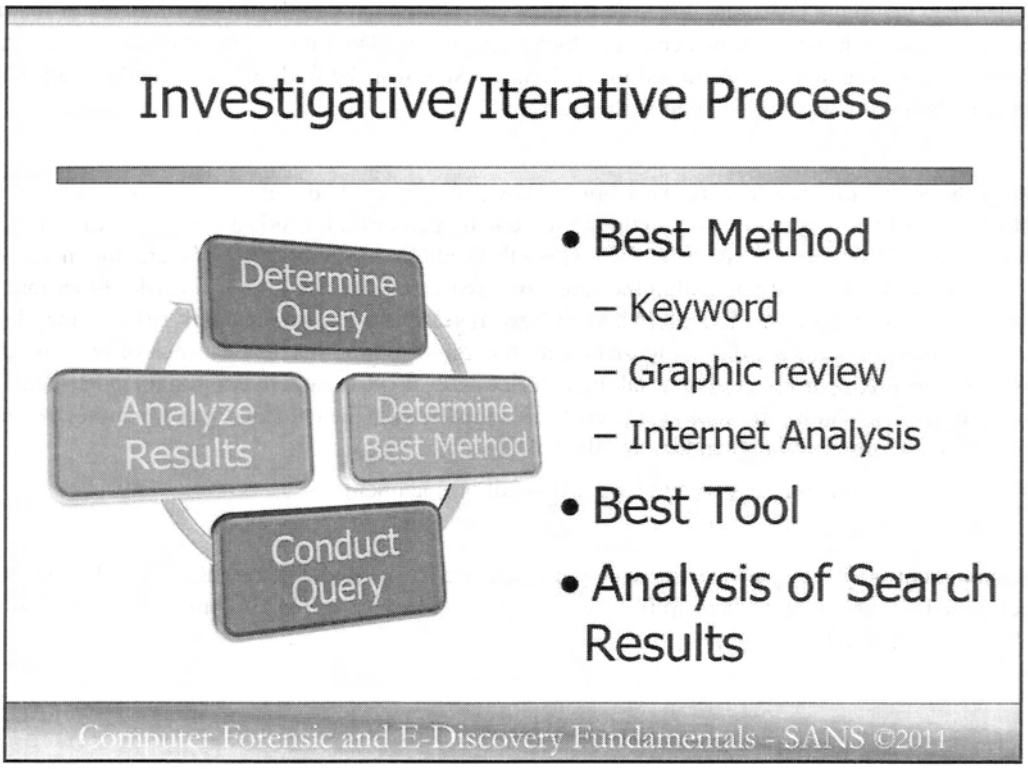
No Requirement to Detail Search Methodology - This surreptious method of storing files can refer to any technique used to hide specific digital information that is evidence of a crime law enforcement have authorization to search for. One of these techniques might include the act of changing the file 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 inside files other than graphic files? ANSWER: YES Just like in a physical search of a room for drugs, officers may look through a 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 cane be found at http://laws.lp.findlaw.com/getcase/10th/case/044255.html, this site is also at the bottom of this slide.



Best Method –

When we say that computer forensic analysis if an Investigative or Iterative Process, we mean that while staying within the scope of the warrant, a great deal of thought must go into what ever you do. You must actually give great consideration to 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 makes it easer 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 in 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 a 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 found the graphic file, you should also want to know how did that file get 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

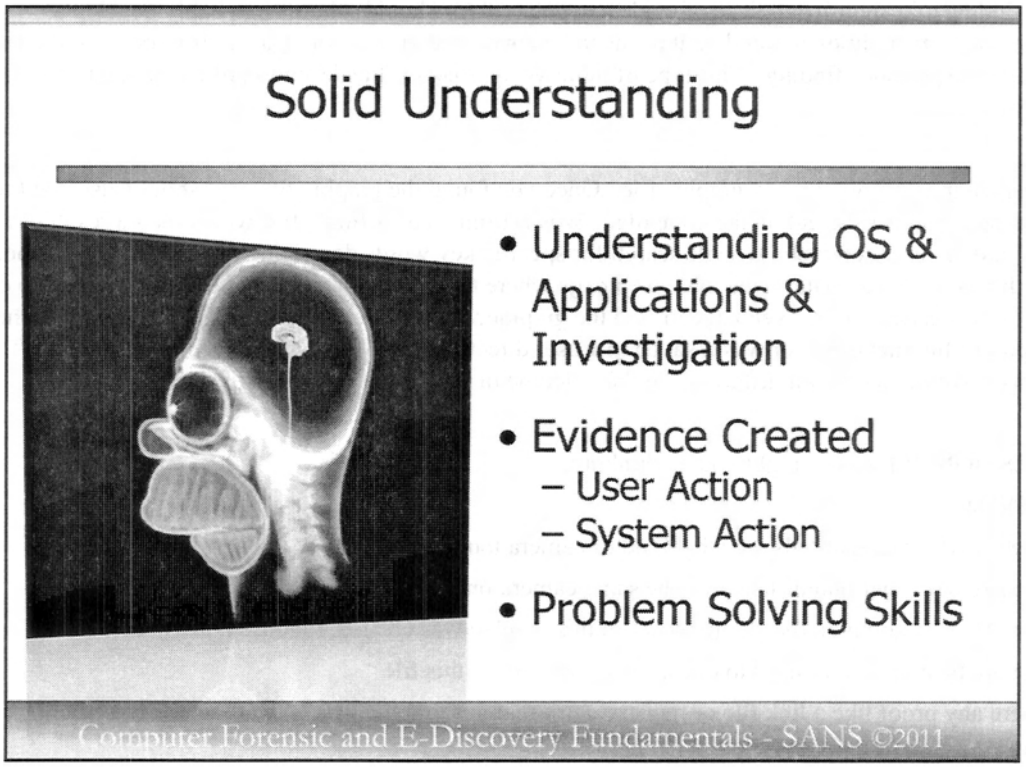
What else was going on the computer when this graphic was created, modified, last accessed

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 go is run key word search and dump the hits to a drive and give it to the case agent.



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 situation 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 with in the scope of the warrant or any evidence they find may be suppressed and not allowed to be used in proceeding against the defendant.

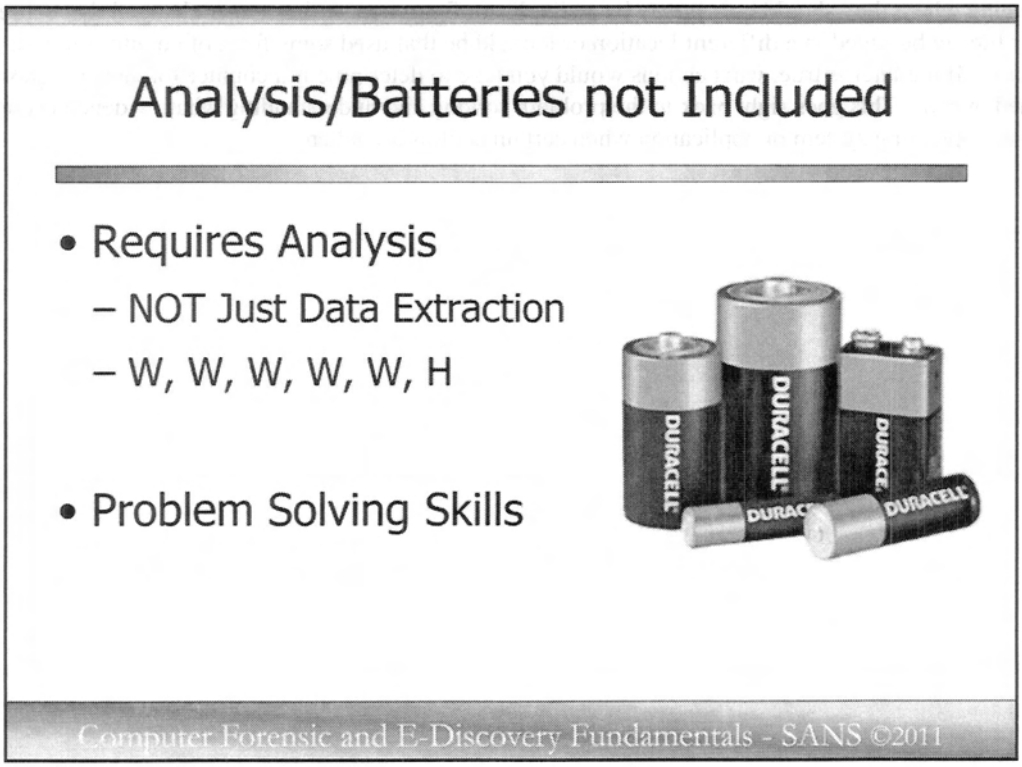
As we have mentioned before about simply conducting a key word search and exporting the results for review by the case agent, do you think a non-technical non-forensic trained agent or investigator understands computer systems enough to ask for link files or know what in the registry could help his investigation?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

Understanding Evidence Created –

Evidence of action or activity are 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 results 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.

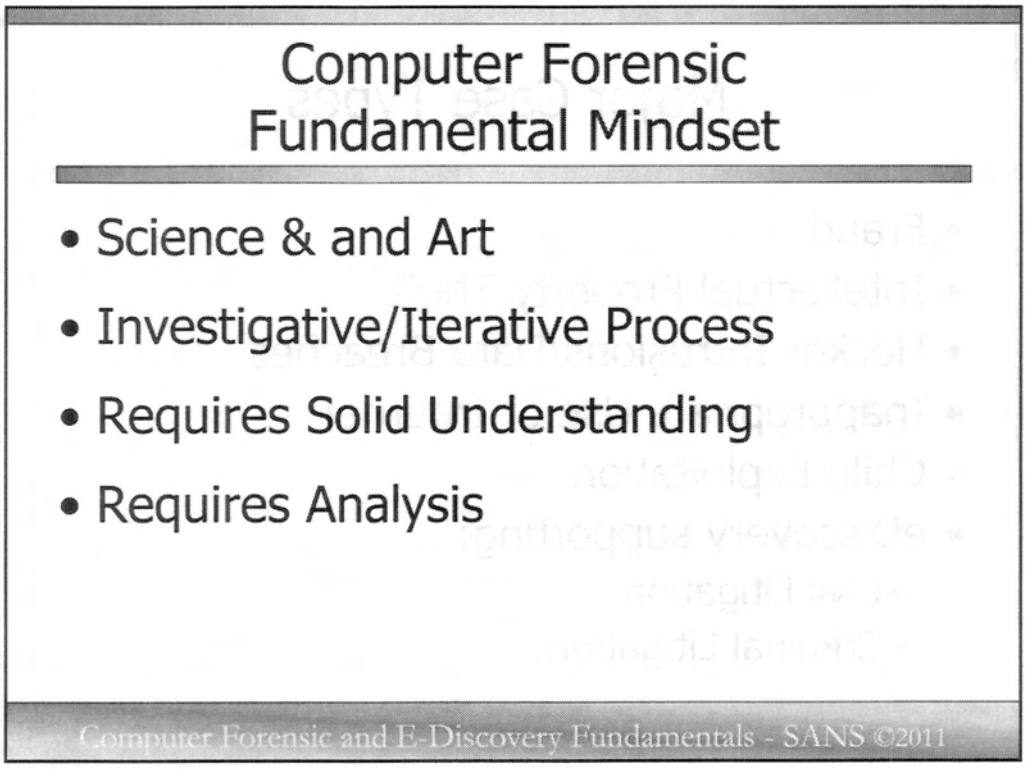
In a court of law, your expert opinion is based on conducting an analysis of the totality of your findings, and the information you have about the investigation as to what events took place and by who. Your opinion must be in turn supported by your findings.

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 explain form an opinion or conclusion as to what happened on a computer.

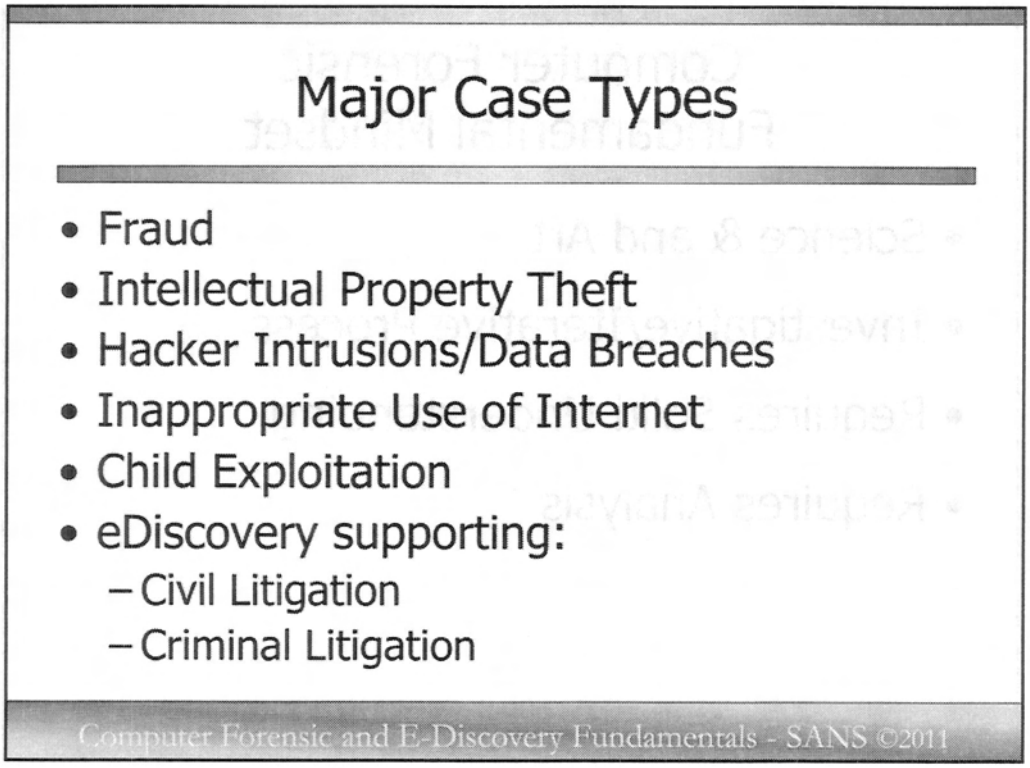
Problem Solving –

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 was committed, what actions would 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 that used some form of counter forensic programs. If the later 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 what evidence is created by a user, operating system or application when certain actions are taken.

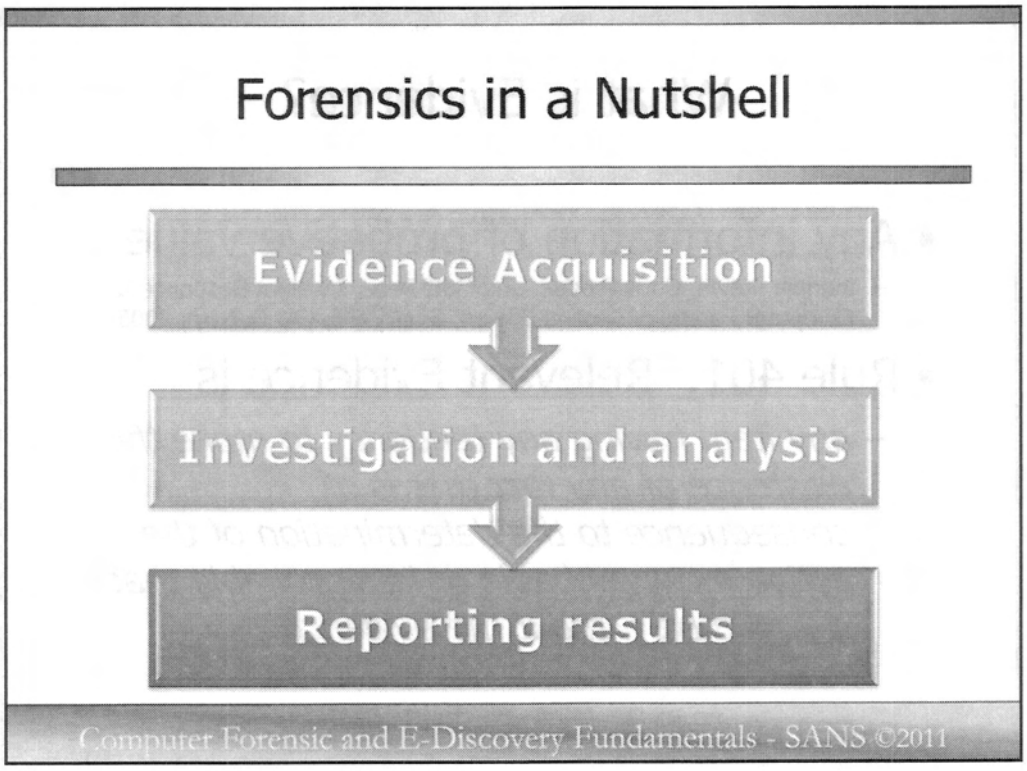


So when we think about the computer forensic fundamental mindset, we know that computer forensics is as much an Art as it is a Science. That it takes an investigative and Iterative approach, with the forensic analyst looking at each item, file and finding and asking themselves if that finding warrants 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.



These are some of the major cases that an investigator might encounter. In many of these cases, similar principles are followed regardless if you are looking for evidence of intellectual property theft, a user e-mailing documents home, or a hacker e-mailing payment card data It is all occurring on a computer system. All forensic analysts need to do is investigate what happened using a process that would answer the key questions of the case.

Our aim in this class is to arm you with the tools and methodology in order for you to succeed at solving any type of case you are involved in.



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 contains key IP addresses of the attacker or subject. Non-volatile data is a hard drive that is powered off, or static CD-ROMs.

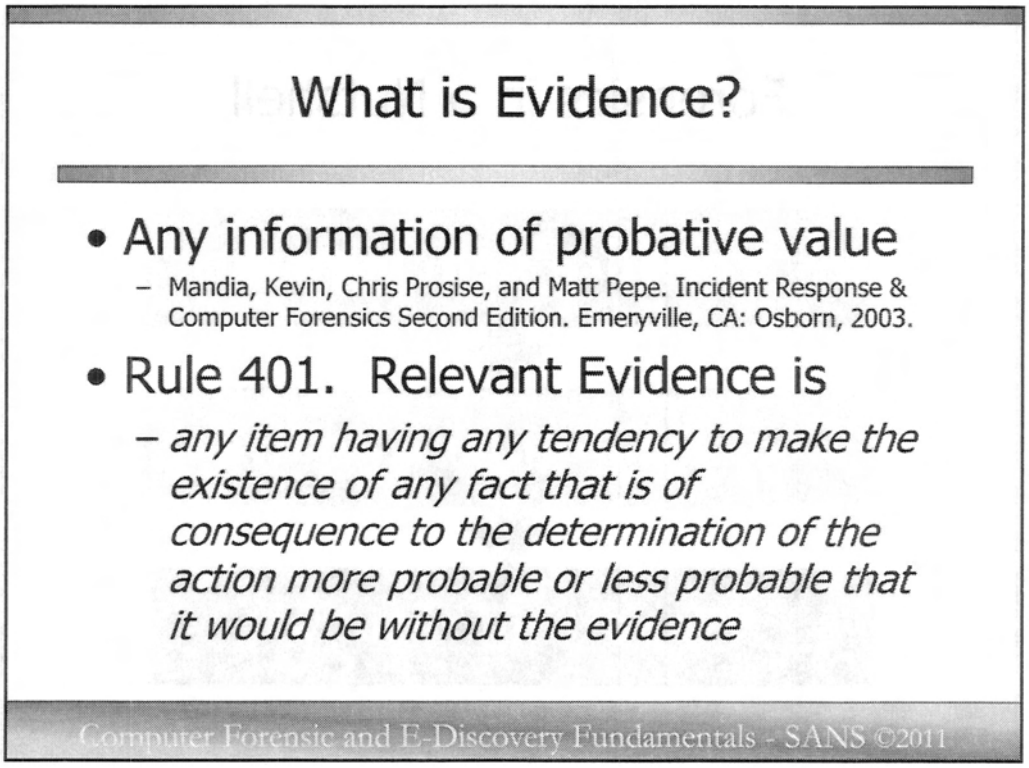
Investigation and analysis occurs when the investigator takes what is collected and analyzes it to form a clear picture of the incident. This analysis uses tools and techniques that require data recovery, piecing together the puzzle of what happened, and forming a timeline of events.

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

www.fish.com/security/forensics.html

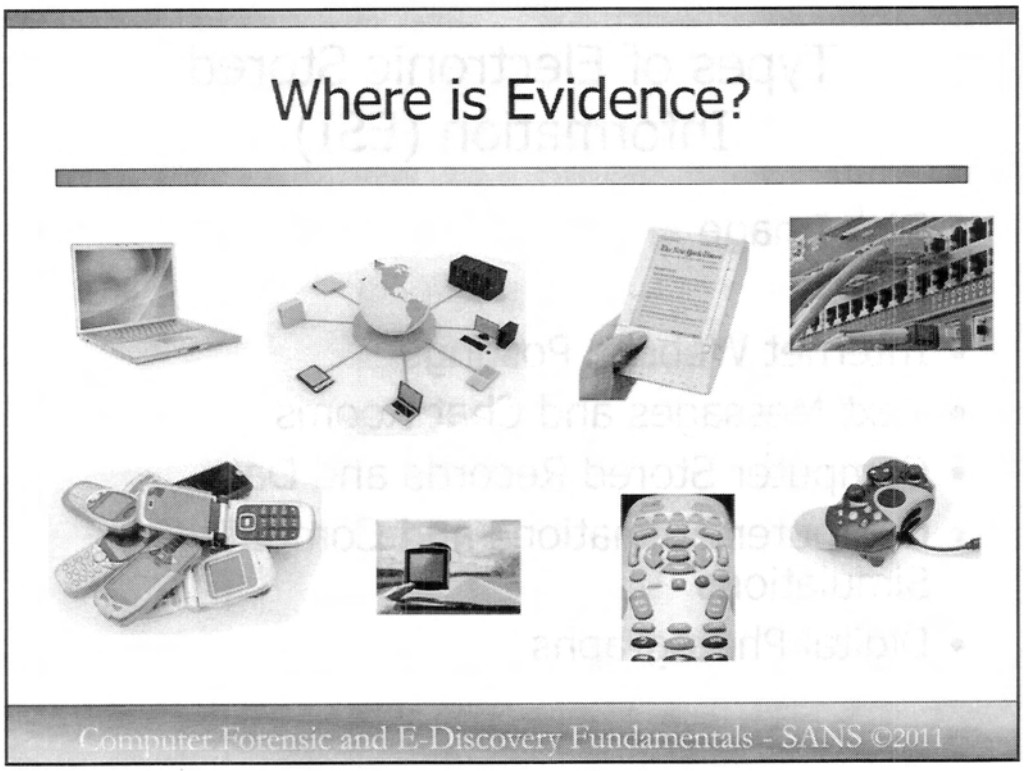


Let's start by defining what evidence is. I think Kevin Mandia put it best in this Incident Response & Computer Forensics Second Edition book when they stated Evidence is any information of probative value.

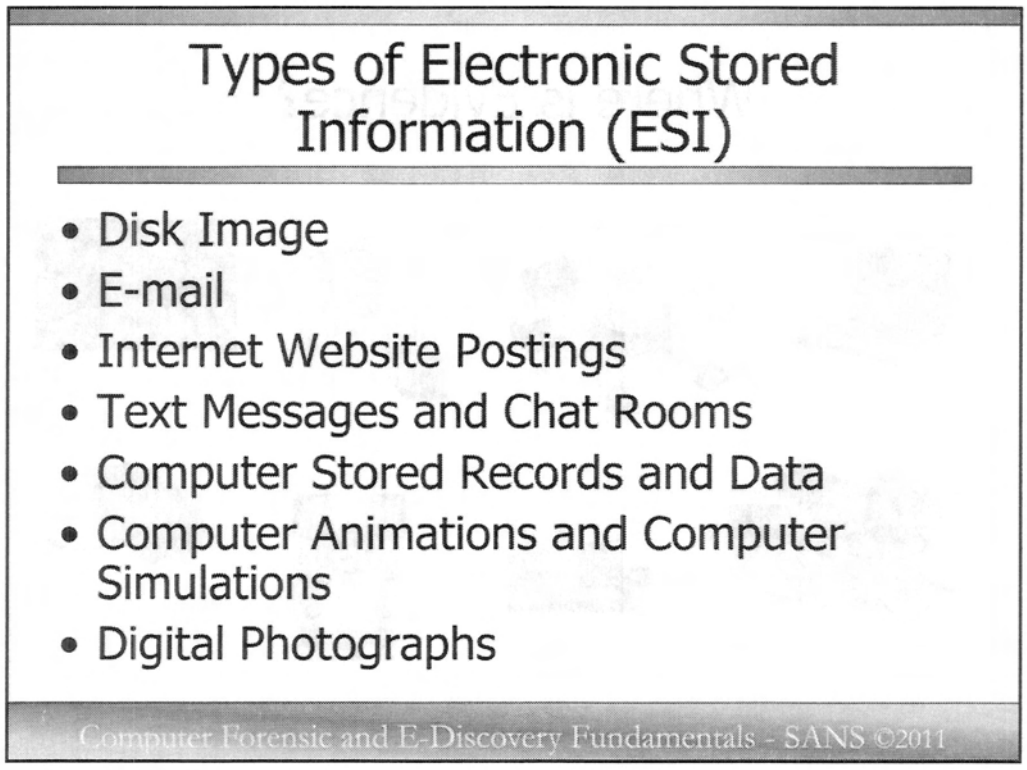
From more of an official point, Rule 401 defines Evidence to be Relevant Evidence as any item having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable that it would be without the evidence.

Because computers are a ubiquitous part of our every day life they hold a great deal of information, otherwise known as evidence, about our thoughts and actions. In most cases, this makes their content relevant to any action or event that may be under investigation, whether through legal channels or our workplace.

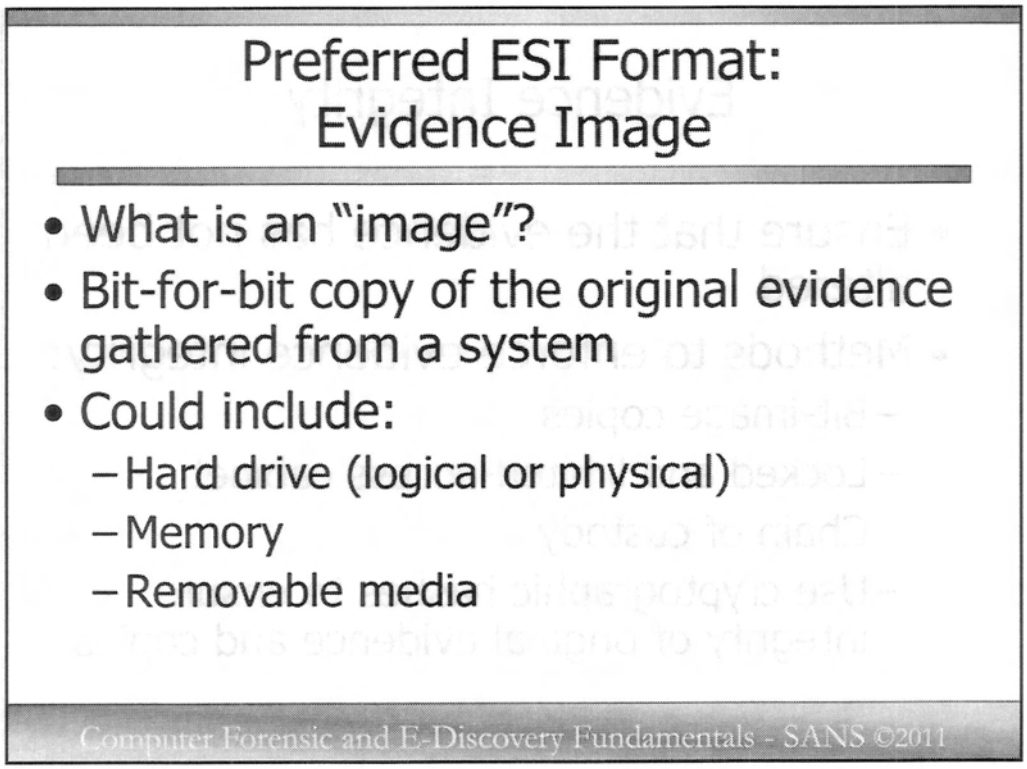
Your understanding of what is evidence and how to collect, protect and testify to it's authenticity is a critical role of a computer forensic examiner.



This page intentionally left blank.

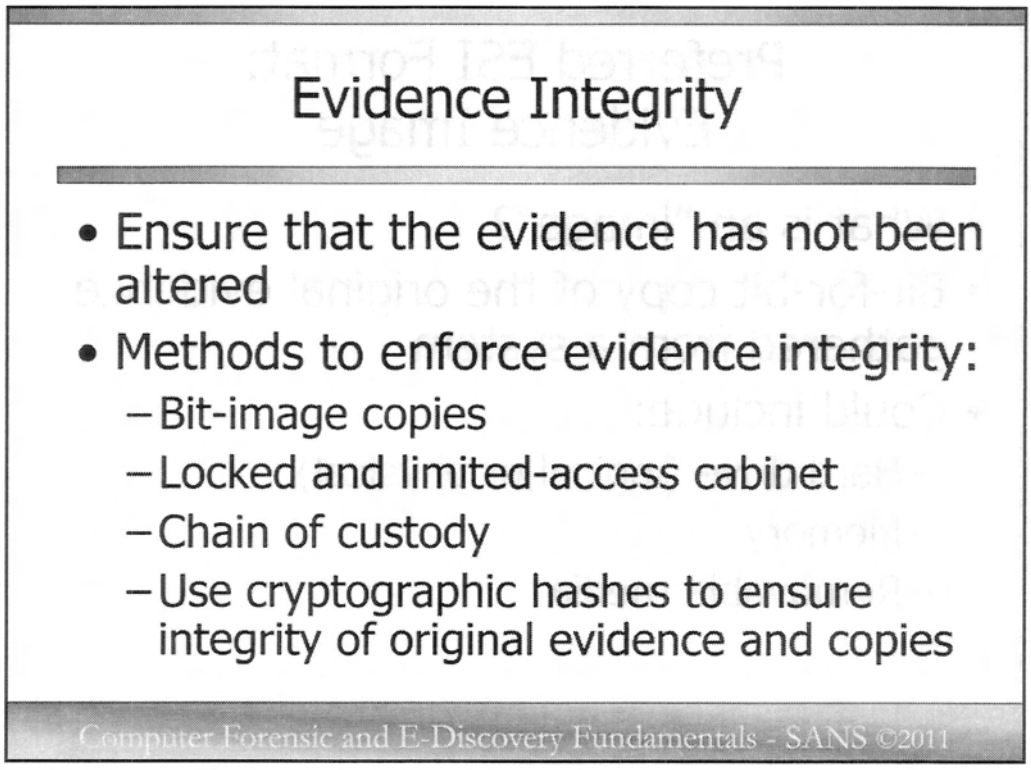


These are some of the types of Electronic Stored Evidence that you might encounter when performing computer forensics. The reason I bring these up is that it is entirely important to ensure that you have an idea of where evidence might exist in a network or a computer system.



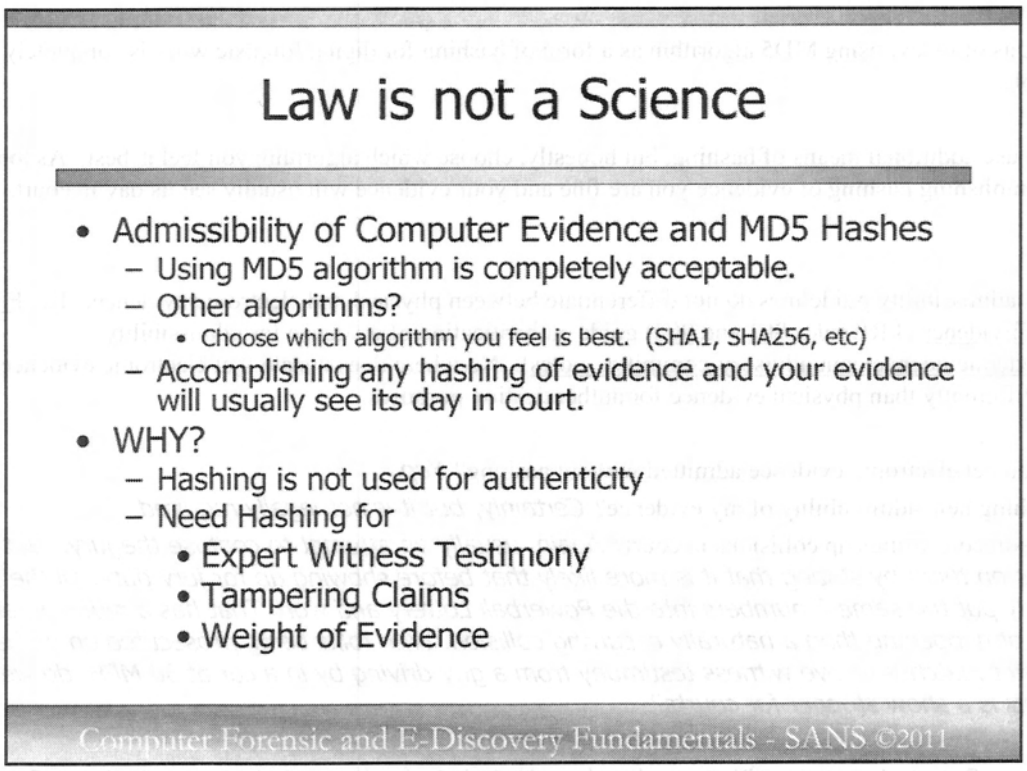
A disk image is a copy of original evidence generally collected by a tool that performs bit-level copying from one location to another. An image is a copy of the original media that is used in media analysis. Like a photograph, it is a snapshot frozen in time of the state of that system and is generally static. Images could include a physical or logical copy of a hard drive, memory dump, or copies of removable media like a CD-ROM.

You should always clearly document how you obtained your image and the process you performed to maintain the image 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 went 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 form to show who has current and previous control of original or best evidence utilized in a case.



FROM AN ARTICLE AT http://sansforensics.wordpress.com/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 seems 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 Federal Rules of Evidence (FRE rules 901 and 902) guide authentication of evidence for admissibility (http://federalevidence.com/advisory-committee-notes). No where 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://www.harvardlawreview.org/forum/issues/119/dec05/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," (http://federalevidence.com/advisory-committee-notes#Rule702). 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 of 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 (see http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm 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*** 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 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. 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 ***1+1=3*** in their world.

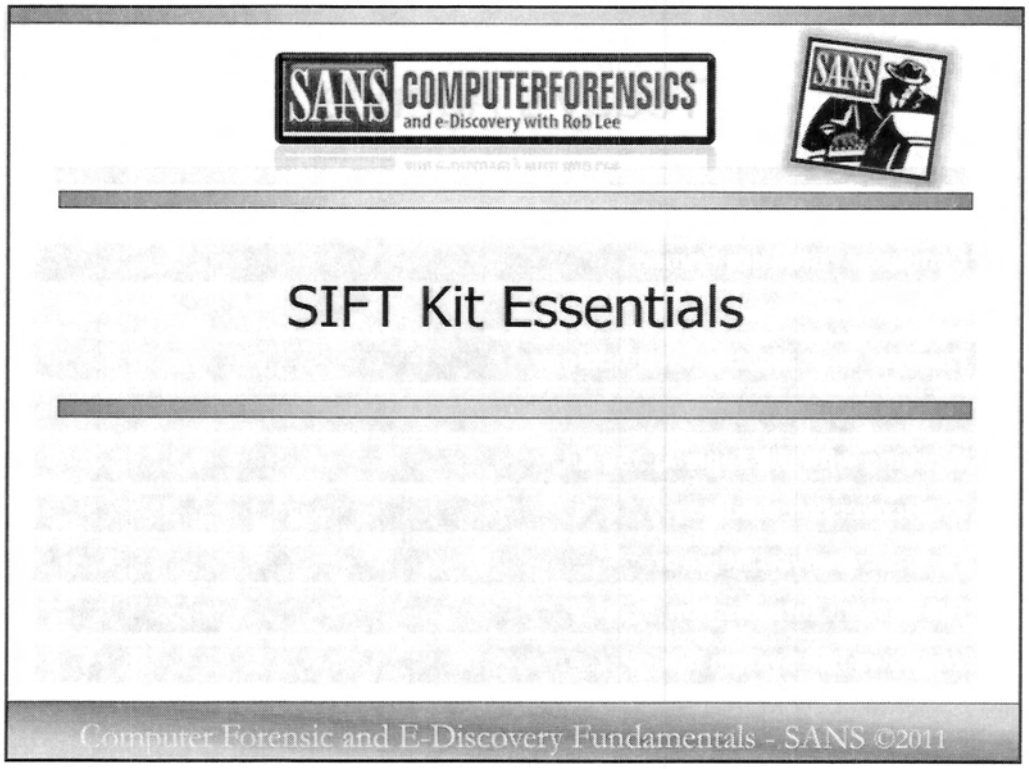
From the blog: (http://ralphlosey.wordpress.com/2008/08/24/tech-v-law-a-plea-for-mutual-respect/)

...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 delusionary 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.***

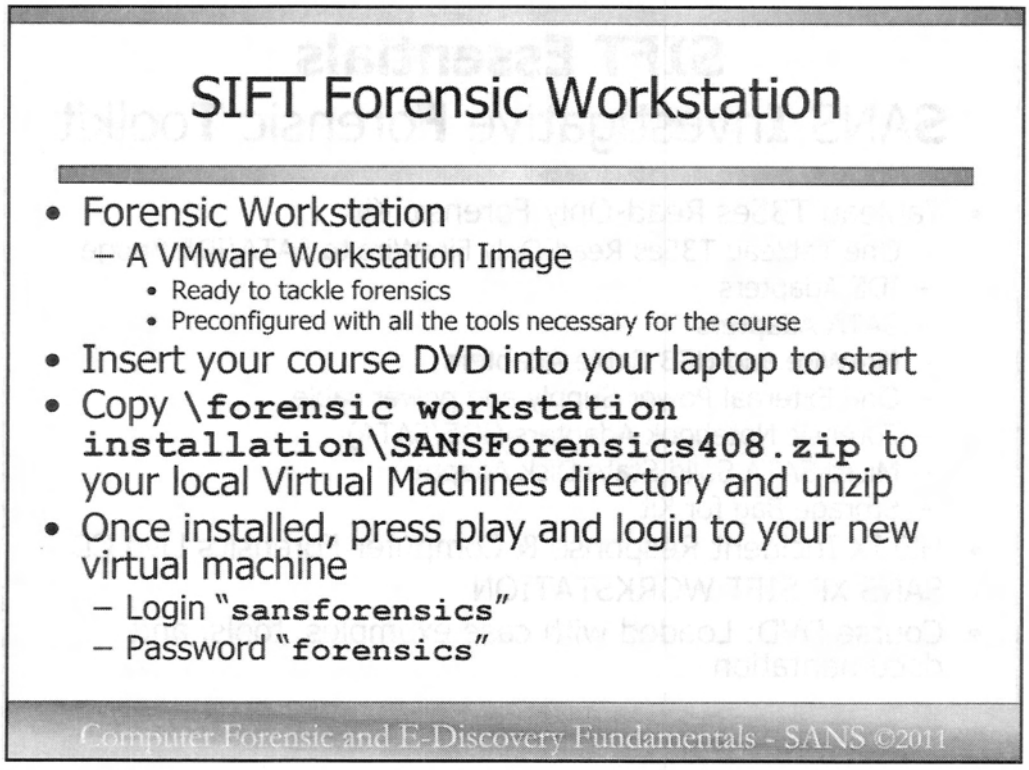
This page intentionally left blank.



This page intentionally left blank.

As part of the course, you will receive the SANS Investigative Forensic Toolkit (SIFT). Using the hardware and software in this toolkit, you will gain first-hand experience in collecting and analyzing evidence recovered from a system under investigation. You will learn best practices on how to investigate and recover deleted data. The course will demonstrate how forensic tools recover evidence so you can articulate how the tool works in-depth. We will examine various investigation methodologies and techniques discovering new places to find evidence and discover the tracks of a motivated suspect who is trying to stay hidden.

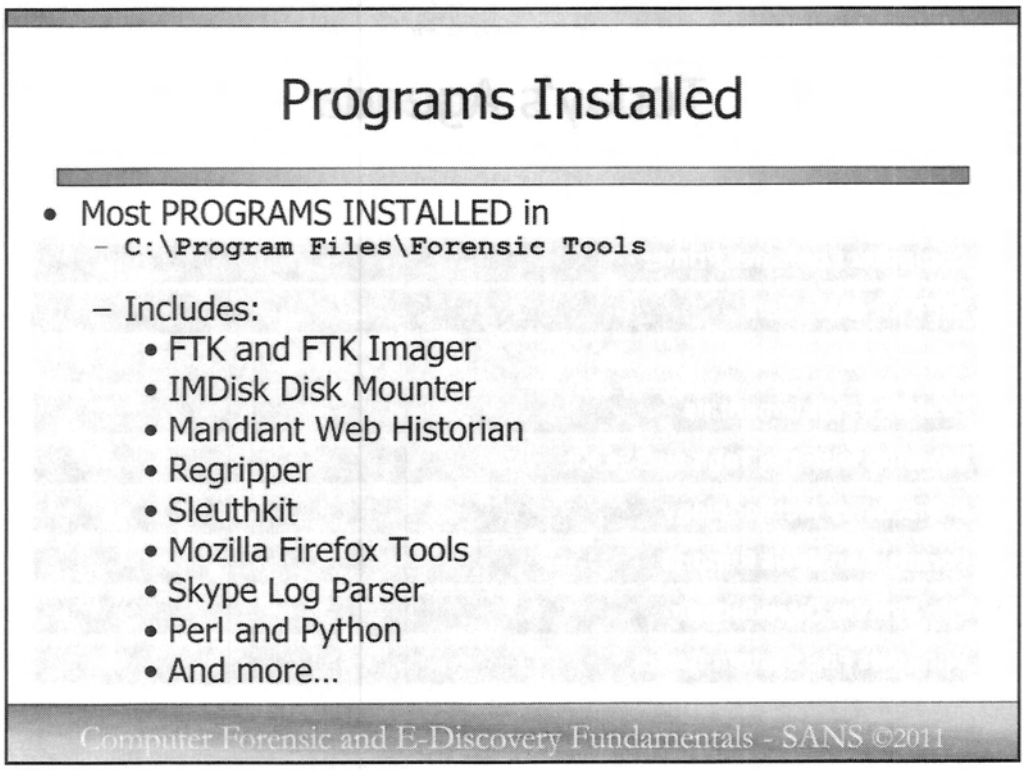
With the T35es in your forensic toolkit, you'll have a robust and reliable forensic bridge with four different host interface connections (eSATA, FireWire 800, FireWire 400, and USB), and two device-side connections (SATA and IDE).



SANS teaches the latest tools and techniques available. In addition, our aim is also to create a laptop setup that is simple to use to accomplish the daily exercises utilizing forensic tools. To solve both challenges, the SANS Institute has released a cutting edge course DVD that includes a new preconfigured **XP VMware Forensic Workstation** that is ready to tackle forensics right off the DVD.

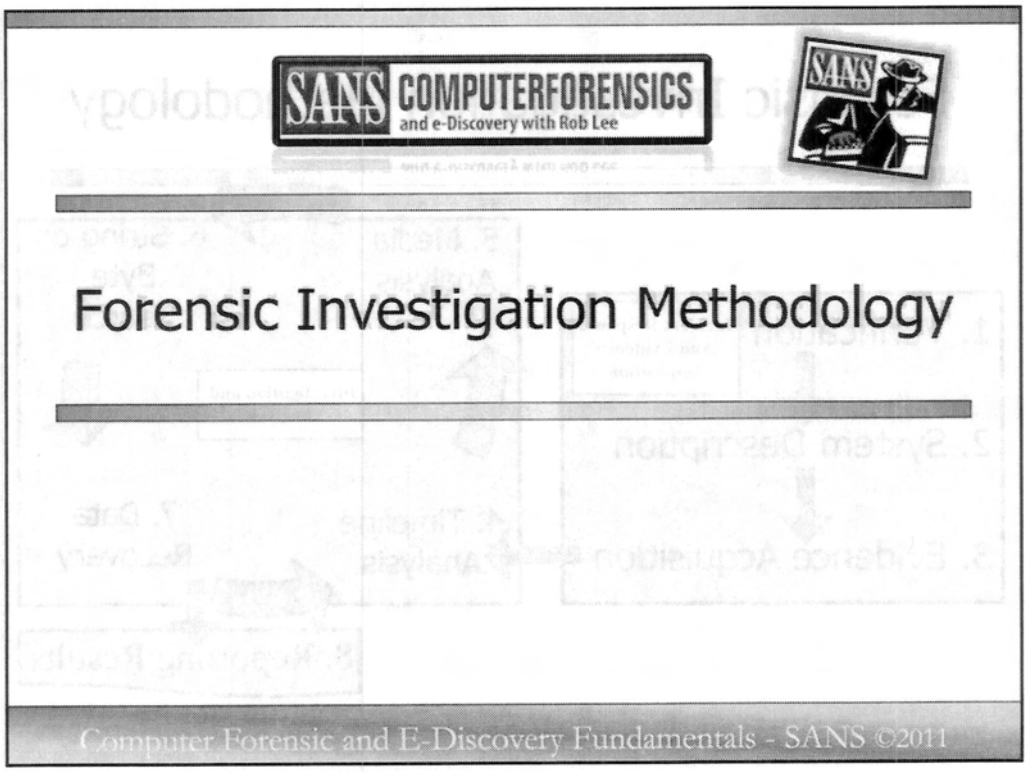
The new VMware image is already pre-configured with all the tools so you can just concentrate on learning the material and not configuring your machine. You will only need to copy over a gzipped tar archive from your DVD to your VMware directory.

For best results on Windows use **WINZIP Version 10 or higher** or **7ZIP. If you do not have WINZIP version 10 or higher, there is one located on your COURSE DVD in the "forensic workstation installation directory."**

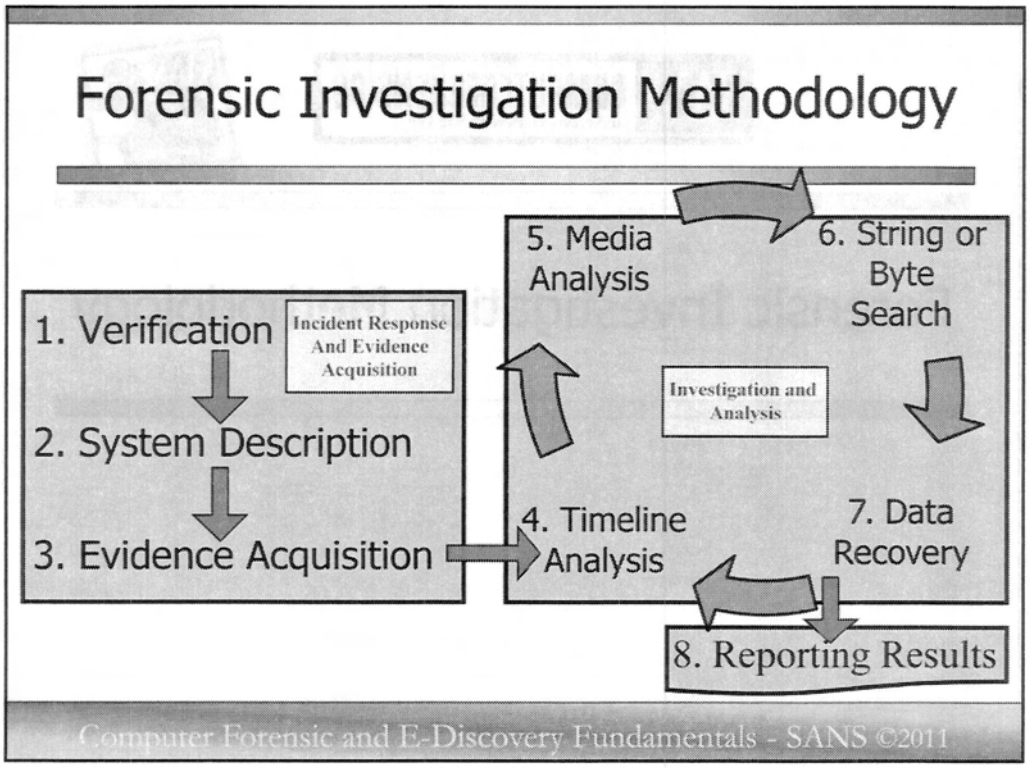


All the programs you will be utilizing in class to analyze Windows and UNIX systems are included pre-installed on the SIFT Forensic Workstation. This will enable you to be ready for the upcoming exercises without having you to install a bunch of tools on your system.

This page intentionally left blank.



This page intentionally left blank.



The overall forensic investigation methodology will remain the same from operating system to operating system. You will probably conduct some, if not all, of these steps in every investigation. Despite the tool that you use, your overall process will and should remain the same. If you use a commercial tool versus an open source toolset, you will still gather evidence, obtain investigation leads, and perform data recovery. Regardless of what your tools are, your methodology will aim to solve the case.

The methodology will help an investigator stay on track during an investigation. You first verify that an incident has taken place. You then provide a in-depth system description that would include the type of operating system and the role the system plays on your network. The third step requires an investigator to gather both volatile and non-volatile evidence from the system. Once evidence has been acquired the investigator would begin his offline analysis of the evidence that was gathered.

The first step of the investigation would be to obtain a timeline of the entire system. The timeline would include the date and time of notification as well as a listing of all files and their modification, access, and changed/created times in a human read-able output. Using this timeline, one could step through file by file discovering additional files and artifacts that the investigator would need to examine closer. The fifth step would be to examine those specific files or entries and determine what they are used for and if they are pertinent to the investigation. For the 4th and the 5th step, the investigator would be collecting information to search and examine at the data layer, looking for relevant strings and bytes that are specific to the case. This is the 6th step, the string or byte search. Once these bytes or strings have been located, the 7th step would be to recover and analyze data that were discovered. Once you recover the data, would return to the timeline and continue analyzing the next entry and continue to perform the subsequent steps until all data has been collected and analyzed from the suspect system.

Finally, once a thorough analysis has been completed, a report will need to be created. The report will detail the investigation, the acquisition and analysis steps, and the conclusive results from the analysis. The methodology is a template to follow as every type of case will need these steps to be performed in order to analyze the evidence from the system.

Evidence acquisition: Evidence is defined as anything that can be collected from the system under investigation. It does not necessarily have to be an image. It could include process information, network connections, log files, and user information. It is best to obtain evidence in as forensically sound a method as possible. This means trying to avoid data loss during any actions that you perform. Take your actions into consideration when you collect evidence and in what order it is collected. Collecting evidence in the wrong order could potentially result in evidence loss.

Evidence collection is a step that needs to be performed and your results from this step need to be clear in your documentation. Not only do you need to describe the tool you used to collect the evidence, you need to describe how you ensure the integrity of that collected evidence.

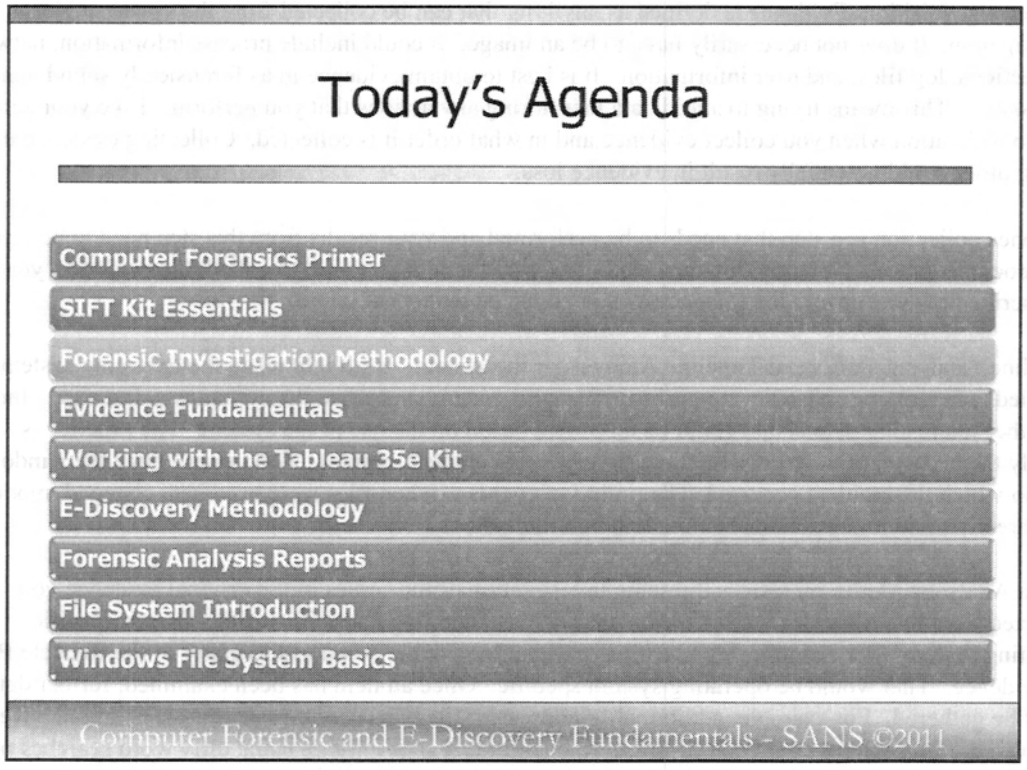
Timeline Analysis: Perform a Timeline Analysis of the system. Highlight when the operating system was installed, when major updates were performed on the system, and when the system was last used. Include any other interesting details that could be discerned based on the use of the system. The timeline is usually the bedrock of your investigation. Everything centers around it. You usually have the window of time in which the incident occurred. The timing of events -- when files were accessed, changed, modified will directly point to the actions that occurred on the system.

