ENCASE CYBER-SECURITY FORENSICS

Email Investigation
&
Recovering Digital Photograph Evidence
CIS 4385 Project Report

Dr. Chi

Michael Simmons

Florida A&M University

23 November 2011

PURPOSE

1. Scope and Purpose

This case involves recovering Email and Digital Photograph evidence on an employee named Michael Simmons who may possibility be involved in providing confidential information to his company's business competitor concerning a *new kayak.* Michael Simmons is sending altered graphic files attached in his company's email. He is considered to be an insider threat.

1.1 Specification Objectives

EnCase v7 Forensic Tool will be used to attempt to locate and recover Michael Simmons emails and graphic file to be used as evidence again Mrs. Michael Simmons for violating company policy of confidentially. Utilenilizing

EnCase® Cybersecurity

Network-enabled Incident Response and Endpoint Data Control through Cyberforensics

Guidance® SOFTWARE

A. The Name and URL and Operating System Requirement of digital forensic tool you have chosen.

EnCase Forensic V7 Forensic Tool (Commercial)

http://www.guidancesoftware.com/

Operating System Minimum Requirements

For best performance, you should configure examination computers with at least the following hardware and software for small workloads:

- An EnCase security key (also known as a *dongle*)
- An optional certificate file for users who wish to activate an EnCase Version 6 dongle to run EnCase Version 7
- The downloaded installation files for the current release of EnCase
- Processor speed: Dual Core 2GHz memory
- Network: Gigabit Network Card
- I/O Interfaces: USB 2.0, Serial, Parallel
- Flash Media Readers: Multi-Reader
- OS Drive: SATA 7200 RPM
- Evidence Storage Drive: SATA 7200 RPM
- RAID Card: Adaptec 29320 (PCI Express)
- 2 GB RAM (32-bit computer); 4 GB RAM (64-bit computer)
- Windows 2000, XP Professional, 2003 and 2008 Server, Vista, and Windows 7
- Optical drive: Dual Layer DVD +/-RW Drive
- Display: Single 19", 20", 21", or 22"
- 55 MB of free hard drive space
- Uninterruptible power supply: 650 VA
- Printer: Monochrome Laser Printer
- Evidence Backup: 1 or 1.5 TB Western Digital Green Hard Drives

EnCase supports 64-bit versions of Windows XP, Server 2003 and 2008, Server 2008 R2, Vista, and Windows 7 with the following applications and modules:

Examiner 32-bit and 64-bit

ProSuite 32-bit and 64-bit, consisting of these modules:

− EnCase Decryption Suite (EDS)
− Virtual File System (VFS)
− Physical Disk Emulator (PDE)
− FastBloc SE

B. **The Studies have you done in the last project for this tool included a previous investigation with Encase v7.**

It involved recovering Digital Photograph evidence on an employee named Bob Aspen, who may possibility be involved in providing confidential information to his company's business competitor concerning a *new kayak.* Bob Aspen is receiving altered graphic files attached in his company's email.

I conducted the following research on EnCase

I conducted some online studies with the following

- 2005 FBI Computer Crime Survey Report
- Computer crime study at Maryland and Investigation
- Digital Forensics How Experts Uncover Doctored Images
- U.S. Department of Justice
    - https://www.ncjrs.gov/pdffiles1/nij/199408.pdf
- EnCase Forensic Website

Course	Course Website
First Responder with EnCase® Forensic,Tableau, and EnCase® Portable	http://www.guidancesoftware.com/EnCase- First- Responder.htm
EnCase® Computer Forensics I	http://www.guidancesoftware.com/computer- forensics- training- encase1.htm
EnCase® Portable Configuration and Examinations	http://www.guidancesoftware.com/encaseportable- examinations.htm

Results of study conclude:

EnCase is a know industry-standard computer investigation solution

EnCase is used by forensic practitioners like the FBI, who need to conduct efficient, forensically sounds data collection and investigations using a repeatable and defensible process.

