SECTION 2 - OVERVIEW OF THE FORENSICS PROCESS

2.1. DESCRIPTION

Your main goals in this section are to get an overview of the actual work you will do in a forensics investigation. You will learn what forensics is (are?), some of the main steps you will take in a Forensics Investigation, and the documentation and reporting requirements. You'll also get an overview of the different software tools and suites used by forensics investigators.

You will then learn about the various types of crimes you'll be investigating and how they may affect the forensics investigation. For example was the computer used to commit a crime, or are you looking to see if the computer was attacked. If the computer was used to commit a crime, say ID theft, you'll look for files like fake social security numbers. But if the computer was attacked you'll do things like check logs to try and find where the attack came from.

You will also be introduced to some of the laws that define the crimes and place restrictions on the investigative process in an attempt to strike a balance between protecting an individual's rights with stopping crime.

Remember that this section is an overview, so you'll get a lot of general information but you won't get many details about analyzing data. This will come later in the class. You'll also be flooded with various laws, types of computer crimes, names of Trojans and DoS tools, and forensics tools. Don't worry about memorizing all of these at this point; the goal is for you to be aware that the laws, crimes and tools exist. Learning to become a forensics investigator is just like starting out in most technical fields. There's an entire universe of knowledge that you'll be exposed to, which may seem extremely foreign at first, but will become very familiar as you work with the items on a daily basis. And once again, don't worry about memorizing all of the laws etc. for the test, because the test is open book so you can always look these things up.

WARNING - You will learn how to use different tools that can be used to commit computer crimes in this chapter. Remember that you are NOT allowed to try these procedures or tools to break into the CBC network or any other network unless you have explicit permission. Using these tools or procedures without permission may result in expulsion from the class, expulsion from the college or criminal charges.

2.2. READING

The reading for this section covers the first three book chapters. Since the first chapter is an overview there's a lot of information but not much detail. Don't panic, because most of this is covered in greater detail in later chapters.

Try and absorb the big picture concepts but don't try to memorize the details of every law, software tool or program the book references. Just make sure you can know where to look information up (in case you need it to answer a test question). For example you should understand when a search warrant is required

and what it allows you to do, or what the Daubert standard is; but you don't need to memorize the specifics of the Sarbanes-Oxley Act 2002 or Low Orbit Ion Cannon as you can always look these up.

1. Chapters 1, 2 and 3 of System Forensics, Investigation, and Response by Chuck Eastom (Jones & Bartlett)
2. http://www.evidencemagazine.com/index.php?option=com_content&task=view&id=116&Itemid=49
3. http://computer.howstuffworks.com/computer-forensic1.htm
4. http://www.edwardpscheidt.com/index.html - Read the three articles on this web site

2.3. Objectives

When this section is completed the student should be able to:

1. Define Computer Forensics
2. List the steps in Forensics Process
3. Be familiar with the laws that affect forensics
4. Identify the types of Crimes and describe their effects on an investigation
5. Identify different Forensics Tools and Suites
6. Identify the industry certifications available for computer forensics

2.4. Assessment

The Canvas Test for this section mainly covers the reading in the first three chapters of the book. There are practice questions at the end of each chapter which you should use to prepare for the Canvas exam. There are also sets of practice questions in the Canvas Test 1 Module that can be used to help prepare for Test 1.

Remember that the Test 1 (and all tests for this class) are open book and open note.

SECTION 2 LAB MANUAL

2.5. PROBLEM SOLVING EXERCISES

As you'll soon see, a small portion of a forensics investigation can be done by following a checklist. For example, one of the things you may check for are pornographic images. If you find them, then it doesn't take much deduction to figure out that there's a problem. However the checklist won't show you everything you need to know. For example, you may find proof that a suspect has visited several websites, but simply visiting web sites isn't suspicious behavior. However you may be able to use the fact that suspect visited specific web sites at specific times as evidence.

The point of this is that the thing that distinguishes a good forensics investigator from someone who can follow steps on a checklist is the ability to solve mysteries or problems by looking at a variety of clues. Think of Sherlock Holmes or Shawn Spencer from the Psych TV show, and their ability to observe tiny details, and use these to draw conclusions. (Shawn Spencer usually makes 4 or 5 incorrect conclusions first, so try not to emulate him too closely.)