Media Analysis: Media analysis is the static investigation of the copies of the original evidence you collected from the system. Usually, media analysis is examining a specific artifact from a specific operating system. For example, an investigator might look at the Windows Registry or the Recycle Bin for evidence. That would be operating system specific. Once an item has been examined, further details might be gathered. For example, additional IP addresses, file names, or e-mail addresses, might have been discovered. These items could be utilized to find additional files through using dirty word searches or through timeline analysis. Rarely should you perform media analysis on a live system. However, if given no other option, you may not have a choice. Your media analysis should focus on recovering specific operating system files and information that will aid your investigation.

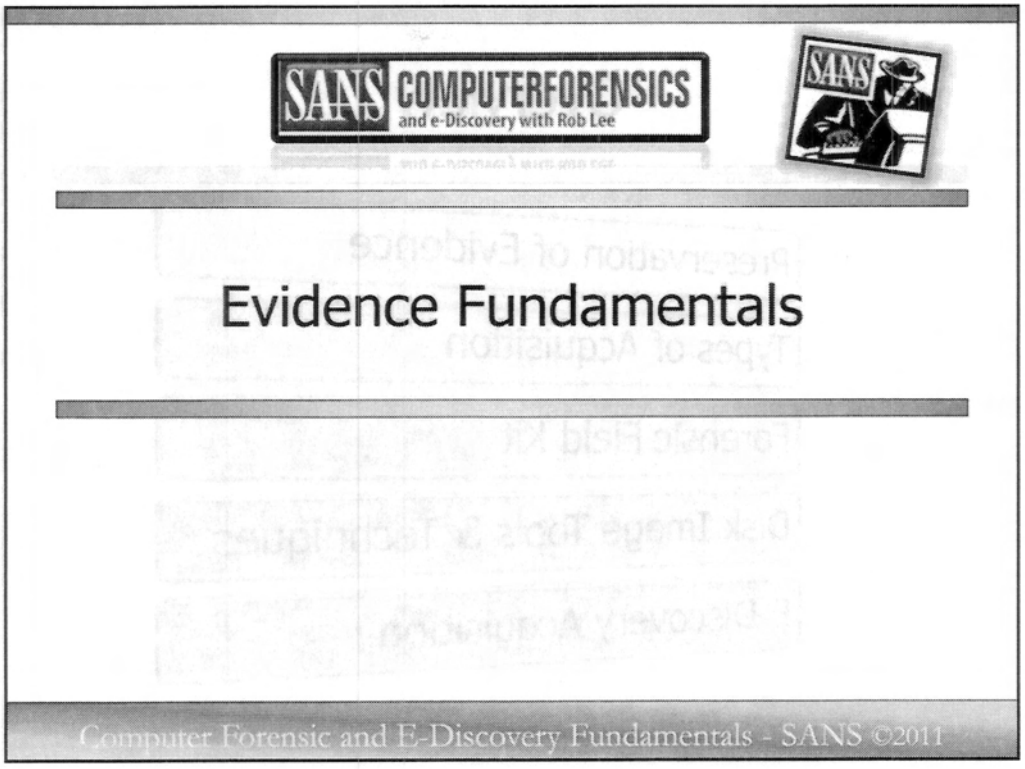
String/Byte Search: String searches make finding data on your collected evidence easy. You can conduct multiple-word string searches on your evidence looking for every term on your dirty word list. The tools you use can find these words in unallocated space, allocated space, or file slack. Your tools should also be able to give you an idea where these hits are made so that you can recover any other information surrounding the file. For example, you may want to look for an e-mail address. If you do, then you have a high likelihood of finding the e-mail body even if the e-mail was deleted, saved, residue in memory or is merely a fragment on your system. This technique is quite invaluable once you have decent dirty word lists associated with your case type.

Data recovery: Recovering data is obviously a key function of forensics. This process would include recovering deleted files, images, and e-mails. It would involve looking for file fragments and unrecoverable data.

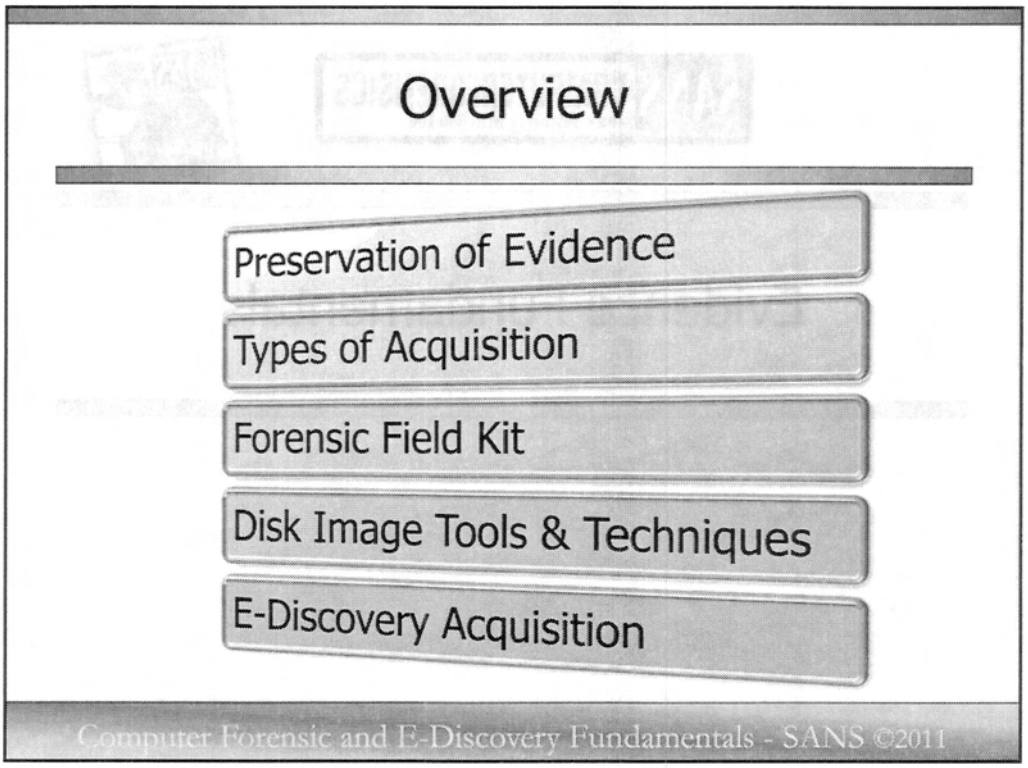
Reporting results: Reporting is not entirely a technical aspect of computer forensics, but it is probably the most important step of the forensic process. Most reporting is done to individuals who may not be educated in computer hardware, networking topics, or computer crime law. You need to ensure that your reporting clearly explains the evidence you found, the techniques you used, and defines everything that is technical. Many investigators unfortunately overlook this easy step because they think that most people can understand how the Internet works or even topics as simple as file downloading. However, in a court of law, or even in your own company, for anyone to utilize your results, they need to make sure that it is understandable. In a nutshell, document everything, explain and define basic and advanced topics, and show the results of your investigation.



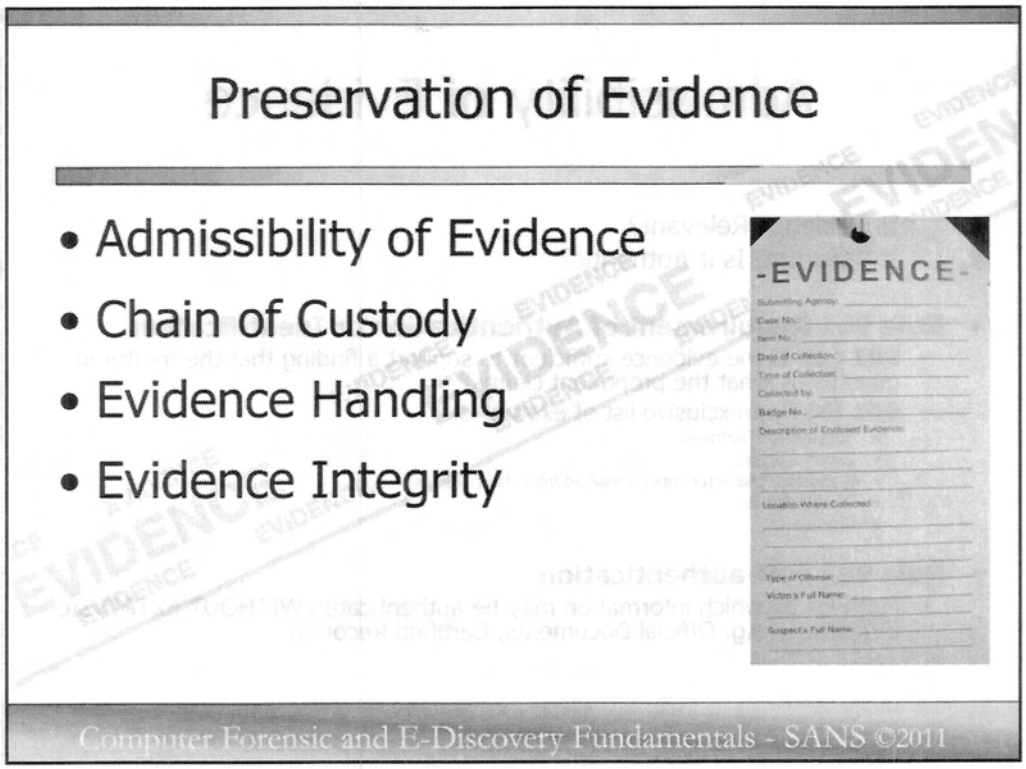
This page intentionally left blank.



This page intentionally left blank.



Today we are going to talk about the fundamental mindset you need to have to be a good forensic examiner/analyst. While we understand many of you will go back to agencies or organizations that may already have established evidence handling procedures, we are also going to discuss the basics of proper preservation of evidence and chain of custody best practices. We will then talk a little about the different types of forensic acquisition, including memory acquisition and volatile data collection, how to name, document and store image files. We will then discuss some of the things that you will want to put into your forensic response kit so when you get out to a search scene you will have all the fundamental tools you need to successfully accomplish the mission. We will talk about acquiring a forensic image across a network and finally we will have a brief discussion about E-Discovery.

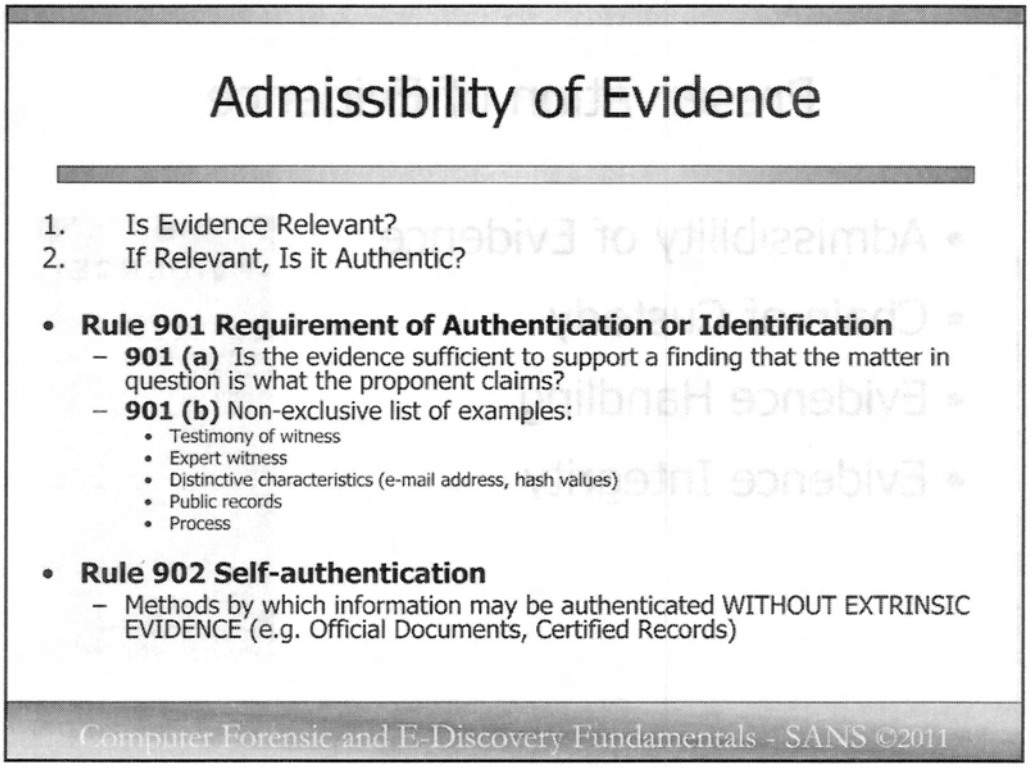


We are going to talk for a few minutes about what evidence is, how and why it is important to maintain a chain of custody. Additionally, we will talk about proper evidence handling and how to insure the integrity of any evidence you may come in contact with.

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, this it is very difficult to argue against the findings. Digital evidence almost speaks for itself.

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



Rule 901. Requirement of Authentication or Identification

(a) General provision.

The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.

(b) Illustrations.

By way of illustration only, and not by way of limitation, the following are examples of authentication or identification conforming with the requirements of this rule:

(1) Testimony of witness with knowledge. Testimony that a matter is what it is claimed to be.

(2) Nonexpert opinion on handwriting. Nonexpert opinion as to the genuineness of handwriting, based upon familiarity not acquired for purposes of the litigation.

(3) Comparison by trier or expert witness. Comparison by the trier of fact or by expert witnesses with specimens which have been authenticated.

(4) Distinctive characteristics and the like. Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances.

(5) Voice identification. Identification of a voice, whether heard firsthand or through mechanical or electronic transmission or recording, by opinion based upon hearing the voice at any time under circumstances connecting it with the alleged speaker.

(6) Telephone conversations. Telephone conversations, by evidence that a call was made to the number assigned at the time by the telephone company to a particular person or business, if (A) in the case of a person, circumstances, including self-identification, show the person answering to be the one called, or (B) in the case of a business, the call was made to a place of business and the conversation related to business reasonably transacted over the telephone.

(7) Public records or reports. Evidence that a writing authorized by law to be recorded or filed and in fact recorded or filed in a public office, or a purported public record, report, statement, or data compilation, in any form, is from the public office where items of this nature are kept.

(8) Ancient documents or data compilation. Evidence that a document or data compilation, in any form, (A) is in such condition as to create no suspicion concerning its authenticity, (B) was in a place where it, if authentic, would likely be, and (C) has been in existence 20 years or more at the time it is offered.

(9) Process or system. Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.

(10) Methods provided by statute or rule. Any method of authentication or identification provided by Act of Congress or by other rules prescribed by the Supreme Court pursuant to statutory authority.

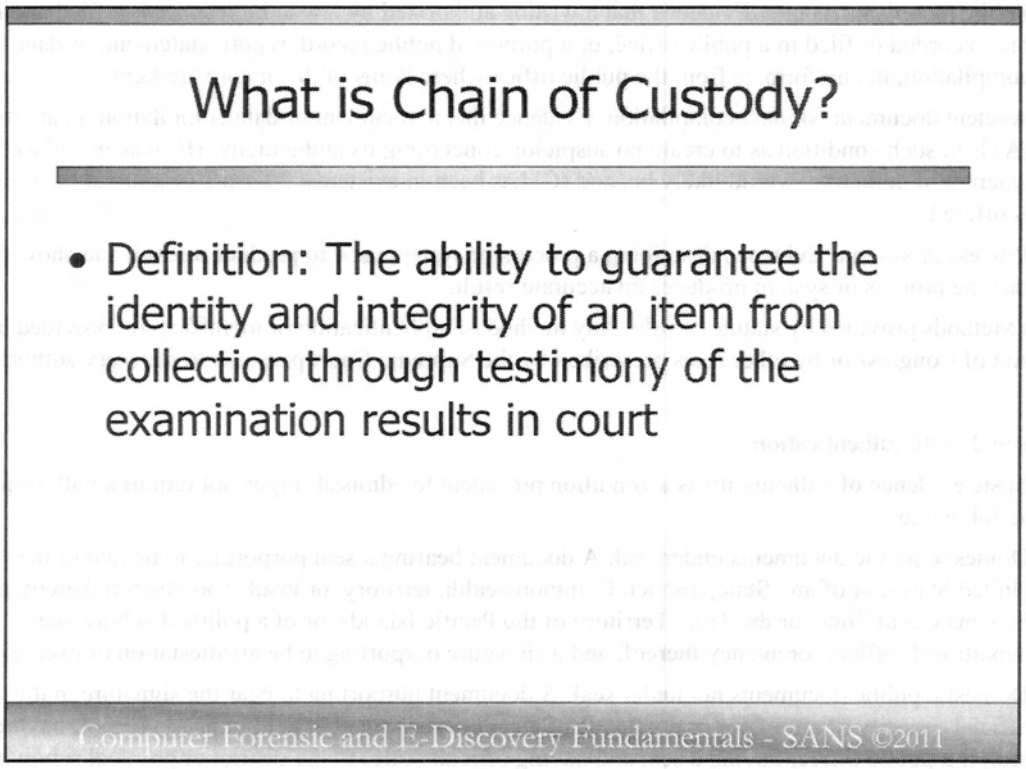
Rule 902. Self-authentication

Extrinsic evidence of authenticity as a condition precedent to admissibility is not required with respect to the following:

(1) Domestic public documents under seal. A document bearing a seal purporting to be that of the United States, or of any State, district, Commonwealth, territory, or insular possession thereof, or the Panama Canal Zone, or the Trust Territory of the Pacific Islands, or of a political subdivision, department, officer, or agency thereof, and a signature purporting to be an attestation or execution.

(2) Domestic public documents not under seal. A document purporting to bear the signature in the official capacity of an officer or employee of any entity included in paragraph (1) hereof, having no seal, if a public officer having a seal and having official duties in the district or political subdivision of the officer or employee certifies under seal that the signer has the official capacity and that the signature is genuine.

Reference: http://www.law.cornell.edu/rules/fre/rules.htm#Rule901

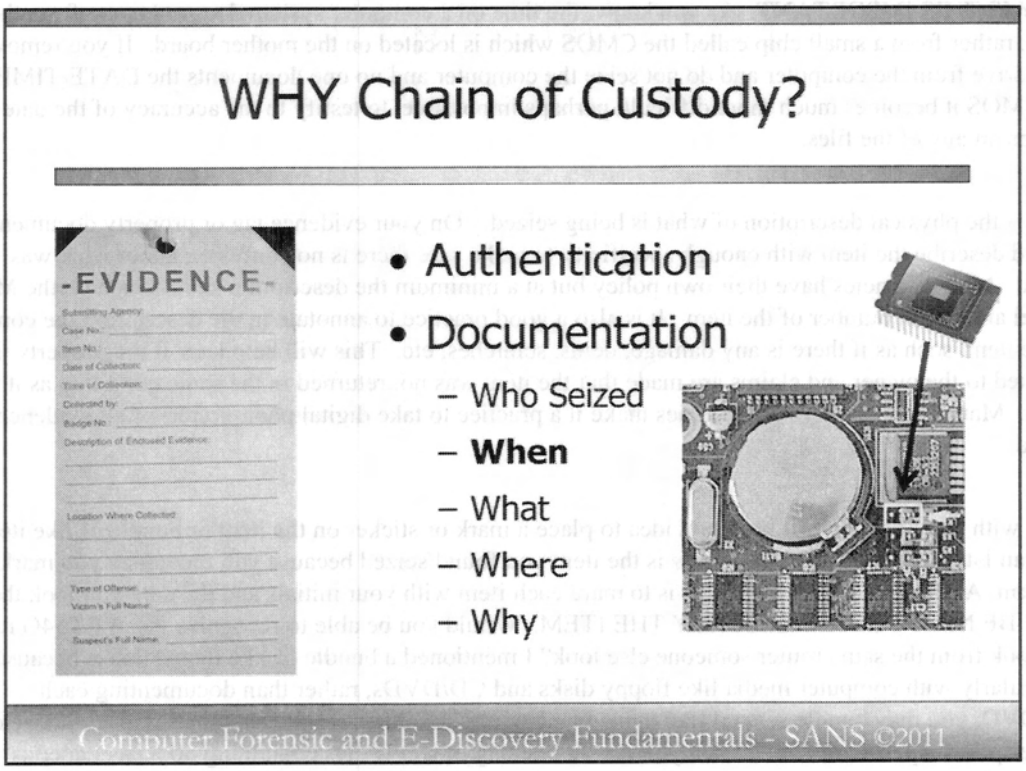


Now that we know what evidence is, let's define Chain of Custody. Essentially, chain of custody is the ability to guarantee the identity and integrity of an item from collection through testimony of the evidence in court. It is the chronological documentation, and/or paper trail through the lifespan 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 it to guarantee the item of evidence has not changed since someone seized it.

There is something slightly different with digital evidence that 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 items 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.

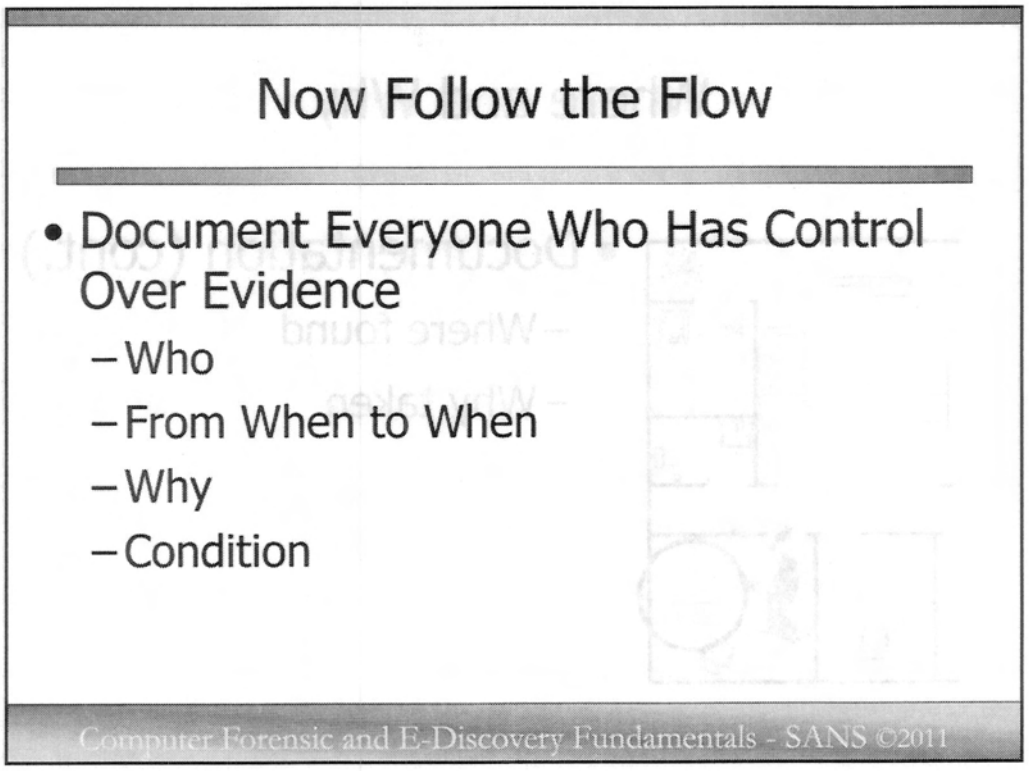
The next item to be documented is when the item was seized. This will establish the starting point for the chain of custody. With computer systems, there are TWO times that should be documents. The first is the actual time. This should be as accurate as possible and frequently seizing officials will 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 the CMOS (complementary metal oxide semiconductor) time.

WHY IS THIS 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 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 you mark on the item. A good practice used by LE is to mare 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

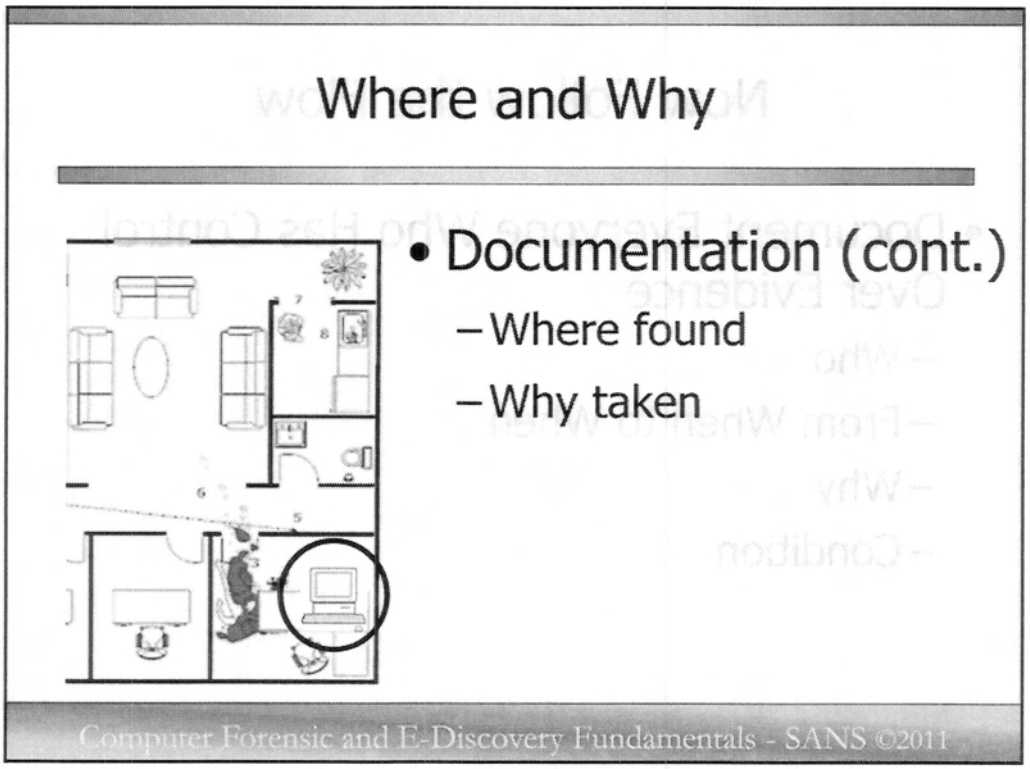
Full name of the person taking control of the evidence

Date/Time of the transfer of evidence

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"

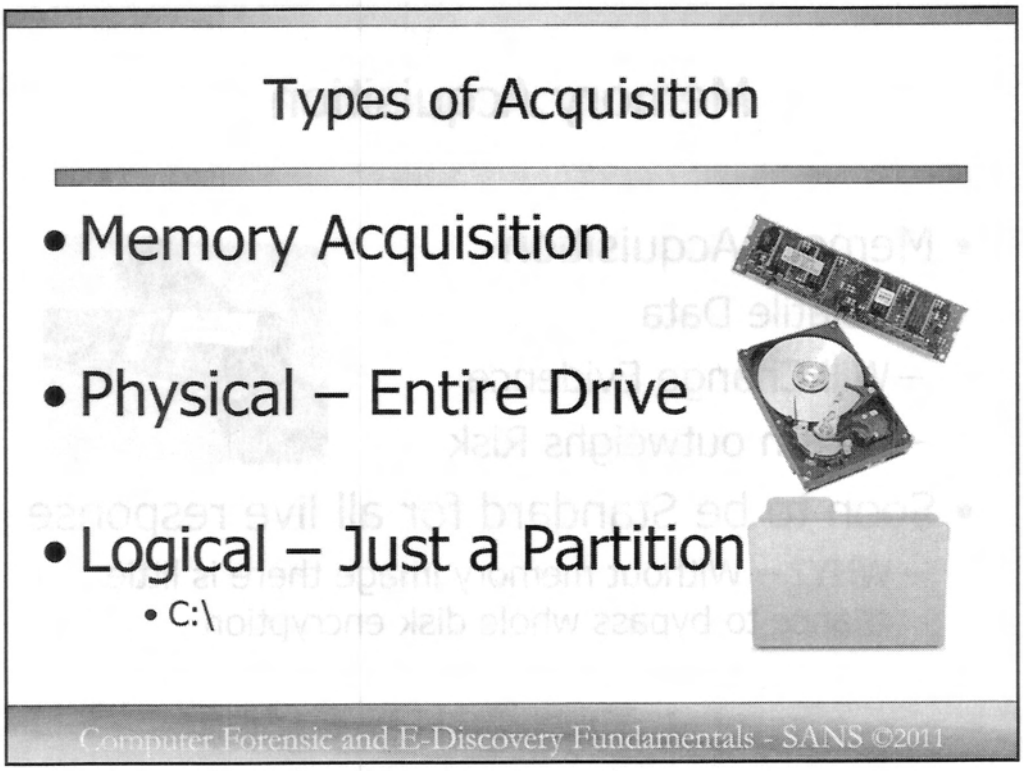
If you have an evidence custodian, you should also document the transfer of evidence to and from the evidence custodian.



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 North West 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 mention 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 has 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.



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

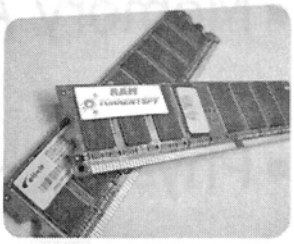
The first is memory acquisition which is also sometimes referred to as volatile data collection. For incident responders investigating hacking cases this is not really anything dramatically new but for non-hacking cases, cases like child porn or any other type of crime, in the past, incident responders 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 or image portions of a server, perhaps only imaging certain directories that the subject/user has write permissions to access and store data.

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

Computer Forensic and E-Discovery Fundamentals - SANS ©2011

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 10 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.

The Department of Justice advocates incident responders to be trained so they can collect/preserve as much volatile data as possible. The old argument that you are changing/altering evidence to 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 collect volatile data.

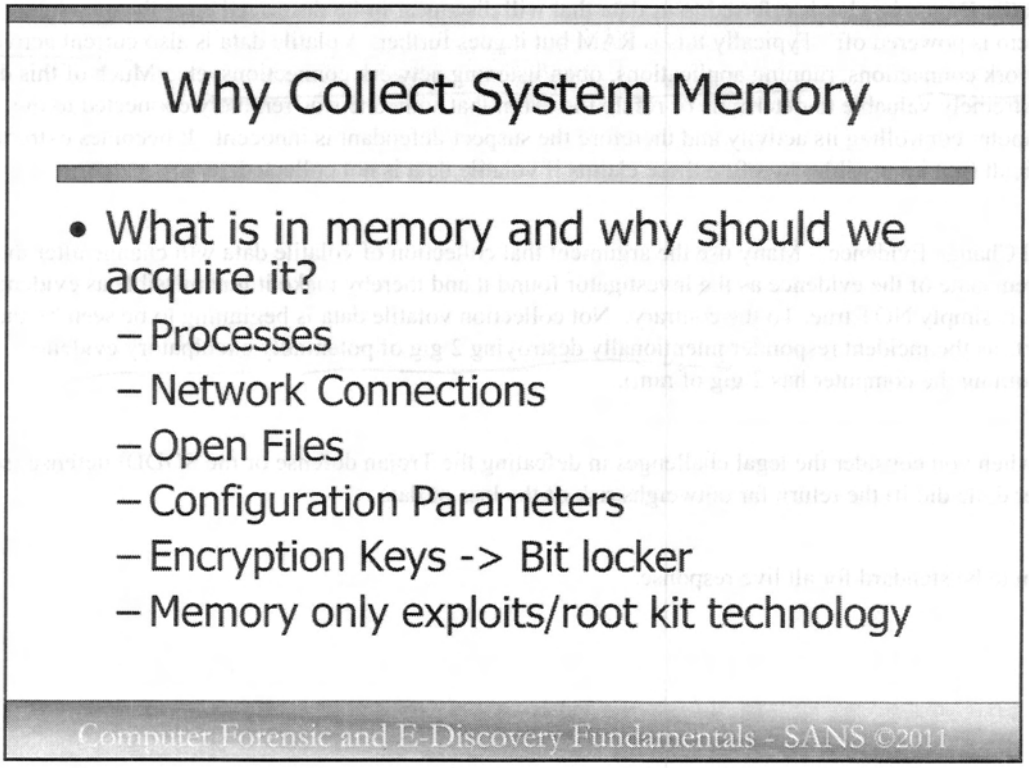
With the increased popularity of encryption programs, pulling the power plug has already resulted in LE having noting to examine. Additionally, a growing popular claim from defense attorneys is that the system was being controlled by a remote administrative utility/Trojan or a virus was causing all the activity. Without the collection of volatile data, it becomes much more difficult to defend against or refute.

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 collection volatile data is beginning to be seen by the courts as the incident responder intentionally destroying 2 gig of potentially exculpatory evidence (assuming the computer has 2 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.



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 website 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.

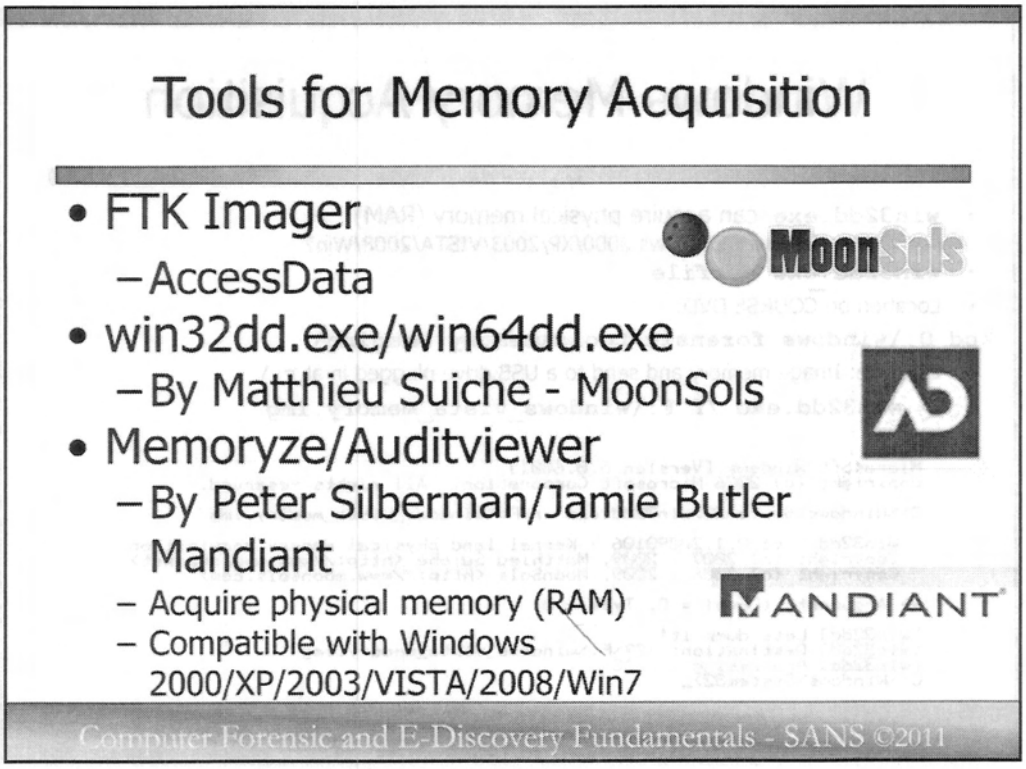
With the increase use of encryption, particularly whole disk encryption utilities like Windows Bit locker, PGP and True Crypt, it is more important now than ever before for incident responders to image RAM and collect volatile data on any powered on system they respond to. While it is the most volatile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

Sec 508 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)



There are currently a few tools available for memory acquisition. F-Response is 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. It will show up as a physical drive. 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.

Brand new memory imaging capability was released by Matthieu Suiche. win32dd.exe acquires a forensic image of physical memory in a raw format. The program written by Matthieu Suiche create an open-source and free solution to provide an ability to acquire a raw image of memory.

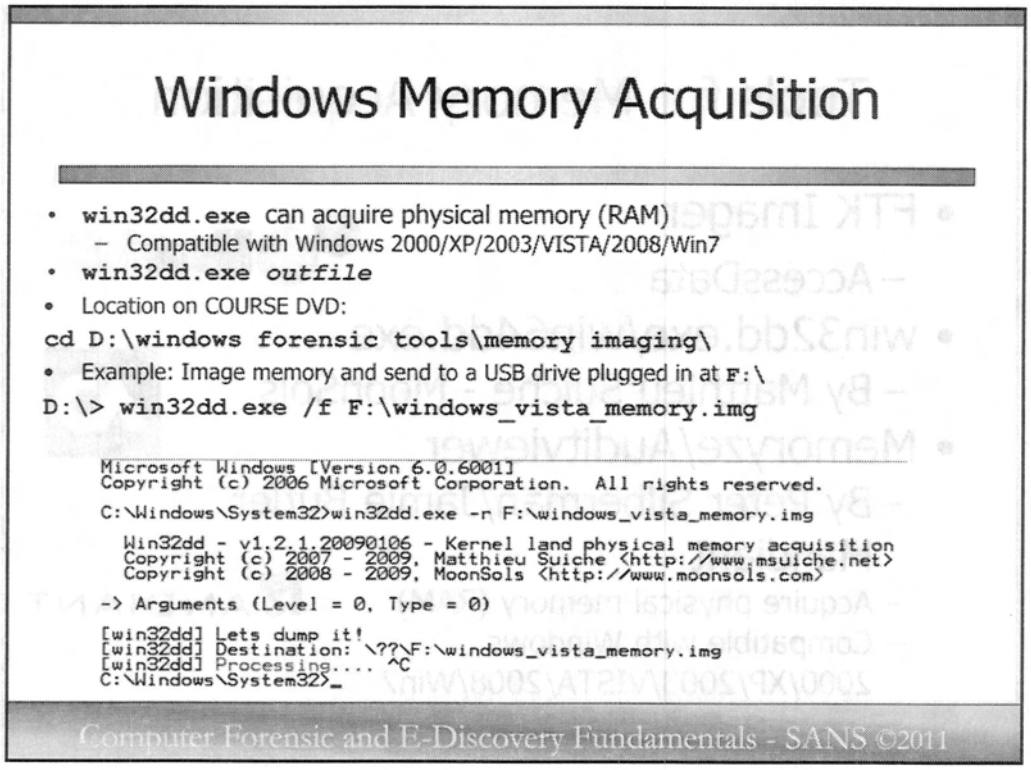
The tool will automatically produce an MD5 hash as a part of its output. In addition, while it is running you can watch the progress "meter" by seeing the percentage of completion on the command prompt window title.

MDD is a physical memory acquisition tool for imaging Windows based computers created by the innovative minds at ManTech International Corporation. MDD is capable of acquiring memory images from Win2000, XP, Vista and Windows Server.

You can take HELIX with you to your response scene and use it to acquire live images on most platforms as well as use it to image difficult platforms such as Servers using Raid cards.

HELIX has many purposes but the basic two are for obtaining live data from running systems and acquiring a forensics image from a system. HELIX works very well on acquiring systems that utilize large RAID devices. HELIX has many uses and they are only limited by hardware.

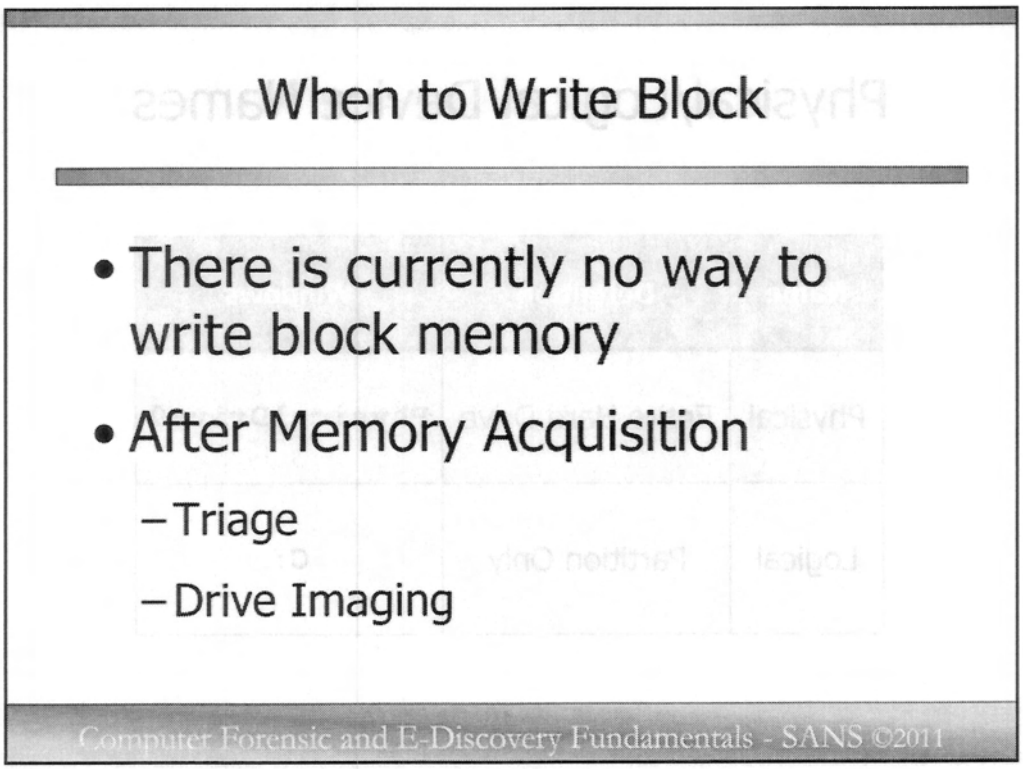
You can get the HELIX ISO file from the e-fense web site at http://www.e-fense.com/tools



Brand new memory imaging capability was released by Matthieu Suiche. win32dd.exe acquires a forensic image of physical memory in a raw format. The program written by Matthieu Suiche create an open-source and free solution to provide an ability to acquire a raw image of memory.

The tool will automatically produce an MD5 hash as a part of its output. In addition, while it is running you can watch the progress "meter" by seeing the percentage of completion on the command prompt window title.

This is an example of win32dd.exe collecting memory from a VISTA machine with 4GB memory. Notice only 3GB of memory is collected? Why? Windows 32 Bit can only see a max of 3 GB of memory even though you might have a total of 4 GB of RAM in the computer itself.



There is currently now 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 wont this invalidate you evidence? NO.

As long as you can document your actions and what changes you caused, you 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.

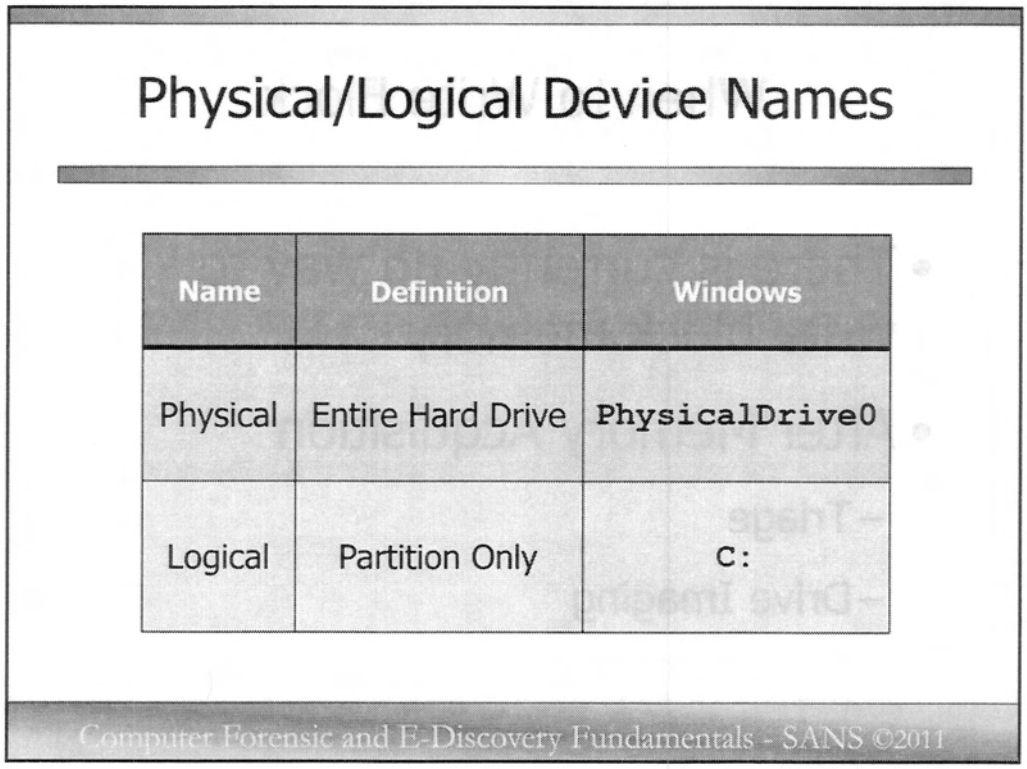
After memory acquisition, you can now shut the system down and apply a write block. We will discuss some of the various types of write blocks later.

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. Once write blocked, a review or extraction of specific files are areas of the computer files are quickly given an initial analysis.

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.

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



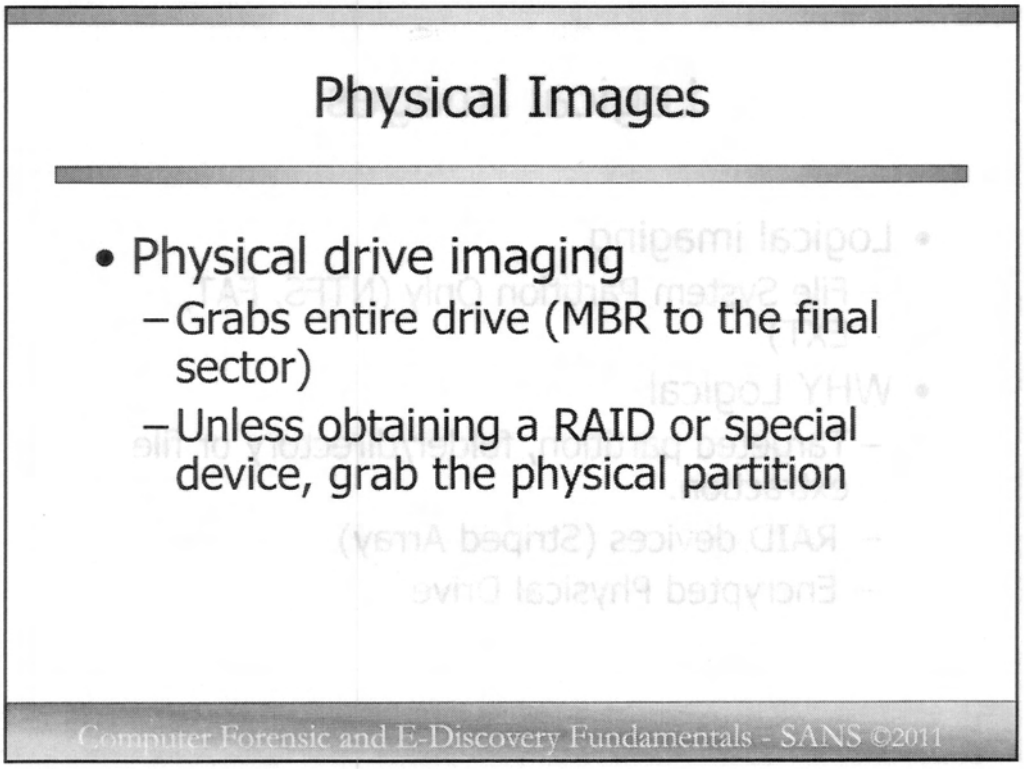
This is a chart to easily show you the differences in architecture between a typical Linux-based system and a Windows one.

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 systems main partition. In the Unix world, this would be equivalent to the /dev/hda1 or /dev/sda1.

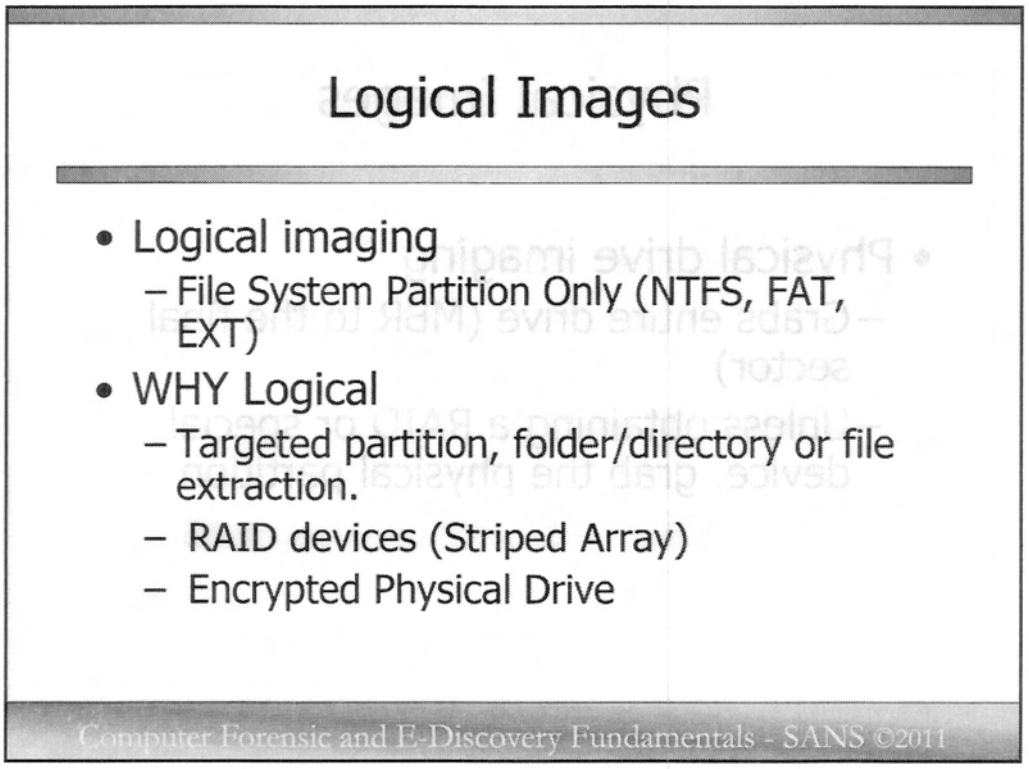
For dd.exe to work correctly you need to become familiar with how Windows calls the nomenclature of these entire drives instead of looking for a single file on these drives. The entire drive C: is called "\\.\C:" or the entire D: is called "\\.\D:"

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.



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.

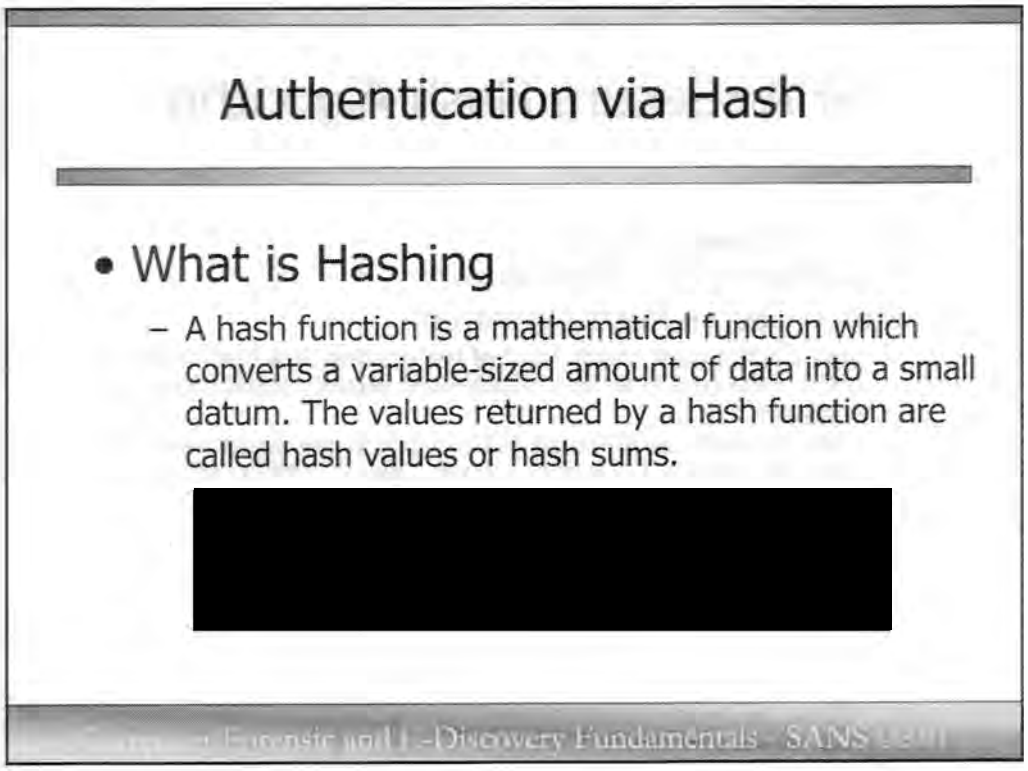


Logical backups are most commonly used when imaging RAID systems or corporate systems where you only need or are authorized to image/extract a specific partition, directory/folder or set of files.