EnCase Data Acquisition

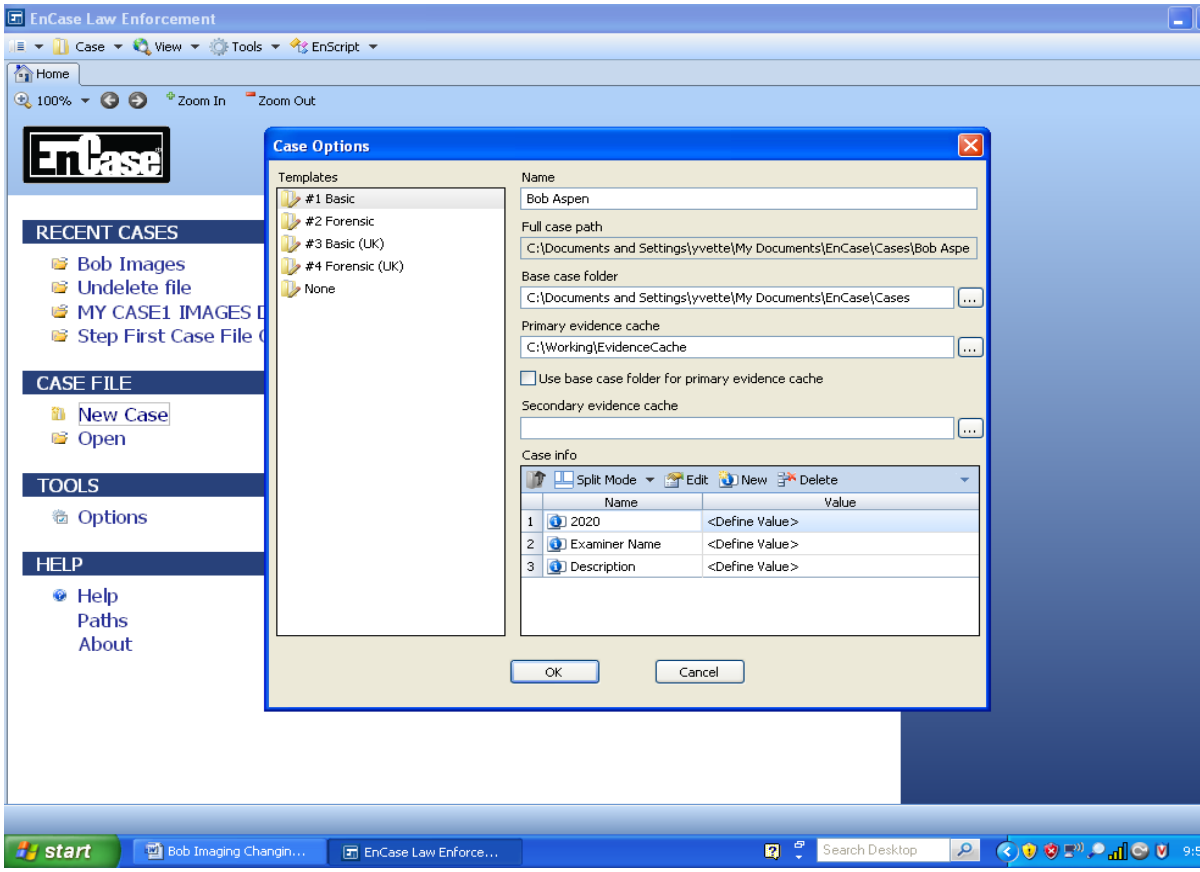
EnCase allow you to acquire data from disk or RAM, documents, images, e-mail, webmail, Internet artifacts, Web history and cache, HTML page reconstruction, chat sessions, compressed files, backup files, encrypted files, RAIDs, workstations, servers, and with Version 7: smartphones and tablets.

EnCase Evidence Management

The case management structure allows you to process large datasets that can be segmented through distributed processing capability. Also you can encrypt your evidence files, easily allowing you to secure your findings.