In this set of exercises you'll practice looking at or reading clues and making deductions. These have nothing to do with forensics, but they're a fun way to practice being a detective. You don't have to write anything down for these exercises, and most of the sites show you the answers if you can't figure them out. But be forewarned that one of them may show up on the test, so you should at least give them a look.

1. Try solving the mysteries at each of the following web sites:

   http://www.oneminutemysteries.com/samplechapters.pdf
   http://answers.yahoo.com/question/index?qid=20070503135318AAMPAwa

2. In the old West a man rides into town on Friday. He stays for three days, and leaves on Friday. How can this be?

3. A burglar enters a house and reaches for something on a shelf. He accidentally knocks over a clock which falls to the floor and breaks, stopping the clock. When the police arrive they aren't able to tell what time the robbery occurred. Why not?

4. There is a man walking down the road dressed entirely in black. There are no lights on anywhere and no moon. A car with no lights comes down the road and manages to avoid the man. How?

5. A father and son are in an auto accident. The father dies and the son is rushed to the hospital in critical condition. The doctor looks at the boy and says, "I can't work on him, he's my son." How can this be?

6. You are in a cabin with four walls all facing south. There is a bear outside. What color is the bear?

7. You walk into a room with only one match. You must light a lantern, a gas stove, the pilot light of a water heater and a fire in a fire place. What do you light first?

8. Sandy goes to restaurant for her lunch break. She orders a salad, sandwich and coffee. She eats the food, drinks the coffee, then pays. When she walks out of the restaurant she stops and looks around. The sky is black and the entire city seems to be deserted. What happened?

9. Two fathers and two sons went out for breakfast. In total, they ate three eggs and each person present ate just one egg. How is this possible?

10. There is one fish in this picture. Can you find it? (You can download a color version of this image from Canvas. It's called **octopus.jpg**.)

11. There is a cat in this picture. Can you find it? (You can download a color version of this image from Canvas. It's called **cat logs.jpg**.)

12. Find the six hidden words in this picture. (You can download a color version of this image from Canvas. It's called **hidden words.jpg**.)

    If you like this type of puzzle there are more at: http://socialnewsdaily.com/60390/can-you-spot-the-six-words-in-these-picture-puzzles/

13. What can you hold in your right hand that you can't hold in your left hand?

14. Solve the following equation: 9 – 3 ÷ 1/3 +1 =

15. Einstein's Brain Teaser. When Einstein invented this brain-teaser, he stated that 98% of the population would be incapable of solving it. Are you among the other 2%?
    Five houses are painted different colors.
    The person living in each house is of a different nationality.
    Each person likes a different drink, smokes a different brand of cigars, and has a different pet. With the following hints, you must determine who owns the fish:

    - The Brit lives in a red house.
    - The Swede has a dog.
    - The Dane drinks tea.
    - The green house is to the left of the white house.
    - The person living in the green house drinks coffee.
    - The person who smokes Pall Malls has birds.
    - The person who owns the yellow house smokes Dunhills.
    - The person who lives in the middle house drinks milk.
    - The Norwegian lives in the first house.
    - The person who smokes mixed cigars lives next to the one with cats.
    - The person who has horses lives next to the one who smokes Dunhills.
    - The person who smokes BlueMasters drinks beer.
    - The German smokes Princes.
    - The Norwegian lives next to the blue house.
    - And the person who smokes mixed cigars has a neighbor who drinks water.

ANSWERS:

2. The horse's name is Friday.
3. The clock is a digital clock.
4. It's day time.
5. The doctor is the boy's mother.
6. The cabin is at the tip of the North Pole. The bear is, of course, white.
7. The match.
8. Sandy works at night and takes her lunch.
9. There are only three people, a grandfather, father and son.
10. The solution is shown in an image file
11. The solution is shown in an image file
12. The solution is shown in an image file
13. Your left hand
14. The way to solve this problem is shown at https://www.youtube.com/watch?v=07Abat5iBbw
15. First of all I hope you don't really believe that Einstein came up with this problem, that's a myth and makes this problem clickbait. The way to solve this problem, and the solution if you don't have the patience to work through it, are shown http://www.businessinsider.com/how-to-solve-einsteins-riddle-video-2015-9

2.6. Create Your Curriculum Vitae (CV)

When you apply for a search warrant or write a report for a forensics investigation one of the items that generally must be included is your Curriculum Vitae or CV. The CV is meant to assure people that you know what you're talking about, so it should describe your technical background and experience. In this exercise you will write two CVs. The first CV will be for your main hobby since you'll have a little more to write about. The second will be your Forensics Investigator CV. This CV may be very brief since you probably don't have much experience yet.