We will demonstrate later in the course that you can use FTK Imager to image specific partition, directory/folder or set of files yet still do this in a way 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.

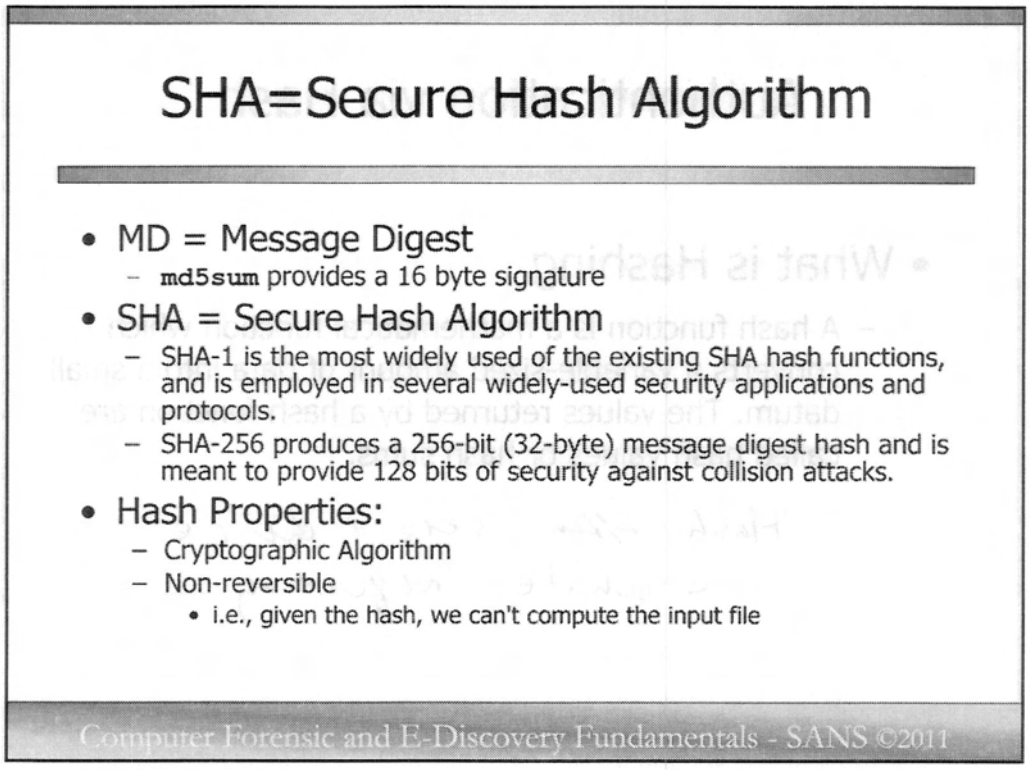


The Hashing process uses "hash" algorithms, which verify that the acquired image is an exact copy of the original media. The Message Digest 5 (MD5) and Secure Hash Algorithm-2 (SHA-2) are the two most common hash algorithms.

Hashing take 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.



The two most common Hashes are the MD5 Hash and SHA256 (sometimes called SHA-2).

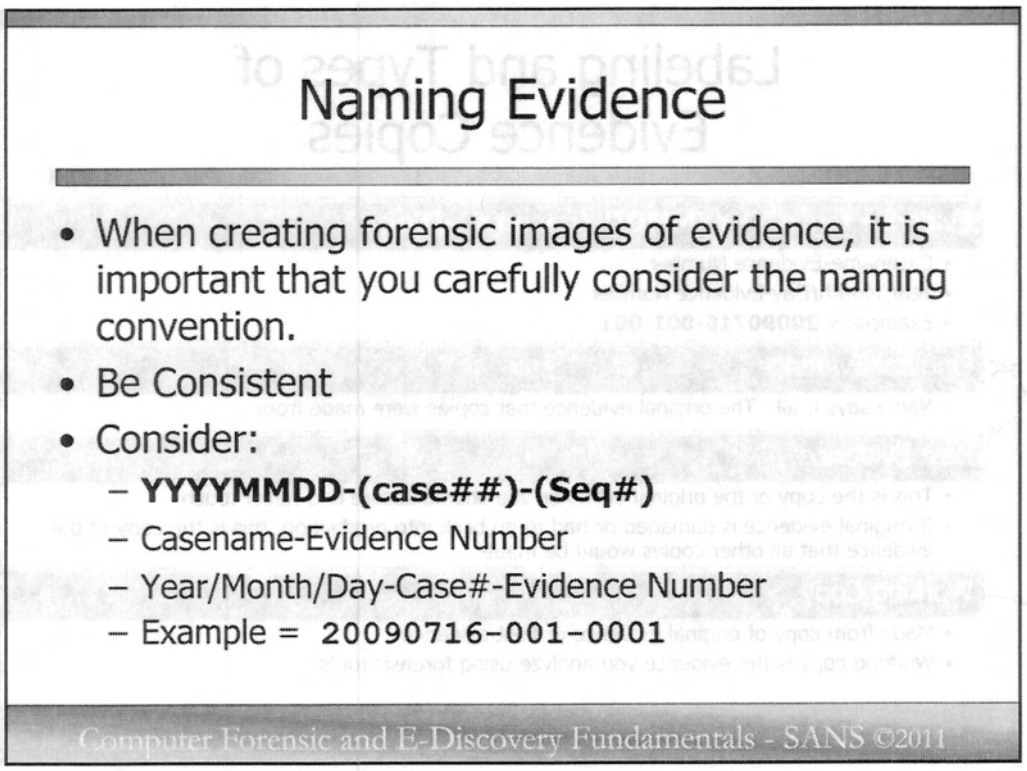
The command md5sum will compute a 128 bit or 16 byte signature of the content of a file(s).

The Sha256 will compute a 256-bit (32 byte) signature of a file(s).

These and other hashes can be used to verify that zero 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 copies hash.

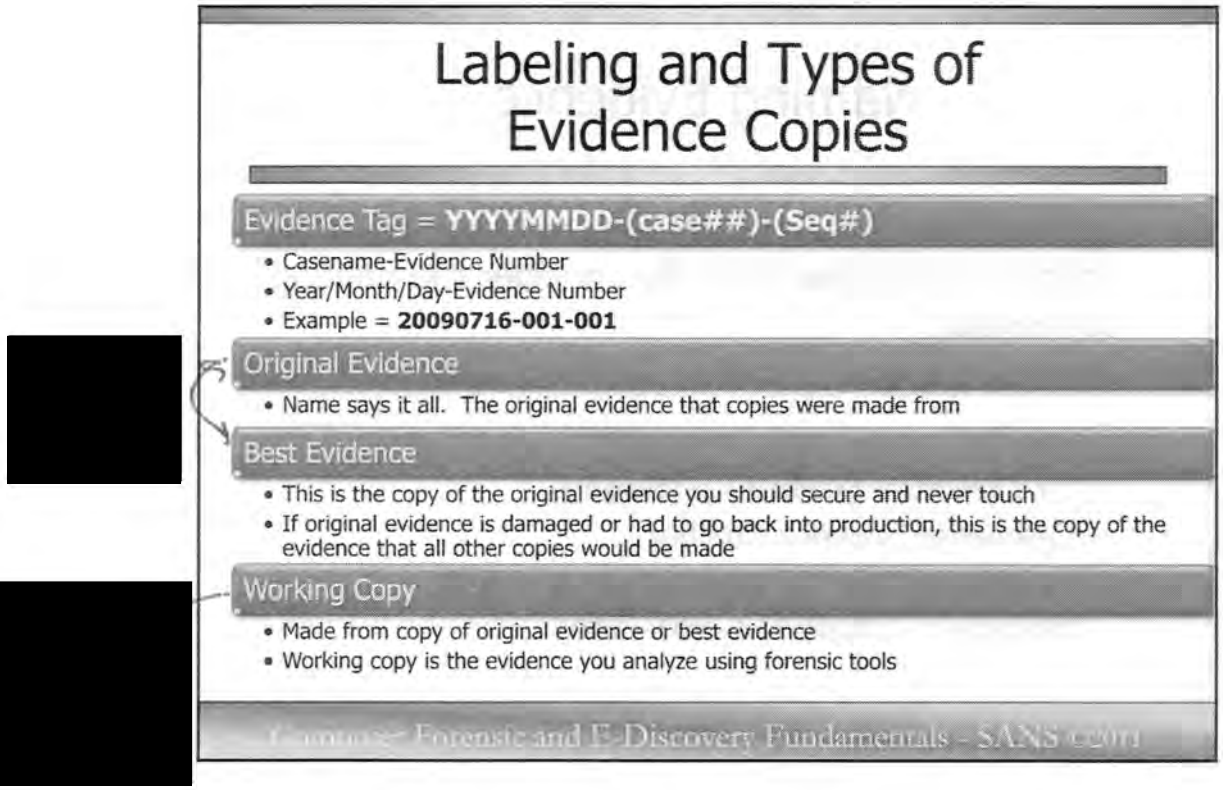
If a single bit of data is different from one version to another, it will have a different md5 signature.

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.



This naming convention will allow you to immediately date the evidence and know which case and evidence tag number it is. 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 what 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 moved 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 intro 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

This is the copy of the original 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

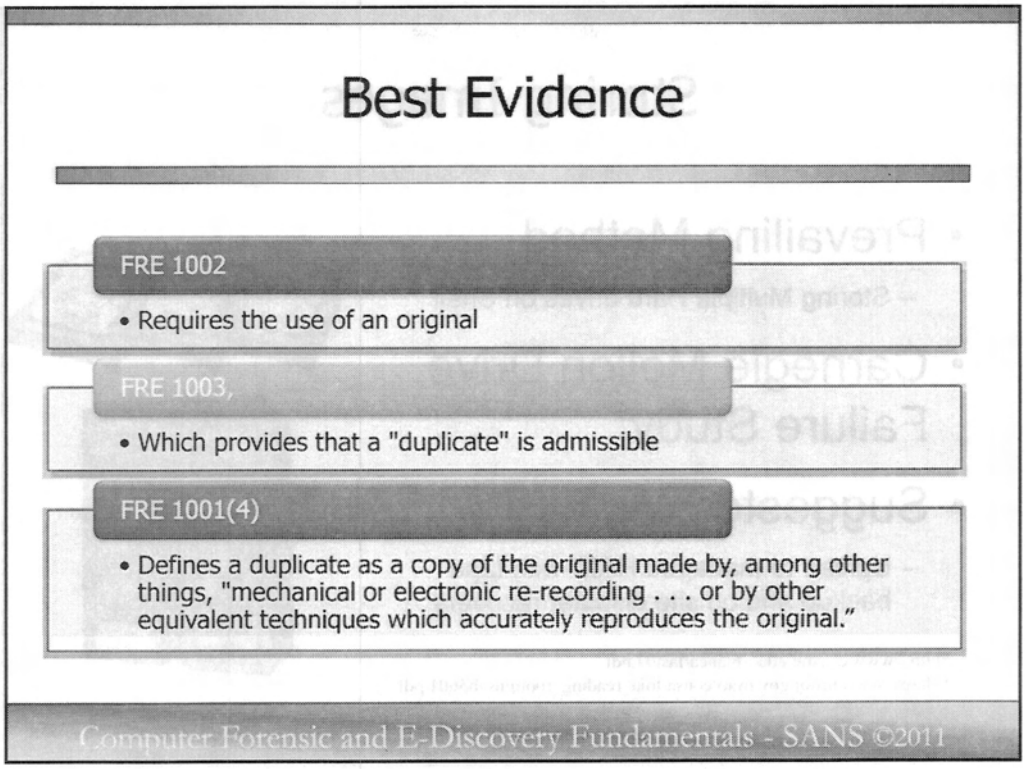
The second copy of the evidence you make should be labeled the WORKING COPY. The WORKING COPY is the evidence you will actually examine.

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.



Best evidence issues

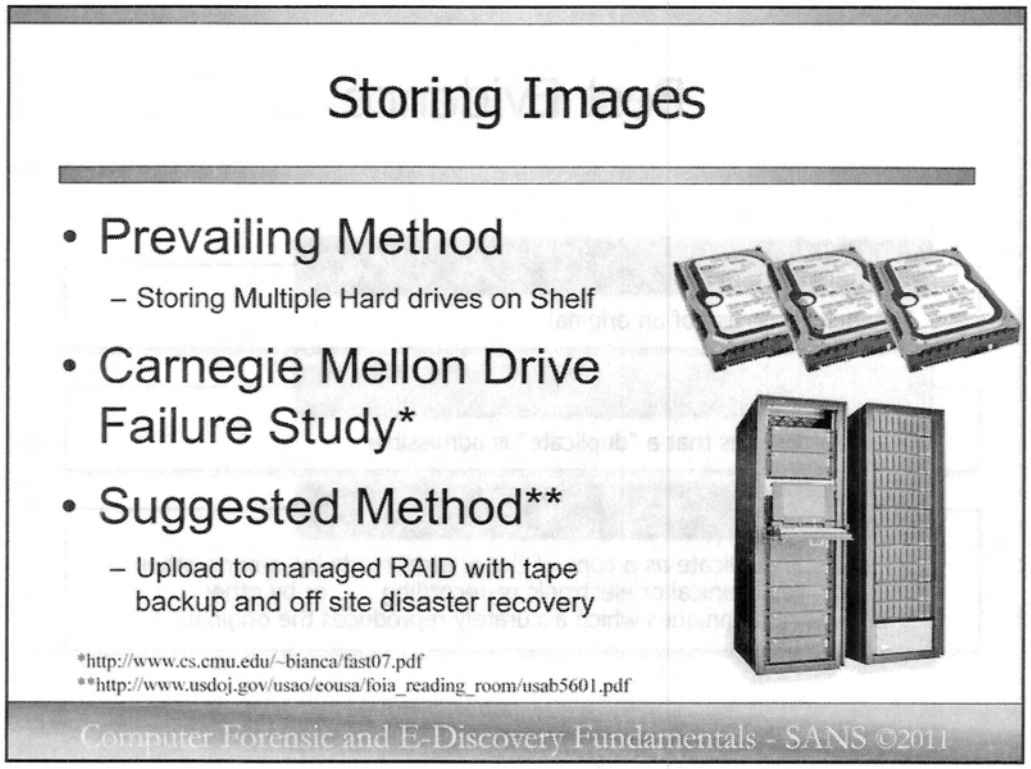
Federal Rule of Evidence 1002 requires the use of an original

Federal Rule of Evidence 1003, which provides that a "duplicate" is admissible

Federal Rule of Evidence 1001(4) 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."

Based on the Federal Rule of Evidence 1001(4) 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.



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.

There have been 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. Some failure rates were as high as 13%. 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 up to a managed RAID (Redundant Array of Independent (or Inexpensive) Disks) systems that has off sit 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).

http://www.ncjrs.gov/pdffiles/nij/178280.pdf

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, No1 which can be found online at the link listed.

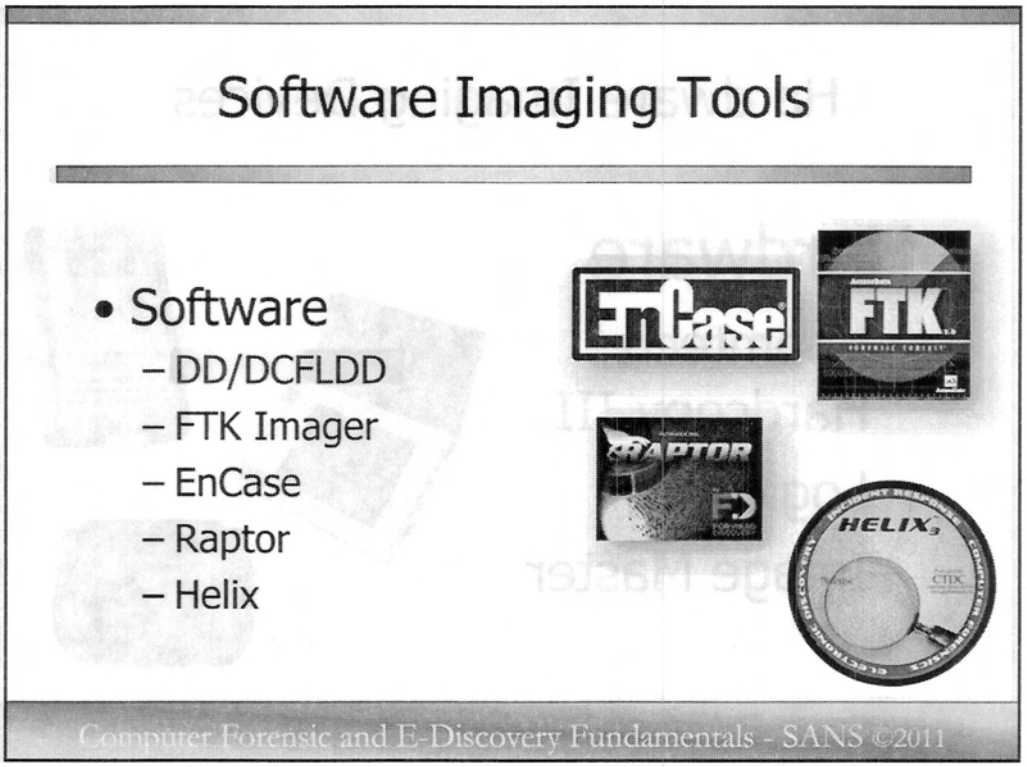
There are several different models of Hardware imaging devices. If you do a lot of incident response it will pay to contact the vendors and see if you can get a demo version to test and compare which of the devices perform the best. Some of the systems advertise they image at 3-6 gigabyte a minute but actually image at less than 1 GB per minute.

The Voomtech Hardcopy is my favorite device. It is a light weight device with only three buttons. The makers modified this from their original device when I asked them to because the first device requires one extra step to create hash when imaging. Now, you plug your drive into the correct labeled slots, push the green button three times and off you go. It is also the least expensive.

The Solo Image master II is a solid device with a touch LCD screen. It has a lot of extra features and the metal cover makes it pretty rugged.

The Logicube is another handheld imaging device that is much like the image master. It also has a lot of features, very easy to use, is rugged but is the most expensive of the bunch.

These of Hardware imaging devices can really be a force multiplier out at the search scene because you can set one or two of these up imaging drives while you are imaging another with your software imaging tools.



The most common way to create forensic image files is with the use of hard ware write blocks and software tools. So let's quickly discuss a few of these tools.

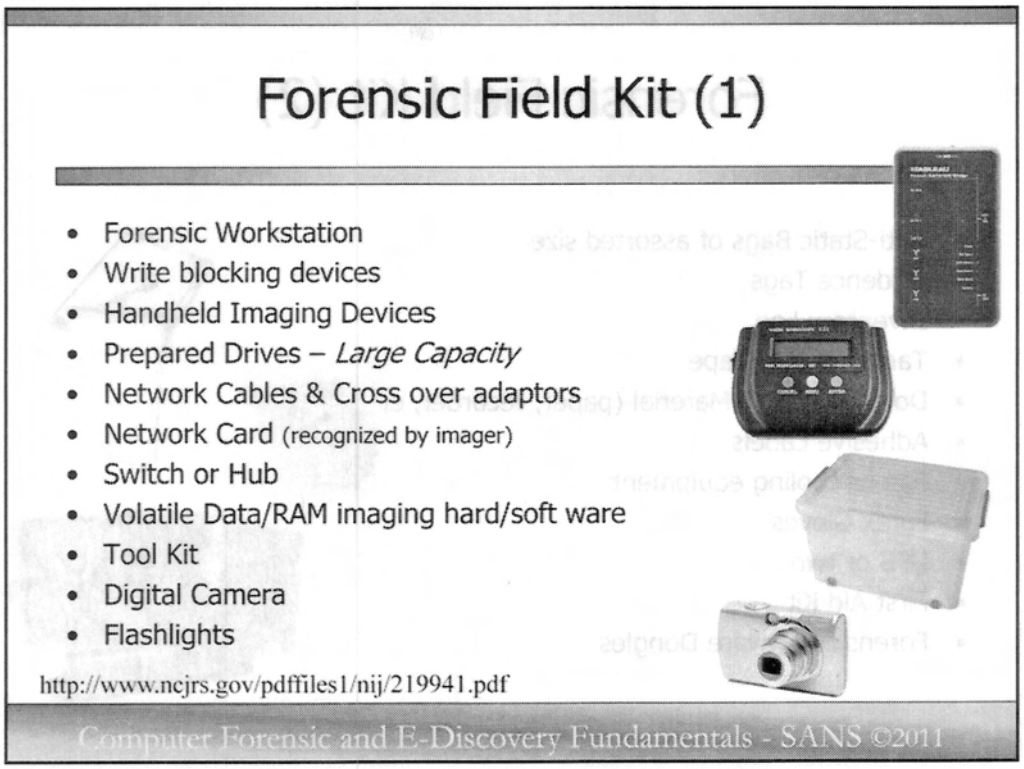
First, you have the old rugged standby which is DD or DCFLDD. DD is a standard Unix tool and has been ported to Windows 32 and DCFLDD is a modified version of the dd tool that provide the ability to perform hashing on the raw data that it is being collecting. It works just like the normal dd tool but with two extra options.

The hash window contains the minimum amount of data to grab before a hash is taken. Typically the most common option is to set the size of the hash window to zero. This will take the hash of the system once. It will hash the entire data that was collected.

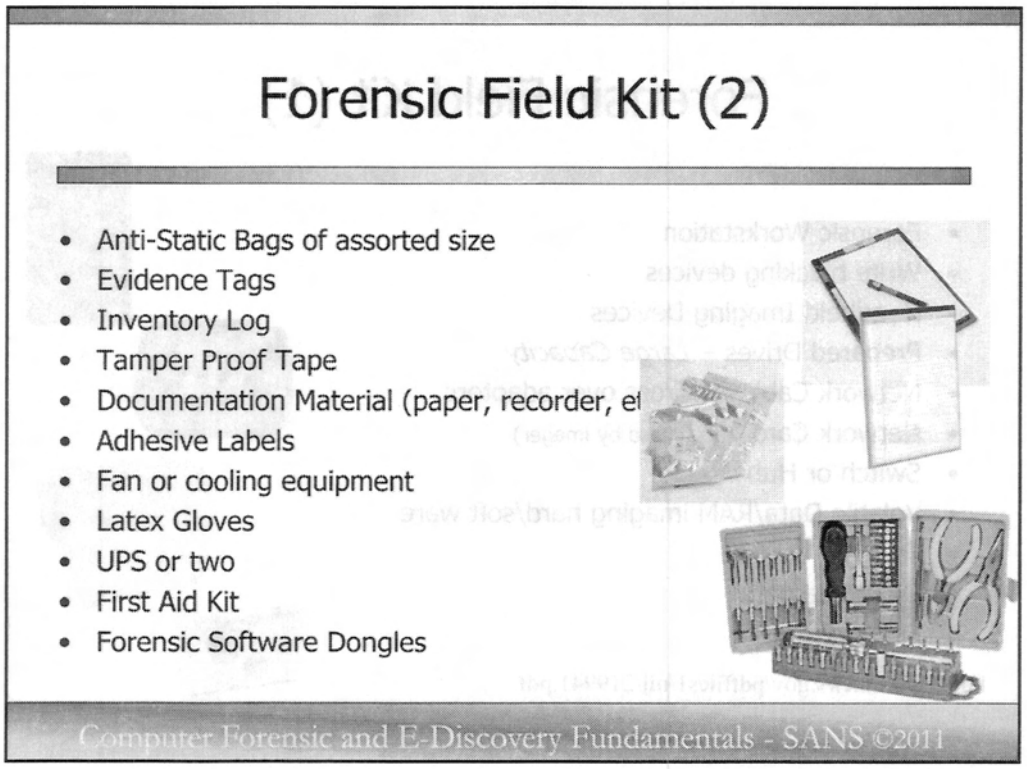
FTK Imager is what we will demonstrate and go over this afternoon. It is a free download from Accessdata.com. It is a Windows 32 bit tool that also has a standalone version, that is to say you can download a version that you can copy on your thumb drive and it does not need to be installed on any system,. All the files necessary for it to run are on the thumb drive. This makes it real convenient to walk around with. Another nice thing about FTK imager is that it will allow you to create an EnCase E01 image as well as a raw DD, or even a SMART image file format. You can also use it to preview the drive you are going to image and it will even allow extraction of locked files on a live system such as the registry, the system volume information (restore point) directory, etc. We will talk more about that later.

Guidance Software allows the creation of an EnCase boot CD. This EnCase boot CD will allow you to create forensic images like all other forensic imaging tools but also will allow you to create an image across the network or with cross over cables.

Raptor is a free modified Linux boot CD with GUI interface. Raptor will allows you to mount, image and hash drives in a forensically sound manner. Raptor can image to FAT32, NTFS, HFS+ and EXT3 file systems as either an .E01, DD or even create a clone. Raptor will also allow two forensic images to be created at the same time.



- Portable Forensic Workstation
- Write blocking devices for a variety of drive and digital evidence interfaces (IDE, SATA, SCSI Ultra, SCSI Wide, USB, SD, CF, etc)
- Handheld Imaging Devices (HardCopy II) – these are great but be careful not to become totally dependent on them
- Prepared Drives – Large *Capacity – Do you know how much data you will be imaging. Bring a lot.*
- Network Cables – If you have to image via the network, you should always have your own network cables and CROSS OVER CONVERTER ADAPTORS
- Volatile Data/RAM imaging hard/soft ware
- Tool Kit – to remove drives, etc
- Digital Camera – for documentation of the scene as well as the CONDITION of the equipment they will accuse you of damaging during seizure
- Network Card (recognized by imager) I like to bring a 3COM gigabit card to slip into the machine in the even I have to do a network acquisition and the subject box only has a 10/100 network card
- Switch or Hub to set up network
- Anti-Static Bags of assorted size – to store drives in for transport.
- Evidence Tags- to document necessary information
- Documentation Material (paper, recorder, etc) I love my PULSE LITESCRIBE
- Adhesive Labels – to tag items
- Fan or cooling equipment – to keep drives cool while imaging. Heat slows data transfer rate.



- Cardboard boxes
    - Notepads
    - Gloves
    - Evidence inventory logs
    - Evidence tape
    - Paper evidence bags
    - Evidence stickers, labels, or tags
    - Crime scene tape
    - Antistatic bags. – (Pack all digital evidence in antistatic packaging. Only paper bags and envelopes, cardboard boxes, and antistatic containers should be used for packaging digital evidence. Plastic materials should not be used when collecting digital evidence because plastic can produce or convey static electricity and allow humidity and condensation to develop, which may damage or destroy the evidence.)
- Permanent markers
- Nonmagnetic tools. Anti-Static Bags of assorted size – to store drives in for transport.

Evidence Tags- to document necessary information

Documentation Material (paper, recorder, etc) I love my PULSE LITESCRIBE

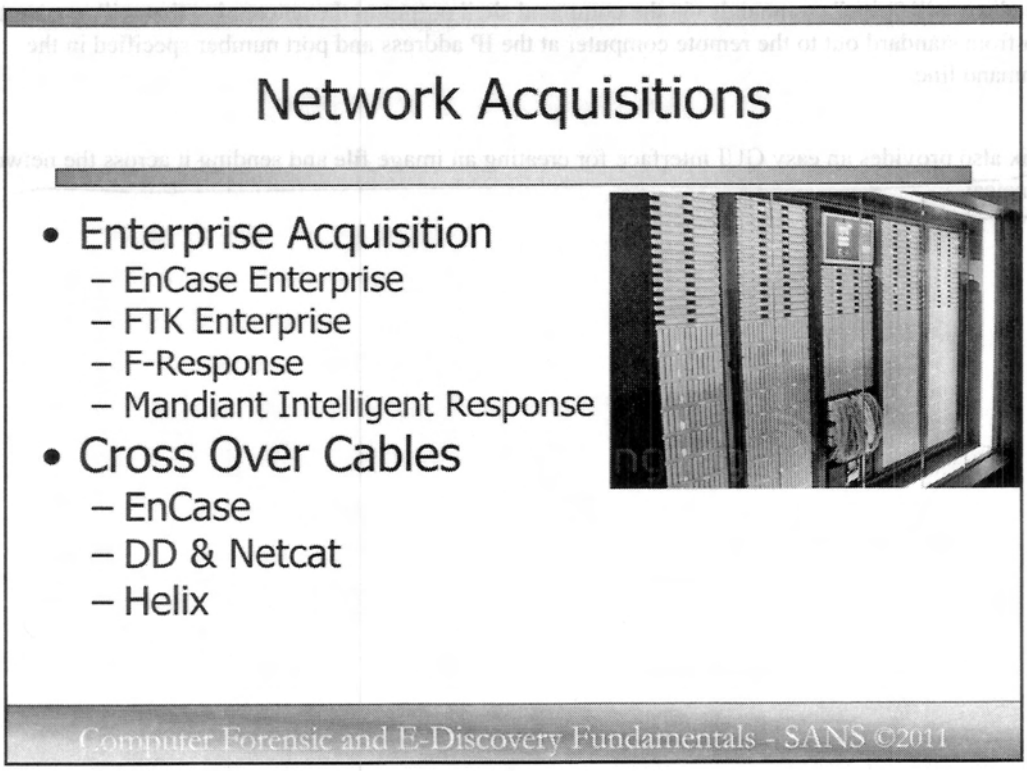
Adhesive Labels – to tag items

Fan or cooling equipment – to keep drives cool while imaging. Heat slows data transfer rate.

First Aid Kit

Forensic Software Dongles

The list goes on.



Particularly when dealing with businesses with remote offices, new technology is available to allow remote imaging of systems across the network. Techniques such as EnCase and FTK Enterprise allow the installation of a small application to be installed or pushed to the remote system that will allow investigators to connect, preview, examine and image the system across the network. Depending on the number of systems you want to image simultaneously and how many systems you want to have the remote application installed on, the cost of implementation and annual licenses can easily exceed $100,000. A new contender in the enterprise remote preview, examination and imaging is F-Response. F-Response uses a read only iSCSI connection to allow investigators to connect to remote systems in a forensically sound manner to any number of systems for $5000.

There will also be situations where it is impossible or impractical to remove the hard drive from the computer you need to image.

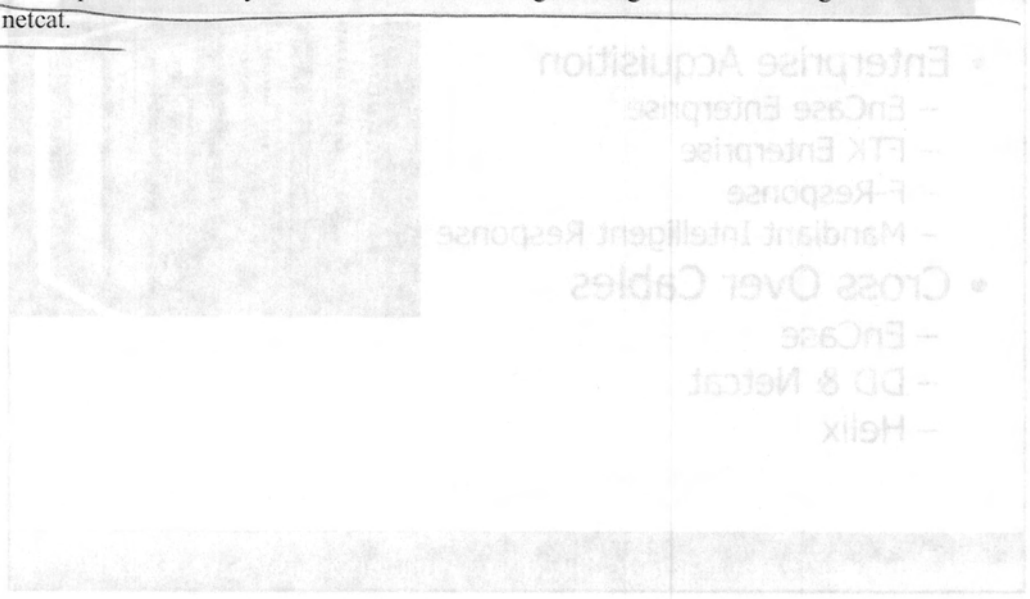
One situation is when dealing with RAID systems. In situations like this you will need to create an image across the network.

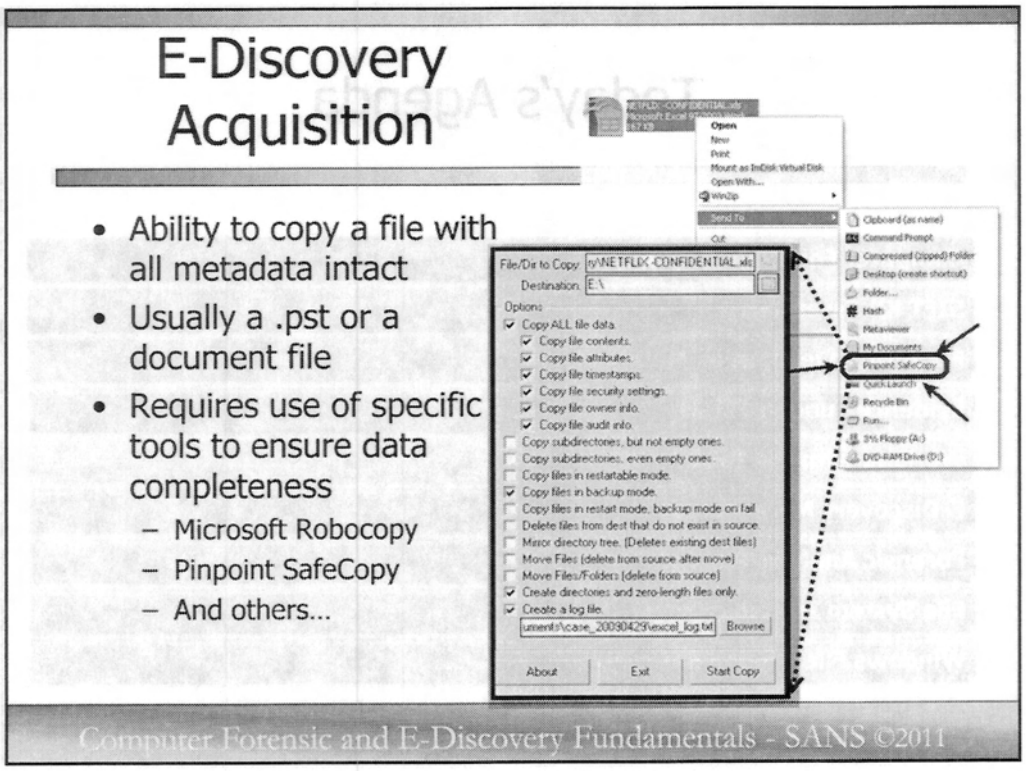
You can also accomplish the creation of an image file across the network or via cross over cables by using the EnCase Boot CD. With this CD you can boot target system with the EnCase boot CD then select the network acquisition method, select the destination computer and directory and encase will initiate the imaging across the network. Starting with EnCase version 5, if the imaging is interrupted during the process, you can re initiate the imaging process and it will pick back up where it left off.

This network imaging technique can also be easily conducted using DD or DCFLDD and Netcat. Simply start netcat server on the destination machine in listener mode using the–L option and assign the port for netcat to listen on with the –p.

The client will "pipe" commands via the command shell output to the netcat pipe that will reroute the data from standard out to the remote computer at the IP address and port number specified in the command line.

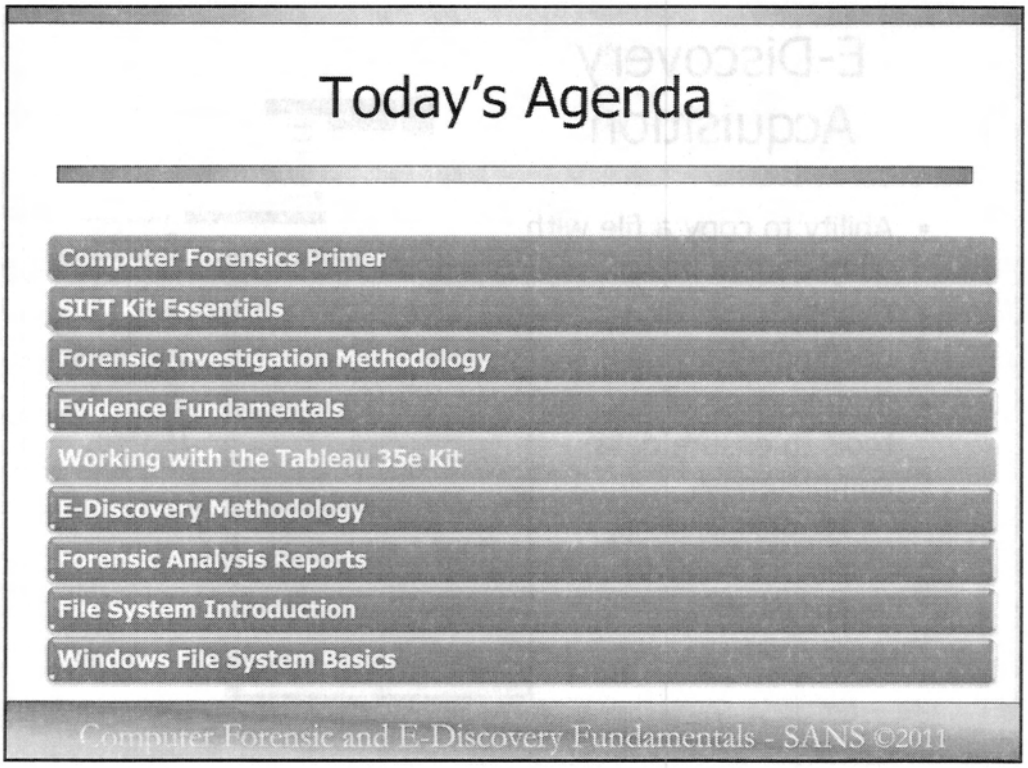
Helix also provides an easy GUI interface for creating an image file and sending it across the network via netcat.



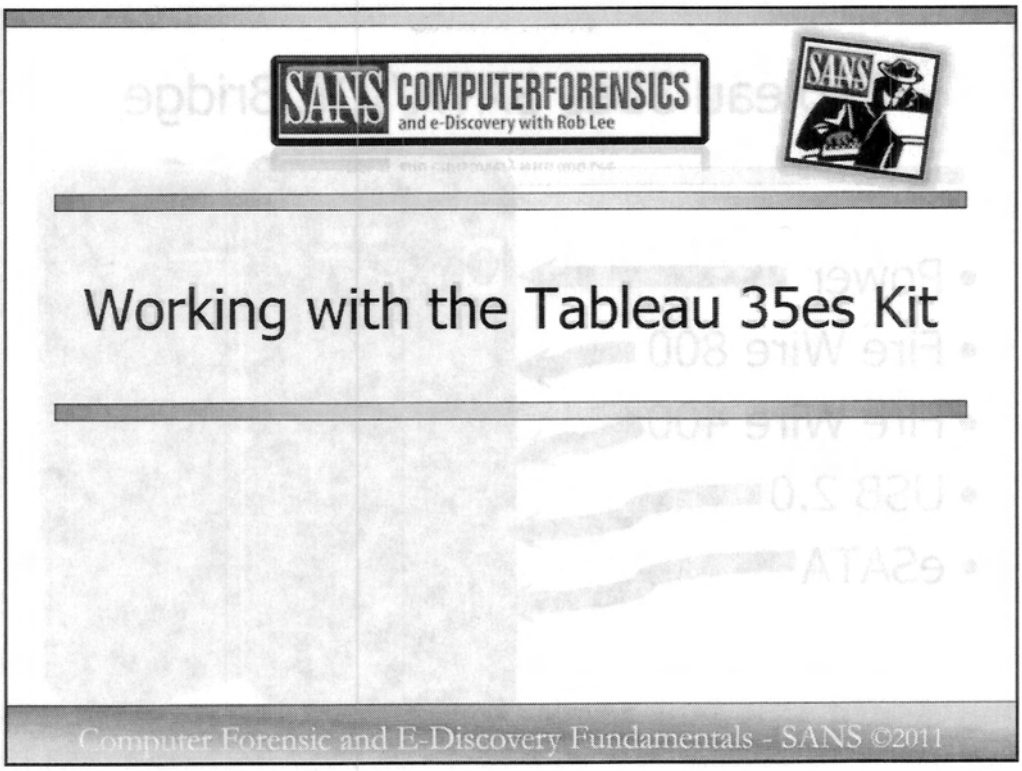


In many e-discovery situations you will need to provide a capability to copy files off a machine in an extremely safe fashion. If you have to do this manually, no better tool than the one provided with the XP SIFT Workstation.

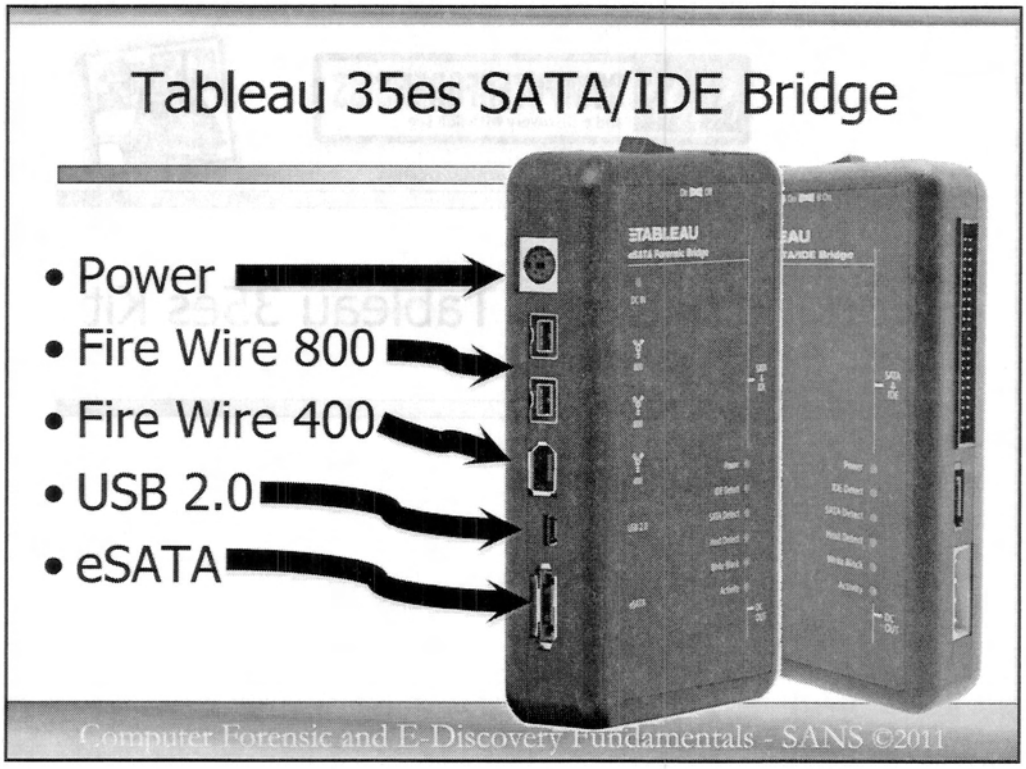
http://sansforensics.wordpress.com/2009/01/08/robocopy-%E2%80%93-a-computer-forensics-tool/



This page intentionally left blank.



This page intentionally left blank.

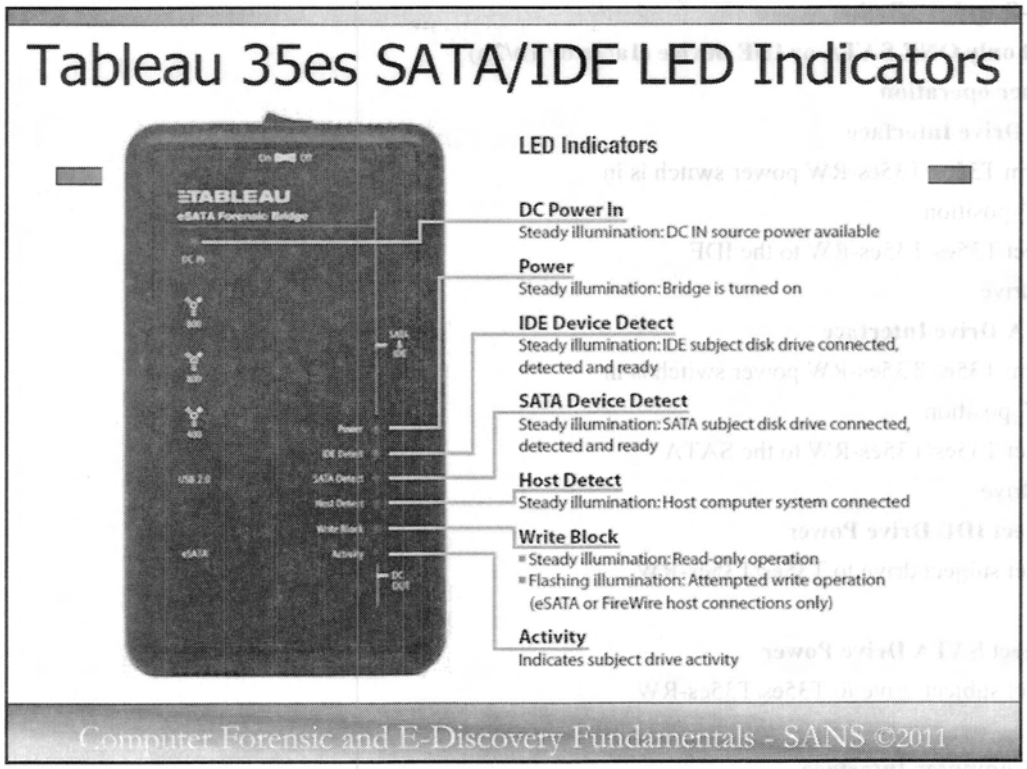


The Tableau T35es provide the ability to image IDE devices (Parallel ATA hard disk devices with LBA (Logical Block Addressing)) or SATA 1 or SATA 2 hard disk devices. The T35es also provides two native 9-pin FireWire800 (1394B).

And one native 6-pin FireWire400 (1394A) connection to your forensic system as well as one USB Mini-B (5 pin, allowing USB2.0 high/full/low speed data transfer speeds.

These devices are also ruggedized 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 90% humidity.

Tableau also offers firmware updates to deliver high-quality, high-performance, and robust device capability for many years to come. The Tableau Firmware Update (TFU) utility offers users a fast, convenient method to maintain the T35es and all of our forensic bridge products.



LED Indicators

DC Power In

Steady illumination: DC IN source power available

Power

Steady illumination: Bridge is turned on

IDE Device Detect

Steady illumination: IDE subject disk drive connected, detected and ready

SATA Device Detect

Steady illumination: SATA subject disk drive connected, detected and ready

Host Detect

Steady illumination: Host computer system connected

Write Block

■ Steady illumination: Read-only operation

■ Flashing illumination: Attempted write operation (eSATA or FireWire host connections only)

Activity

Indicates subject drive activity

Step-by-Step Installation

Connect only ONE SATA or IDE device (1a/2a or 1b/2b) for proper operation

1a. IDE Drive Interface

■ Confirm T35es/T35es-RW power switch is in the "Off" position

■ Connect T35es/T35es-RW to the IDE subject drive

1b. SATA Drive Interface

■ Confirm T35es/T35es-RW power switch is in the "Off" position

■ Connect T35es/T35es-RW to the SATA subject drive

2a. Subject IDE Drive Power

■ Connect subject drive to T35es/T35es-RW DC Out

2b. Subject SATA Drive Power

■ Connect subject drive to T35es/T35es-RW DC Out

3. Host Computer Interface

■ Connect host to T35es/T35es-RW using ONE of the eSATA, USB 2.0, FireWire 800, or FireWire 400 connectors

4. Power (DC In)

■ Toggle the power switch to the "Off" position

■ Connect TP2 power supply using the 5-pin DIN

Powering on the T35es/T35es-RW

With the TP2 power supply and the IDE or SATA subject drive properly connected to the T35es/T35es-RW, toggle the power switch to the "On" position.

Disconnecting the Subject Drive

Prior to disconnecting either the T35es/T35es-RW or the subject drive, issue the appropriate OS command to ensure that all current or pending transfer operations are completed. Toggle the power switch to the "Off" position before disconnecting the subject drive.

Converting to Read/Write Operation

Visit the document library at www.tableau.com for specific DIP switch settings to convert the T35es-RW between read/write and read-only modes of operation.

Pictured here are the primary items you will find in your T35es 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. The adaptors on the right hand side of the screen are for adapting to the smaller 1.8 or 2.5 inch IDE, SATA or Zero Insertion Force drives that are more typically found in laptops or portable devices. To use the adaptors, you would simply plug one end of the IDE cable, pictured here on the left, into the T35es write block then plug the other end of the IDE cable into the adaptor. Then you would plug the 1.8 inch or 2.5 inch drive into the adaptor. From there, all you have to is connect power and then connect the T35es to your forensic system via the USB, Fire Wire 400 or 800 cable and you are ready to star imaging.

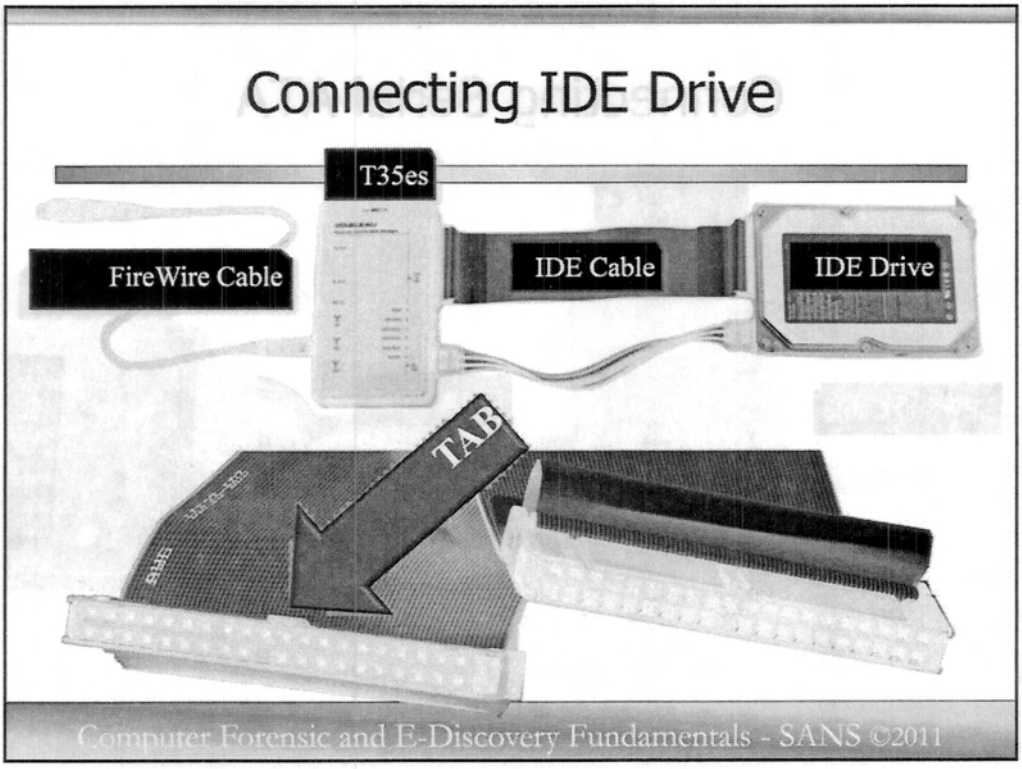
Now some have asked why the two different color ends on the IDE cable. For imaging it really does not matter but for those of you who have built computer systems before you know that manufacture instructions tell you to plug the blue end of the IDE cable into the motherboard. For the T35es, it really does not matter but as a matter of course, I typically plug the blue end into the T35es.