EnCase Customizable Reports

You can produces consistent, professional reports for every case. With an easy to use configuration capability, you can create customize report templates for every type of case.



EnCase **install type** on Windows XP Laptop Computer, 32bit, 2GB of RAM. 30MB of 160 gigabytes free disk space.

C. Brief introduction of this tool and include types of investigations that this tool is good at.

EnCase Forensic

Provides investigators with a single tool for conducting largescale and complex investigations from beginning to end. It features superior analytics, enhanced email/Internet support, and a powerful scripting engine.

With EnCase v7 you can:

• Acquire data in a forensically sound manner using software with an unparalleled record in courts worldwide.

• Investigate and analyze data from multiple platforms – Windows, Linux, AIX, OS X, Solaris, and more – using a single tool.

• Find information despite efforts to hide, cloak, or delete.

• Easily manage large volumes of computer evidence, viewing all relevant files, including deleted files, file slack, and unallocated space.

• Transfer evidence files directly to law enforcement or legal representatives as necessary.

• Review options that allow non investigators, such as attorneys, to review evidence with ease.

• Use reporting options for quick report preparation

FORENSICALLY SOUND ACQUISITIONS

- EnCase v7 produces an exact binary duplicate of the original drive or media, then verifies it by generating MD5 hash values for related image files and assigning Cyclic Redundancy Check (CRC) values to the data. These checks and balances reveal any inconsistencies with acquired data. EnCase v7 maintains the reliability and functionality of previous versions while simplifying usage, and powerful new features, and significantly increasing performance.

- EnCase v7 is accessible to several types of users:
  - Those responsible for collecting evidence
  - Forensic examiners and analysts
  - Forensic examiners who develop and use EnScript code to automate repetitive or complex tasks

D. What A Forensic Examiner Can Do With EnCase:

- Investigate inappropriate web surfing.
- Search the contents of files for inappropriate images, photos and movies.
- Identify traces of abusive behavior in emails and stored documents.
- Protect highly sensitive information such as tests, grades and confidential student/teacher data (social security numbers, addresses, etc.).
- Enforce computer use policies.
- Respond to network breaches and identify compromised systems.
- Identify rootkit and rogue process propagation.
- Universities can ensure their compliance with HIPAA.
- Determine whether a computer system contains evidence and is within the scope of our investigation
- Restore entire disk volumes back to their original state
- Do a basic keyword search of the entire case using any number of search terms
- Do advanced searches using the powerful UNIX GREP syntax
- Acquire data in a forensically sound manner using software with an unparalleled record in courts worldwide.
    - Investigate and analyze data from multiple platforms – Windows, Linux, AIX, OS X, Solaris, and more – using a single tool.
    - Find information despite efforts to hide, cloak, or delete.
- Easily manage large volumes of computer evidence, viewing all relevant files, including deleted files, file slack, and unallocated space.
    - Transfer evidence files directly to law enforcement or legal representatives as necessary.
    - Review options that allow non investigators, such as attorneys, to review evidence with ease.
    - Restoring A Drive
    - Use reporting options for quick report preparation