Your CV will be very similar to your resume but the structure and content will be just a little different. A great example of a CV for a forensics investigator can be found in the **Chris-Roberts-Application-for-Search-Warrant.PDF**, which is available in Canvas. This file contains the Search Warrant application filed by the FBI in the case of the hacker who claimed to have hacked into the control systems on airplanes. Read the entire PDF, but pay particular attention to the **Introduction and Agent Background** section at the beginning where he provides his CV.

A. You probably don't have a lot of experience with forensics investigations at this point in your career, so it can be hard to write anything about your digital forensics background or experience. However, you can write about your background and experience with one of your hobbies. Write a brief CV for your main hobby. It should be at least 4 sentences, but don't spend too much time on this as it's simply meant to give you an idea of what a CV is.

   Also remember that you can make statements such as "I have over 20 years of experience as a brain surgeon"; you don't have to prove it in the CV by listing the parts of the brain. You may be asked to prove your CV statements in real life, but I won't require to supply proof for the CV you create for this assignment. So go ahead and be a space shuttle astronaut or killer ninja assassin squirrel if that makes you happy.

B. Write your Digital Forensics Investigator CV. I realize you may have very limited experience, but go ahead and explain how many years you've been using computers, if you've taken any Network Administration or Cyber Security classes or if you have any other experience. Be truthful in this CV. Once again, don't spend a lot of time on this.

2.7. FORENSICS INVESTIGATION – THE HOME VERSION OF THE GAME

Like any process the whole forensics investigation can seem a little complicated and daunting at the first introduction. There are all the various aspects of an investigation, like acquiring evidence, establishing a chain of custody, analyzing data, etc. And analyzing data really seemed like a complicated process. You may have seen TV shows or movies where the only person who can find evidence is some computer whiz, using specialized tools or writing custom code to sort through mountains of binary data. And then there are the magazines and web sites dedicated to forensics that refer to specialized tools like Kali, or EnCase or FTK.

This set of exercises has been designed to help step back from looking at "the trees" and look at "the forest", with the goal of showing you that the process isn't really all that difficult. In this exercise you will perform the main steps in a forensics investigation using your existing computer skills. These steps are:

A. Obtaining proper authorization
B. Acquiring evidence
C. Analyzing evidence
D. Preparing reports

The first exercise in this section will contain details about the process for each step. You must follow the same process for each of the remaining exercises in this section.

2.7.1. Pornography

In this exercise you will be asked to check a computer for evidence of pornography use. I'm obviously not going to use real porn as evidence. However the evidence will consist of filthy pictures and videos with dirt or mud instead. Or maybe text documents or presentations that talk about dirt. So you're looking for photos, videos etc. of actual dirt, or dirty things like muddy animals, muddy people etc.

A. **Obtain Written Authorization**. The first step in the investigation process is to protect yourself legally by obtaining authorization. In the real world you would obtain a search warrant for a criminal investigation or authorization from a company officer for a private investigation. For this exercise you will simulate real world authorization by filling out a form to obtain written permission from the instructor or an authorized designee prior to beginning the investigation. (Note – While this form may look official it is a fake and it doesn't provide any real authorization. Don't try to use the signed form anywhere else on campus.)

- Download a copy of the "Investigation Authorization" form.
- Fill out the form with the proper information
- Submit the form to the instructor to obtain written authorization.