So let's look a little closer at the 1.8 or 2.5 inch adaptors. Starting from the top, you will find the Zero Force Insertion adaptor. These are also sometimes called the ZIF drives or ZIF connectors. Also in your kit you will find a small zip lock bag that contains several extra ZIF ribbon connectors. They include these because they sometimes get bent or damaged so now you have some extra ones. If you like you can take one of these out of the zip lock bag and try inserting it into the ZIF adaptor. For those of you that do try this, the first thing you might say is this is not Zero Force. Yes, when sliding the ZIF ribbon connector into the adaptor you will actually have to apply some moderate pressure to get the ribbon cable to slide into the connector.

The 1.8 and 2.5 inch adaptors are pretty straight forward. Just look at the PINs on the laptop, notating where the middle missing PIN is then make sure you have the alignment right and simply push the adaptor onto the drive. Sometimes, if you are dealing with law enforcement you may feel a little resistance and if you do I think you will find using a night stick or billy-club will usually provide the proper force necessary to attach the two devices (JOKE).

The adaptor shown here at the bottom is for when you have a Micro SATA laptop drive, this will enable you to connect this adaptor to the drive then connected the SATA and power cable provided with your T35es kit to the adaptor.

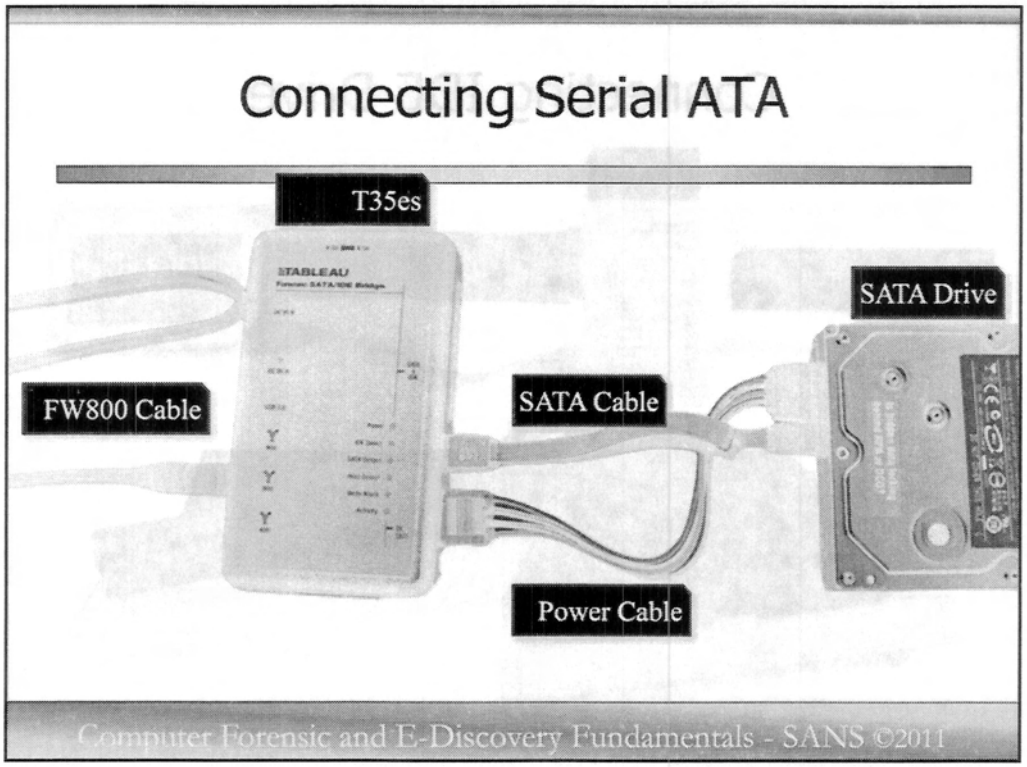
With all of these adaptors, you should find the power connected that will provide the necessary power to the drive in the side of the adaptor.



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 T35es write block device.

Now if you 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 if 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 T35es 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 other 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 support, Fire wire 800, fire wire 400 or USB 2.0.

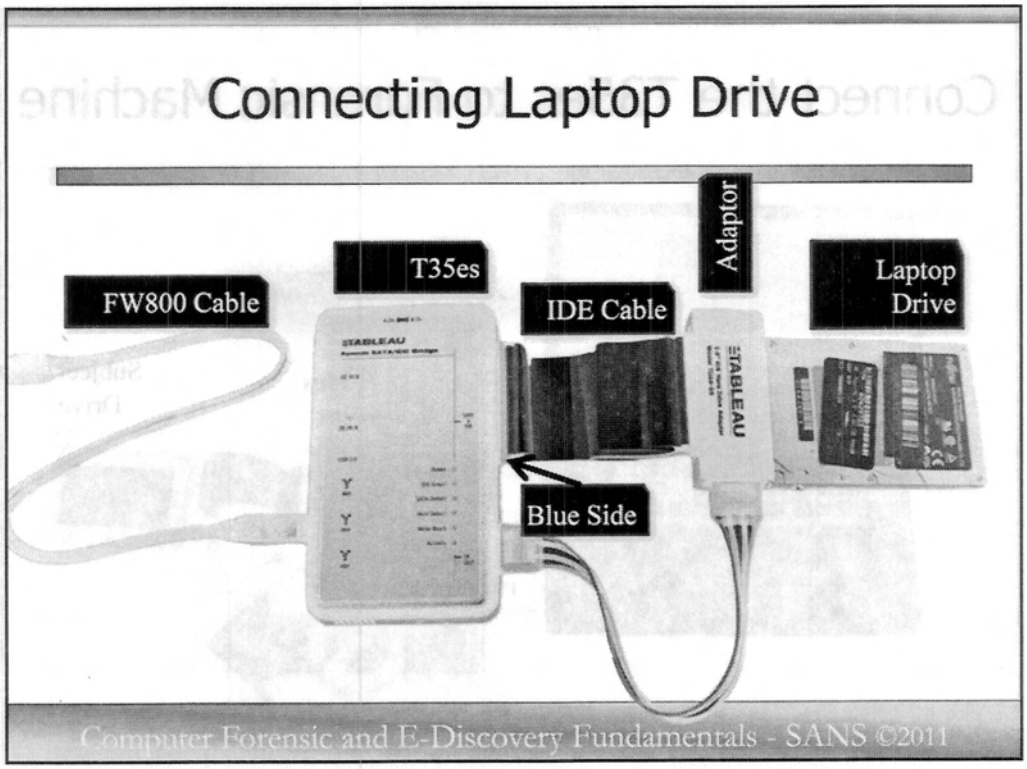


Now here in this slide we see the same kind of setup but this time with a Serial ATA drive. The only two things that are different are that the IDE cable has been replaced with the red SATA cable and we are now using the SATA power cable.

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 higher, i.e. data can be read and moved off the target or subject drive faster than a typical IDE drive. Also, the through put on the SATA cable is faster.

Also, another thing to remember when imaging, because imaging is such a time intensive process, 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.

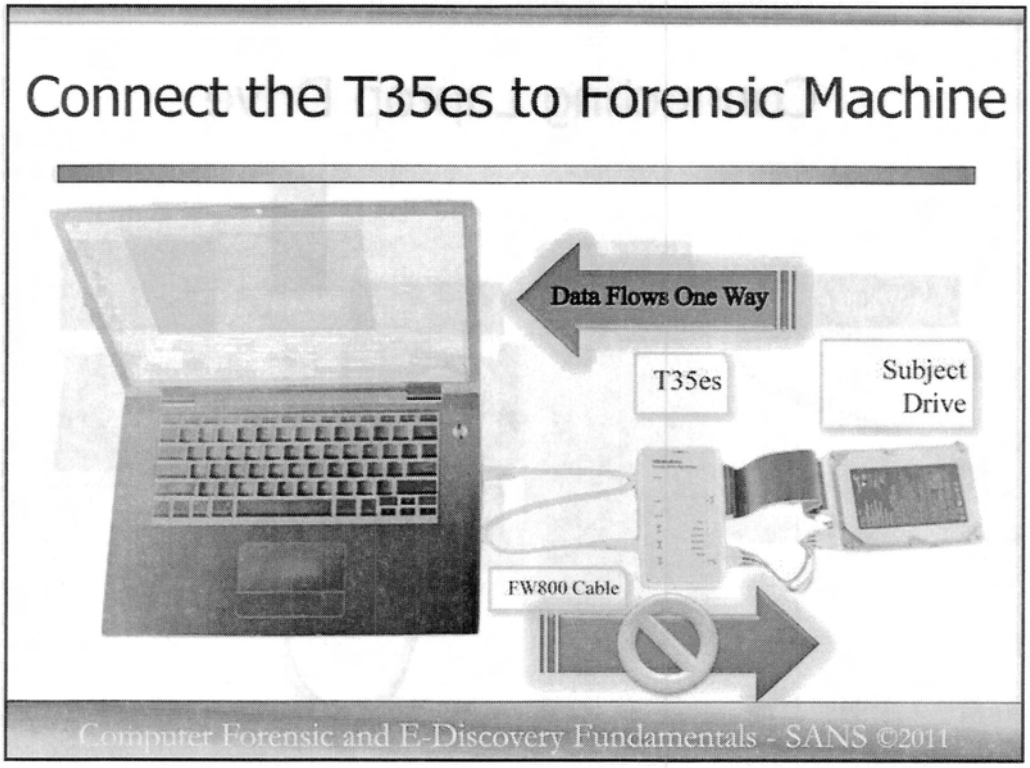
You would not want to be imaging a subject s 10,000 RPM SCSI drive to your old 4200 RPM IDE drive over USB a cable.



Now these 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.

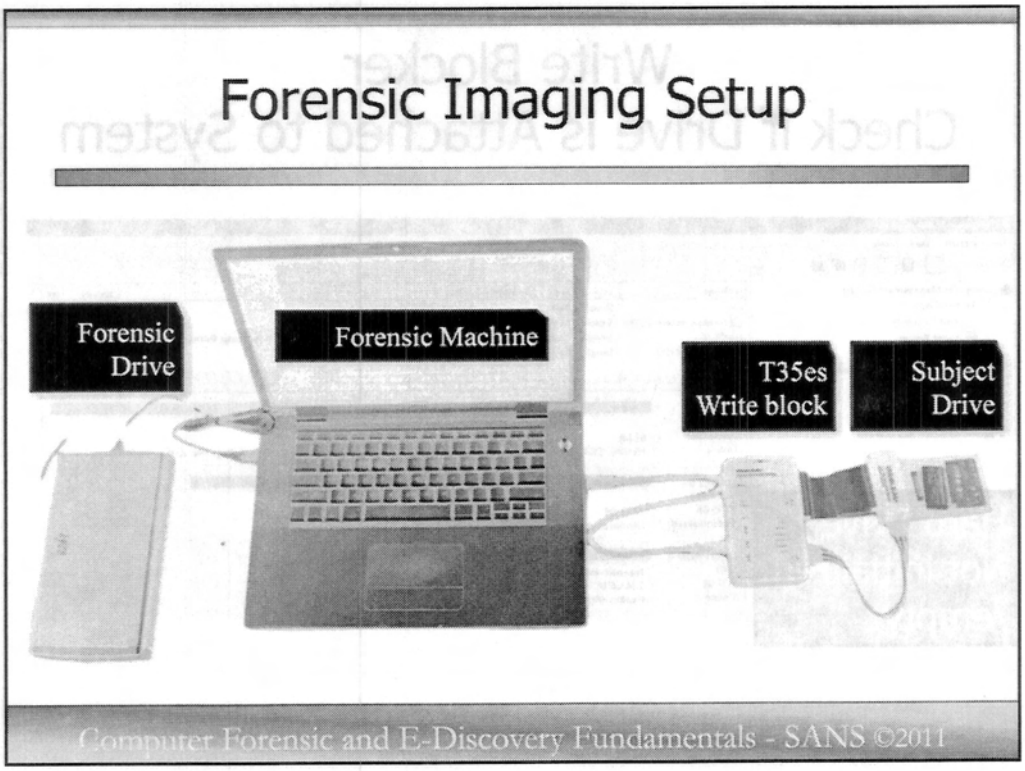
IMPORTANT NOTE: The blue side of the IDE CABLE should attach to the T35es directly. As they say in Ghostbusters… "Do not cross the streams!" Connect the blue side of the IDE cable to the T35es adapter and the opposite side to the Tableau Drive Adapter as shown above.

Again, here you can see we have the 2.5 inch drive connected directly to the 2.5 inch drive adaptor, from there, we have the IDE cable connected from the adaptor to the T35es write block device, then the power attaches from the side of the adaptor to the T35es as normal.



Once you have this all connected, you simply plug in the fire wire cable as shown her 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 devices 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.

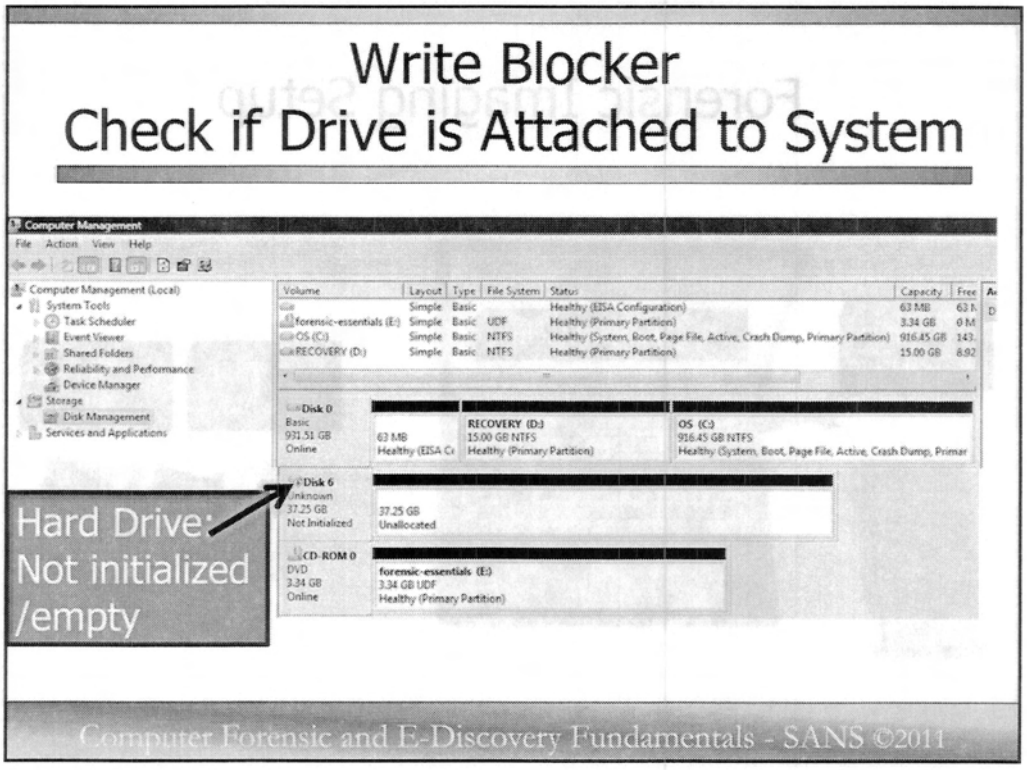
(The actual power device for the T35es is not shown here to in an attempt to keep the example as visually clean as possible.)



The last image here shows the entire setup as it is most typically used in the field, you have the subjects drive on the right, then your T35es hard ware write block, which is connected to your forensic machine which 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 bottle necks in this process.

Also, while we have this screen up, it is the perfect time reminds you all that the forensic imaging machine you are using should be set up so that ALL the power saving features is turned off. You do not want a screen save 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 uninterruptable power during this whole process.



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 drive can be seen by windows via the GUI -

Click on:

Control Panel-> Administrative Tools -> Computer Management

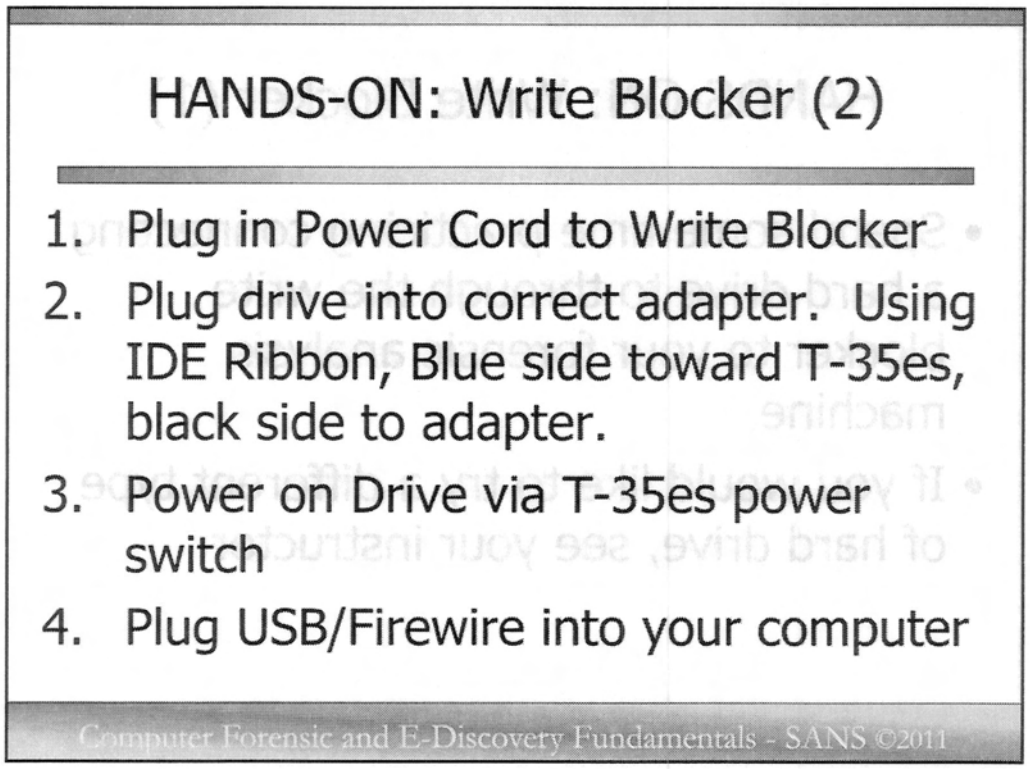
Select Storage -> Disk Management

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

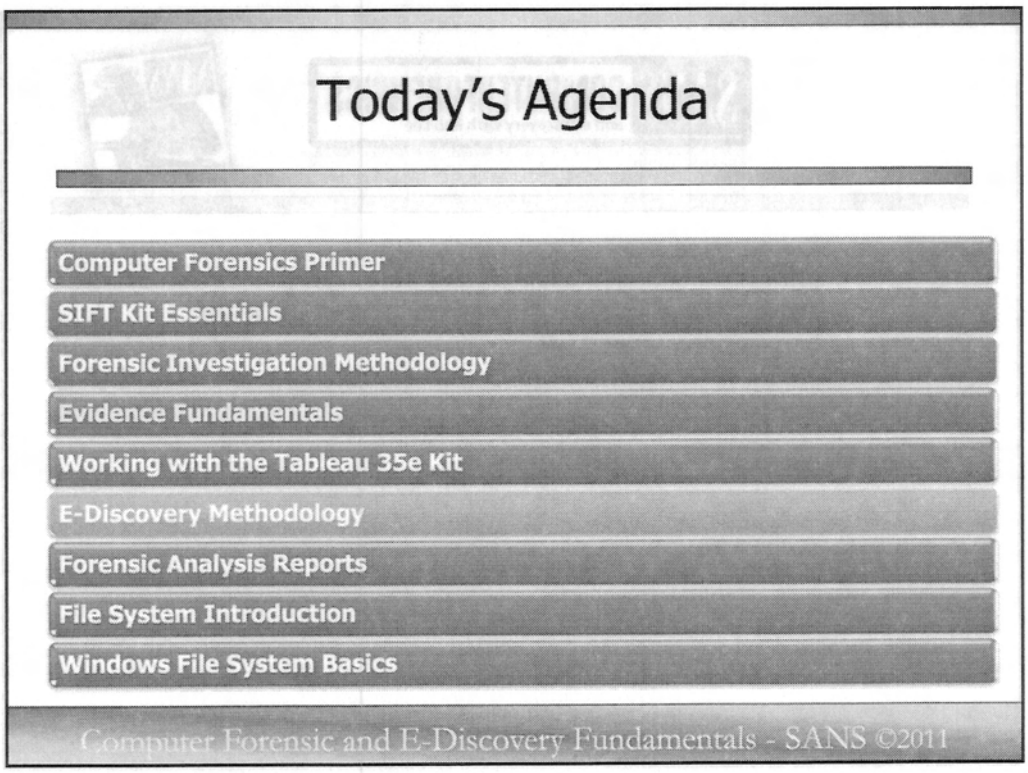
HANDS-ON: Write Blocker (1)

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

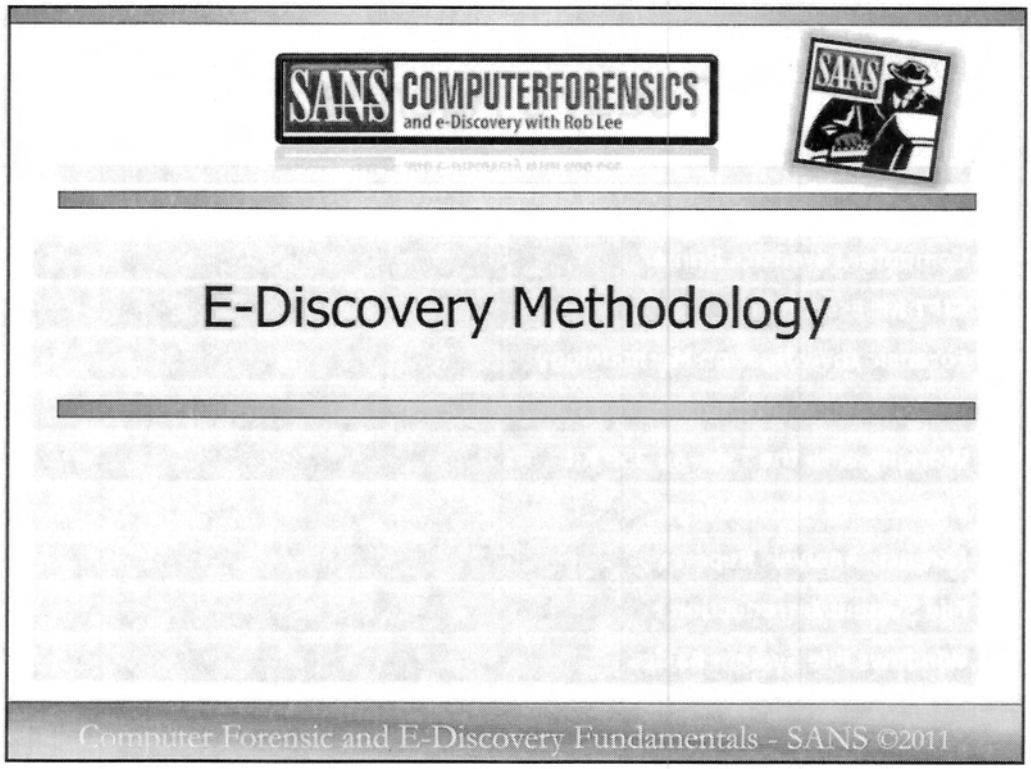
This page intentionally left blank.



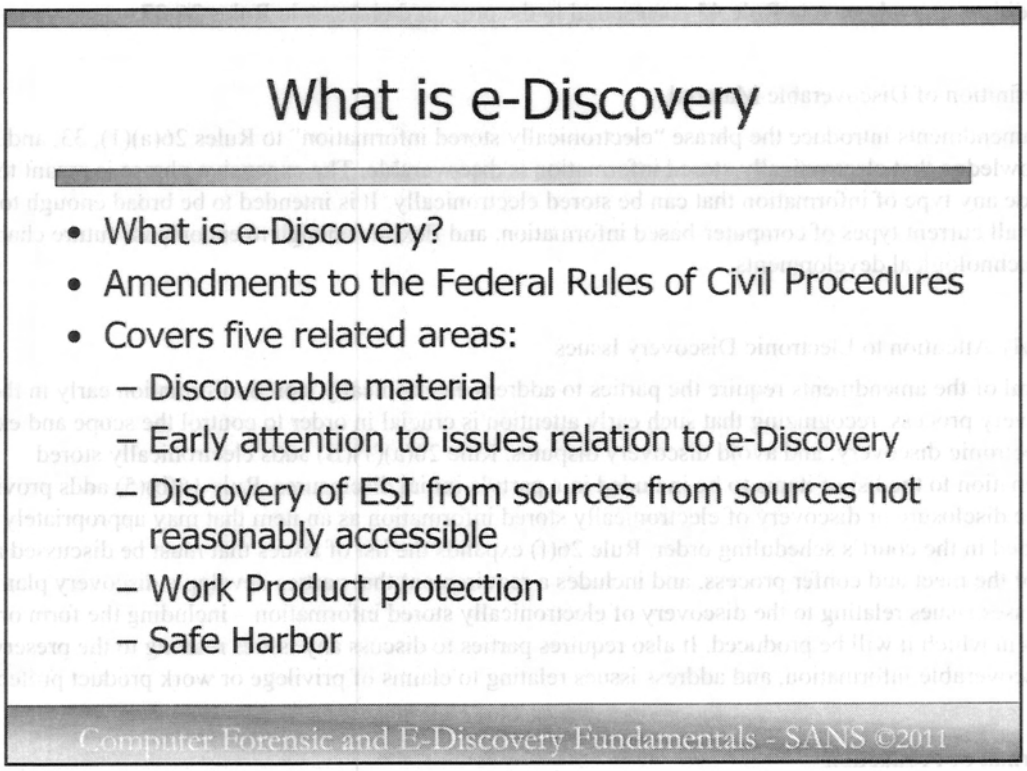
This page intentionally left blank.



This page intentionally left blank.



This page intentionally left blank.



With our every increasing world of reliance on speed, quickness, and effectiveness, it is only expected that our world of data would go virtually paperless overnight. Who knew that a paperless world would become more complex and take away our speed, quickness, and effectiveness (at times) when doing business.

Sourced From: http://electronicdiscovery.info/law/federal-rules-civil-procedure/

On Dec 1, 2006, the amendments to the Federal Rules of Civil Procedure concerning the discovery of "electronically stored information" go into effect today. The package includes revisions and additions to Rules 16, 26, 33, 34, 37, and 45, as well as Form 35.

The e-discovery amendments originated with the Advisory Committee on Civil Rules, which first heard about problems with computer-based discovery in 1996 and began intensive work on the subject in 2000. The Advisory Committee considered numerous alternatives, perspectives, and ideas in determining whether amendments specifically addressing electronic discovery were necessary, and, if so, what the language of any such amendments should be. In August 2004, the Committee published its proposed amendments. Following the public comment period – during which over 250 individuals and organizations provided feedback – the Advisory Committee made several additional modifications, resulting in the final package of amendments that was ultimately approved by the Judicial Conference and the United States Supreme Court.

The amendments cover five related areas, which are described in more detail below:

(a) definition of discoverable material;
(b) early attention to issues relating to electronic discovery, including the format of production;
(c) discovery of electronically stored information from sources that are not reasonably accessible;
(d) the procedure for asserting claim of privilege or work product protection after production; and
(e) a "safe harbor" limit on sanctions under Rule 37 for the loss of electronically stored information as a result of the routine operation of computer systems.

In addition, amendments to Rule 45 correspond to the proposed changes in Rules 26-37.

1. Definition of Discoverable Material

The amendments introduce the phrase "electronically stored information" to Rules 26(a)(1), 33, and 34, to acknowledge that electronically stored information is discoverable. The expansive phrase is meant to include any type of information that can be stored electronically. It is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and technological developments.

2. Early Attention to Electronic Discovery Issues

Several of the amendments require the parties to address electronically stored information early in the discovery process, recognizing that such early attention is crucial in order to control the scope and expense of electronic discovery, and avoid discovery disputes. Rule 26(a)(1)(B) adds electronically stored information to the list of items to be included in a party's initial disclosures. Rule 16(b)(5) adds provisions for the disclosure or discovery of electronically stored information as an item that may appropriately be included in the court's scheduling order. Rule 26(f) expands the list of issues that must be discussed as a part of the meet and confer process, and includes a requirement that parties develop a discovery plan that addresses issues relating to the discovery of electronically stored information – including the form or forms in which it will be produced. It also requires parties to discuss any issues relating to the preservation of discoverable information, and address issues relating to claims of privilege or work product protection.

3. Format of Production

An amendment to Rule 34(b) addresses the format of production of electronically stored information, and permits the requesting party to designate the form or forms in which it wants electronically stored information produced. The rule does not require the requesting party to choose a form of production, however, since a party may not have a preference or may not know what form the producing party uses to maintain its electronically stored information. The rule also provides a framework for resolving disputes over the form of production, in the event that the responding party objects to the requested format(s). Finally, the rule provides that if a request does not specify a form of production, or if the responding party objects to the requested form(s), the responding party must notify the requesting party of the form in which they intend to produce the electronically stored material – with the option of producing either (1) in a form in which the information is ordinarily maintained, or (2) in a reasonably usable form.

4. Electronically Stored Information from Sources that Are Not Reasonably Accessible

Amended Rule 26(b)(2) creates a two-tiered approach to the production of electronically stored information, making a distinction between that which is reasonably accessible, and that which is not. Under the new rule, a responding party need not produce electronically stored information from sources that it identifies as not reasonably accessible because of undue burden or cost. If the requesting party moves to compel discovery of such information, the responding party must show that the information is not reasonably accessible because of undue burden or cost. Once that showing is made, a court may order discovery only for good cause, subject to the provisions of the current Rule 26(b)(2)(i), (ii), and (iii). *

This two-tier system seeks to provide a balanced, equitable approach to resolve the unique problem presented by electronic stored information which is often located in a variety of locations of varying accessibility – strongly favoring the production of relevant information from more easily accessible

sources where possible. This provision received a great deal of attention during the public comment period, and the Advisory Committee made substantial changes to both the proposed rule and to the accompanying notes to address the concerns voiced, and to balance the interests of both requesting and responding parties. The responding party receives protection from being forced to tap hard-to-access sources, where retrieving information or determining the presence of responsive content cannot be achieved without incurring substantial burden or cost. The requesting party benefits from knowing the sources the responding party does not intend to search, and has a method of obtaining this information if it is truly warranted.

5. Asserting Claim of Privilege or Work Product Protection After Production

The addition to Rule 26(b)(5) sets forth a procedure through which a party who has inadvertently produced trial preparation material or privileged information may nonetheless assert a protective claim as to that material. The rule provides that once the party seeking to establish the privilege or work product claim notifies the receiving parties of the claim and the grounds for it, the receiving parties must return, sequester, or destroy the specified information. The Committee Note clearly states that the rule does not address whether the privilege or protection was waived by the production, but simply prohibits the receiving party from using or disclosing the information, and requires the producing party to preserve the information, until the claim is resolved.

6. "Safe Harbor"

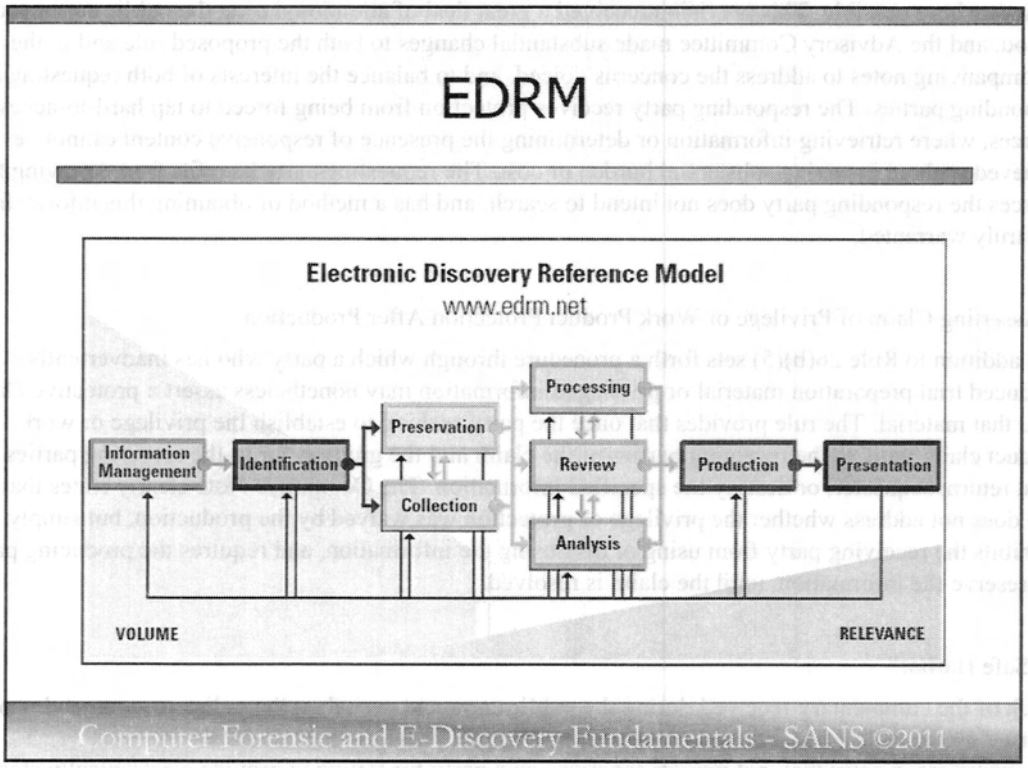
Much of the commentary received during the public comment period on the e-discovery amendments focused on the Rule 37(f) safe harbor provision. This rule provides that, absent exceptional circumstances, a court may not impose sanctions on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system. It responds to the routine modification, overwriting, and deletion of information that attends the normal use of electronic information systems.

The Advisory Committee notes that the "routine operation of an electronic information system" refers to the ways in which such systems are generally designed and programmed to meet the party's technical and business needs, and includes the alteration and overwriting of information that often takes place without the operator's specific direction or awareness. The Committee further observes that such features are "essential to the operation of electronic information systems," and that there is "no direct counterpart in hard-copy documents."

The protection of Rule 37(f) applies only to information lost due to the routine operation of an information system, and only if such operation was in good faith. The Committee Note discusses the effect that the existence of a preservation obligation may play in determining whether or not the operation was in good faith, and expressly cautions: "A party cannot exploit the routine operation of an information system to evade discovery obligations by failing to prevent destruction of stored information that it is required to preserve."

*In the pending rules, these provisions are located at Rule 26(b)(2)(C).

Reference: http://www.ediscoverylaw.com/2006/12/articles/news-updates/ediscovery-amendments-to-the-federal-rules-of-civil-procedure-go-into-effect-today/



Currently, there is no 'industry standard' for the Electronic Discovery process, but there are many groups out there who are trying to establish a open standard and supplemental guidelines. The EDRM, Electronic Discovery Reference Model, addresses the key pieces to the e-Discovery process:

1. Information Management
2. Identification
3. Preservation
4. Collection
5. Processing
6. Review
7. Analysis
8. Production
9. Presentation

Information management: is getting your electronic house in order to mitigate risk & expenses should electronic discovery become an issue, from initial creation of electronically stored information through its final disposition.

Identification: Covers locating potential sources of ESI and determining its scope, breadth, and depth.

Preservation: Ensures that ESI is protected against inappropriate alteration or destruction.

Collection: Gathering ESI for further use in the electronic discovery process (processing, review, etc.).

Processing: Reducing the volume of ESO and converting it, if necessary, to forms more suitable for review and analysis.

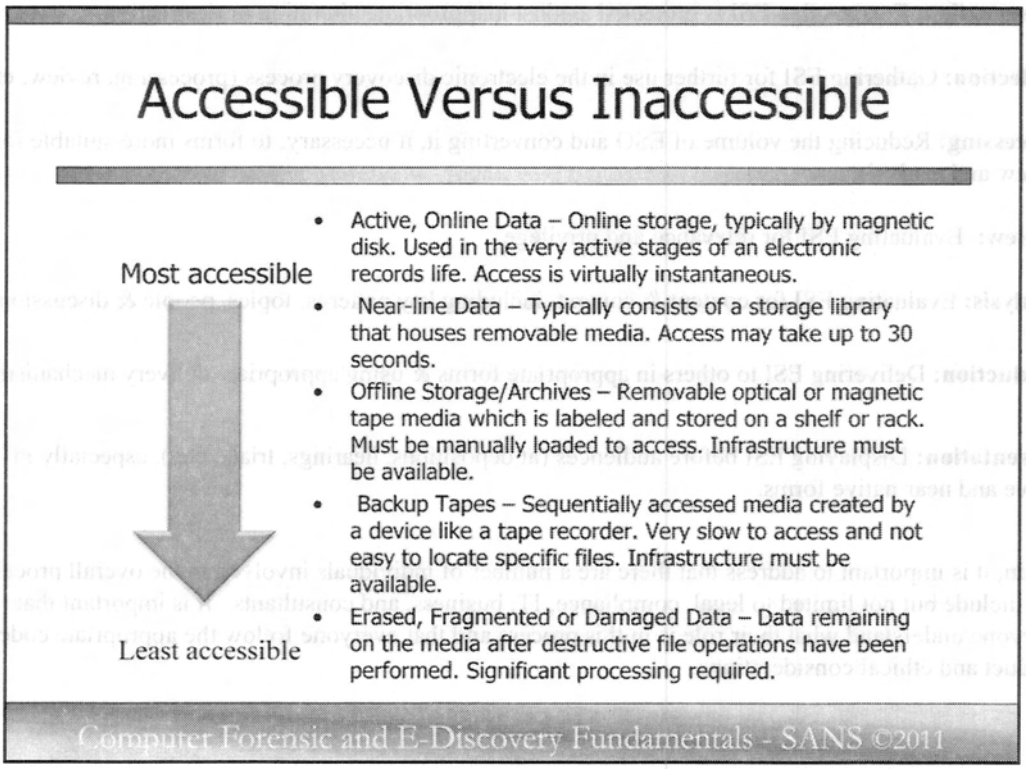
Review: Evaluating ESI for relevance and privilege.

Analysis: Evaluating ESI for content & context, including key patterns, topics, people & discussion.

Production: Delivering ESI to others in appropriate forms & using appropriate delivery mechanisms.

Presentation: Displaying ESI before audiences (at depositions, hearings, trials, etc.), especially in native and near native forms.

Again, it is important to address that there are a number of individuals involved in the overall process that include but not limited to legal, compliance, IT, business, and consultants. It is important that everyone understand what their role is in this process and that everyone follow the appropriate code of conduct and ethical considerations.



As part of the Identification phase of the e-Discovery process and EDRM standard, determining the relevance of the information in scope ties directly to the accessibility and inaccessibility of the information. As we can see, active online-data is going to be the most accessible and your primary target when starting the process. Erased, fragmented and/or damaged data is when you are going to have to bring in your forensics and/or data recovery specialist (if applicable to the scope of the inquiry).

Regardless though of the accessibility and/or inaccessibility of the data in scope, organizations need to take the necessary steps in order to ensure that the data is available and the retention policy is reasonable based upon the type of data it is.

Make data less accessible after the facts and/or preservation phase (which is our next phase) is a whole separate matter that we will address in future slides (sanction and spoliation).

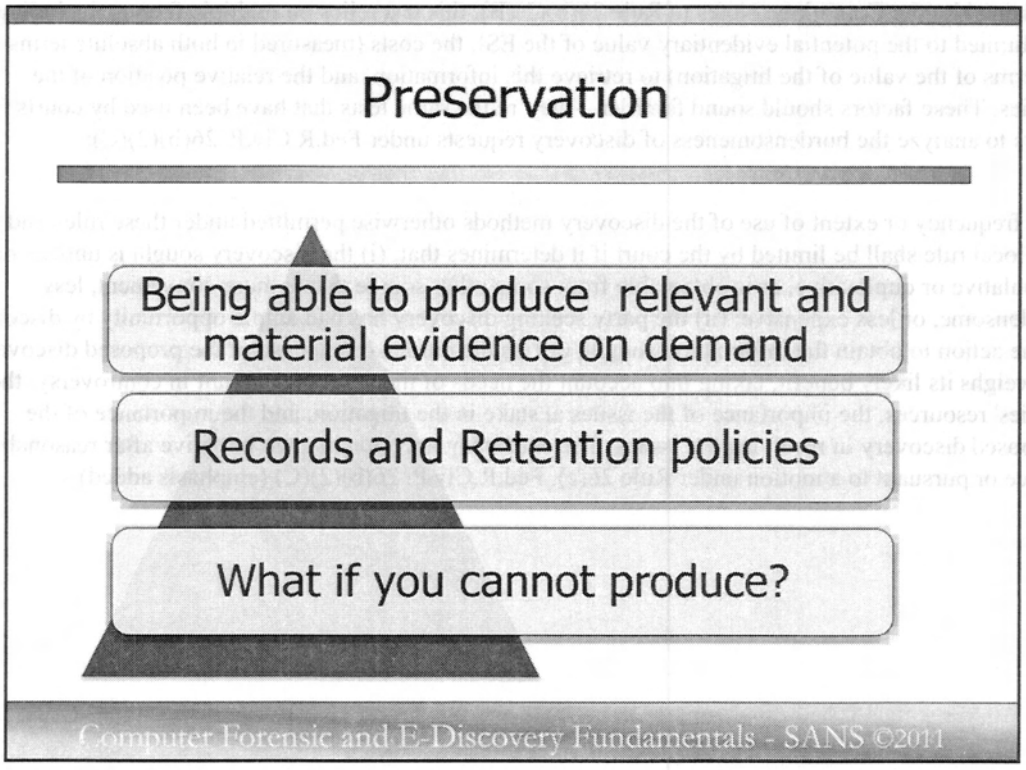
Looking through the levels though, think about your organization and where these data sources lie within your organization and how you address their retention- is it based on information management? Is it based on information classification? Or is based solely on risk/budget?

The language from Rule 26 states the following: "A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost." Fed.R.Civ.P. 26(b)(2)(B).

As you can imagine this somewhat subjective, but fear not, there is a 'standard test' for this statement. If it can be established that information stored in a specific repository is theoretically accessible through some process, Rule 26 requires litigants and courts to assess the reasonableness of this effort. As

explained by the Committee Notes to Rule 26(b)(2)(B), this test relies on multiple factors, including but not limited to the potential evidentiary value of the ESI, the costs (measured in both absolute terms and in terms of the value of the litigation) to retrieve this information, and the relative position of the parties. These factors should sound familiar—they're the same tests that have been used by courts for years to analyze the burdensomeness of discovery requests under Fed.R.Civ.P. 26(b)(2)(C):

The frequency or extent of use of the discovery methods otherwise permitted under these rules and by any local rule shall be limited by the court if it determines that: (i) the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought; or (iii) the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues. The court may act upon its own initiative after reasonable notice or pursuant to a motion under Rule 26(c). Fed.R.Civ.P. 26(b)(2)(C) (emphasis added).

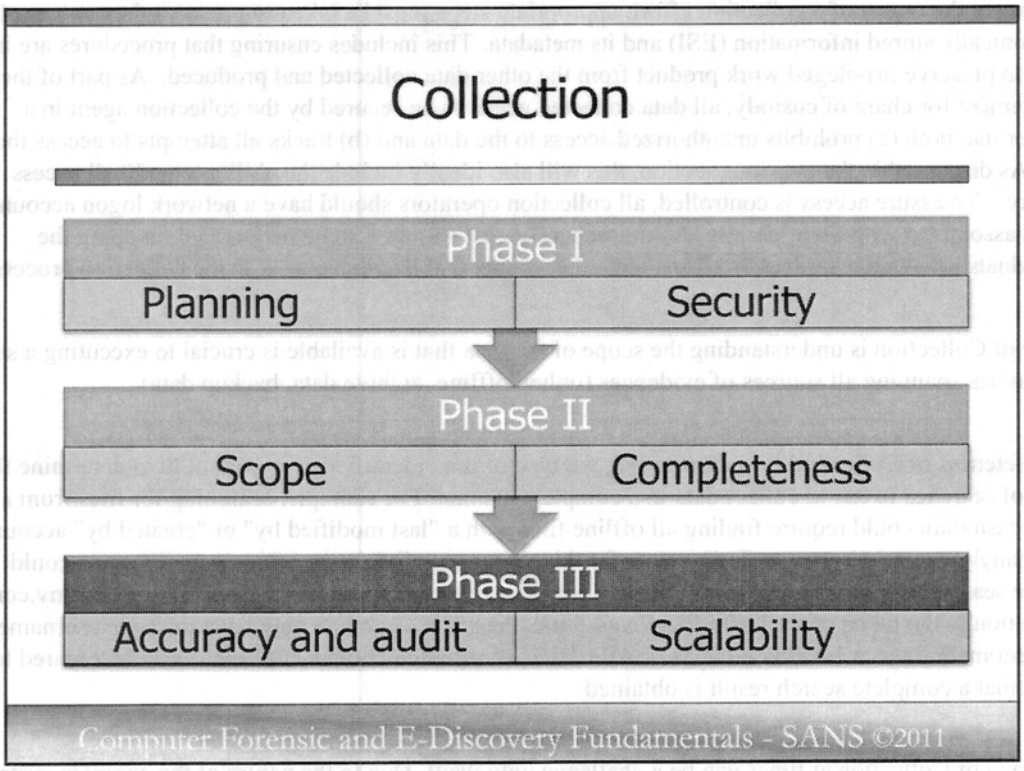


Continuing on with our EDRM standard, the next phase is Preservation. Now, in theory, we have identified where our information is, or should be, now we have to see if it was preserved.

Again, there are many steps associated with the Preservation phase including: legal requirements/standards for documentation preservation (this would be our records and retention policies, preservation letters, due diligence before preserve attaches (generally the pieces associated with Identification and Information Management),and implementation of preservation/litigation hold.

Now, it's hard to produce data if it is not preserved- right? But, FRCP 26(a) and FRCP 26(b) set forth the guidelines for producing, both spontaneously and upon request relevant and material evidence. Inherent in the reasoning behind these rules is the requirement that in order to produce a thing, one must first have preserved it. For those parties who are not inclined to appreciate this inherent reasoning, there are other rules (and corresponding sanctions) designed to enhance this understanding.

FRCP 37 details various procedures that lead up to the levying of sanctions by a court on a party for failing to comply with discovery obligations, however a detailed discussion of the duty to preserve is notably lacking. It is another source of law that more directly asserts this duty.



The next phase will be address in our EDRM/e-Discovery process is Collection. What is data collection? The acquisition of electronic information (data) marked as potentially relevant in the identification phase. This discussion assumes collection of electronic information by the owner of that information which is intended to be reviewed before production to opposing parties. The exigencies of litigation generally require that electronic information should be collected in a manner that is comprehensive, maintains its content integrity and preserves its form. Increasingly, metadata is required to be collected and maintained during this process and information regarding the chain of custody and authentication is required. Also, today the presumption is that this information will be producible in its native file format whenever possible. The process of collecting electronic information will generally provide feedback to the identification function which may impact and expand identified content.

Collection guidelines address planning, security, scope of the collection, completeness of the collection, accuracy of the collection, scalability, and auditability. The collection processes include scope of the collection, sources of collection (which are covered in Identification) and collection methods. The last piece of collection address cost driver, which include the volume of the data, location of data (on or off site), keyword searching, and old technology/legacy systems and databases.

At a high level, Planning is based on the results of the Identification phase, adequate planning of the search strategy is a major key to overall effectiveness in the collection effort. The first question that should be asked is where is the data. A good strategy is to work from a topology of the network and then create a map of the types of data, the locations and the custodians. Search terms, phrases and concepts need to be documented at the outset, along with a list of key company events and timeframes, as well as custodians of interest and relevance.

Security at the outset of a collection effort, appropriate steps must be taken to preserve the content of the electronically stored information (ESI) and its metadata. This includes ensuring that procedures are in place to preserve privileged work product from the other data collected and produced. As part of the requirement for chain of custody, all data collected needs to be secured by the collection agent in a manner that both (a) prohibits unauthorized access to the data and (b) tracks all attempts to access the data. As discussed in the previous section, this will also ideally include the ability to audit all access activity. To assure access is controlled, all collection operators should have a network logon account that is associated with their identity. A comprehensive list should also be maintained mapping the individuals involved in collection to any and all accounts that they have used in the collection process.

Scope of Collection is understanding the scope of the data that is available is crucial to executing a series of searches spanning all sources of evidences (online/offline, archive data, backup data).

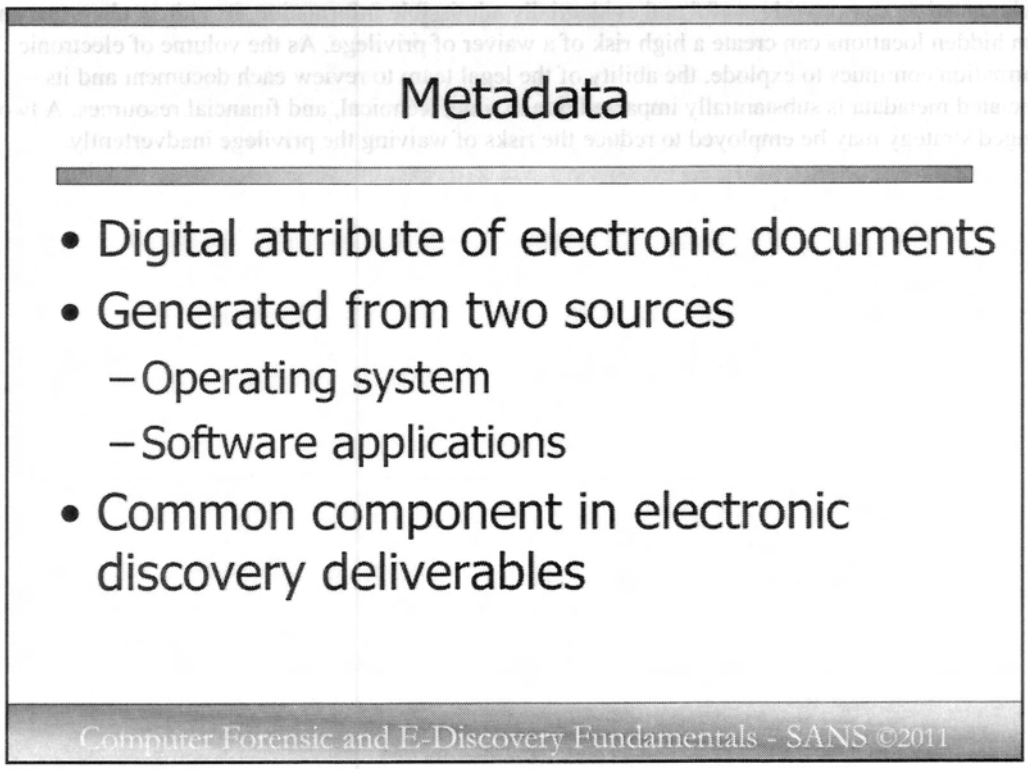
Completeness of Collection is understanding the type of data identified is important in to determine the kinds of searches to use to collect data in a complete manner. For example, searching for files from a given custodian could require finding all offline files with a "last modified by" or "created by" account of "company\joeuser." However, finding data for this same custodian in the active e-mail system could require searching for all items "from," "to" or "cc" that contain the e-mail address "joe@company.com" in addition to the name of the custodian. In addition, the same custodian may have multiple usernames in different mailboxes or in other databases. All of this information about a custodian must be secured to insure that a complete search result is obtained.

Accuracy of Collection at times can be a challenge unto itself. Due to the nature of the complex systems in use in most companies today, files typically undergo numerous transformations throughout their lifecycle. These transformations occur both at the hands of end users and automatically by the operating system or other software in use. Operating system and file specific metadata are added or modified, file formats are transformed, encoded, decoded, encrypted, and many other potential changes make it difficult to assess the evidence was actually created, modified or viewed by a particular custodian.

Scalability of the collection mechanisms is paramount. Performing a comprehensive series of searches across any company's infrastructure can involve searching potentially large amounts of data, often resulting in tremendous volumes of data to be de-duplicated and culled, reviewed and redacted. Because of the uncertainty of many data search results, in many situations it is simpler and less-risky to break a large search into several smaller searches. This will help avoid running out of memory or other glitches during a search. Of course breaking things into bite-sized chunks requires careful management of the overall search process to ensure nothing is overlooked or otherwise left out.

Auditability address the chain of custody with records. Regardless of the collection method employed, strict chain of custody records must be maintained for all documents, data, and objects collected so that their authenticity can be assured. Without this assurance the data may not be reliable as evidence in litigation. Every collector, whether a third party vendor, an internal corporate representative or outside counsel representative should document procedures for accepting, storing, and retrieving documents, in the event that he or she may be called upon to testify.