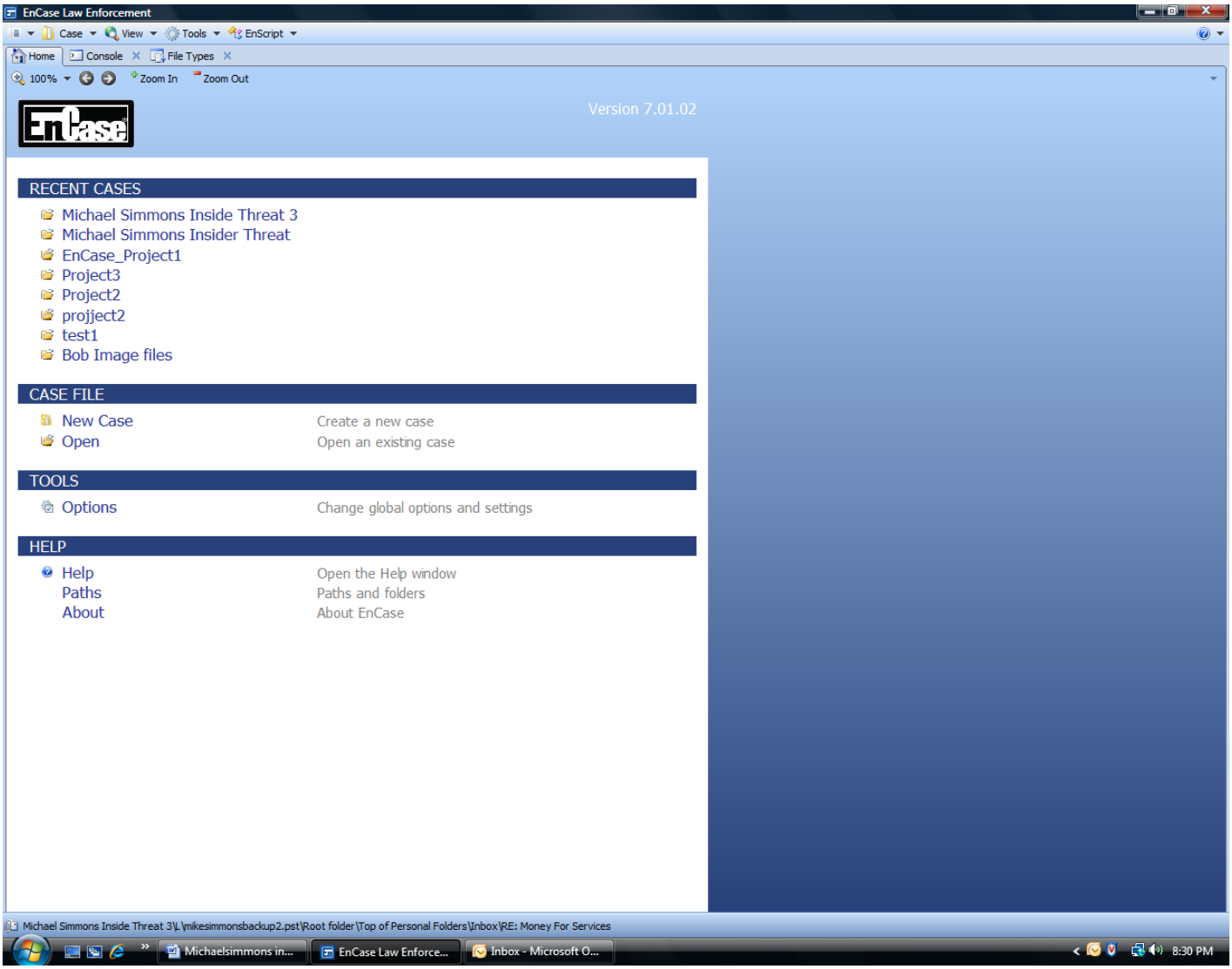
E. As an investigator, what type investigation that you are planning to use this tool?