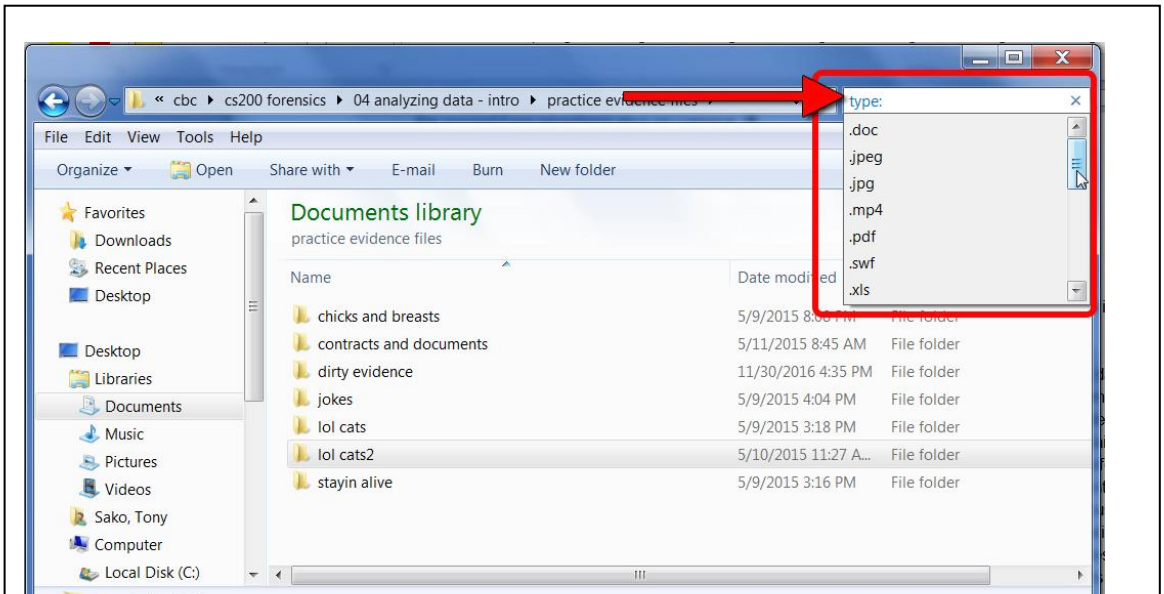
B. **Acquire Evidence.** At this point, after you have written authorization, you can acquire the evidence. In a real investigation there will be several steps to acquiring evidence, but the acquisition has been greatly simplified for this exercise; all you need to do to acquire the evidence is download the zip archive **Porn.zip**, and then extract the files.

C. **Analyze Evidence**. Now you are ready to start analyzing the evidence, looking for files or data that will support or refute any allegations. This is where most of the work in happens in an investigation, and most this work consists of simply looking at files. In a real investigation you'll look at hundreds or even thousands of files, by simply opening them up and looking for evidence. There are specialized forensics tools, which you'll learn about later in the class, that will help you narrow down the list of files to search, or they may decrypt files or help you find hidden files; but sooner or later you're going to open up a bunch of files an inspect the file's content. There's no magic tool that does all of the analysis for you.

In this portion of the exercise you will have to search through all of the files looking for possible evidence. You could do a brute force search and look at every file in every folder, but that will most likely take a long time. A better alternative would be to narrow down the list of files you need to visually inspect by using the Windows Search function. Use the following steps to accomplish this:

- Start Windows Explorer and open the top level folder of the files you're investigating
- Click in the Search box in the upper right, and either use wildcards to search for files with a specific extension, for example `*.jpg`, or select **Type:** or type **Kind:** and then the type of file you're searching for from the list. For this particular exercise searching for **Kind:video** or **Kind:picture** would probably be the simplest.
- Windows will search this folder and all of it's subfolders and display a list of all the matching files. You now get to open and view each of the files and decide whether it contains evidence that supports your case or not.
- You will need to develop some method for tracking files that you want to use as evidence as you will need them to complete your report in the next portion of this exercise.

Remember to take the time to actually look at the content of the files, not just the file names, so you don't return any false positives.



D. **Write the Evidence Report**. The last step in our simplified forensics process is to build or write a report. Your report must contain the following sections:

- Case information. In a real investigation this would include details about the case including the alleged crime, jurisdictional information, dates, investigator information etc. For this exercise you must include at least your name and the date.