Reference: http://edrm.net



Metadata refers to the digital attributes of electronic documents that are appended to those documents either during their creation or use in their native application. Metadata is created and exists in its natural state before the electronic discovery process is initiated.

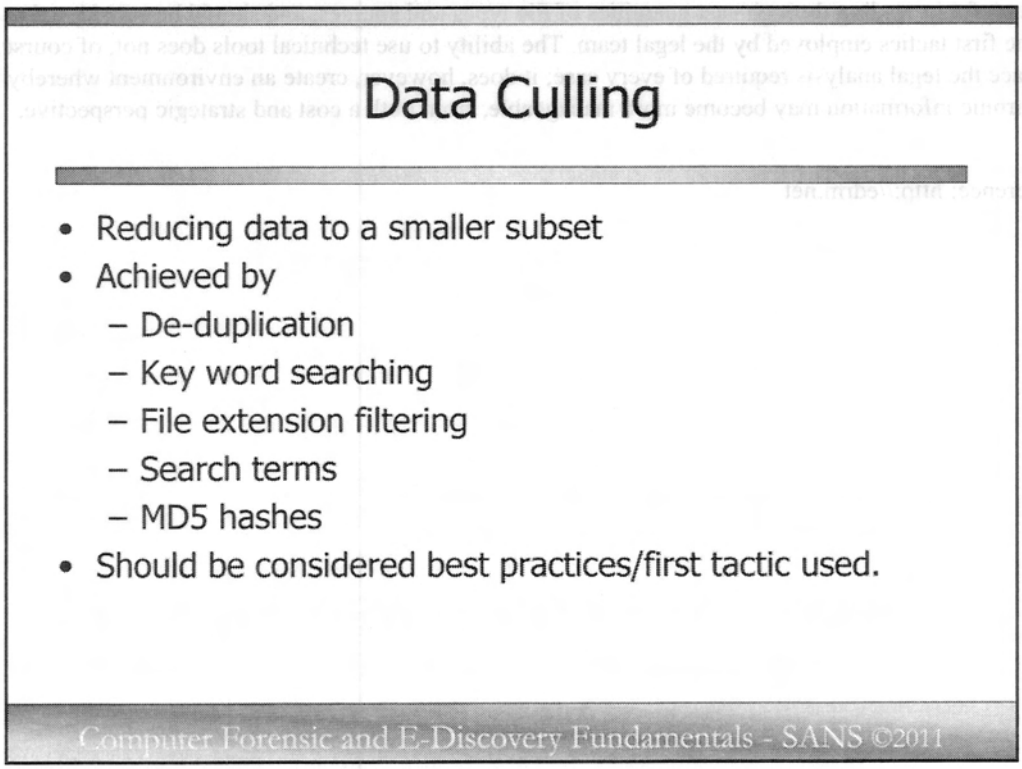
The existence of metadata is referenced in the comments to the proposed Federal Rules of Civil Procedure, and is characterized as the historical, managerial, and tracking components of a document or file; these components can be lost when the document is printed to paper or quasipaper.

Metadata can be generated from two sources, the operating system and the software application itself. The types of metadata that are recorded by the operating system are name, dates (create, modified and accessed), file type, and size for all files. Sent, received and modified dates, subject and recipient information for e-mail files. Some of that same data is recorded by the file itself, such as dates and file type.

There is other important data captured by the file itself; authorship, revision information, and comments. This information can be an important component of a legal strategy. Metadata provides search criteria and contextual information, which may not be in the body text. The ability to search for and correlate data during the review process is dependant on how well the metadata was processed. For example, data with altered metadata may compromise a search based on dates of files that were modified between two dates. If this happens, you may end up with more responsive data than if all metadata for all files is pristine.

Whether a legal team decides to use the metadata or not, it is a commonly provided component in electronic discovery deliverables. Metadata is extracted and archived as part of processing the source data so that it is available during review. Although metadata may not be used during processing, it is still critical that it be maintained for purposes of electronic discovery. If not, the integrity and authenticity of the data can be brought into question.

While metadata can provide useful and evidentially admissible information, its unique character and often hidden locations can create a high risk of a waiver of privilege. As the volume of electronic information continues to explode, the ability of the legal team to review each document and its associated metadata is substantially impacted due to time, technical, and financial resources. A two pronged strategy may be employed to reduce the risks of waiving the privilege inadvertently.



Data culling is the umbrella term used to describe the technical tactics or processes employed to reduce a large document population to a much smaller set. De-duplication, key word searching, and file extension filtering are a few examples of common data culling strategies. Each strategy can reduce the number of non-responsive files and e-mails substantially, a critical step in controlling the explosive growth of electronic information.

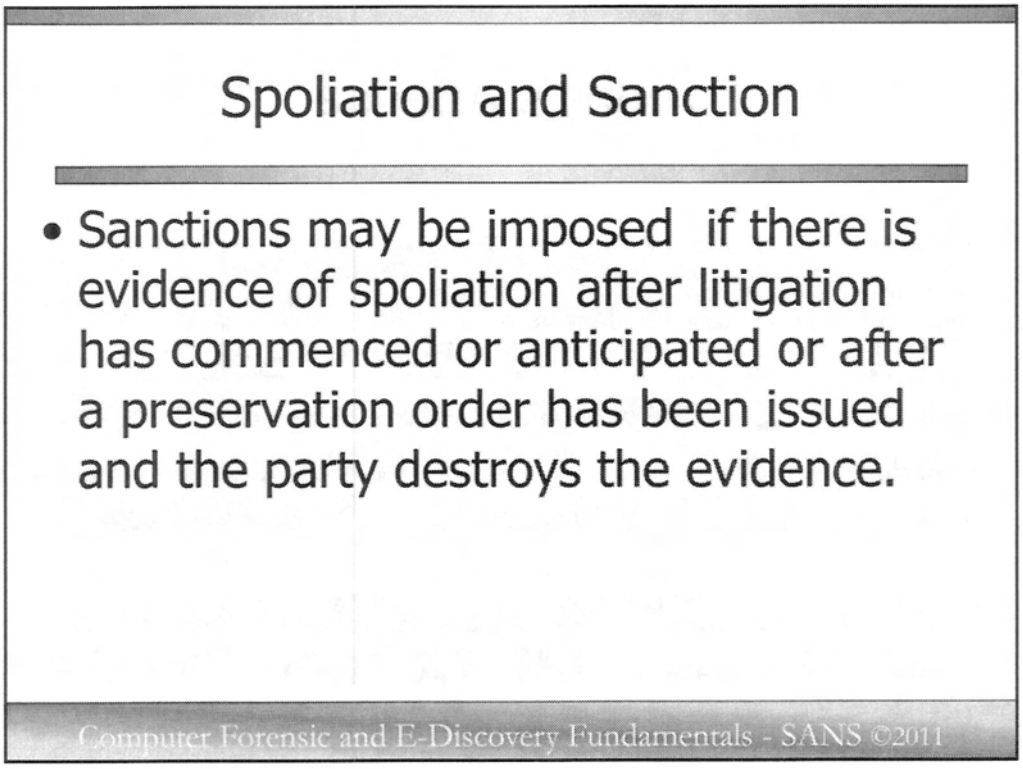
Filtering can narrow a dataset by selecting responsive files based on file-level criteria such as metadata. The custodian list, file type and timeframe associated with the matter are standard criteria. When using time as a culling criteria, it is important to remember that there are several time stamps that can be associated with any one file (i.e., for application files, create, modified and accessed dates may be available for use, and for e-mail files, time sent, received, created and last modified may be usable). Being specific about which of these time stamps is to be used as the filter parameter will help to ensure the resultant dataset meets expectations.

Other methods of data culling can also yield significant results. System files can be culled from a responsive data collection. Known system types recognized and assigned a common MD5 hash value provided a virtual digital fingerprint that can be used to weed out files not of interest. Such a mechanism allows large system files to be set aside as demonstrably non-responsive so that the size of the document collection is correspondingly reduced, a significant cost reducing strategy. Segregating the operating system files from a source hard drive early in the processing phase can greatly cut down the data set, helping to minimize processing time, when there is no intrinsic value that could be gained from these common types of file. Other file types, such as Internet cookies - files stored to a person's hard drive as the person uses the Internet, can also be programmatically segregated. These options help hone the dataset to the most relevant documents.

One of the most common culling strategies is the use of search terms, such as the names of key employees implicated by a lawsuit or investigation and specific words likely to be at play in the litigation, whether contained within the text of a document or within the metadata. These methodologies

are helpful in wading through vast quantities of file types and sources, and should be considered as one of the first tactics employed by the legal team. The ability to use technical tools does not, of course, replace the legal analysis required of every case; it does, however, create an environment whereby the electronic information may become more manageable, from both a cost and strategic perspective.

Reference: http://edrm.net



Last but not least, we need to address spoliation of information and the ramification of such spoliation . In simply terms, with regards to e-Discovery, if you are given a preservation letter on in scope, identified information/data and then take it upon yourself to delete or have this information mysteriously gone, you have now entered the world of spoliation and the potential of sanctions.

The spoliation law as explained by the court:

"Spoliation is the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation." West v. Goodyear Tire & Rubber Co., 167 F.3d 776, 779 (2d Cir. 1999) (citation omitted). A party bringing a spoliation claim must demonstrate

(1) that the party having control over the evidence had an obligation to preserve it at the time it was destroyed;

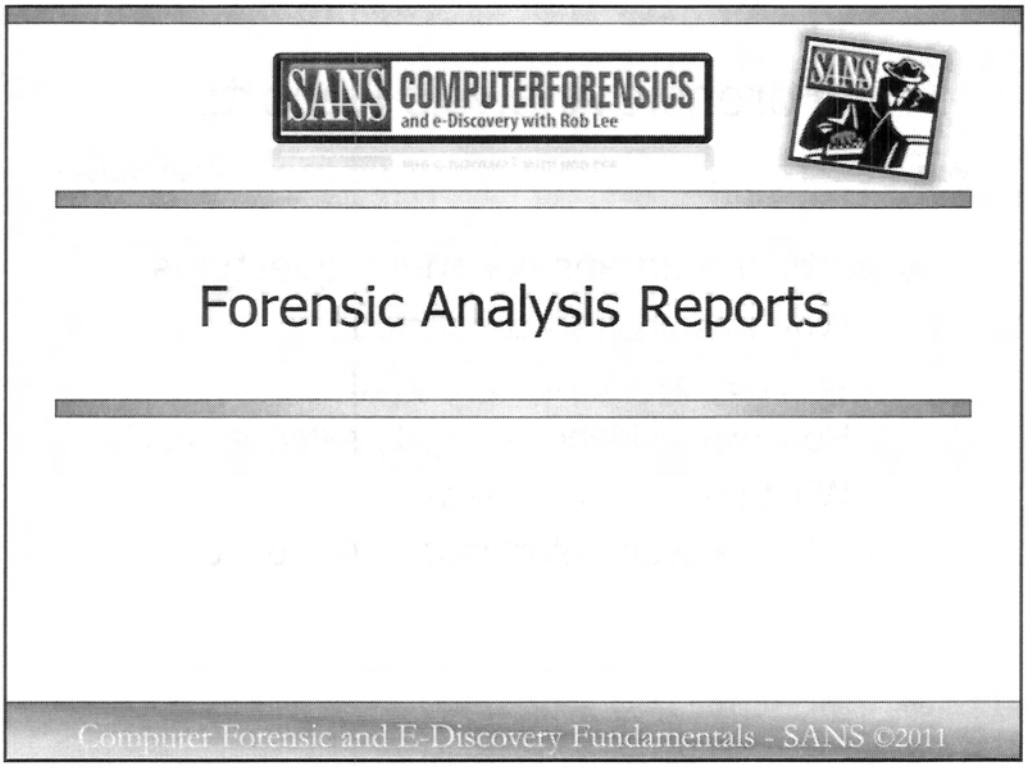
(2) that the [evidence was] destroyed with a culpable state of mind; and

(3) that the destroyed evidence was relevant to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense.

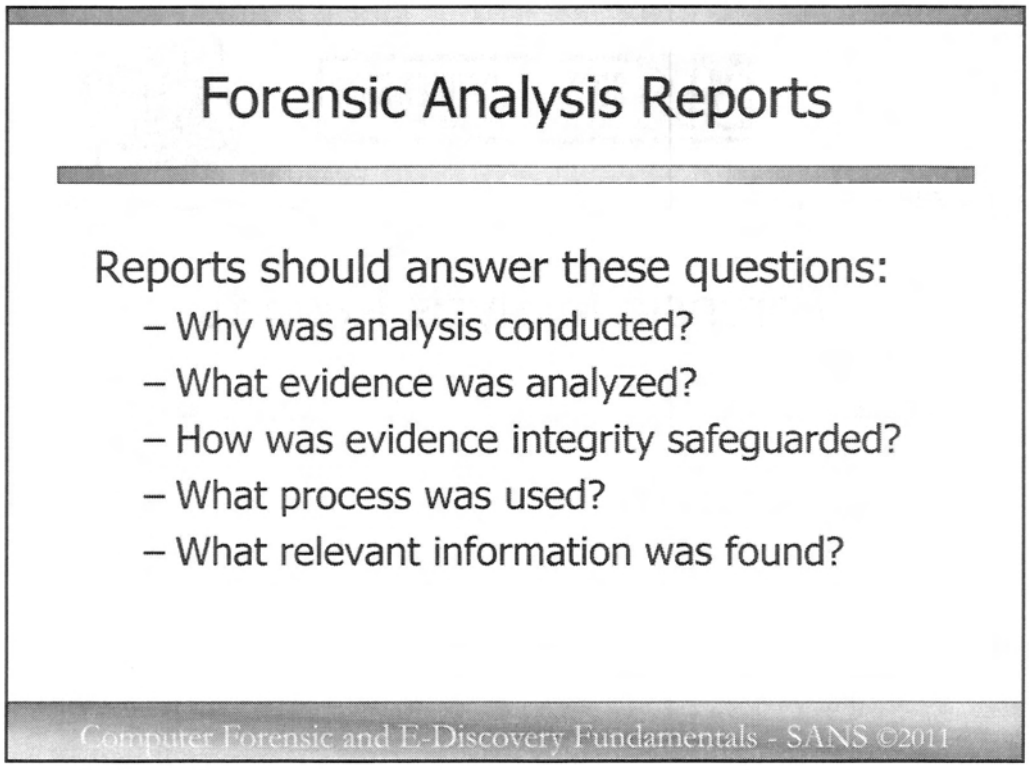
Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 107 (2d Cir. 2002) (internal quotation marks and citation omitted).

Sanctions are penalties or fines imposed for not complying with the applicable laws and regulations. For more details around sanction precedence with regards to e-Discovery I would recommend reading Electronic Sanctions in the Twenty First Century (http://www.mttlr.org/voleleven/scheindlin.pdf).

This page intentionally left blank.



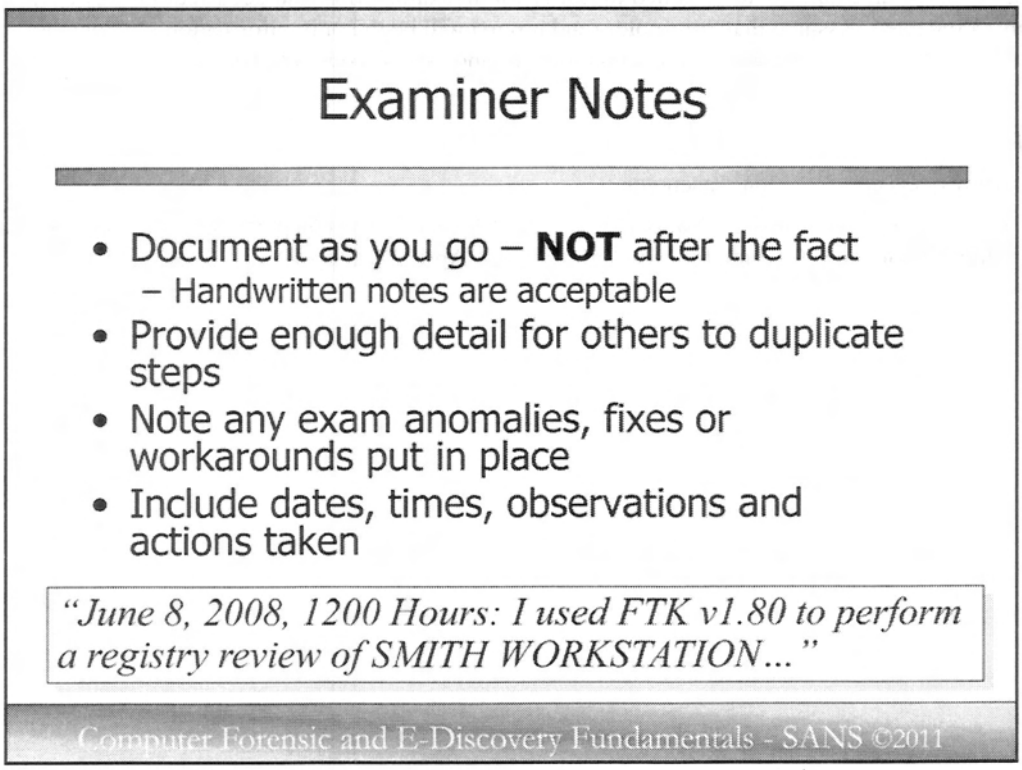
This page intentionally left blank.



The final report must be considered an essential component of your forensic exam. Many would argue that the report is the entire reason for performing the forensic investigation. The details of the examination conducted will need to be communicated effectively and comprehensively enough to satisfy a widely varied audience.

Reports can be relatively short in the case of little or no findings, or extremely voluminous in sensitive cases with large amounts of evidence uncovered. When writing a report, the investigator should seek to answer a series of questions that the reader may have about the investigation. The case facts and scope of the investigation should be communicated to explain why the analysis was conducted. Evidence should be listed to explain what the analysis was conducted upon. The details of the examination should be covered to demonstrate the investigator's process, prove sound forensics techniques and allow others to be able to repeat the steps. Finally, the findings of the examination should be listed and any conclusions supported by those findings should be clearly stated.

The hardest report to write is always your first, and it is rare to find a practitioner who loves writing reports. However, it is a "soft" skill that often differentiates examiners. You may be the best forensic investigator on the planet, but if you can't communicate your findings, that talent will have gone to waste.



Introduction

Note taking is a fundamental skill for conducting computer forensics. Accurate and comprehensive notes facilitate writing your final report and are critical for preparing to testify in court. Notes should start with a system description and system clock information and continue through the life of investigation.

Electronic versus Handwritten Notes

While there are no hard and fast rules for how to record notes, often the best mechanism is the simplest – pen and paper. Notes should be legible and contain enough information for both you and others to understand what actions you took and why they were taken. At a minimum, the date, time, and any observations or actions should be recorded. Electronic solutions are subject to fail and could be unavailable if your forensic platform is tied up while doing something like evidence acquisition. That being said, many investigators successfully keep notes in digital form. *Casenotes* is a freely available tool for Windows platforms which can be used by investigators to record their notes securely and includes features such as encryption, auditing, and tamper-proofing. [1]

Exam Anomalies

Every case presents its own set of challenges, and despite diligent planning it is likely that problems will be encountered. In some cases, the investigator will need to deviate from standard policies or procedures in order to accomplish the acquisition or analysis. In these circumstances, it is critical that a note be made explaining such deviations. [2] Examples include performing a logical acquisition of a hard drive due to the existence of a RAID or a forensic review being accomplished on a live system due to time or business constraints.

Summary

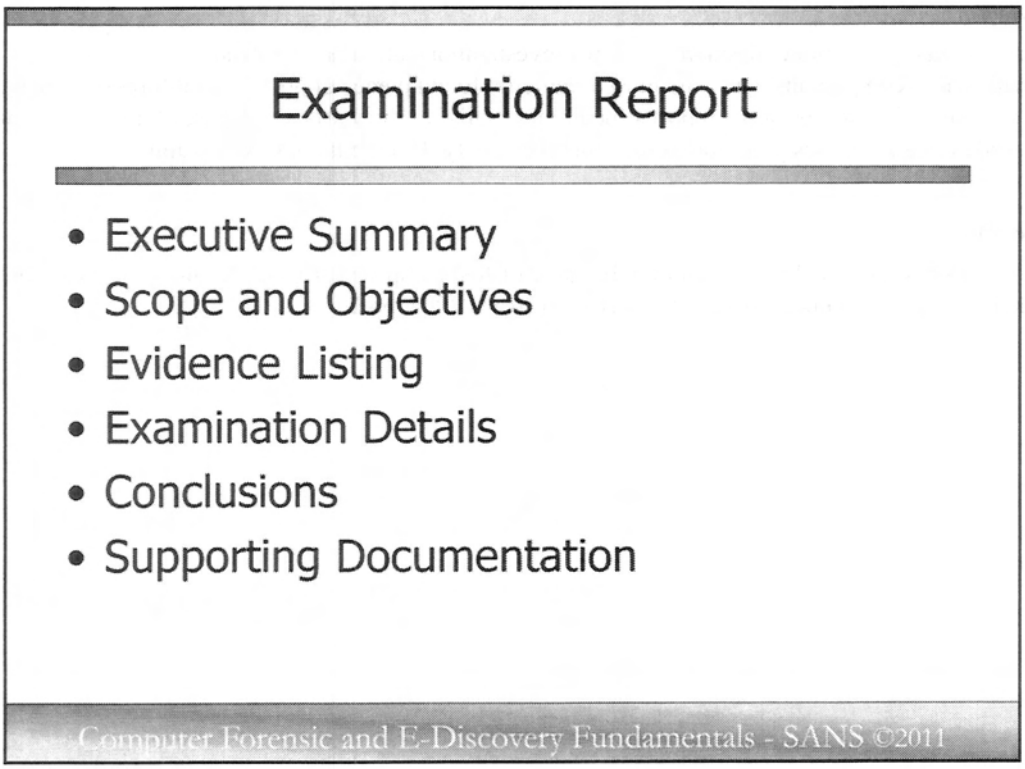
It is important to understand that notes are not only for the investigator. They are often critical for teammates or successors to understand the breadth and depth of a given examination. Many examiners have horror stories of having to re-complete an examination after inheriting a case that contained insufficient documentation. In the case of court proceedings, examiner notes are often discoverable and made available to both sides. It is not

unheard of for an examiner to be called to testify for an examination that occurred three or even six years in the past! Assume that your notes (and report) will be the only information you have to reconstruct the acquisition and examination process and defend your conclusions.

References

[1] www.qccis.com/?section=casenotes

[2] U.S. Department of Justice, National Institute of Justice Special Report: Forensic Examination of Digital Evidence: A Guide for Law Enforcement, April 2004, pp 19



Introduction

Forensic reports typically include several key sections. Each section should aim to answer any questions a reviewer may have regarding your analysis.

Executive Summary – The executive summary is likely to be the most read component of your report. For some audiences, particularly decision makers within your business, it may be the only component of your report that is read. Your summary should rarely be more than one page and should include all of your key findings and conclusions.

Scope and Objectives – Advises the reader about the goals of the investigation and what limitations were put in place.

Evidence Listing – Identifies the media which were examined and provides a reference point for reporting findings on that media throughout the report (i.e. 'USB DRIVE 1').

Examination Details – Should cover the entire examination process, including the tools that were run, their output, and the relevant results that were found.

Conclusions – Conclusions should be based on facts, not opinions, based and should follow logically from the results reported in your *examination details* section.

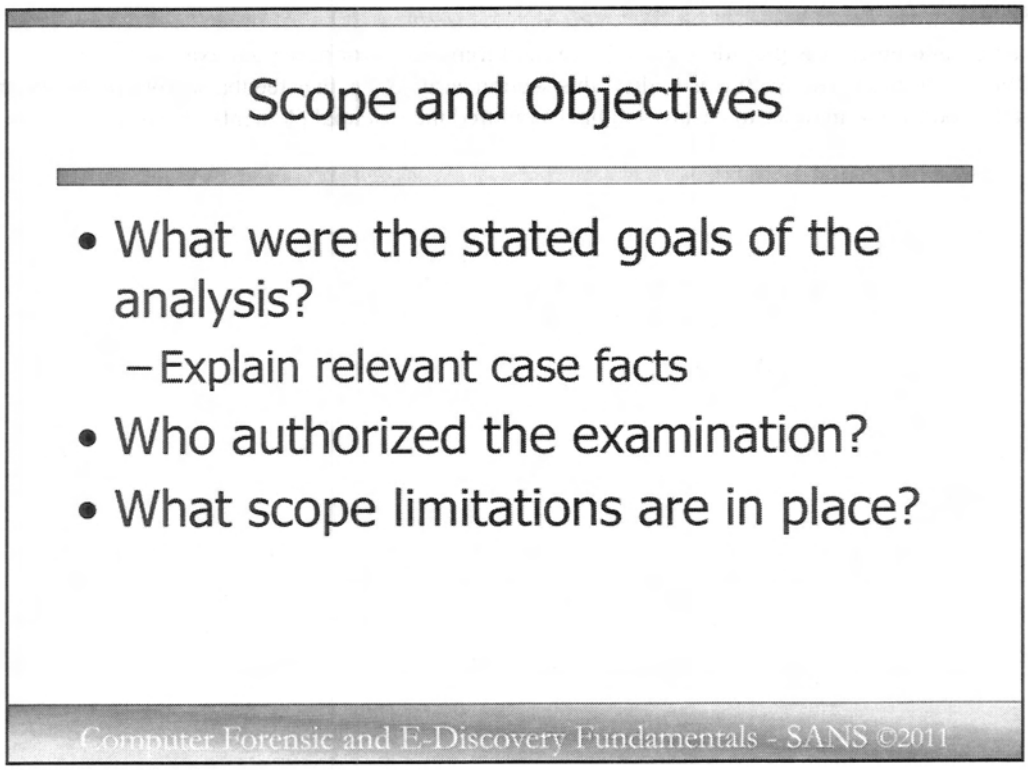
Supporting Documentation – Includes all of the documentation that is too long or would be distracting to put in the body of the main report. Candidates for inclusion could be: tool command line parameters used, output files, and evidentiary files found such as e-mails or log files, etc. This section is often broken up using appendices.

Summary

Organizations who conduct frequent forensics investigations often have a standardized reporting format. These components cover the most commonly found pieces of professional forensic reports. [1] The goal should be to develop a report structure that satisfies the various audiences for whom the report is intended and facilitates your ability to comprehensively document your examination.

References

[1] U.S. Department of Justice, National Institute of Justice Special Report: Forensic Examination of Digital Evidence: A Guide for Law Enforcement, April 2004, pp 20-38



Introduction

The days of an examiner being handed a hard drive and being told to "find stuff" are thankfully long gone. As media sizes continue to grow, it is increasingly importantly that the examiner take the time up front to identify the scope and objectives of the examination.

Objectives

Work with your intended audience to identify what the goals of the investigation should be. What are you attempting to prove or disprove? Law enforcement often structure their goals in terms of the Elements of Proof for the crime they are investigating. These elements are the criteria that must be proved for a person to be considered guilty of the crime. If relevant, the facts of the case can be included to give context to your stated objectives.

Authorization

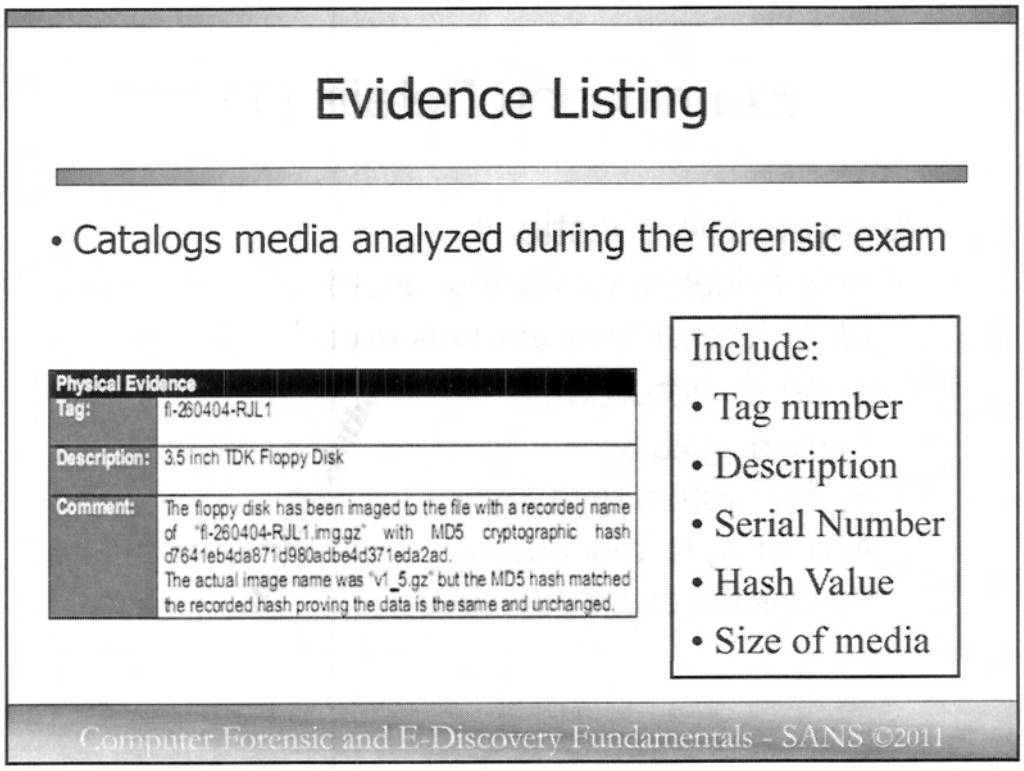
Every examination must be authorized, and this section is a good place to document where that authority came from. The authorization official should provide guidance on what actions to perform and what they expect to be included within the report. You should remain in close contact with the authority, updating them on progress and modifying the scope of the examination as necessary.

Scope

Scope identifies the boundaries of your examination, including what you can examine, and in some cases, what examination methods can be used. It is inherently tied to the authority to examine and is informed by requirements or covenants such as court orders, privacy policies and contracts. As an example, if your scope is to investigate media for evidence of intellectual property theft, you should be prepared to justify how your analysis led you to the discovery of pornographic images on the system.

Summary

The scope and objectives provide the conditions and framework for how your examination was conducted. A good best practice is to draft this section early and gather feedback from peers and those you are reporting to in order to ensure you have captured the essential elements of the investigation.



Introduction

The evidence listing in your report gives the reader a quick snapshot of the media which was analyzed and should provide a means for the writer to refer back to that media within the report.

Description of Evidence

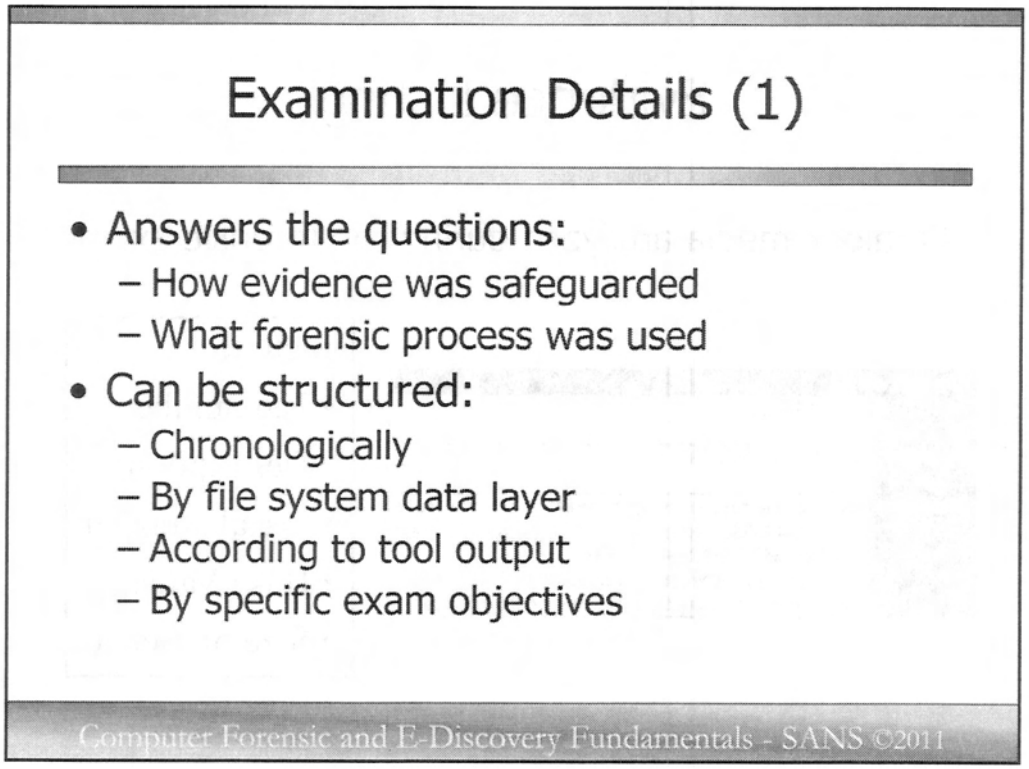
This section allows you to tie pieces of physical evidence to your analysis. The description should be thorough, including the type of device, the make, serial number, data capacity, any physical markings, and a hash value of the evidence if available. This not only provides a quick reference for you to use during your examination, but also allows you to reference the media without needing to repeat the key information. To this end, investigators will often select labels for the evidence, such as 'LAPTOP 1', to make it easy to indicate to the reader which piece of evidence yielded the given result.

Summary

Making an evidence list is usually done long before the final report is written and is critical for ensuring that all evidence was taken into account during the exam. If the examiner was diligent with recording all of the necessary information, creating an evidence listing for the final report should be very straightforward.

References

Physical Evidence Graphic from SANS GIAC GCFA Practical, Tom Chmielarski, Oct 2004. http://forensics.sans.org/community/papers/forensic_analysis_of_a_sun_ultra_system_125



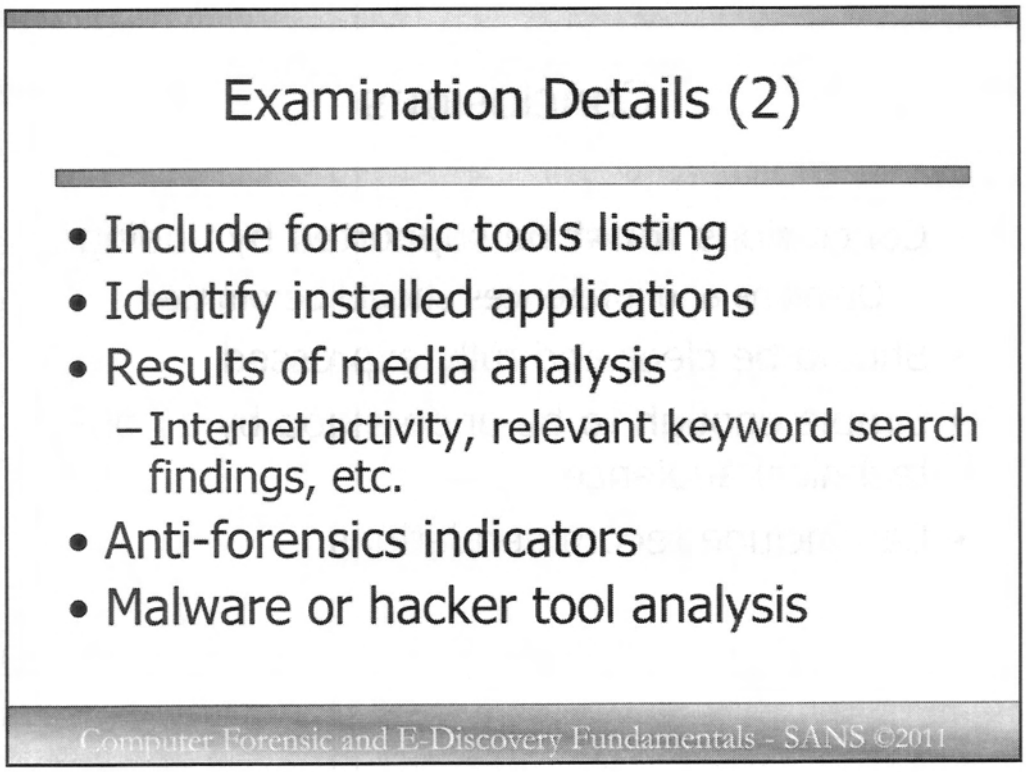
Introduction

The bulk of the work in documenting a forensic examination will occur in the details section. This is where the examiner will explain how the examination was conducted and what key results (if any) were discovered.

It is important to include everything a reader may need to know to understand how the analysis was conducted. You should explain your steps in enough detail so that another examiner could replicate your process and find the same set of results. This is more than just a mental exercise - it is common for an outside expert to be used to perform a secondary analysis of the evidence in both criminal and civil trials. If describing the tool setup parameters will be distracting, utilize an appendix to list exactly how each tool was run. Some forensic tools make this easy for you by providing an audit trail of all commands entered. Similarly, if the tool results are too lengthy (greater than half of a page), a summary should be provided and the reader directed to the *supporting documentation* section to see the full material.

How to Structure the Details

Examiner preferences will dictate the overall structure and could be different for various types of cases. Chronological may be the most common, but structuring according to tool output could be relevant in situations where procedures dictate a strict order of tool use. Organizing the report details by the stated goals or elements of proof within the *objectives* section could also be helpful to a particular audience.



What to include

The examiner should list all of the steps taken to complete the investigation. This includes the steps to acquire the evidence, the measures taken to ensure evidence integrity, and the entire forensic process used to conduct the media analysis and identify the results relevant to the goals in your *objectives* part of the report. It is common for investigators to include their findings along with the description of the tool that was used. As an example:

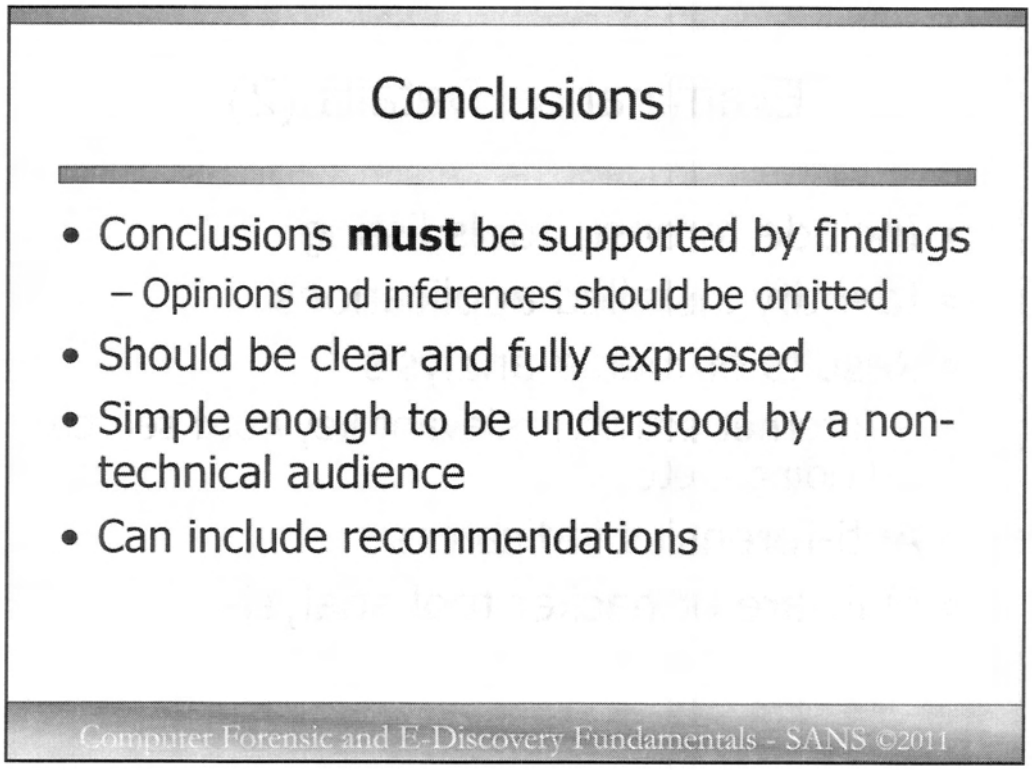
"On January 12th, 2009 at 1100 hours I performed file carving on the unallocated space of SMITH WORKSTATION using the Foremost utility. As a result, 54 documents were recovered. Review of the recovered documents identified two that appear to be relevant to the improper sales made to XYZ Corp. (see Appendix B)"

In addition to documenting the forensic process, it is often useful to include background information like the set of forensic tools used, what (relevant) installed applications were found on the system, and any evidence found of anti-forensics tools or indicators of data spoliation.

If a detailed analysis is conducted of any findings, such as malware or unknown executables, the results are often summarized and the full analysis included as an appendix.

Summary

The examination details section will be the core of your report. It describes your entire investigation and the key findings and results. The other sections of your report should be built to support the information covered in this section.



Introduction

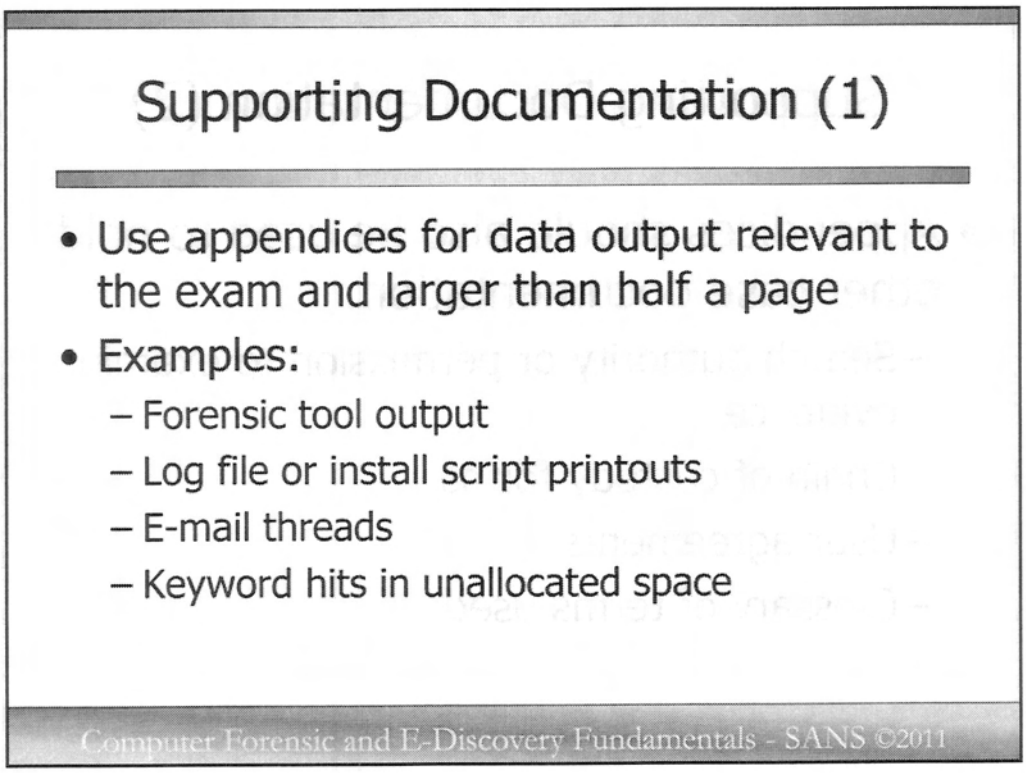
Your conclusions are used to tie together the results found within the *examination details* section and answer the questions posed within the *scope and objectives* at the beginning of the report.

Just the Facts

The conclusions section can be the most difficult to write for some examiners. It is critical that conclusions be squarely based on the facts of the case and the results found during the forensic examination. Computer forensics is as much art as it is science and very rarely will the investigator be able to recreate what happened on a given computer system perfectly. Thus it is tempting for examiners to make guesses or jump to conclusions about what *may* have happened. As an example, secure deletion software could be found on a machine and a relevant file name identified for an unrecoverable file. Without further proof, it would be improper for the examiner to opine that the file was "probably" removed with the anti-forensics tool. On the other hand, if the examiner were to conduct testing of the secure deletion tool and find signatures in the unrecoverable file which were consistent with his testing, then it may be appropriate to conclude that the tool was used to delete the file. Simply stated, the job of the forensic investigator is to only present the facts.

Summary

The conclusions of an examination is often the most important piece of the final report. They will be read by a wide audience and thus should be clearly stated and as non-technical as possible. The conclusions of one exam could be the start of an entirely new investigation, and thus it is common for the examiner to recommend other systems to review or other investigative steps that should be taken.



Introduction

To make the forensics report more readable, long or overly technical material is often placed in an appendix. Report writers should feel free to excerpt or summarize material in the main body of the report and reference the full results in the supporting documentation section.

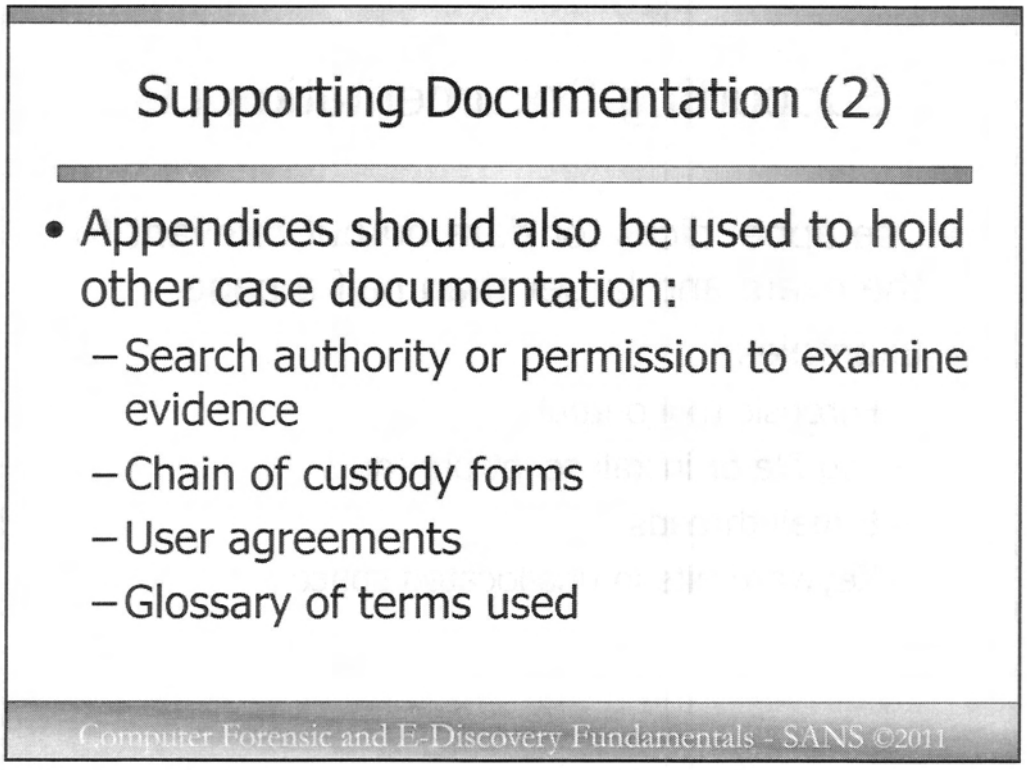
Why use supporting documentation?

Supporting documentation is an important part of making a report accessible for a wide variety of audiences. In many cases readers will be uninterested in the exact command line used to run a particular forensics tool, but this information needs to be documented somewhere for a different type of audience. It often finds itself within an appendix of the supporting documentation section.

A common rule of thumb for writing a forensic report is that any output that is over one half of a page long should be included in an appendix instead. Care should also be taken to not overburden the appendices with information not useful to the investigation. Investigators should be looking to include items that support key findings and are relevant to the stated goals and objectives of the examination. You may find thousands of e-mails located on a system, but only include the few which are deemed relevant. The others can simply be archived.

Keeping results in native form

It is important to keep in mind that the Federal Rules of Evidence (containing the standards applied to allow evidence into court) allow electronically stored information (ESI) to be admitted in its native form. Thus is it perfectly acceptable to reference digitally stored files within your report or supporting documentation. This is particularly useful for large files like spreadsheets, databases, etc.



The supporting documentation section can also be used to hold procedural documents for the exam. All documents which gave authority to conduct the exam and defined the scope of the investigation should be kept with the exam itself. Additionally, evidence integrity documentation like chain of custody forms and examiner notes can be placed in an appendix.

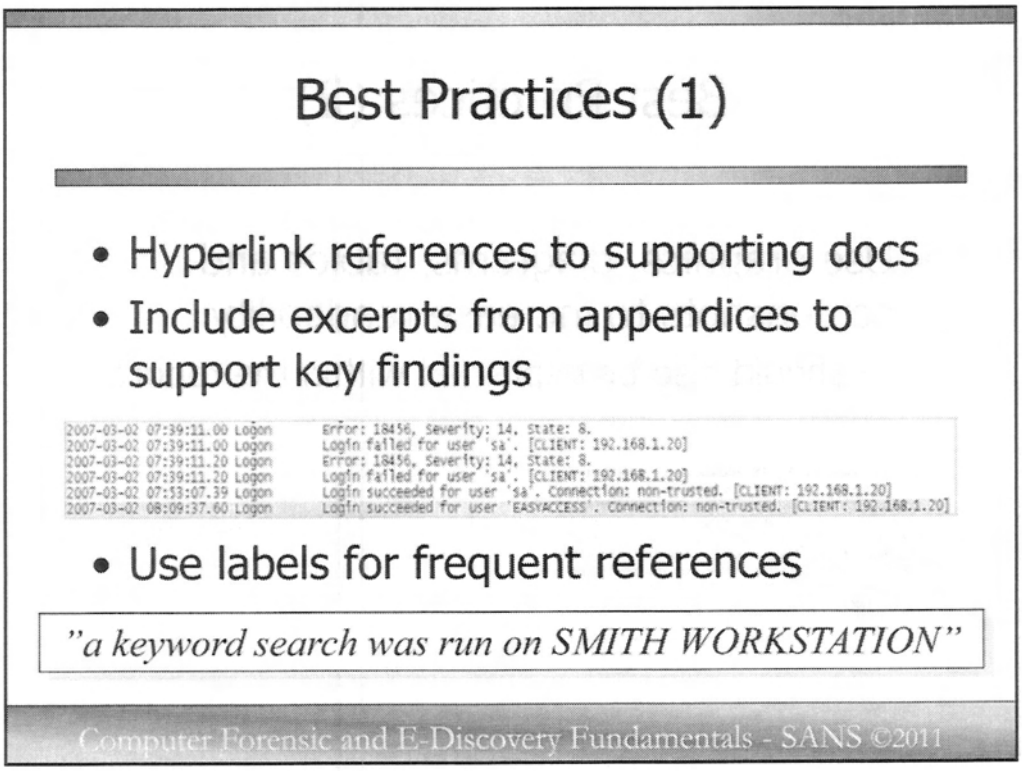
Depending on the report style, glossary terms can defined within the report as the term is introduced, or kept in an appendix. Regardless of the technique used, it is helpful for examiners to collect glossary terms and boilerplate language that can be reused and consistently updated as new explanations are required.

Summary

Well organized appendices are an important tool for keeping reports both readable and comprehensive. Supporting documentation should not be used as a catch-all, but should instead be carefully managed to only include material supportive and relevant to the other parts of the report. Done well, the supporting documentation puts the examination in context and neatly wraps up the report from the initial authorization all the way to the key findings and conclusions.

References

U.S. Department of Justice, National Institute of Justice Special Report: Forensic Examination of Digital Evidence: A Guide for Law Enforcement, April 2004, pp 21



Introduction

The following tips and tricks are often used by successful writers within their forensic reports. If a large number of reports are generated by your organization, it could be useful to create a series of guidelines for forensic reports.

Packaging reports

Since reports are frequently delivered electronically, writers should take advantage of the inherent benefits of using a digital format. It is now commonplace to admit electronically stored evidence into court. Many investigators burn their report onto a CD-ROM and include all of their supporting documentation in digital form. This allows things like keyword search output, relevant images, and recovered e-mails to be hyper-linked directly from the report, greatly increasing usability. Reports are often stored as Microsoft Office documents, PDF, or even HTML documents.