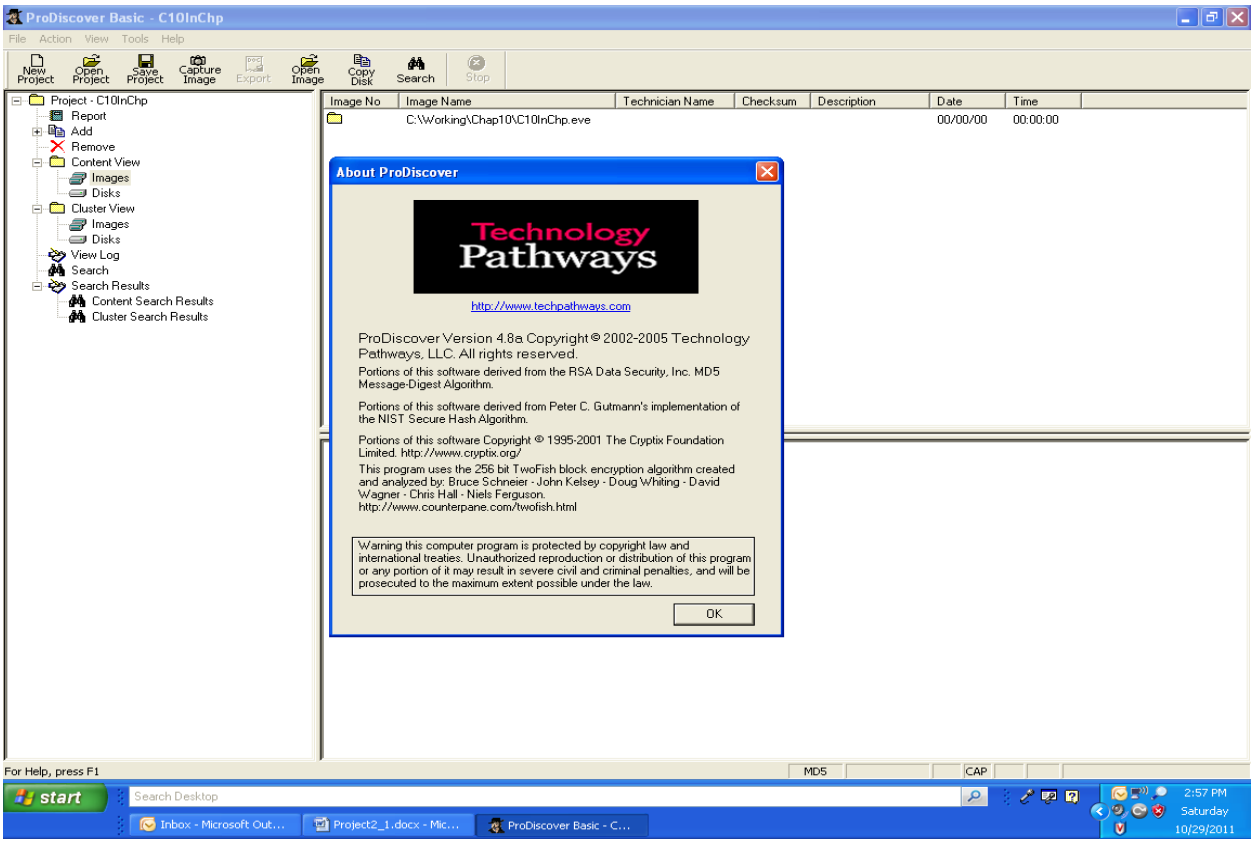
Investigating Email Crime and Violation of an employee named Michael Simmons who may possibility is involved in the sale of the company confidential information to his company's business competitor. Michael Simmons has been sending and deleting large email attachment through his company's email.

F. List the data/image/files that you will use to do your investigation.

Michael Simmons.pst

G. Show the evidence(s) that you download the tool in your computer. A screenshot from your own laptop





H. Make a comparison your tool to FTK or ProDisover

Both EnCase and ProDiscover have the following similarities:

- Both acquired an image of Michael Simmons thumb drive to be used has as evidence at location C:\Working\LocalEvidence. Allowing the original evidence to be preserved on the thumb drive.

- Both use keyword search for pattern(s) type FIF. This also includes *"Search entry slack"* and *"Undelete entries before searching"*.