- The main content of the report will be your findings and the files or data that support your conclusion(s). Include thumbnails of images or portions of text from files that you feel support your conclusions along with their path names. You can include other details such as creation or modification date/time, file size etc. if you wish.

- A copy of your CV.

- A copy of the search authorization form.

An example report is presented on the following page. You can use different formatting in your report, but make sure that the required information is included somewhere in your report. You can also search the Internet for forensics reports if you want more examples. Here are a couple of links to report writing references:

http://digital-forensics.sans.org/blog/2010/08/25/intro-report-writing-digital-forensics

https://www.ncjrs.gov/pdffiles1/nij/199408.pdf (Look at the appendices for example reports)

Example Report

Digital Forensic Examiner: A. Student
Columbia Basin College
Pasco, Washington

Case: Beginning Class Search 1
Date: 3/15/2014
Files: BeginningSearch1.zip

Investigator Background:
I am a student in the Columbia Basin College Cyber Security program. I have taken several Computer Science classes, and have worked with computers, phones, tablets and other digital devices since I was 3 years old. I have watched many television episodes of CSI

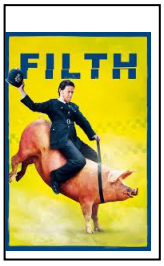
Case Summary:
On _____ I was assigned to research the .zip archive named _____ . I was given authority to perform the investigation by the class instructor _____. The instructor suspected that the one of the lab computers was being used for purposes that violated college and state policies. I was asked to inspect the files in the .zip archive for files that would confirm that the computer was being used for illegal purposes.

Methodology:
I don't have any experience with specialized digital forensics tools, so I extracted the files and folders from the archive, then inspected each file by manually opening it.

Summary of Findings:
Several files were discovered that are evidence that this computer was used to store pornography. There are pictures and videos of mud, dirt, and general filth.

The files were not found in the My Pictures or My Videos folders where images and videos are typically stored. The files were located in folders under the Windows folder, which is typically used to store system files. This means that the user placed the images and videos in this unusual location in an attempt to hide the files.

File Details and Thumbnails:



File name: perfectlyInnocentFile.doc
Location: AppData\Local\Google\Chrome
File Size: 2220 KBytes
Creation Date: Feb 14, 2007
Access Date: Mar 27, 2014
Modification Date: Feb 14, 2007

File name: Sept2014Invoices.xls
Location: AppData\Local\Google\Chrome
File Size: 3320 KBytes
Creation Date: Feb 18, 2007
Access Date: Sept 04, 2013
Modification Date: Feb 18, 2007

Porn Exercise Solution

Here are the files that you should have found:

- PrivacIE Folder
  - 4a0aa55.jpg
  - 34764.jpg
  - Bamboo.mp4
- Temp Folder
  - bike.jpg
  - bike2.jpg
  - dirty 2.jpg
  - dirty patrick.jpg
- Local Settings\Application Data\Microsoft\Windows Folder
  - Dirty video.mp4
  - Dirty story.doc
  - dirtyBSO.jpg
  - ee95d2.jpg
- Local Settings\Temp\APN Folder
  - mhole.jpg
  - mhole2.jpg
- My Documents\java demo\J2SE Downloads_files Folder
  - Noble ranch.mp4
  - Muddy.mp4
  - Mud with Worms.pdf
- My Documents\Arduino\sketch_dec16a\serial_write Folder
  - Punk bike.mp4
  - Soil comp.xls
  - Wedding.jpg

2.7.2. Angry Spouse

In this exercise you have been tasked with searching for evidence that someone's spouse may have started relationships outside of their marriage, or is thinking about cheating. You will be looking for evidence such as web pages for dating sites, pictures from dating sites or files that show someone is planning a trip or vacation. Remember to take the time to actually look at the content of the files, not just the file names, so you don't return any false positives. Use the files in **angrySpouse.zip** to perform the investigation following the same steps used in the previous exercise:

A. Obtain proper authorization
B. Acquire evidence – cheating.zip
C. Analyze evidence
D. Prepare report

Angry Spouse Exercise Solution

Here are the files that you should have found:

- My Documents\restrictions Folder
  - Ashley Madison.html
- 1 Folder
  - eHarmony.com -- Find Compatible Single Men or Women Near You.html
  - Top 10 Best Online Dating Sites 2016.html
- Nethood Folder
  - Match.com - Find Singles with Match.com's Online Dating Personals Service _ Match.com.html
  - Match.com2 .htm
- Application Data\Google\Local Search History Folder
  - dating-profile-headline-6.jpg
  - dating-profile-headline-4-2.jpg
- Application Data\Microsoft\Crypto Folder
  - Hawaii Expedia.html
  - Mauna Lani Bay Hotel .html
  - mauna lani.jpg
  - mauna lani 2.jpg
  - mauna lani 3.jpg
  - mauna lani 4.jpg

2.7.3. Comic Con (Knock Knock, Who's There?)

You have been hired to investigate a comic accused of stealing jokes from other comedians. You are tasked with finding files that contain jokes, however you do **not** need to determine who originally developed the material; you just need to find the files. Remember to take the time to actually look at the content of the files, not just the file names, so you don't return any false positives. Use the files in **comic.zip** to perform the investigation following the same steps used in the previous exercise:

Follow the same steps for performing the investigation as above:

A. Obtain proper authorization
B. Acquire evidence – cheating.zip
C. Analyze evidence
D. Prepare report

Comic Exercise Solution

Downloads\dad10.jpg
Downloads\f07cdb4.jpg
AppData\Local\assembly\tmp\JobsGates.jpg

Multimedia
My Videos\Lights\JSignfild.mp4
My Videos\Lights\ Hahn.mp4

Documents
My Documents\2nd set\geek dad\panda mole.pdf
Downloads\more secrets.doc
AppData\Local\assembly\tmp\ not funny.doc

False Positive
My Videos\Lights\Calliendo.mp4
My Documents\2nd set\geek dad\more jokes.pdf
Downloads\knock knock.doc

3. Forensics Tool Research

The purpose of this exercise is to introduce you to some of the suites of forensics tools. Research the following tools and determine who owns the tool (or if it's open source), the price, and whether or not it is acceptable under the Daubert Standard.

	Owner	Price	Daubert
Encase			
FTK			
Kali (Backtrack)			
P2 Commander			
X-Ways Forensic			

4. Forensics Certification Research

The objective of this exercise is to provide you with some background on industry certifications for computer forensics. Some material is provided regarding the CHFI and ACE certifications. You are expected to research the other certifications and complete the table.

NOTE - You don't have to take these certification exams, and they will not affect your grade. The class will begin your preparation for the exams, a little for the CHFI exam, and a lot for the ACE exam. However, passing any certification exam requires extra study and work on the student's part.

CHFI

The CHFI cert covers the general knowledge you need to know about computer forensics, that is it covers it from an administrative perspective. It's a little difficult because you don't need to know how to use any specific suite of tools, but you need to know about *almost all* of the tools and their purpose. You also need to know about the various types of computer crimes, the investigative process, preparing and presenting reports, etc.

http://www.eccouncil.org/certification/computer-hacking-forensics-investigator - about CHFI

http://www.eccouncil.org/Training/chfi-assessment - practice (lots of encase questions)

It looks like it costs ~$500 to take the CHFI exam. Since this exam covers so many different areas many people take a class specifically designed to help prepare them for the exam.

ACE

The ACE certification requires that you know all about the AccessData FTK tool. FTK has several component programs, a disk imager, a password recovery tool, a case manager, etc. There may be a few questions where it helps to understand the general computer forensics process, but most of the questions will be FTK specific.

The ACE exam is free and AccessData has prepared a set of videos that they've posted on YouTube to help you learn FTK. The videos are a little boring, and blurry, but they're a decent way to get started and learn about every part of FTK (as opposed to paying for another class like CHFI).

http://www.accessdata.com/products/digital-forensics/ftk - AccessData

http://www.accessdata.com/training/ace-process - The ACE exam

https://www.youtube.com/user/accessdatagroup - AccessData Youtube Channel

	Cost	Training or experience pre-requisities	Years until renewal required
EnCE (Encase)			
ACE (FTK)			
CHFI			
GIAC-GCFE (SANS)			
GIAC-GCFA (SANS)			