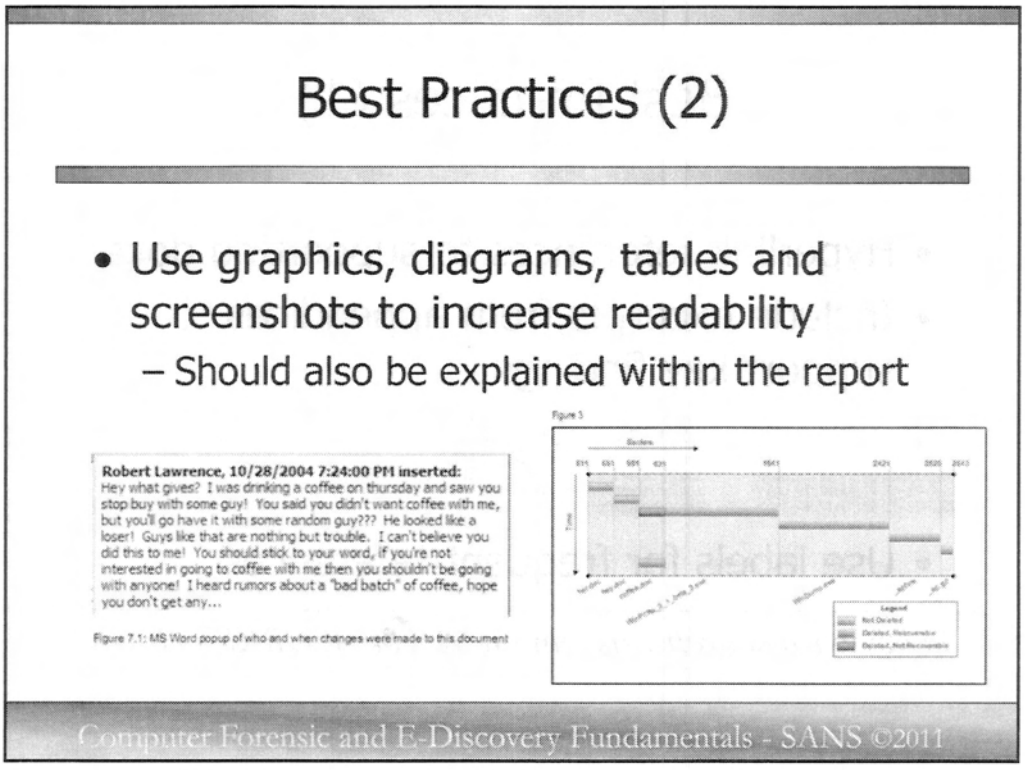
Increasing readability

While many of your results will be stored in appendices, it is often beneficial for the reader to see a short excerpt of what you are describing. This could be a piece of a log file, a short snippet from a long e-mail, or partial results from a tool like netstat.

Using labels for analyzed media provides an easy way to describe where particular results came from, without necessitating a long description of the evidence. An excellent place to define labels is in the evidence listing section of the report.

References

Excerpt graphic from SANS GIAC GCFA Practical, Kevvie Fowler, April 1, 2007
http://forensics.sans.org/community/papers/forensic_analysis_of_a_sql_server_2005_database_server_260



Increasingly Readability (part 2)

Including graphics within your report can greatly enhance a reader's understanding, particularly for audiences who may have a limited understanding of computer forensics. It is one thing to describe metadata within a MS Office document and yet another to provide a screen capture of what that metadata looks like within the application. GUI based forensics tools often provide excellent opportunities for screen output to be captured and included within the report. Examples include the partition layout of the media, text fragments found in unallocated space, or a display of hash matches for a known bad file. Like any report, graphics should always be explained within the body of the report and labeled appropriately.

Other Best Practices

Whenever possible, reports should be peer reviewed before they are released. Having a knowledgeable colleague read the report to look for errors and omissions is invaluable for ensuring your analysis is complete and your reporting is accurate.

Another best practice is to work through your legal department to have your report covered under attorney-client privilege. This often affords your company a high degree of flexibility with how they can respond to the results of your investigation.

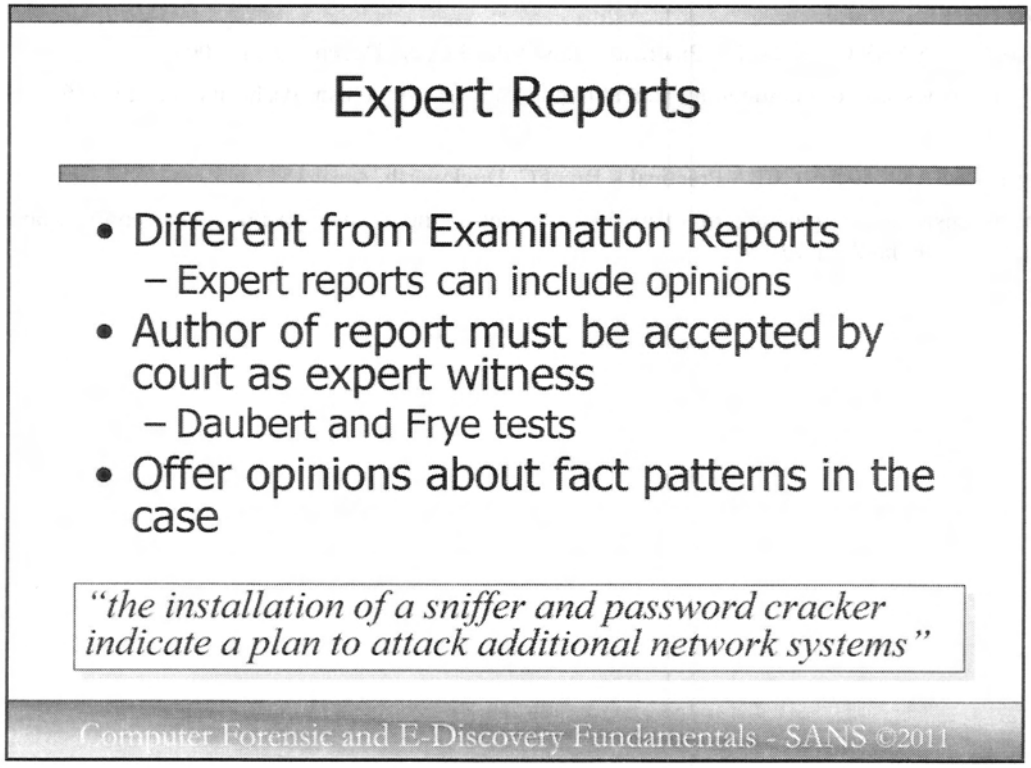
Summary

The key to successful forensic reporting is not unlike any other kind of report writing. The examiner should keep their intended audience in mind, take pains to describe complicated topics in words and images, and provide ample documentation to support their results and conclusions.

References

Figure 7.1 – SANS GIAC GCFA Practical – Raul Siles Pelaez, December 21, 2004
http://forensics.sans.org/community/papers/honors-analysis_of_a_usb_flashdrive_image_146

Figure 3 – SANS GIAC GCFA Practical – Brent C. Duckworth, April 15, 2005
http://forensics.sans.org/community/papers/cc_terminals,_inc.forensic_examination_report:_examination_of_a_usb_hard_drive_206



Introduction

An important distinction should be made between standard forensic examination reports and those reports generated by a court appointed expert. While standard examination reports should not contain opinions, expert reports are typically created specifically to introduce opinions.

Expert Reports

Expert reports are written by court certified expert witnesses, and are evaluated using the Daubert and Frye tests to ensure opinions are grounded in scientific knowledge and derived using the scientific method. [1]

Expert witnesses are typically charged with submitting a report to the court outlining all of the opinions they will express, and providing the necessary data and analysis to support those opinions. [2] Unlike standard examination reports, expert reports hinge directly upon the ability of the court certified expert to make opinions. This allows testimony to be introduced that fills in the gaps between what can be absolutely proved as a result of the examination (i.e. the conclusions in a standard exam) and what most likely occurred based on the totality of the findings.

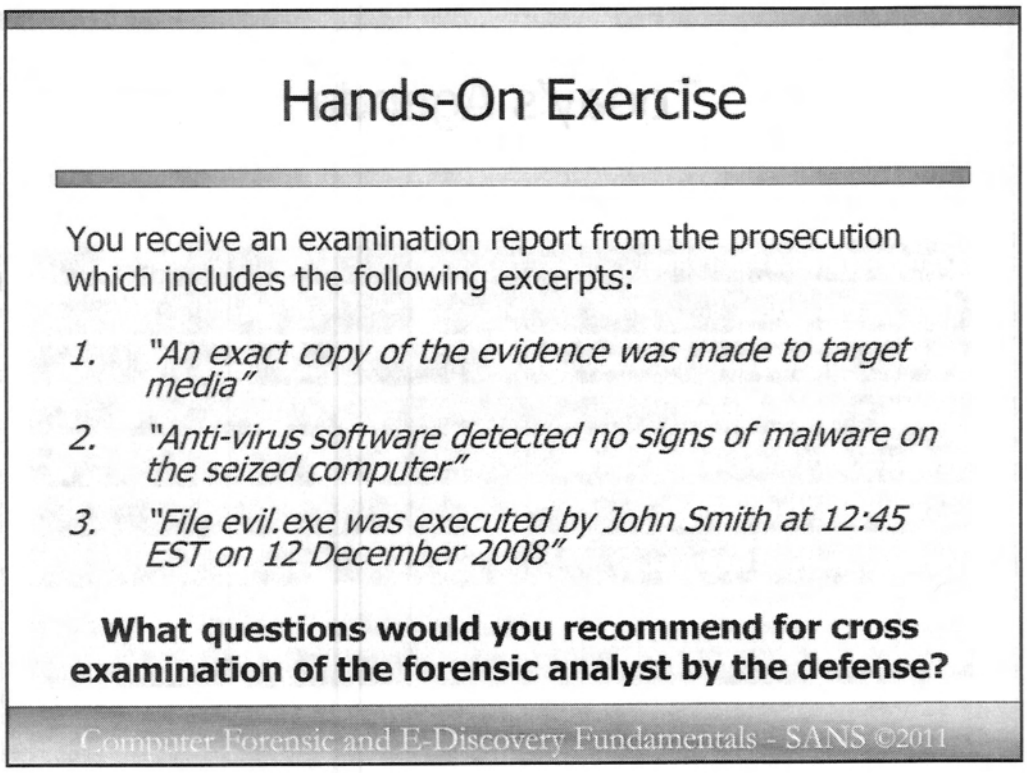
Summary

Expert reports are a small subset of examination reports, but are instructive to show the contrast between the narrow, fact based conclusions made in a standard forensic report and the latitude afforded a court appointed expert witness to introduce opinions based on their knowledge and experience with similar cases.

References

[1] www.daubertontheweb.com

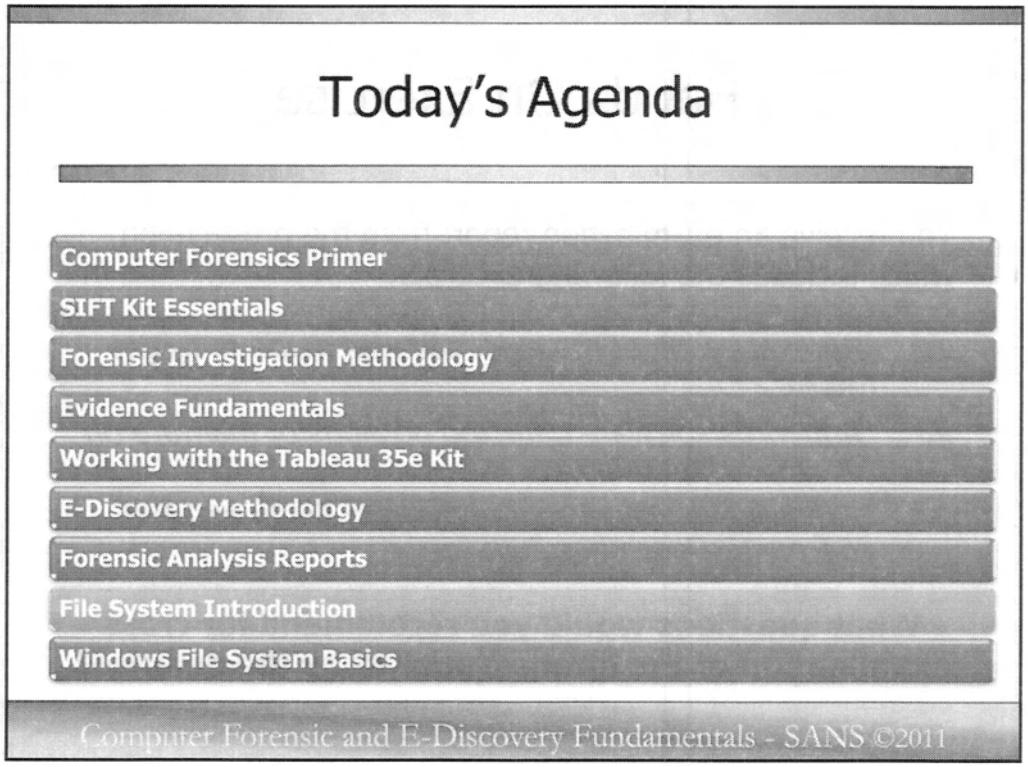
[2] http://www.law.cornell.edu/rules/frcp/Rule26.htm



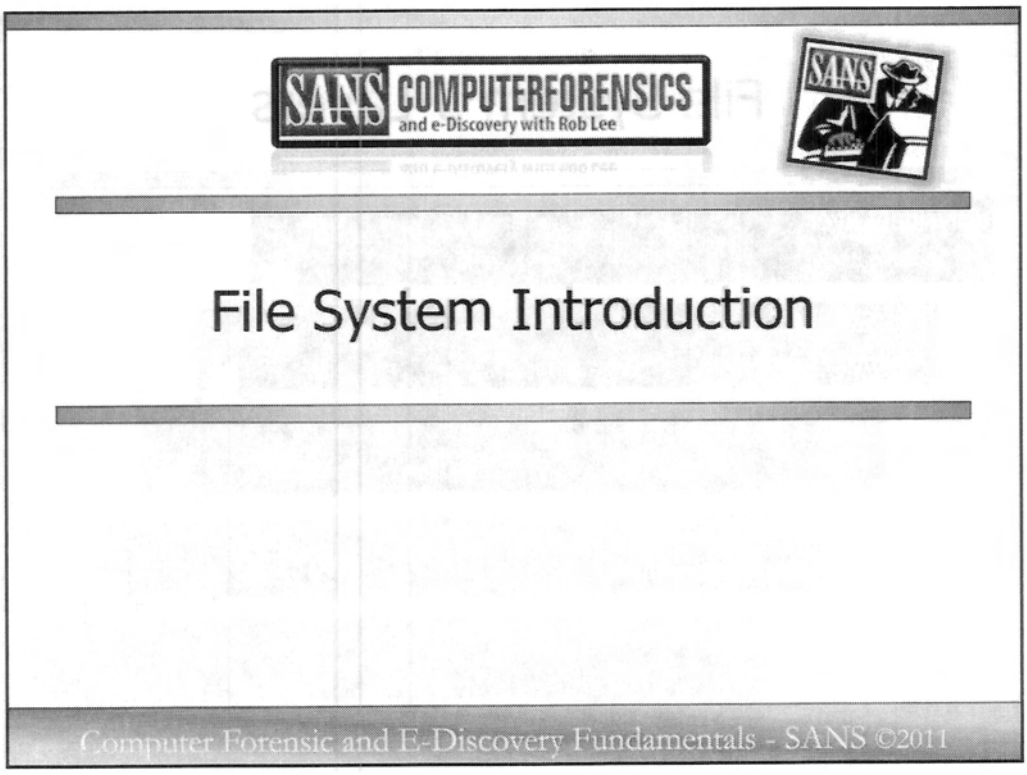
Hands-On Exercise Solution

The statements listed in this exercise range from very broad (#1) to almost too specific (#3). The job of cross-examination is to dig deeper into what was reported by the analyst in order to identify areas where common practices were not followed or where conclusions were made inappropriately. Any questions along these lines would work for this exercise. Some common questions include:

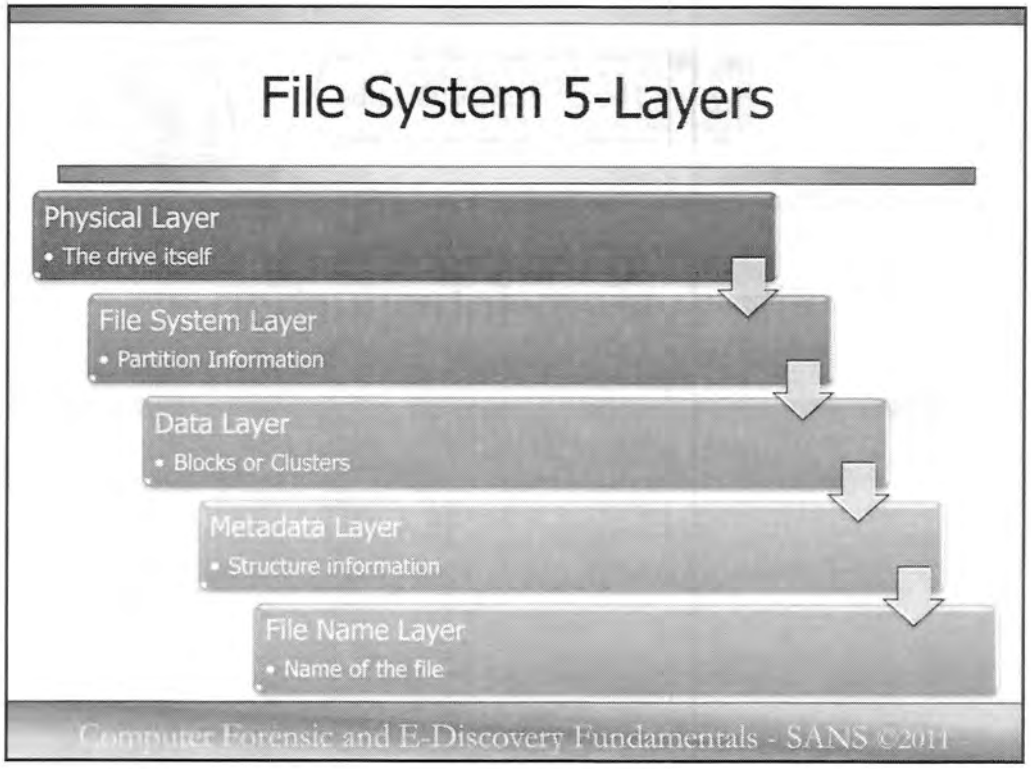
- How was the target media prepared?
- What tool was used to create the evidentiary copy?
- How was the integrity of the evidence maintained?
- What anti-virus tools were used?
- Were the anti-virus signatures up-to-date?
- How was the anti-virus software run to prevent tampering from possible trojans?
- What user account was used to open evil.exe?
- What evidence ties the opening of evil.exe to a user account?
- How can we be sure that John Smith was the one using the account that executed evil.exe?



This page intentionally left blank.



This page intentionally left blank.



This page intentionally left blank.

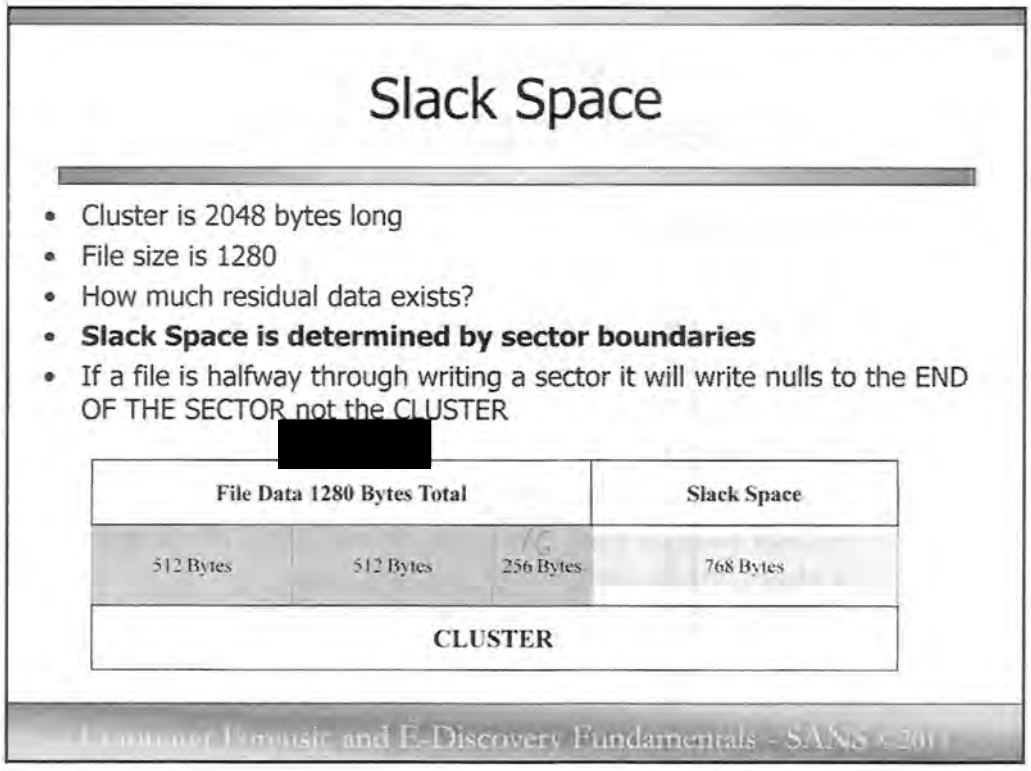
[redacted]

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

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.

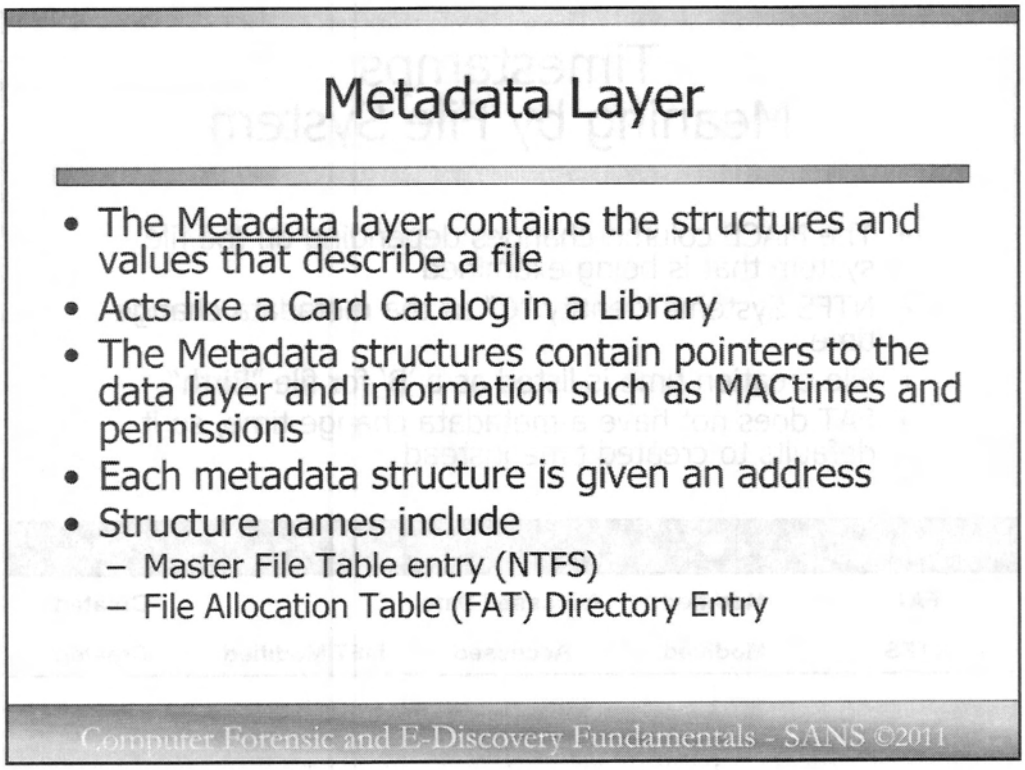
If a file is not fully recoverable, a piece of that file may still be recoverable. That piece of the file is called a file fragment. A fragment may be one or more blocks of data, but alone would not be the full file. For example, an e-mail found on a system may be recoverable, however, you may only obtain 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.



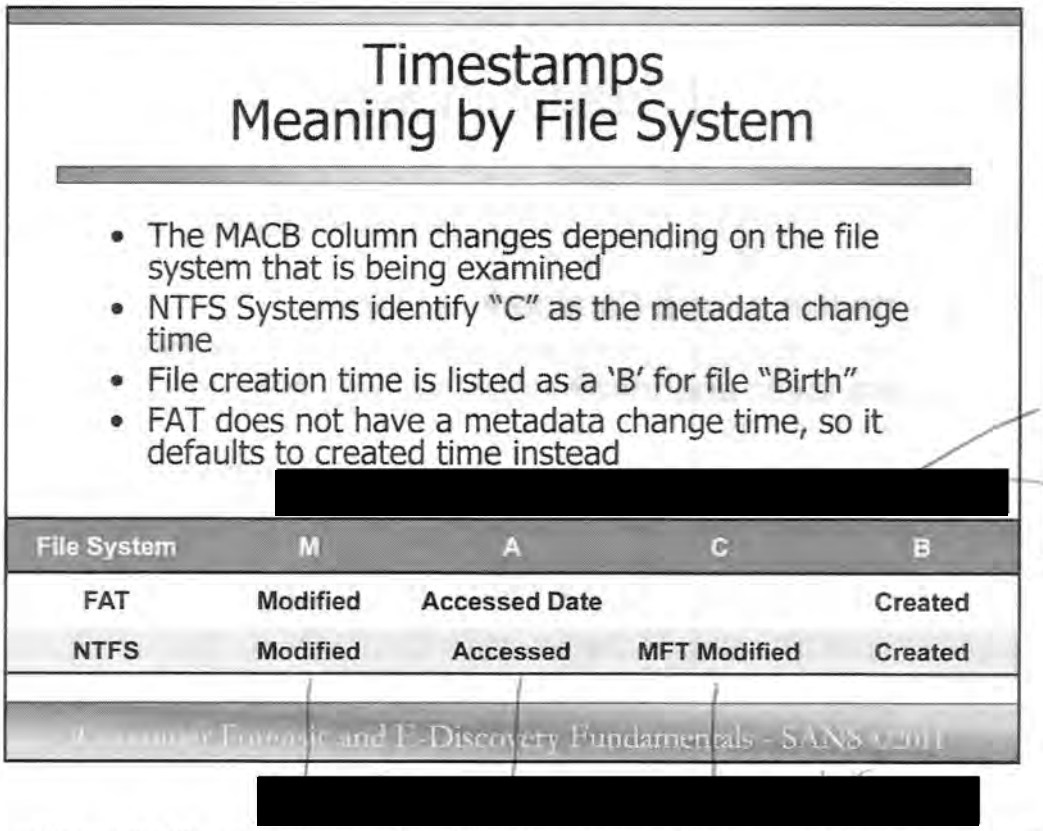
Typical file systems store virtually all data in files. The most important of these are a set of special files, which are typically called *metadata structure*. The prefix "meta-" means self-referring. So "metadata structures" are structures that contain data *about* data. And that's exactly what these 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
File Allocation Table (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 FAT, the File Allocation Table is used to find "Chains" of clusters.

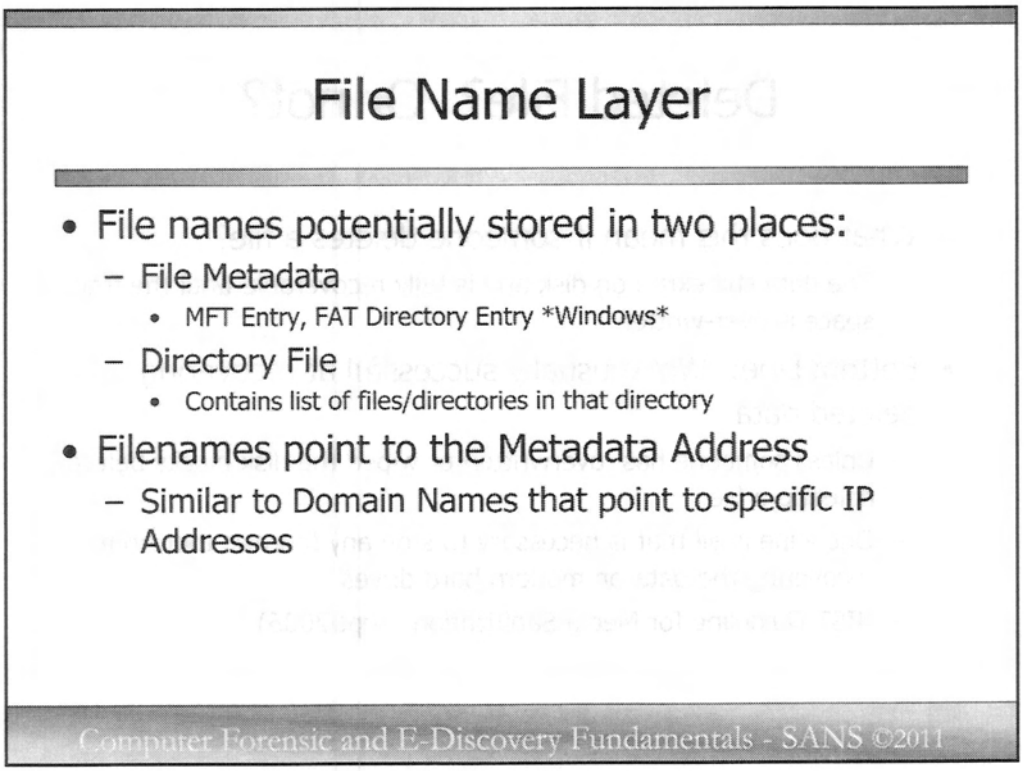
Each structure is given an address. We will use this address when referring to structures in this layer. This structure is typically hidden (especially for deleted files) from users, but there is a lot of useful information in them.



Depending on the file system, the meaning of the letters in the MAC column might change a bit. The largest change occurs in the "C" column. On NTFS file systems, 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.

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.

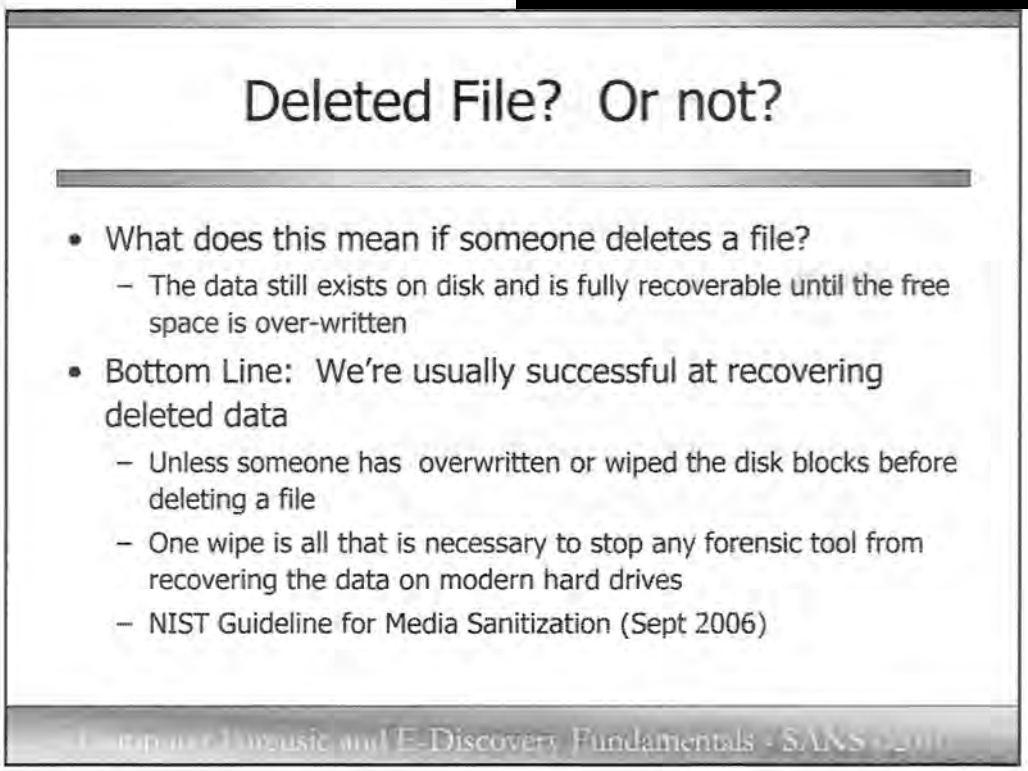
In the latest version of the sleuthkit, the "B" letter stands for the files "BIRTH" or creation time.



The File Name layer is typically a separate structure that gives names to files. The metadata layer can describe everything about a file, but it is often inconvenient to have to remember that /etc/password is inode 312. The file name structures are typically stored in the data units allocated to the parent directory. They contain the name of the file and the address of the metadata structure (except in FAT because everything is stored in the parent directory).

When files are deleted, the file system will hide the file name from the user, but much data can be recovered using forensic tools.

[redacted]

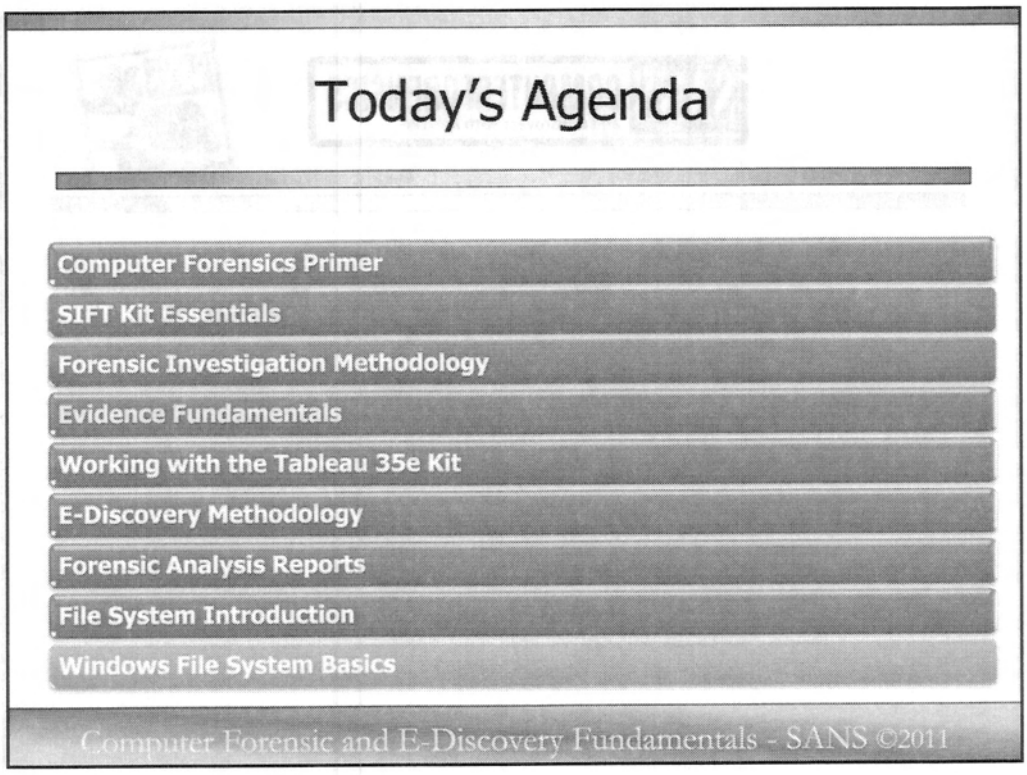


This is important for one reason. If a file is deleted, the contents are not overwritten immediately. The data still exists on disk and can be recovered until the free space is re-allocated by the OS and overwritten.

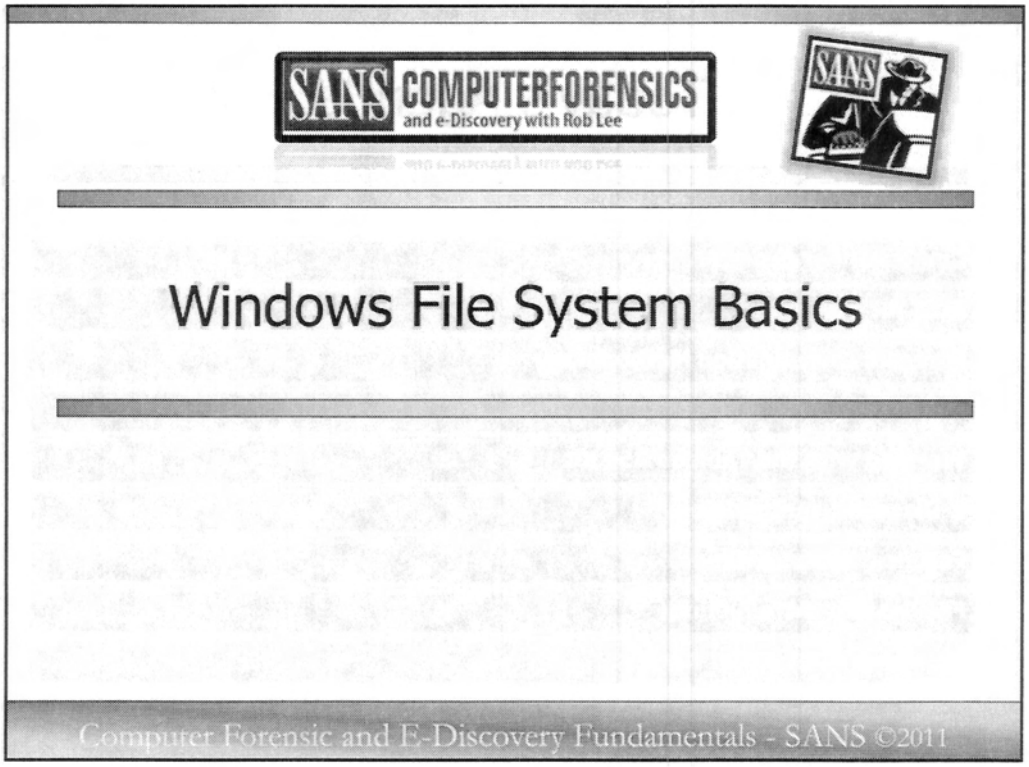
You might think that the lifespan of deleted data is short, and that storage space that has been freed is used again quickly. This isn't necessarily the case. In fact, because of the inode and disk block allocation algorithms, this sort of collision occurs infrequently.

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.

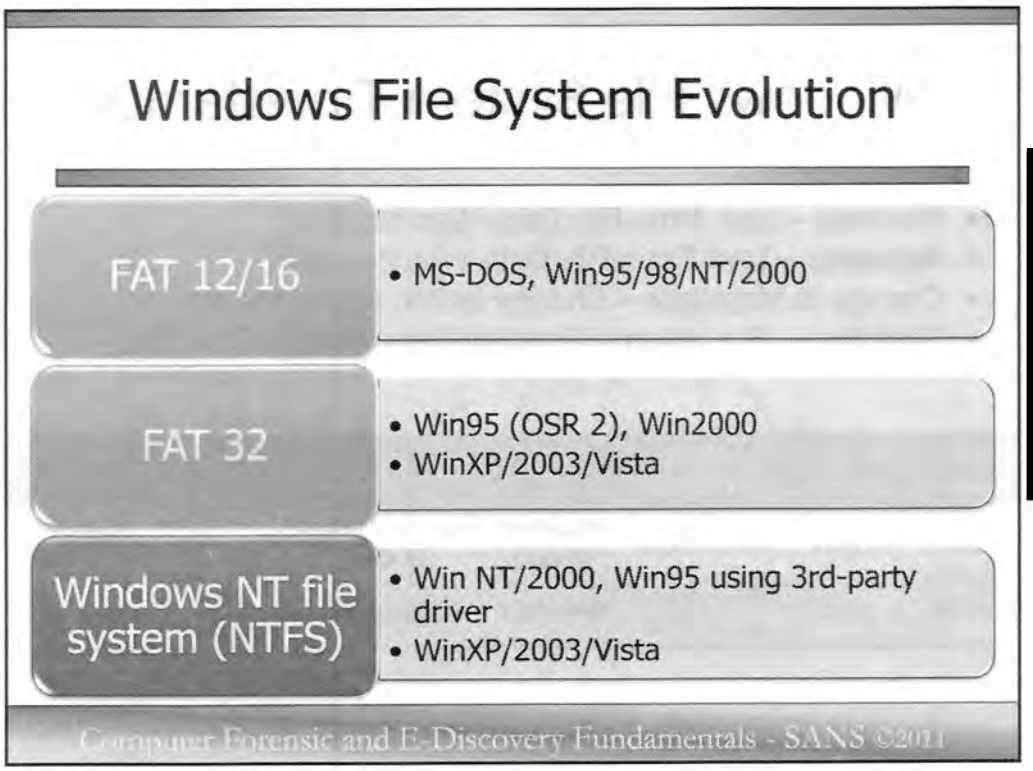
Srm defeats recovery techniques by wiping (or overwriting) the contents of file before the file is deleted. Only one wipe is necessary to stop any forensic tool from being able to recover the data that was once written there. Recently, the NIST guideline, **Guidelines for Media Sanitization** September 2006, states that one wipe is all that is necessary for most modern hard drives.



This page intentionally left blank.



This page intentionally left blank.

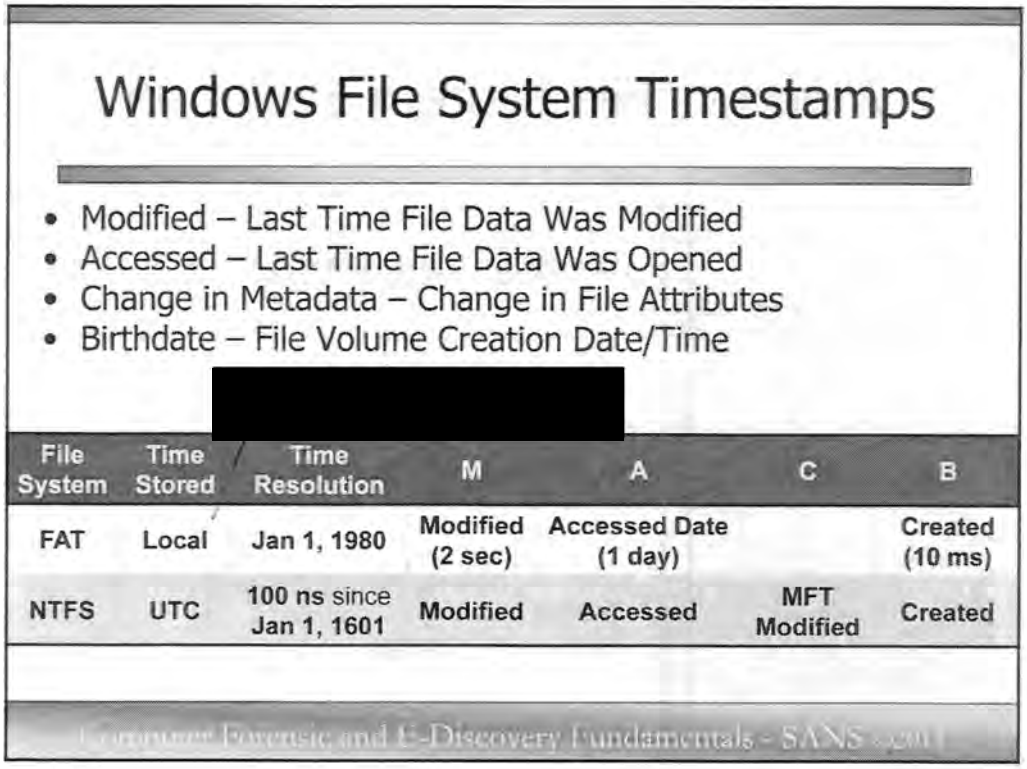


A file allocation table (FAT) is a table that Windows maintains on a hard disk that provides a map of the clusters that a file has been stored in.

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 to the 16th power 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!



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

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 timezones. 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.

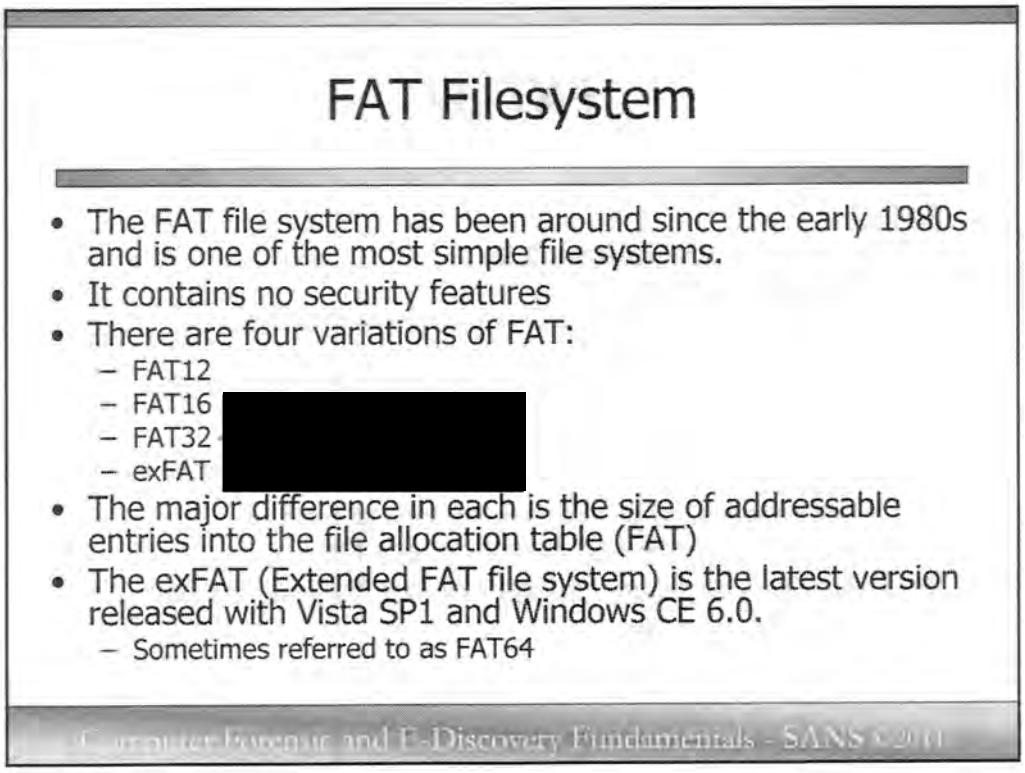
NTFS stores time in UTC -> 12:00 A.M. January 1, 1601 Coordinated Universal Time (UTC).

FAT stores time in Local Time-> 12:00 A.M. January 1, 1980

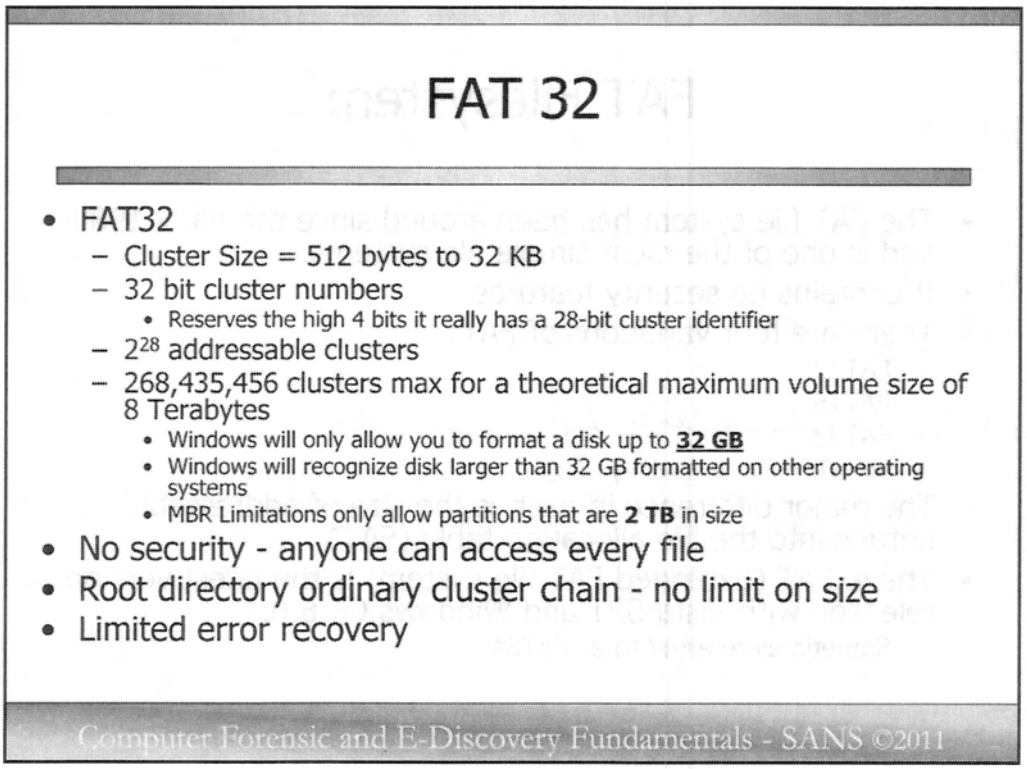
It is important to remember the meaning behind the letters as it changes the context surrounding the event in the timeline. For example, a file might be created on a NTFS volume and then transferred to a USB key with a FAT32 volume. The modified time of the file should remain constant, but the C time 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.

Depending on the file system, the meaning of the letters in the MACB column might change a bit. The largest change occurs in the "C" column. On NTFS file systems, 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 "B" letter stands for the files "BIRTH" or creation time.



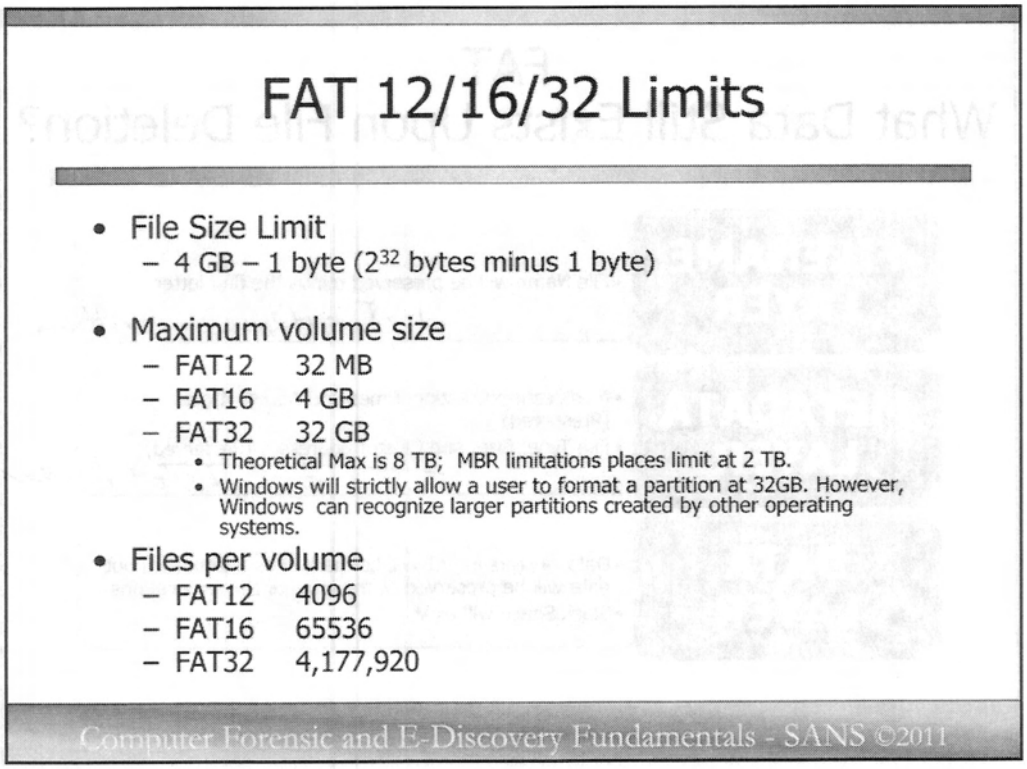
The FAT file system has been around since the early 1980s and is one of the most simple file systems. It contains no security features, few time stamps, and several hacks that have allowed it to still be used today. There are four variations of FAT: FAT12, FAT16, FAT32, exFAT. The major difference in 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.

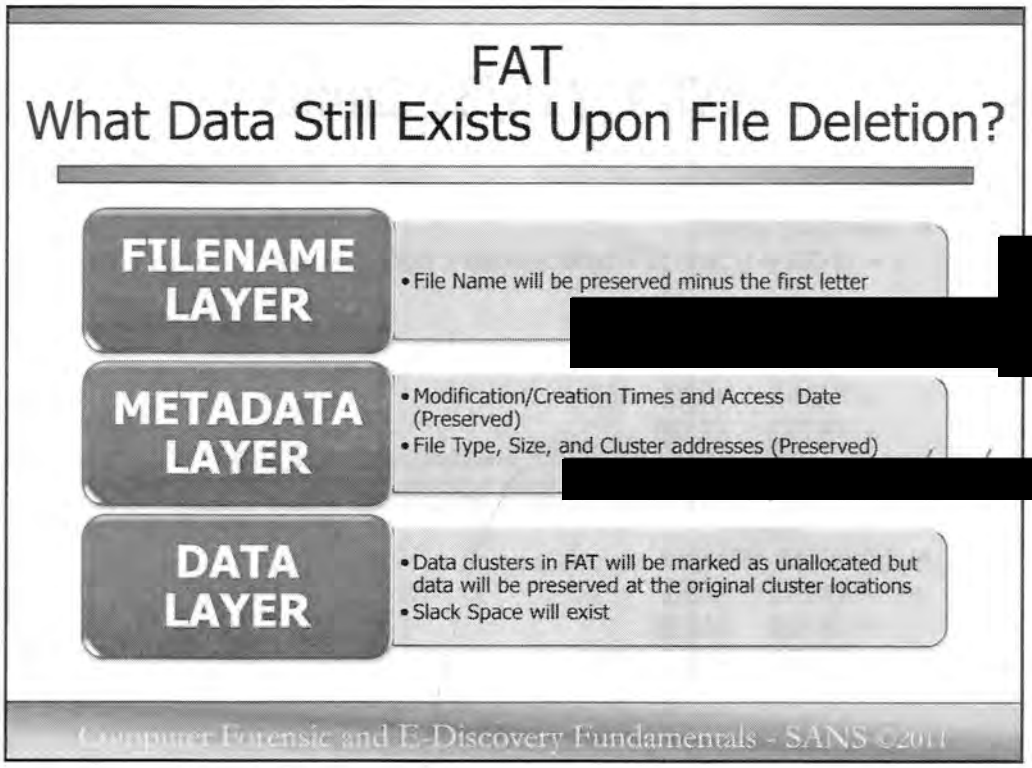
The FAT file system is one the most common PC file system around as it is compatible with so many different computers. FAT is very reliable since it keeps a table of files and free space. If your system crashes, the FAT does not lose data, but may not have written the data before the crash. Typically, 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.

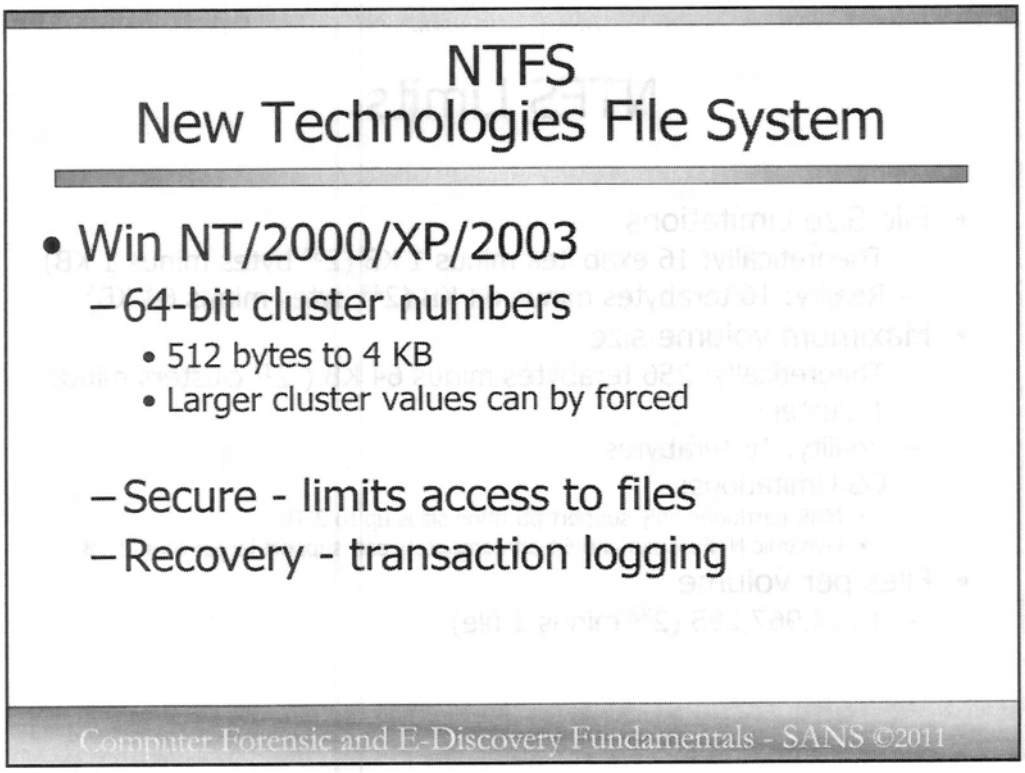


Overview of FAT Filesystem's Limits.

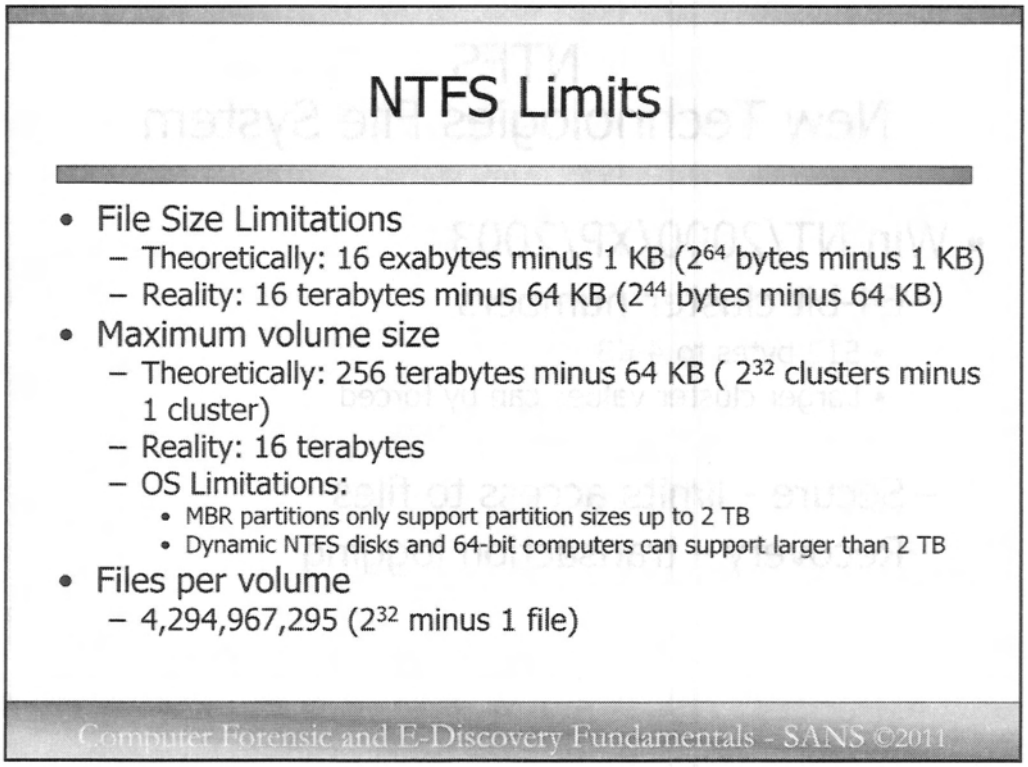
http://technet2.microsoft.com/windowsserver/en/library/810c3217-77bb-4553-b6ce-3ff10dbdbac91033.mspx?mfr=true



Note: Any data preserved after deletion is only preserved until it is overwritten. On Windows machines, cluster and metadata re-use is typically high compared to that of UNIX filesystems.

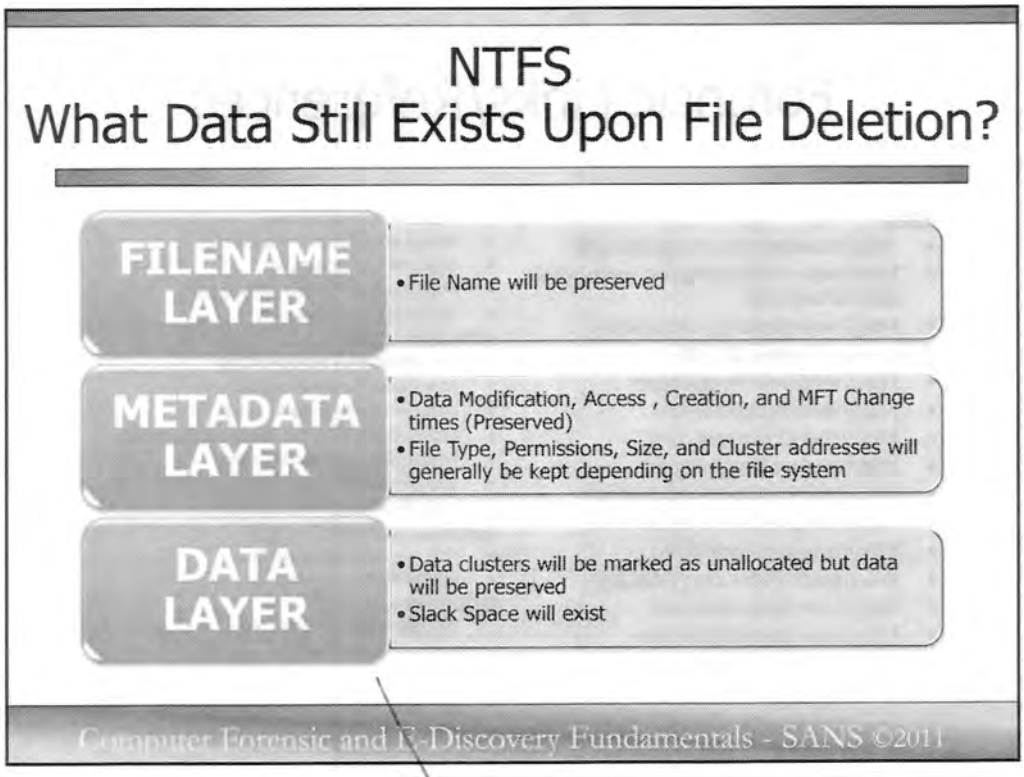


NTFS includes many features not found in the FAT system and was designed to be reliable and efficient even when used on large disk volumes. NTFS provides a great balance of performance, reliability and compatibility. Its design let's it quickly perform file operations like read, write, and search. NTFS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



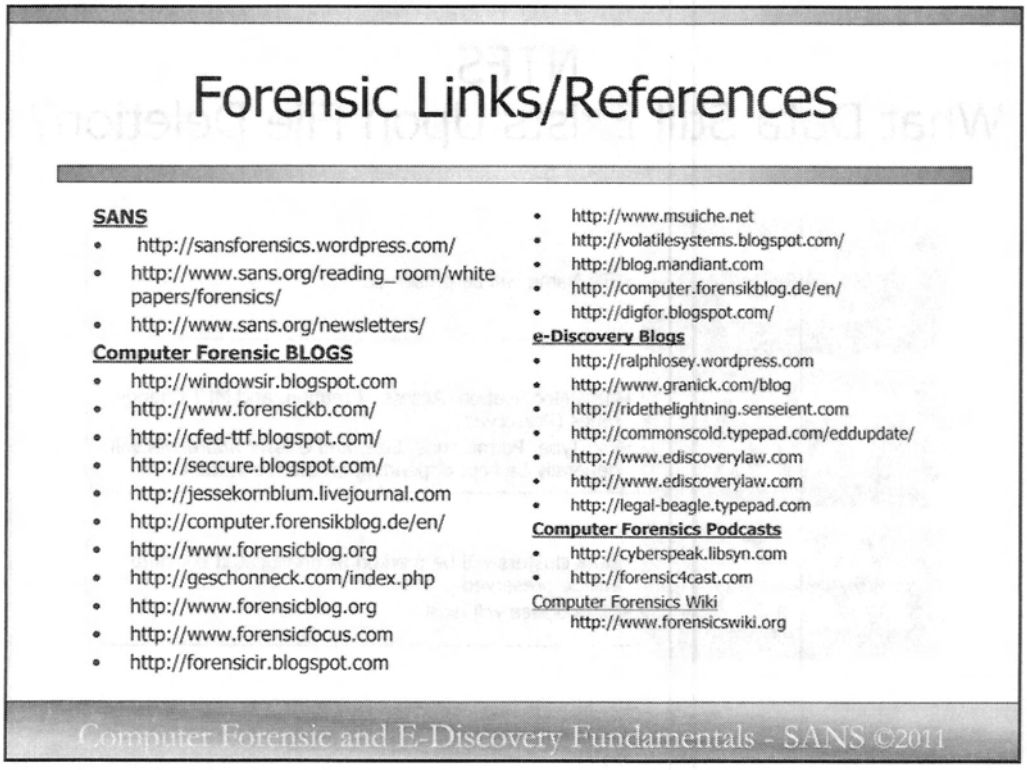
This slide shows the maximum sizes for files, volumes, and number of files possible in an NTFS volume.

Reference: http://technet.microsoft.com/en-us/library/bb457112.aspx

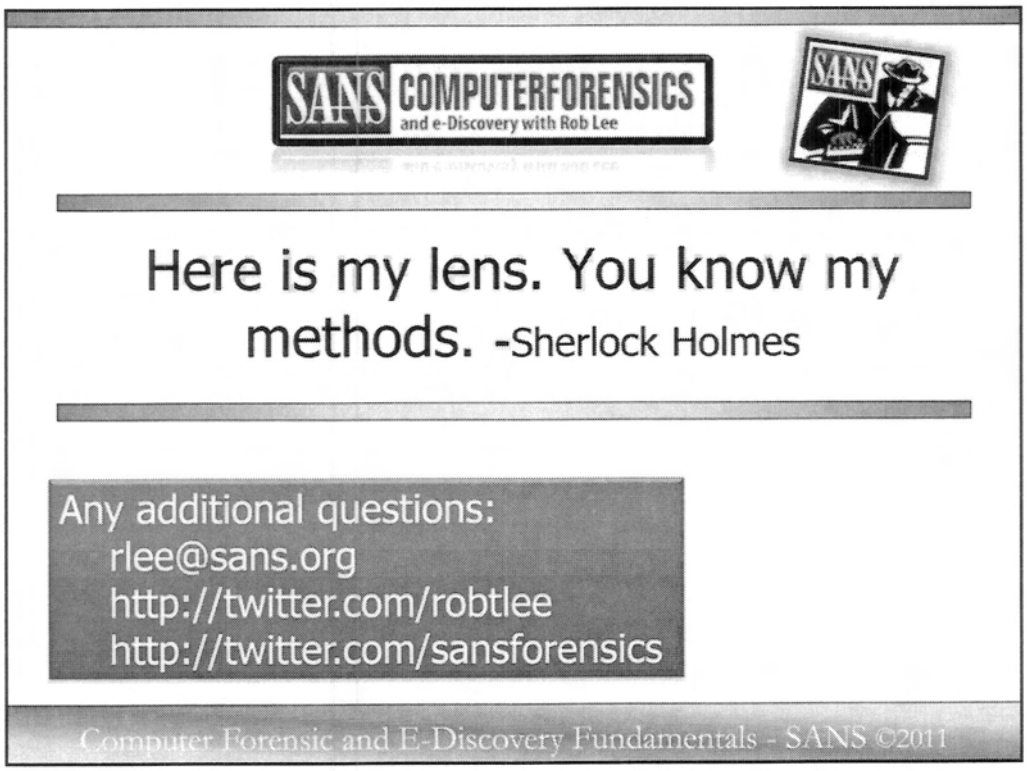


This page intentionally left blank.

[redacted]



This page intentionally left blank.



This page intentionally left blank.

This page intentionally left blank.

LAPTOP INSTALLATION GUIDE
SANS Courses SEC408
Version 2.2

Mandatory Requirements For Class: **2**
License Verification: Microsoft Windows 7 Home **3**
If your BASE OPERATING SYSTEM is Windows: **4**
WINDOWS VMWARE INSTALLATION 4
If your BASE OPERATING SYSTEM is LINUX **5**
LINUX VMWARE INSTALLATION 5
If your BASE OPERATING SYSTEM is MAC OSX **8**
VMWARE FUSION 2.0 INSTALLATION 8

Mandatory Requirements For Class:

BASE OPERATING SYSTEM
LINUX, MAC OSX, or WINDOWS

You can use any version of Windows, MAC OSX, or Linux as your core operating system as long as **VMware Workstation 6.0, VMware Fusion 2.0, or VMware Player 2.5 or higher** is installed and functional. SANS will be handing out multiple VMware guest machines that will be utilized for the course.

Mandatory License Requirements:

- **Very Important:** Student must bring a Microsoft Windows 7 Home License Key with them to class at the beginning of the first day
- The key will look like **XXXXX-XXXXX-XXXXX-XXXXX-XXXXX**
- **Print out the next page and bring with you to class**

Mandatory Laptop Hardware Requirements:

- **CPU: 1.5 GHz or higher is recommended**
- **DVD/CD Combo Drive**
- **Wireless 802.11 B/G Networking Capability**
- **2 Gigabyte of RAM minimum (4 or higher RAM is highly recommended)**
- **100 Gigabyte Hard Drive minimum (HARD DRIVE SIZE IS CRITICAL)**
- **60 Gigabytes of Free Space on your Hard Drive**
- **Download and install WINZIP 14 or higher on your Windows Machine**
- **The student should have the capability to have Local Administrator Access within the Windows OS**

Mandatory Additional Items:

- **One External USB 2.0 or Firewire Hard Drive ~40GB or higher in size**
- **One USB Thumb Drive (2-4 GB in size)**
- **One new, old, used, or out-of-computer IDE, SATA, or Laptop Hard Disk Drive**
    - **Hard Drive Purchased from EBAY or Craigslist**
    - **Hard Drive from USED PC at home/work**
    - **Local computer show**
    - **Hard Drive from any computer store**

License Verification: Microsoft Windows 7 Home

Print this page and bring with you to class.

We will be handing out a VMware Workstation that contains the proper configuration of tools and setup to perform forensics examinations utilizing the common Windows 7 Home OS.. In order to provide the VMware machine to you we need to verify that you have a license for Microsoft Windows 7 Home. If you do not have one on the first day, you will need to call your technical support to have them provide you a license key or obtain one yourself.

- The key will look like XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

In many cases the license key can be found on the CD or the Computer Windows 7 was installed on. If you need to find the key on an existing copy of Windows 7 Home and you do not have it written down, there is a small freeware utility that retrieves your Product Key (cd key) used to install windows from your registry. It has the options to copy the key to clipboard, save it to a text file, or print it for safekeeping. The program will work on Windows 7.

You can download keyfinder v1.5B3 from:
http://www.magicaljellybean.com/beta/kf15b3.zip
http://www.petri.co.il/software/key_changer_15b3.zip

Please write down the license key for Microsoft Windows 7 Home that you will be utilizing for the class. Keep this with you at the beginning of class.

_____

Please write down the last two 5 character sequences here:

_____-_____

I acknowledge that I or my organizations owns the above key and is fully in compliance with Microsoft Licensing Agreements for Windows 7 Home found here:
http://www.microsoft.com/about/legal/useterms/default.aspx

SIGNED: _____

ORGANIZATION: _____

DATE: _____

If your BASE OPERATING SYSTEM is Windows:

WINDOWS VMWARE INSTALLATION

Go to http://www.vmware.com and register to download the latest version of VMware Workstation or Player to run under Windows. You can obtain a free 30 day license if you already do not own a copy of VMware. Download the latest **VMware Workstation 6.0 or VMware Player 2.5 or higher** and place it in your "My Documents" directory. Do not download any BETA versions of VMware products for this class they will be incompatible with the course. Do not download any earlier versions of VMware as the VMware guest machines we distribute for the course are only compatible with the versions we highlighted above or higher. Use the following guide to help you perform the installation

http://www.vmware.com/support/ws55/doc/ws_install_winhost.html

Please make sure that your VMware environment is stable as there will be no time to install or troubleshoot the Windows VMware machine during class. Remember to install VMware tools on your system. VMware support site is located on the web

http://www.vmware.com/support/pubs/ws_pubs.html.

By bringing the right equipment and preparing in advance, you can maximize what you'll see and learn, as well as have a lot of fun.

If your BASE OPERATING SYSTEM is LINUX

LINUX VMWARE INSTALLATION

You can use any version of Linux you can install VMware Workstation 6.0 or VMware Player 2.5 or higher and it is functional. SANS will be handing out multiple VMware Machines that will be utilized for the course.

Go to http://www.vmware.com and register to download the latest version of VMware to run under Linux. You can obtain a free 30 day license if you already do not own a copy of VMware. Download the latest **VMware Workstation 6.0/VMware Player 2.5** or higher rpms and place it in your /usr/local/src directory. Do not download any BETA versions of VMware for this class they will be incompatible with the course. Do not download any earlier versions of VMware as the VMware guest machines we distribute for the course are only compatible with VMware Workstation 6.0/VMware Player 2.5 or higher.

From your command line run the following after your VMware rpm is downloaded to the /usr/local/src directory.

```
#rpm -ivh VMware-workstation-6.0-45731.i386.rpm (or later
version)
```

Ensure eth0 is currently not turned on.

```
#ifdown eth0
```

Wait until installation is complete and run the VMware Configuration Tool.

```
#vmware-config.pl
```

Executed the following command and answer the following questions prompted to you with the response in **BOLD. (*press return*)** means press the return key without typing any value.

```
Do you accept? (yes/no) yes

Thank you.

Configuring fallback GTK+ 2.4 libraries.

What directory contains your desktop menu entry files?  These files
have a .desktop file extension.

[/usr/share/applications] [press return]
```

In which directory do you want to install the mime type icons?

[/usr/share/icons] ***[press return]***

In which directory do you want to install the application's icon?

[/usr/share/pixmaps] ***[press return]***

Trying to find a suitable vmmon module for your running kernel.

None of pre-built vmmon modules for VMware Workstation is suitable for your running kernel. Do you want this program to try to build the vmmon module for your system (you need to have a C compiler installed on your system)? [yes] ***yes***

Using compiler "/usr/bin/gcc". Use environment variable CC to override.

What is the location of the directory of C header files that match your running kernel? [/lib/modules/your_kernel_version/build/include] ***[press return]***

Do you want networking for your virtual machines? (yes/no/help) [yes] ***yes***

Optional Question if you have more than one Ethernet adapter: Your computer has multiple Ethernet network interfaces available: eth0, eth1. Which one do you want to bridge to vmnet0 [eth0] ***[press return]***

Optional Question if you have more than one Ethernet adapter: Do you wish to configure another bridged network (yes/no) ***[press return]***

Configuring a bridged network for vmnet0.

Do you want to be able to use NAT networking in your virtual machine? [yes] ***no***

Do you want to be able to use host-only networking in your virtual machines? [no] ***yes***

Do you want this program to probe for an unused private subnet?

Do you wish to configure another host-only network? (yes/no) [no] ***no***

Do you want this program to automatically configure your system to allow your virtual machines to access the host's filesystem? (yes/no/help) [no] ***no***

Do you want to install the Eclipse Integrated Virtual Debugger [no] ***no***

Do you accept? (yes/no) ***yes***

[press return] for all VMware VIX API questions

```
# vmware &
```

If your BASE OPERATING SYSTEM is MAC OSX

VMWARE FUSION 2.0 INSTALLATION

You can use any version of Intel Based MAC OSX you can install VMware Fusion 2.0 on and it is functional. No beta versions are supported. SANS will be handing out multiple VMware Machines that will be utilized for the course.

Go to http://www.vmware.com/products/fusion/ and register to download the latest version of VMware Fusion to run under MACOSX. You can obtain a free 30 day license if you already do not own a copy of VMware Fusion. Download the latest **VMware Fusion 2.0** or higher dmg.

Do not download any BETA versions of VMware Fusion for this class they will be incompatible with the course.

WIN7 SIFT Workstation and VPN Configuration Guide

SANS teaches the latest tools and techniques available. In addition, our aim is also to create a laptop setup that is simple to use to accomplish the daily exercises utilizing forensic tools. To solve both challenges, the SANS Institute has released a cutting edge course DVD that includes a new preconfigured **VMware WIN7-Based SIFT Workstation** that is ready to tackle forensics right off the DVD. This will allow for you to have either a Windows or a Linux base installation. **The only requirement for you to have followed is that VMware is installed and working correctly following the forensic installation guide.**

This guide will be followed on Day 1 of the course. You will need the course DVD before you begin.

If you run into any challenges, please email virtual-labs-support@sans.org

Contents

Laptop Requirements 2

Installing the WIN7 SIFT Workstation VMware Machine. 3

Setting up the Forensics408 VPN Connection -> FTK/Encase License Server 16

Laptop Requirements

Mandatory License Requirements:

- Very Important: Student must bring a Retail Microsoft Windows WIN7 Home Premium License Key with them to class at the beginning of the first day
- The key will look like XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
- Corporate, Site, and Group Licenses are not acceptable as they fail the Windows Genuine Advantage Test.

Mandatory Laptop Hardware Requirements:

- CPU: 2.0 GHz or higher is recommended (Multi Core Preferred)
- DVD/CD Combo Drive
- Wireless 802.11 B/G Networking Capability
- 2 Gigabyte of RAM minimum (3GB or higher RAM is recommended)
- 60 Gigabyte Hard Drive minimum (HARD DRIVE SIZE IS CRITICAL)
- 40 Gigabytes of Free Space on your Hard Drive
- Download and install WINZIP or 7Zip on your Host Machine

Mandatory Additional Items:

- One External USB 2.0 or Firewire Hard Drive
    - Free Space should be slightly larger than the used Hard Disk Drive
- One USB Thumb Drive (2-4 GB in size)
- One old, used, or out-of-computer IDE, SATA, or Laptop Hard Disk Drive from:
    - Hard Drive Purchased from EBAY or Craigslist
    - Hard Drive from USED PC at home/work
    - Local computer show
    - Hard Drive from any computer store

Installing the WIN7 SIFT Workstation VMware Machine.

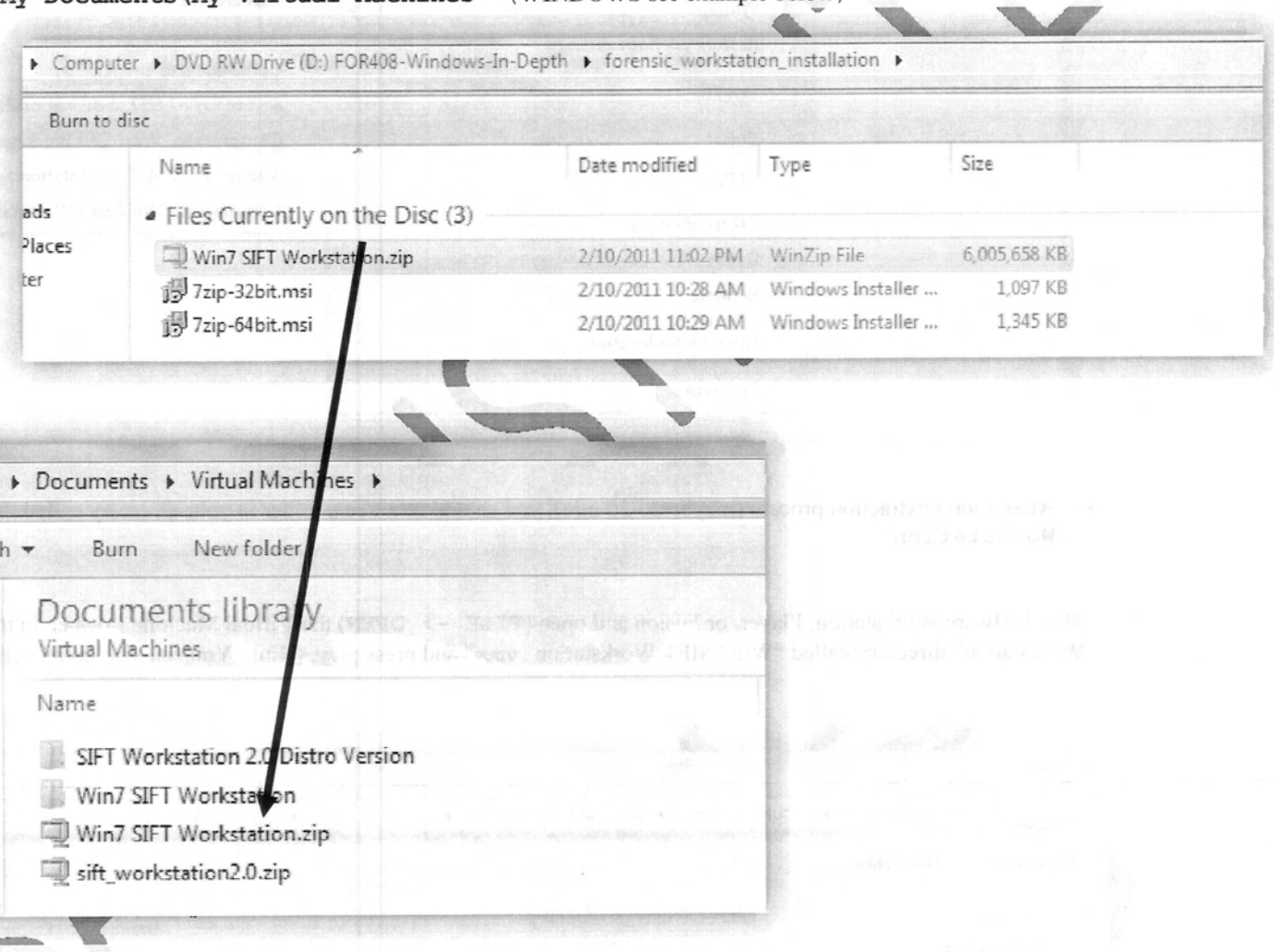
1. Insert the DVD into your laptop. You will receive the DVD by the first day of the course if you do not have it now. Please wait until you receive the FOR408 Course DVD before configuring your system.

2. On the DVD (FOR408-Windows-In-Depth), browse to the directory

   - **`\forensic_workstation_installation`**

3. Copy/Drag the **"Win7 SIFT Workstation.zip"** file to a local Directory of your choice.

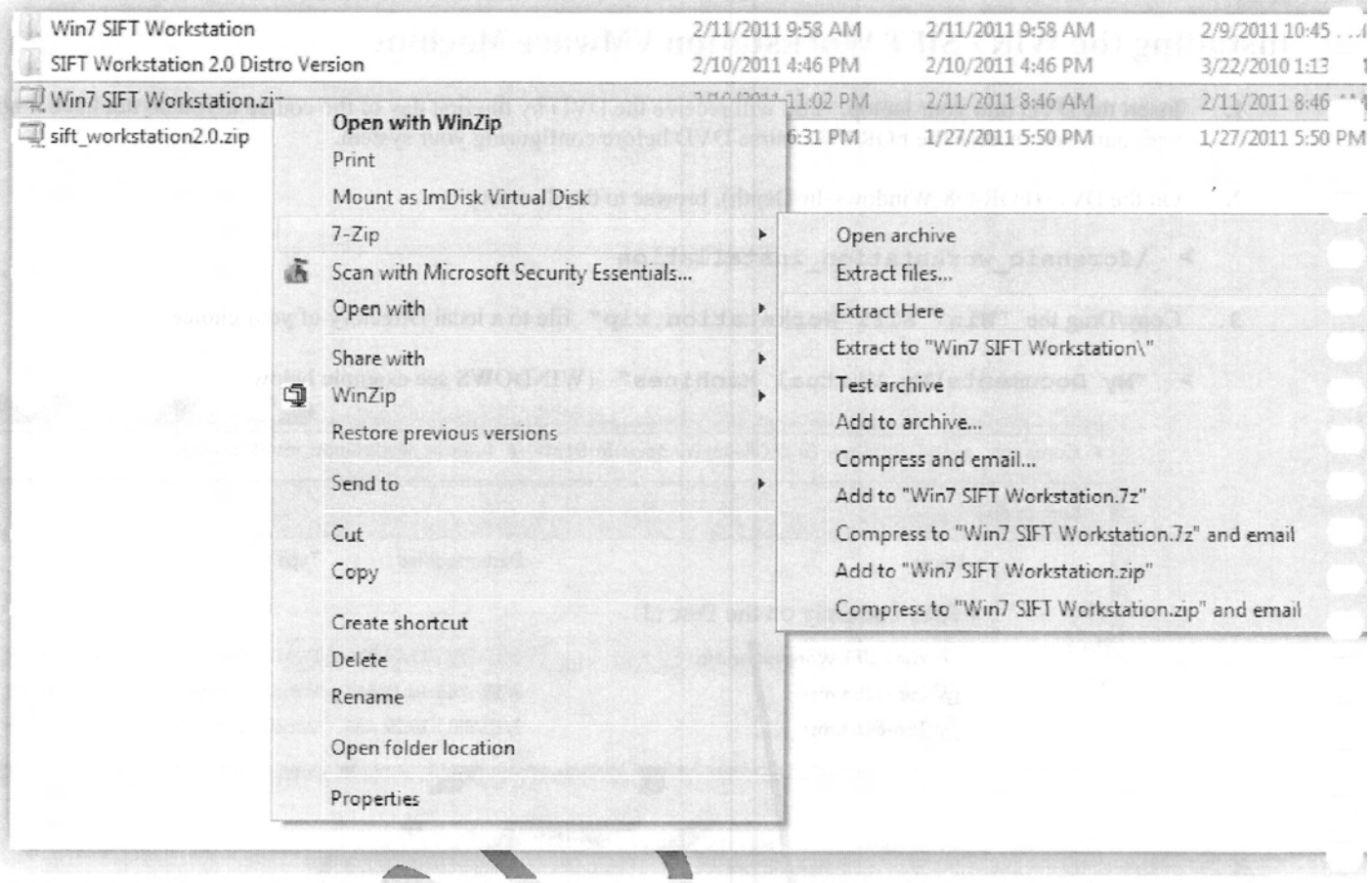
   - **"My Documents\My Virtual Machines"** (WINDOWS see example below)



4. Unzip **"Win7 SIFT Workstation.zip"** file in that directory

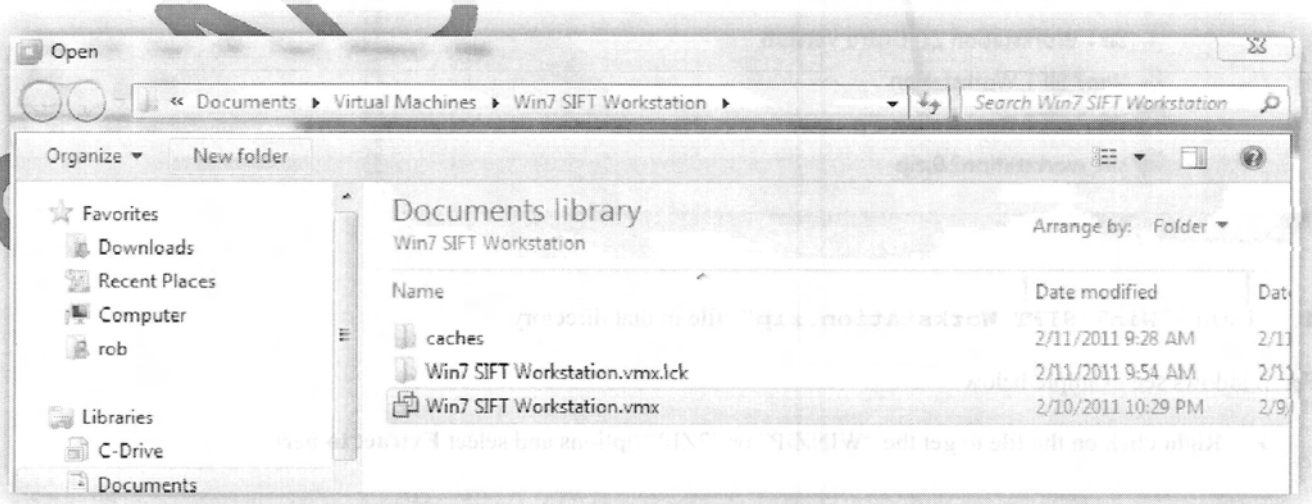
For Windows see example below

- Right click on the file to get the "WINZIP" or "7ZIP" options and select **Extract to here**.



- After a long extraction process (maybe 20-30 min), you should now see a folder in your directory called "**`Win7 SIFT Workstation`**"

5. Start VMware Workstation, Player, or Fusion and open (**`FILE -> OPEN`**) the Virtual Machine Located in the "Win7 SIFT Workstation" directory called "Win7 SIFT Workstation **`.vmx`**" and press play. (Hint: You can also double click on it)



6. Tweak the settings of your VMware configuration to allow for more memory and processor power as your system will allow. Note: Do not ever increase it beyond the maximum recommended settings

a. Upgrade your virtual machine if you can -> VM -> Upgrade or Change Version (Follow Wizard)

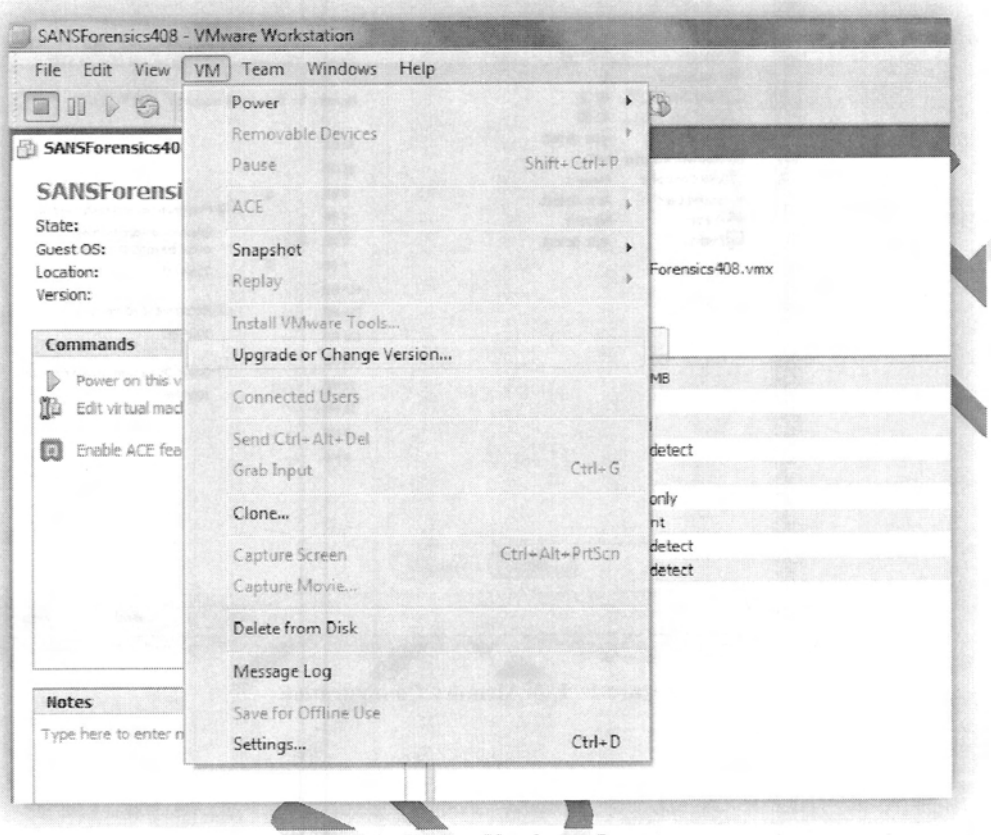


Figure 1 - Update Version to Latest

b. Adjust Memory -> Select "Edit Virtual Machine Settings" -> Select Memory
NOTE: Do not give your VM more than ½ your machines memory. If your machine slows down as a result, reduce the amount of memory allocated to the VM.

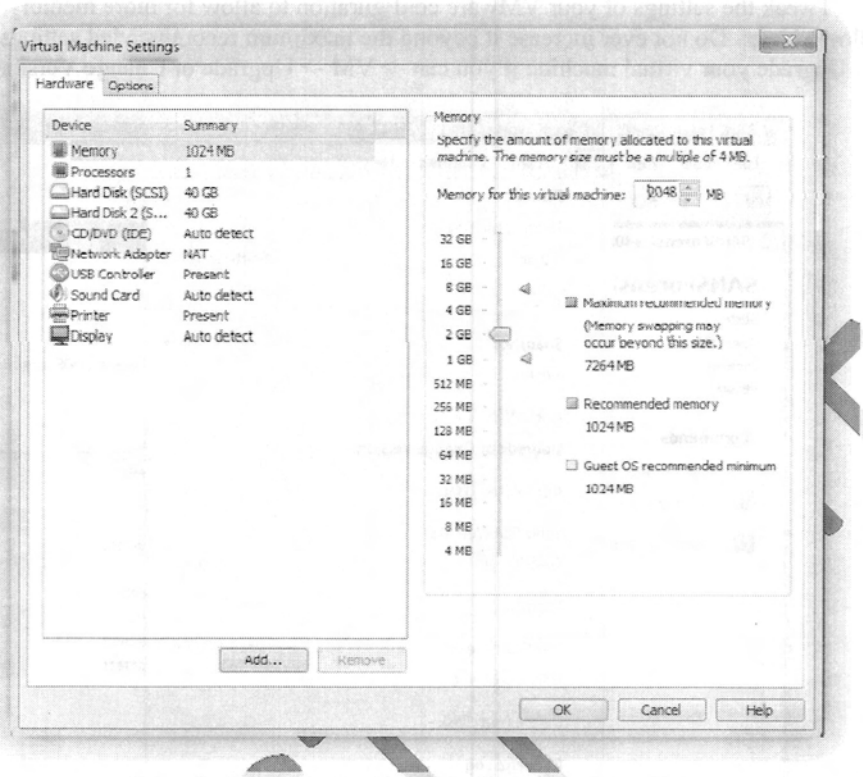
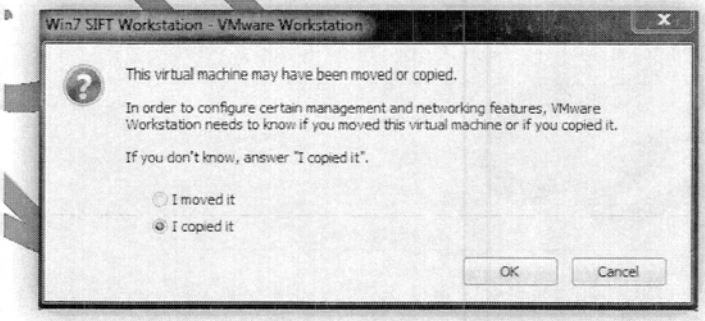
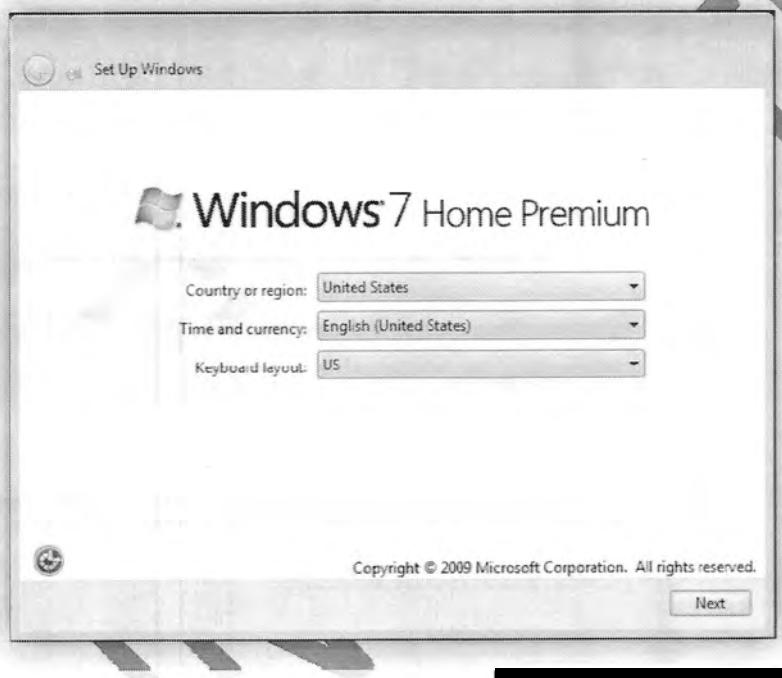


Figure 2 - Edit Memory Configuration

7. Power On Your Virtual Machine
   a. Press "Power on virtual machine" and select "I copied it"

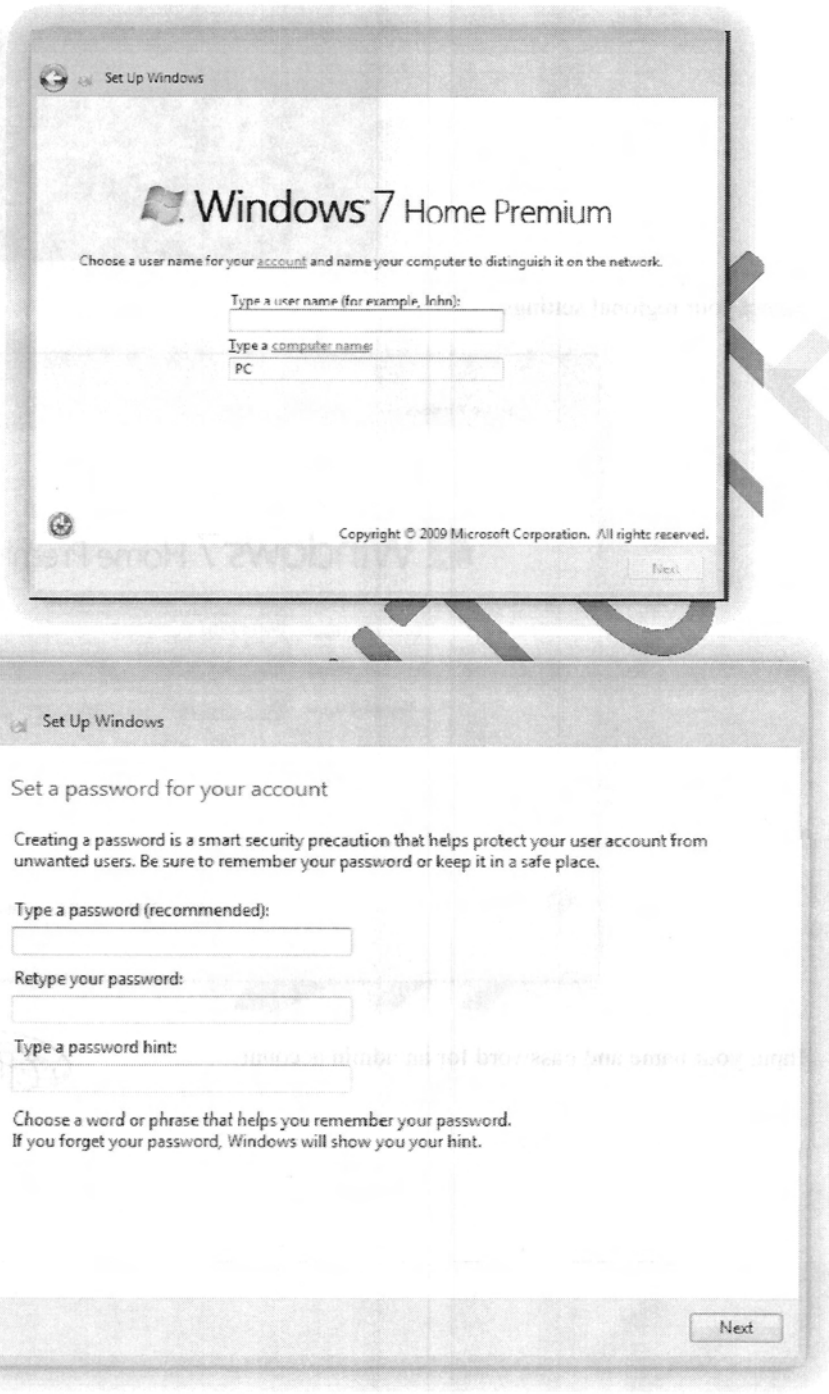


b. Select your regional settings



c. Input your name and password for an admin account

[redacted]



8. Input your Retail WIN7 Home Premium License Key
   a. Need to obtain/purchase a retail Windows WIN7 Key

   b. Note Windows Volume/Sit/Group Licensing tend not to work. You will need to contact Microsoft if that is your only copy of windows. Course requirements clearly stated that you needed a retail copy of WIN7 and that volume licensing would not work.
      i. http://www.sans.org/security-training/forensic_install_408.pdf
      ii. http://computer-forensics.sans.org/course/laptop.php?mid=1207
      iii. http://www.sans.org/security-training/laptop.php?tid=4207

c. Input your license key. If you end up having trouble with your retail key please chat with or email your instructor/mentor and we can see if we can set up a work-around.

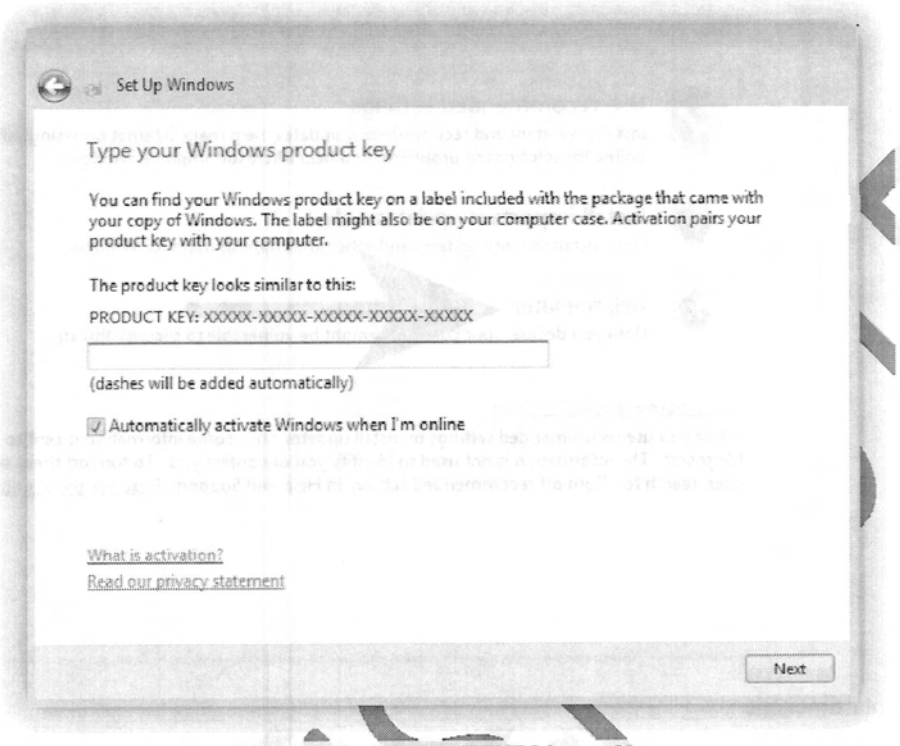
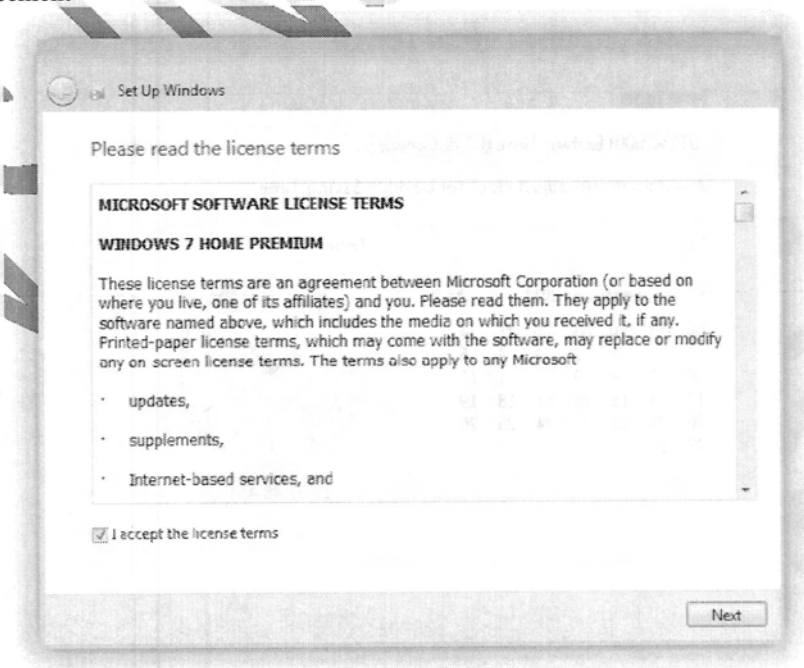
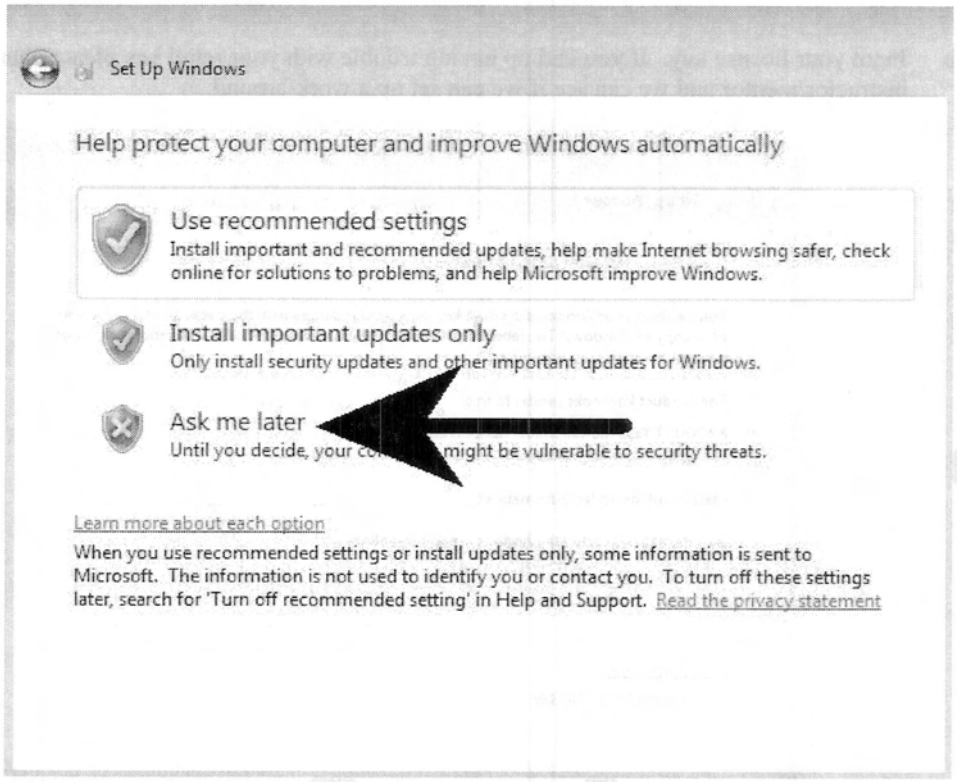


Figure 3 - Insert your WIN7 License Key

d. Accept License Agreement



e. Turn on updates? Select "Ask me later" Why? If every student in class selects to update, the network bandwidth will be reduced greatly. Update your systems back in your own rooms later by turning this back on. But initially, it is best to leave it off.



f. Select your timezone

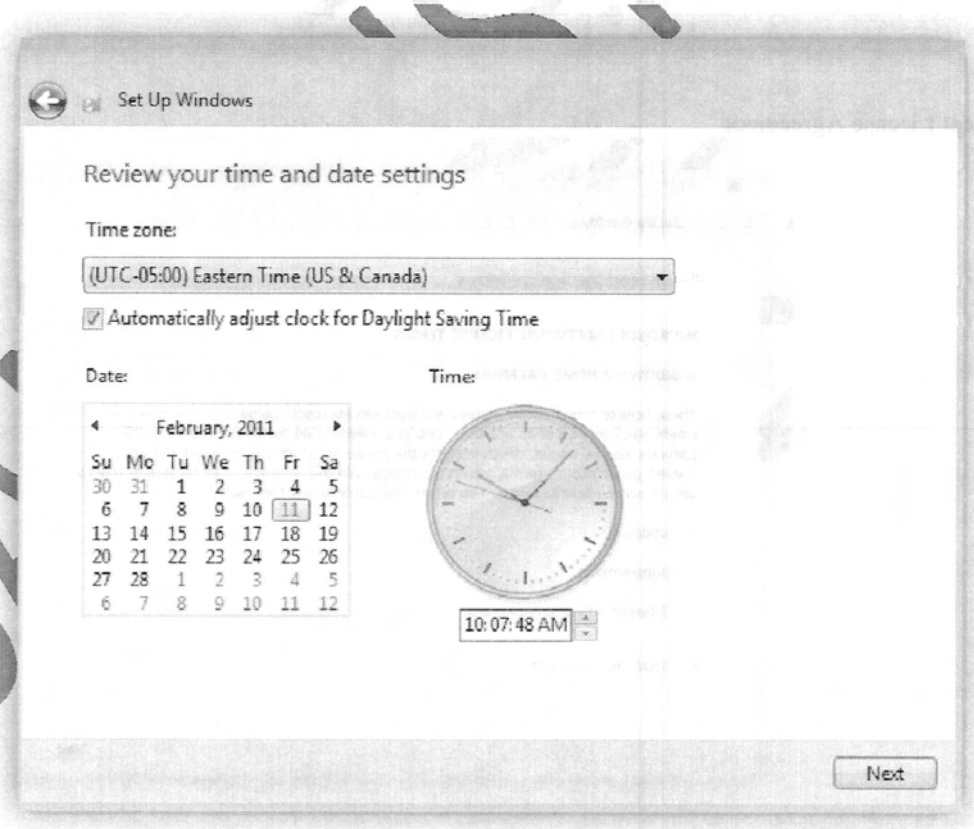


Figure 4 - Choose Time Zone

g. Select Public Network

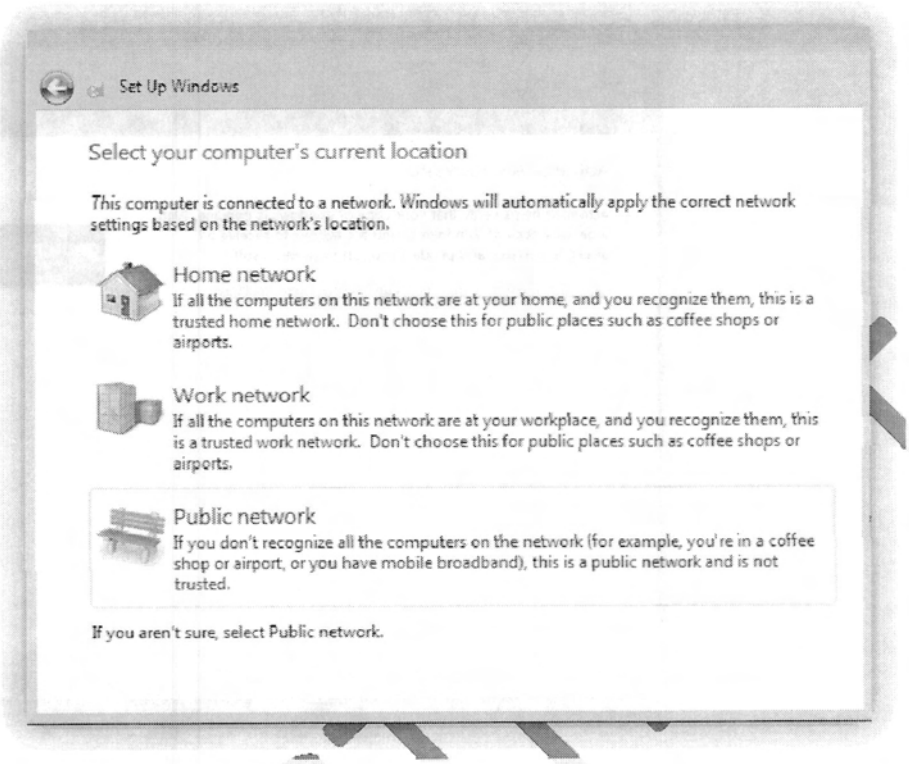
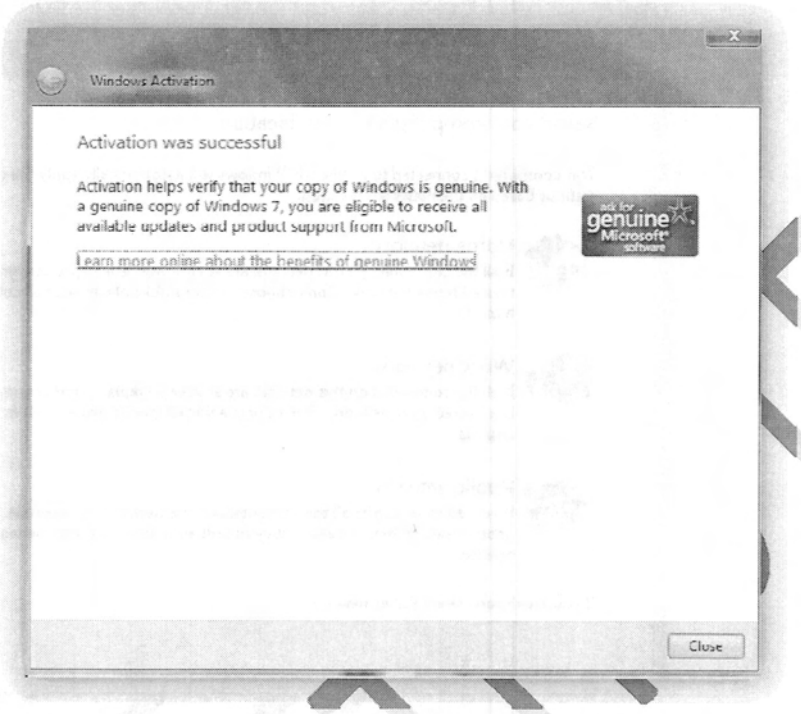


Figure 5 - Choose Public Network

h. The Workstation will now reboot

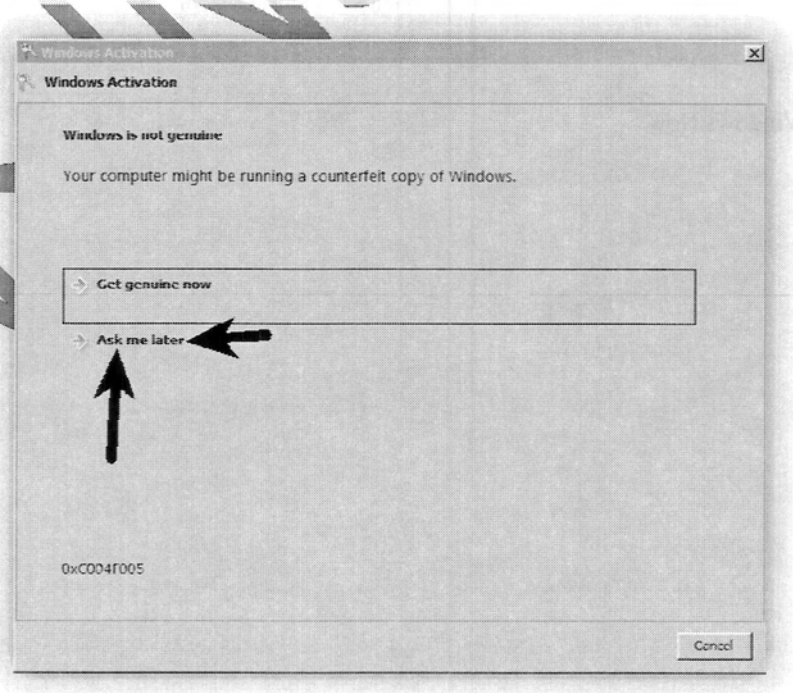
Figure 6 - Select Finish

9. Activate Windows Now

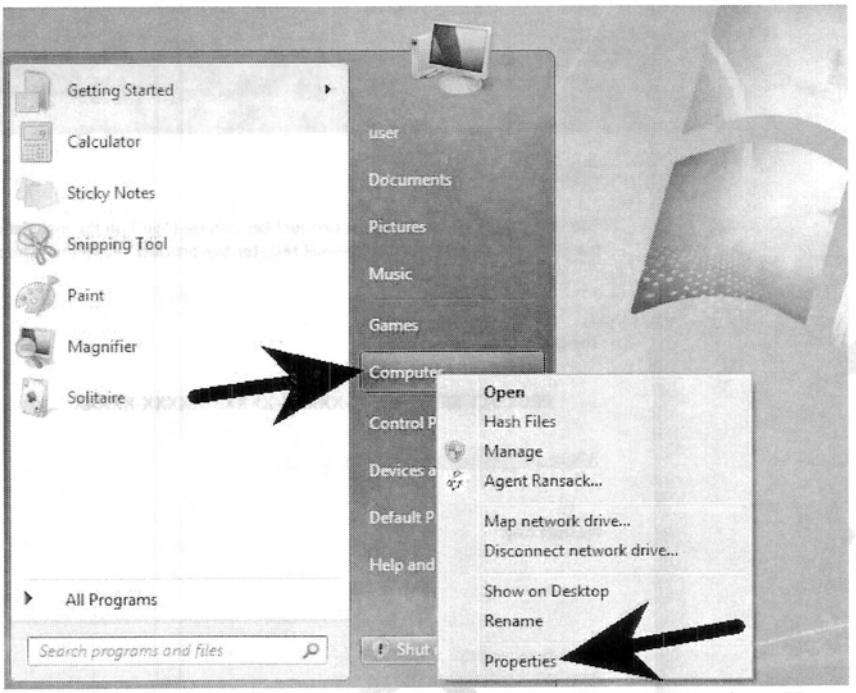


a. TROUBLESHOOTING ONLY: If your copy of windows activated, please go to step 10.

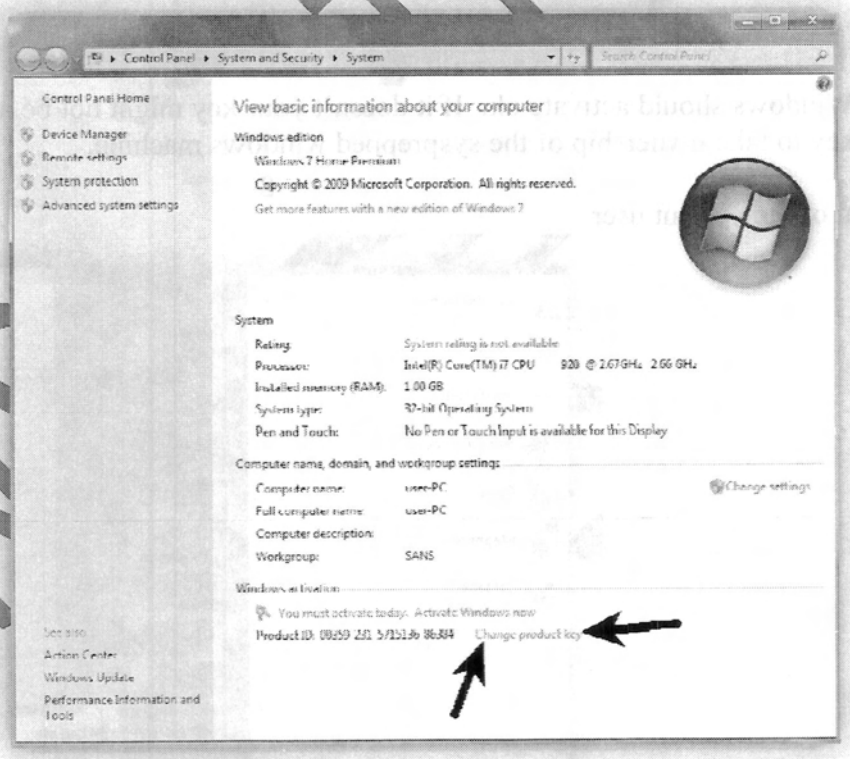
b. Didn't activate on ok? No worries!!! If windows does not activate properly the first time, then it will attempt to try and "Get Genuine now". Do **NOT** select "Get Genuine now." **Select "Ask me later"** and wait for the system to log in.



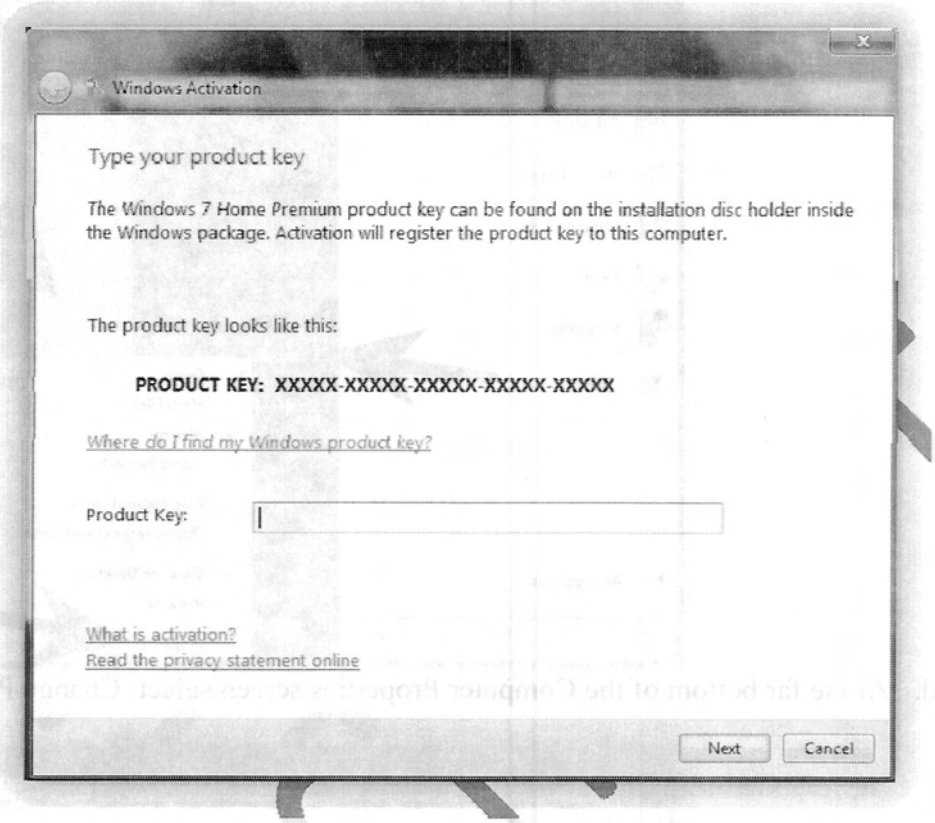
c. RIGHT Click on "COMPUTER" and select PROPERTIES



d. At the far bottom of the Computer Properties screen select: Change Product Key



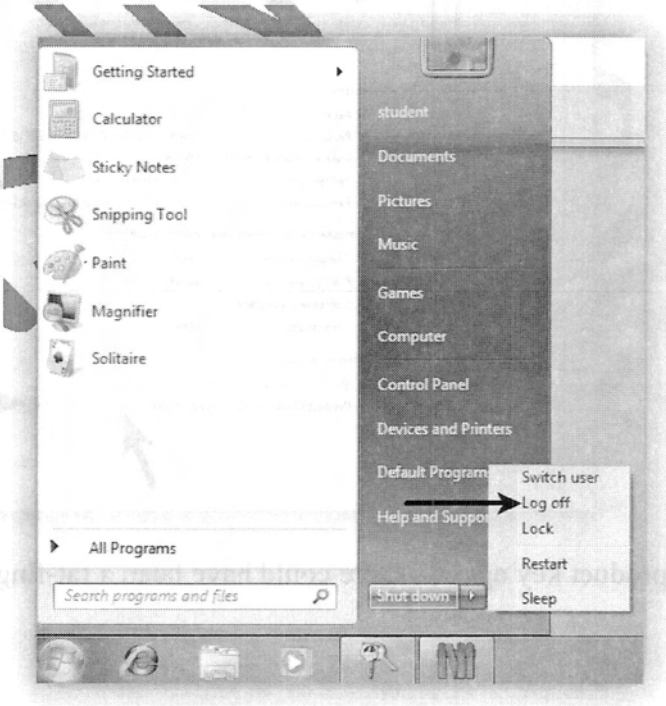
e. Input your product key again. There could have been a fat-finger the first time



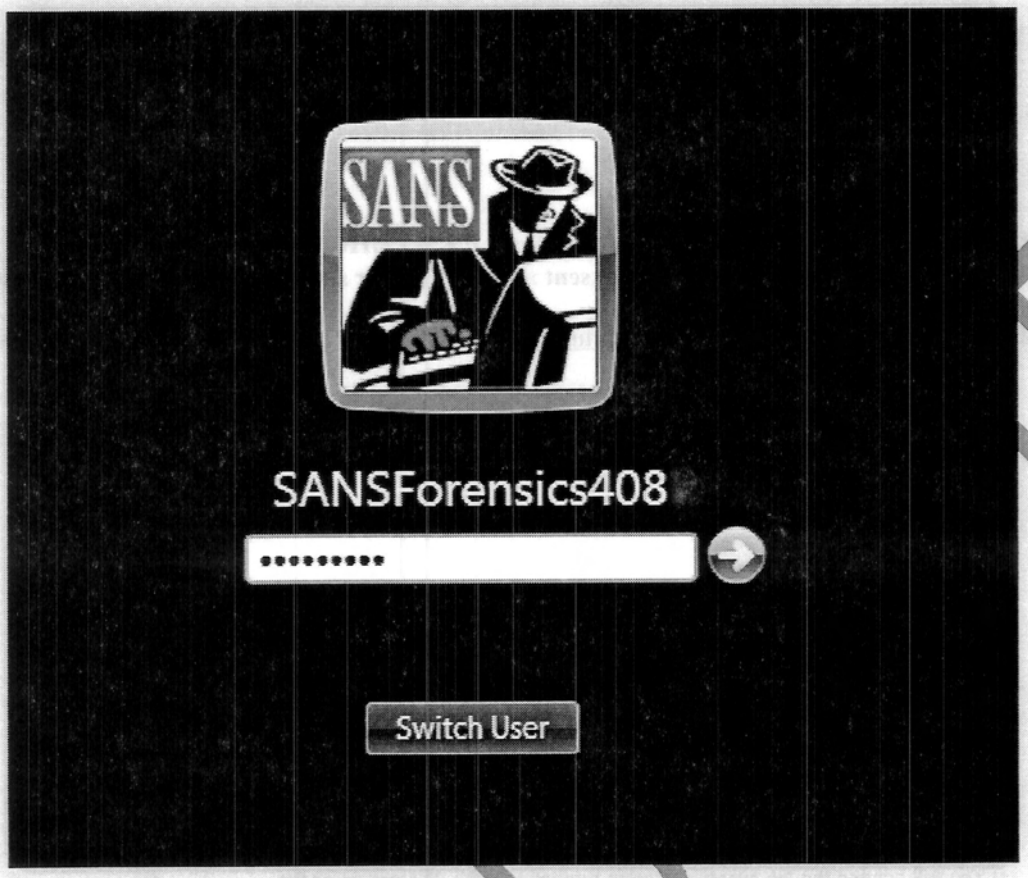
f. Windows should activate ok. If it doesn't your key might not be a retail key. Please try another key to take ownership of the sysprepped windows machine.

g.

10. Log out of the current user

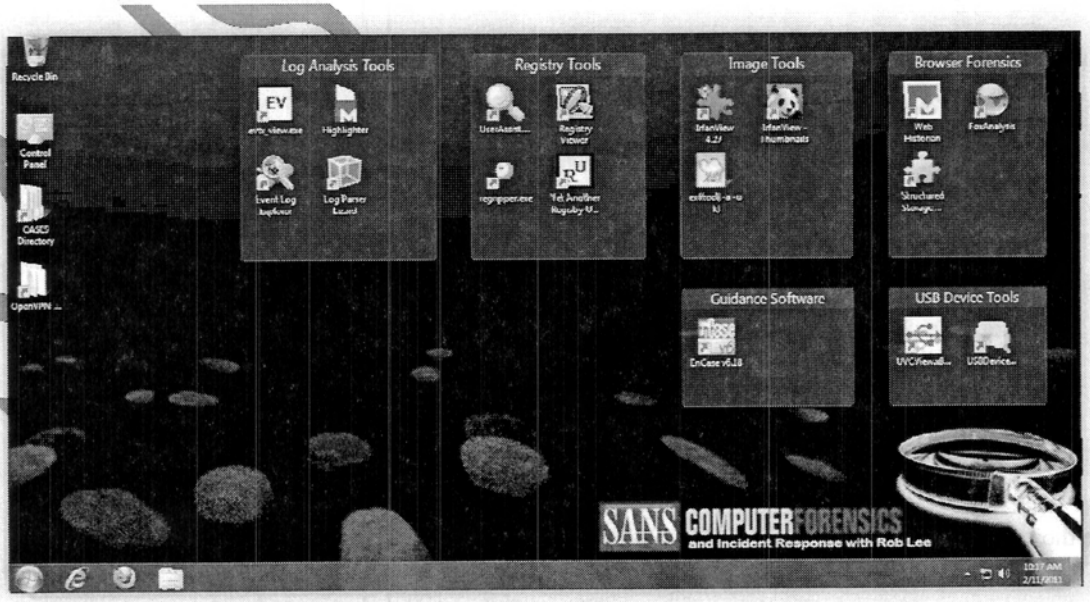


11. Log in as SANSForensics408 using the password "forensics"



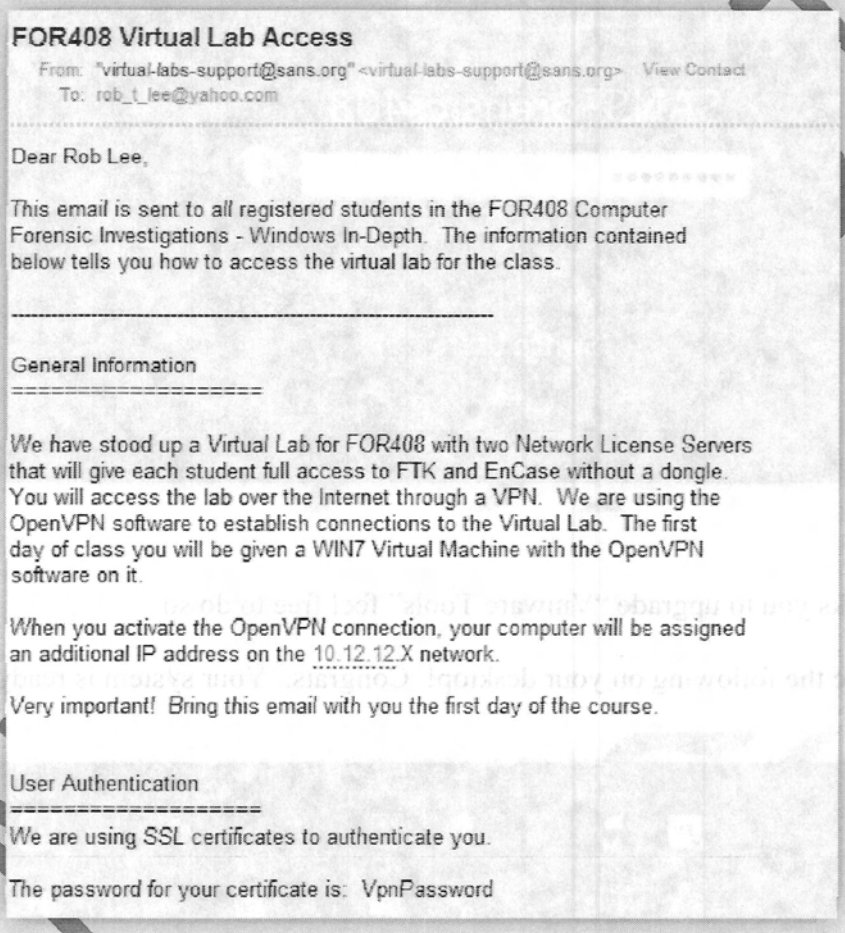
12. If Vmware Asks you to upgrade "Vmware Tools" feel free to do so.

13. You should see the following on your desktop! Congrats. Your system is ready for class.



Setting up the Forensics408 VPN Connection -> FTK/Encase License Server

1. Locate an email from virtual-labs-support@sans.org **sent about 1 week or several days prior to the course**
   a. Subject: **408 Virtual Lab Access**
   b. If you did not receive an email, please email virtual-labs-support@sans.org requesting 408 Virtual Lab Access



FOR408 Virtual Lab Access

From: "virtual-labs-support@sans.org" <virtual-labs-support@sans.org> View Contact
To: rob_t_lee@yahoo.com

Dear Rob Lee,

This email is sent to all registered students in the FOR408 Computer Forensic Investigations - Windows In-Depth. The information contained below tells you how to access the virtual lab for the class.

General Information
==========

We have stood up a Virtual Lab for FOR408 with two Network License Servers that will give each student full access to FTK and EnCase without a dongle. You will access the lab over the Internet through a VPN. We are using the OpenVPN software to establish connections to the Virtual Lab. The first day of class you will be given a WIN7 Virtual Machine with the OpenVPN software on it.

When you activate the OpenVPN connection, your computer will be assigned an additional IP address on the 10.12.12.X network.

Very important! Bring this email with you the first day of the course.

User Authentication
==========
We are using SSL certificates to authenticate you.

The password for your certificate is: VpnPassword

Figure 7 - Virtual Lab Access Email

   c. NOTE: If you did not receive an email at all or do not have a copy of the email in your inbox, please send an email to virtual-labs-support@sans.org. Please include:
      i. full name
      ii. registered SANS portal email address
      iii. date of the class
      iv. class type (conference, vlive, ondemand)
      v. class location. Ask to have them resend the email to you.

2. Locate the User Authentication portion of the email

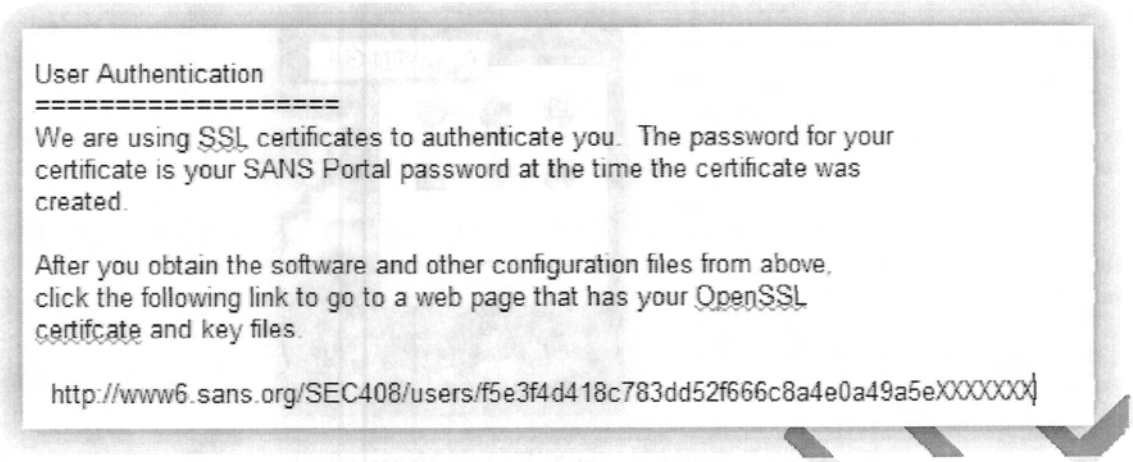


Figure 8 - Locate User Authentication Link in Virtual Lab Access Email

3. Inside your Forensics408 SIFT Workstation -> Open FIREFOX Only and paste the link from your email in the URL bar

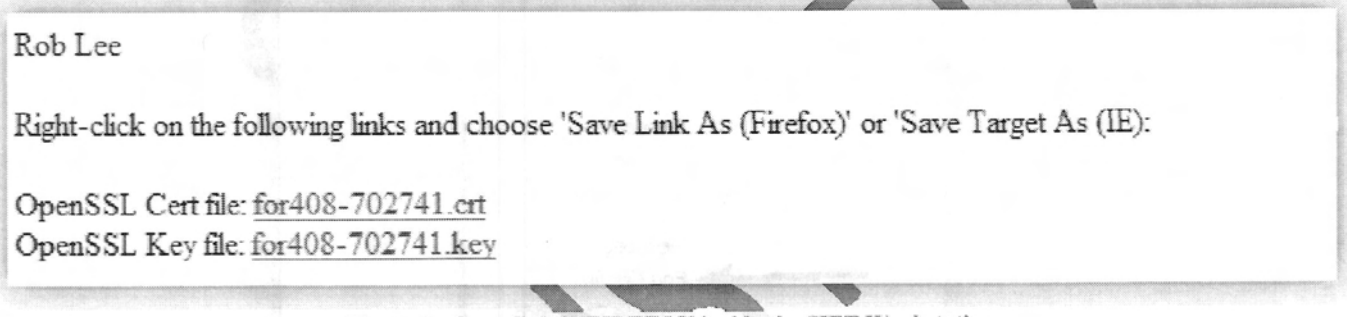


Figure 9 - Open link in FIREFOX inside the SIFT Workstation

4. Save both files to **`C:\Program Files\OpenVPN\config`**

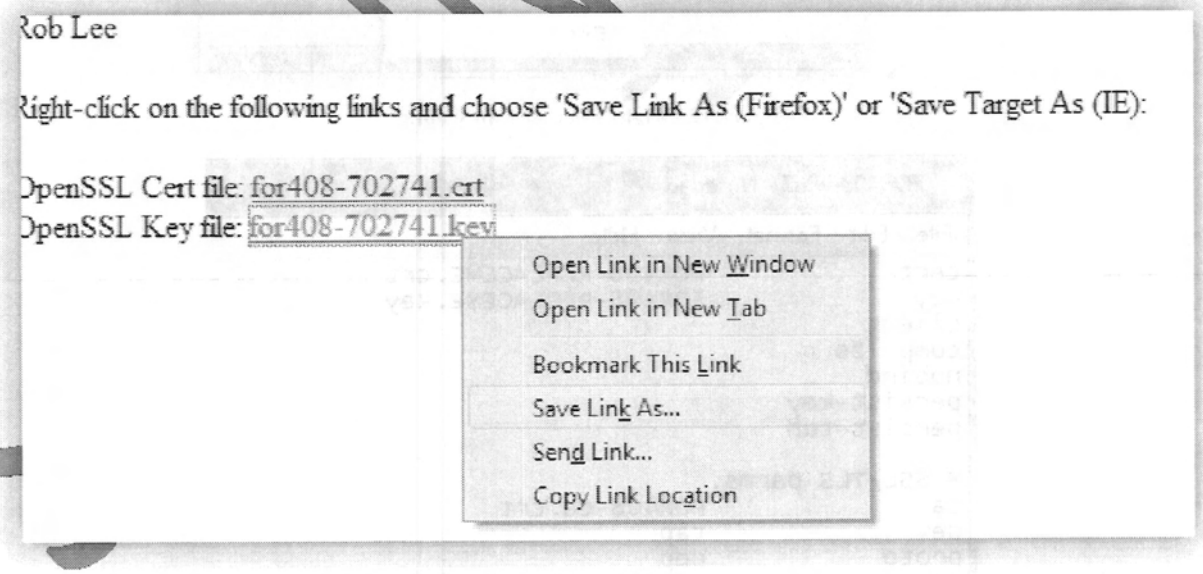


Figure 10 - Save .CRT and .KEY files to C:\Program Files\OpenVPN\Config Directory

5. Ensure that the extensions of the files did not change when you saved them. IE has a habit of changing the crt file to a cer file.
6. In the lower right hand corner you will find a OpenVPN Gui Taskbar Tool -> Right Click on it and select "Edit Config"

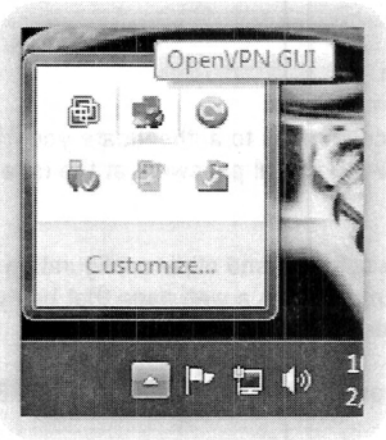


Figure 11 - OpenVPN Task Manager Tool

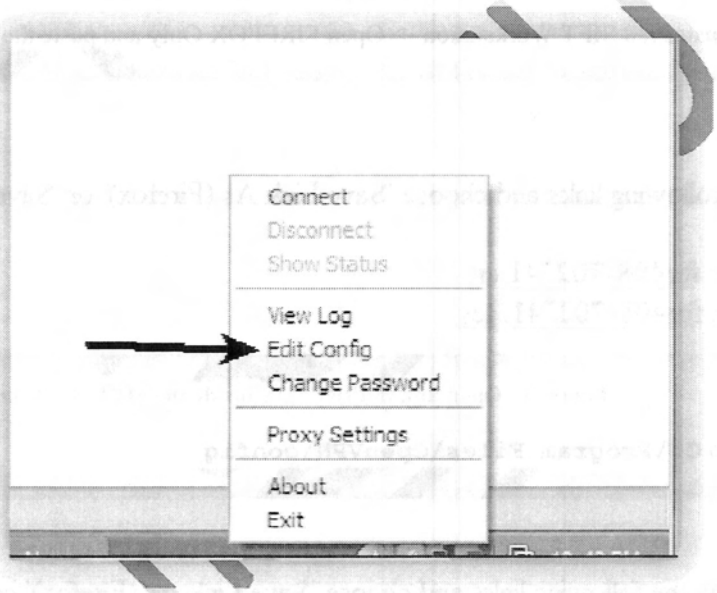


Figure 12 - Right Click -> Edit Config

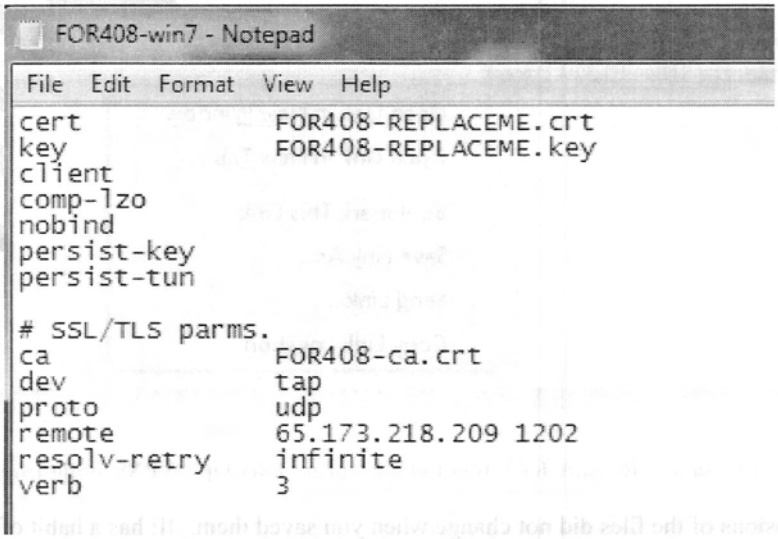


Figure 13 - Editing OpenVPN Config File

7. Change the REPLACE_ME locations with filenames that came with your two files.

Rob Lee

Right-click on the following links and choose 'Save Link As (Firefox)' or 'Save Target As (IE):

OpenSSL Cert file: for408-702741.crt
OpenSSL Key file: for408-702741.key

FOR408-win7 - Notepad

File Edit Format View Help

```
cert                FOR408-702741.crt
key                 FOR408-REPLACEME.key
client
comp-lzo
nobind
persist-key
persist-tun

# SSL/TLS parms.
ca                  FOR408-ca.crt
dev                 tap
proto               udp
remote              65.173.218.209 1202
resolv-retry        infinite
verb                3
```

Figure 14 - Replacing REPLACE_ME with filenames you saved into C:\Program Files\OpenVPN\config Directory

OpenSSL Cert file: for408-702741.crt
OpenSSL Key file: for408-702741.key

FOR408-win7 - Notepad

File Edit Format View Help

```
cert                FOR408-702741.crt
key                 FOR408-702741|.key
client
comp-lzo
nobind
```

Figure 15 - Replacing both file names

8. Save the config file

9. Launch the VPN by Right Clicking the OpenVpn Taskbar Tool and "Connect"

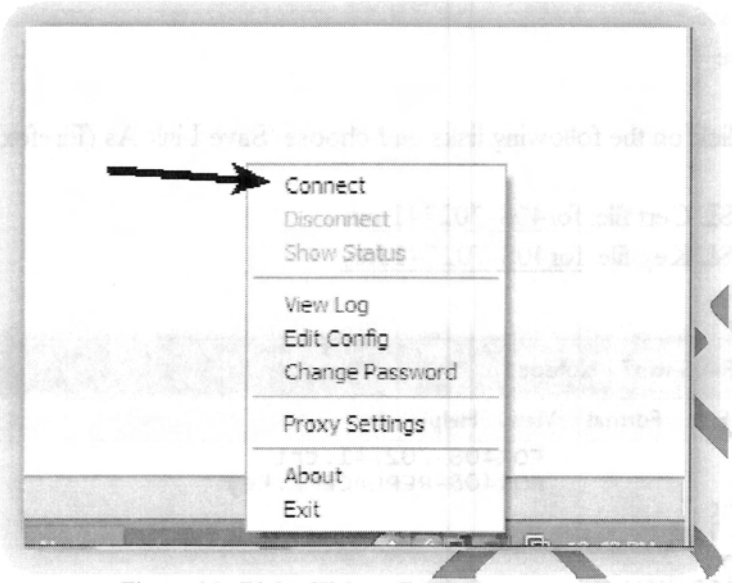


Figure 16 - Right-Click -> Connect

10. Login to the VPN using the password "VpnPassword" (Your VPN Certs are pre-configured with it)
11.

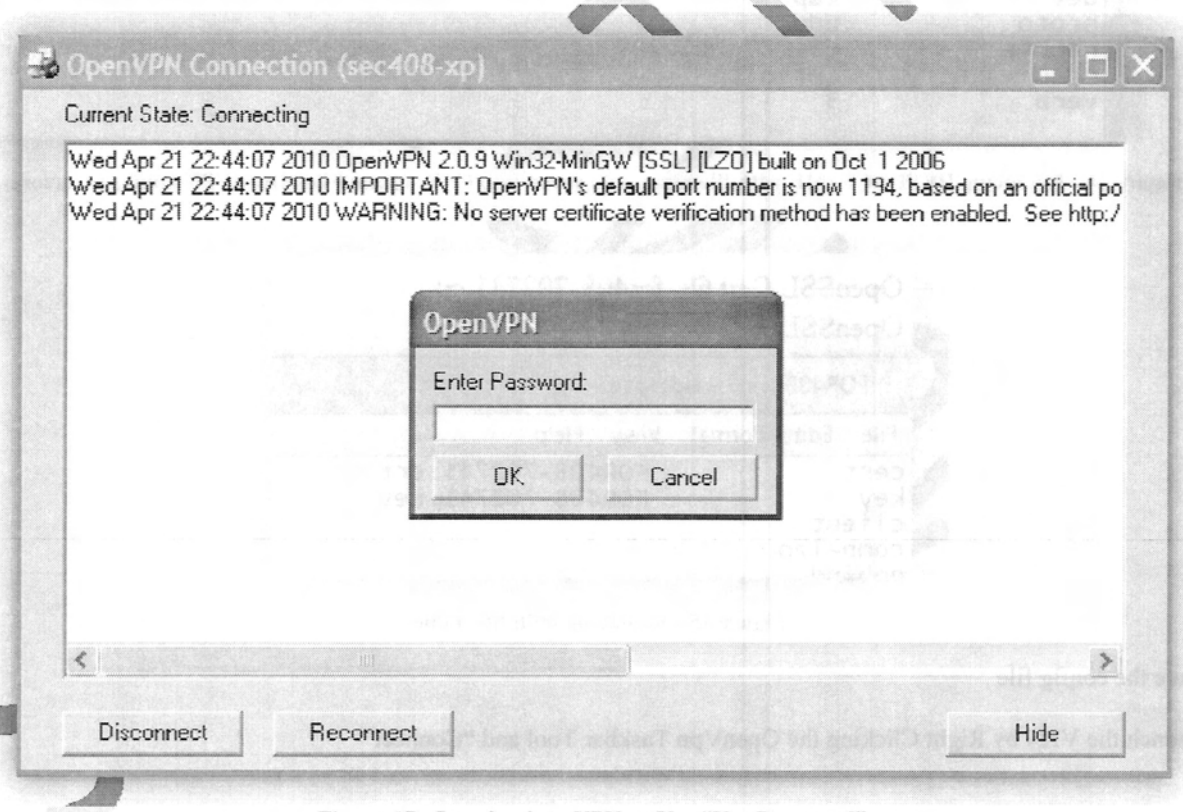


Figure 17 - Logging into VPN -> Use "VpnPassword"

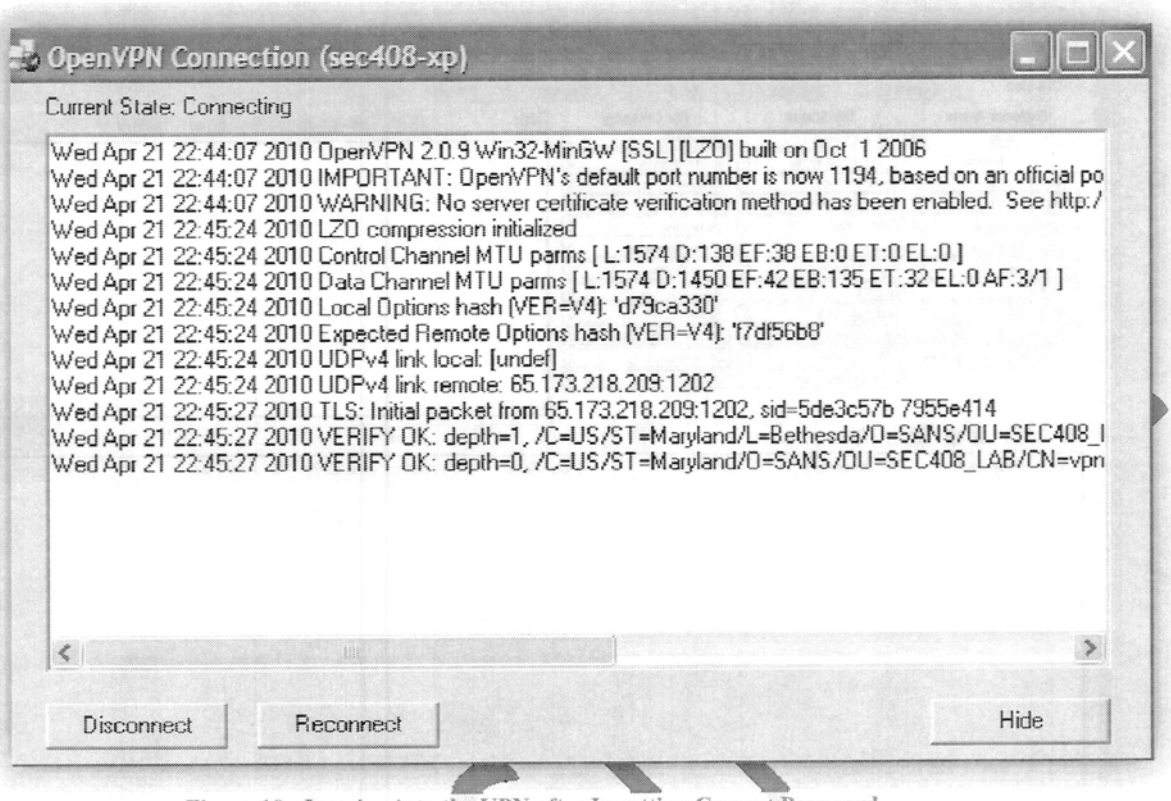


Figure 18 - Logging into the VPN after Inputting Correct Password

12. Once you are logged in, the OpenVPN Connection Windows Will Automatically Disappear

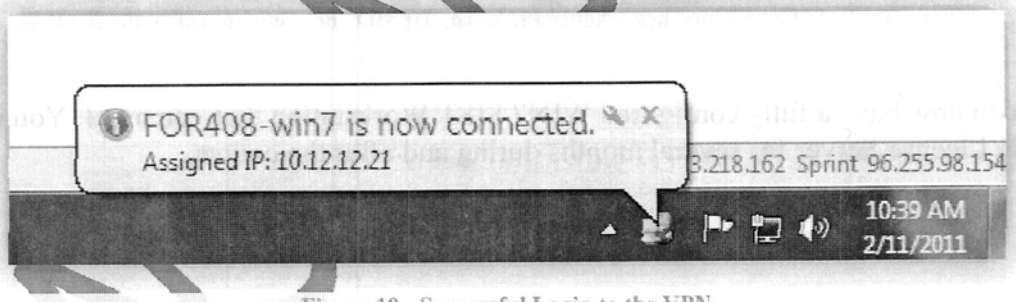


Figure 19 - Successful Login to the VPN

13. Launch Access Data's FTK or Guidance Software's EnCase – The Program should NOT be in Demo mode. This means you have successfully leased a license.
    a. Note you must stay connected to the VPN use the programs
    b. If you successfully connect to the VPN and are not able to launch the program correctly outside of DEMO mode, please email virtual-labs-support@sans.org your problem and asking them to reboot the 408 License Server

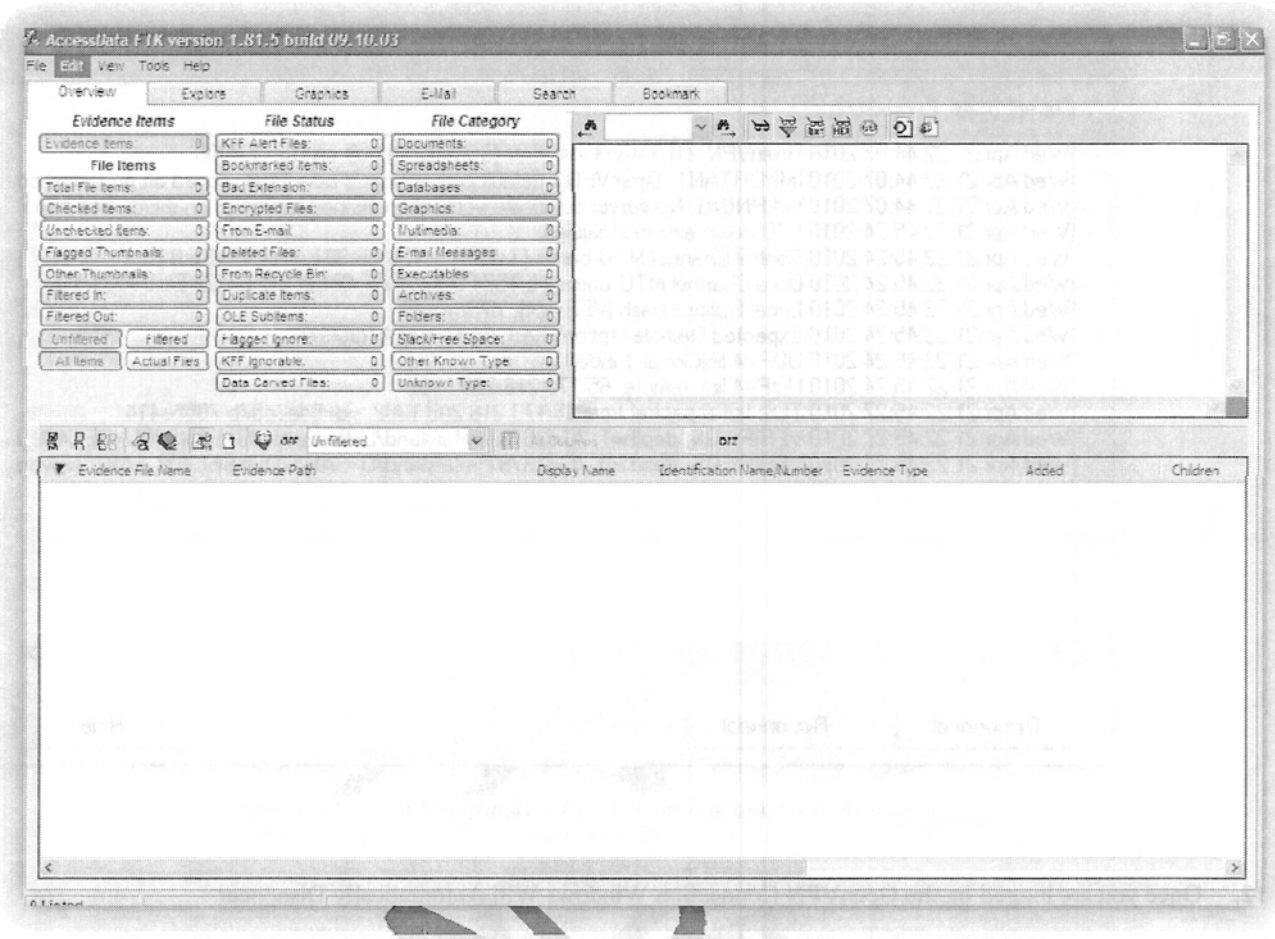


Figure 20 - FTK 1.81.5 Launched - Notice the word "DEMO" does not appear in the top bar

CONGRATS! You now have a fully configured WIN7 SIFT Workstation that you own! You should have access to the FTK License Server for several months during and after the course.

Support

If you are having problems installing or activating the OpenVPN software or if you think one of the target systems is not functioning correctly, you can email virtual-labs-support@sans.org. Please specify with class you are writing in about and whether you are taking it via Mentor, OnDemand, or SANS@Home.

ABOUT SANS

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

IN-DEPTH EDUCATION AND CERTIFICATION

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

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

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

Global Information Assurance Certification (GIAC)

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

SANS BREAKS THE NEWS

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

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

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

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

TRAINING WITHOUT TRAVEL ALTERNATIVES

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

SANS OnSite *Your Location – Your Schedule*

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

Six reasons to consider SANS OnSite:

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

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

SANS Simulcast now available for OnSite classes

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

SANS OnDemand *Online Security Training & Assessments*

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

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

www.sans.org/ondemand

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

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

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

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