Encase only have a built-in Hex-editor to reviewed the file *Recover1.jpg* header, and found the header to be incorrect for a *JPEG image.*

CIS 4385 Hands-on Lab #2 EnCase Lab

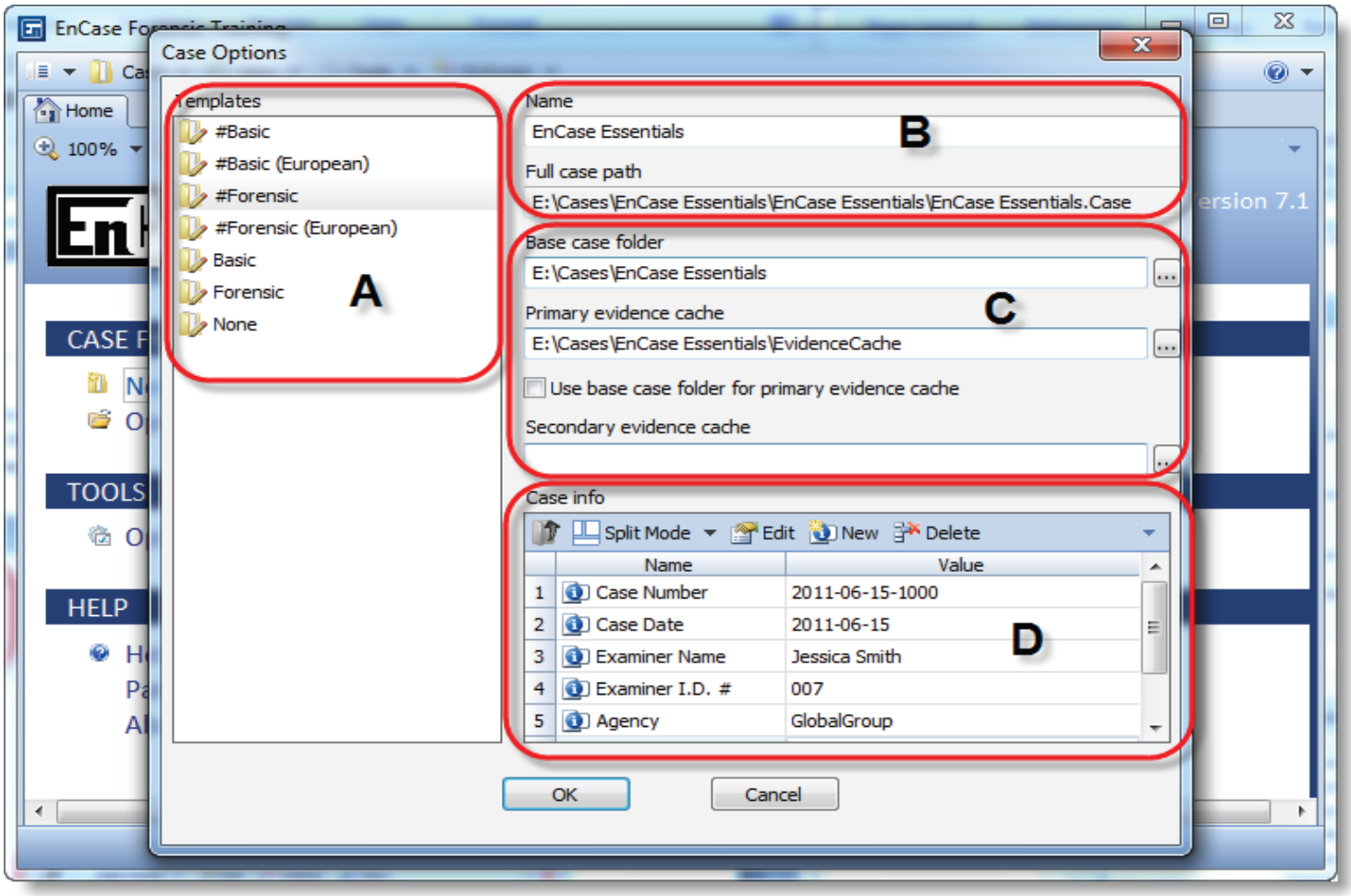
Last Name ____Simmons_____ First Name ___Michael_____

Email Retrieval using EnCase v7.01.02

This case involves recovering Email and Digital Photograph evidence on an employee named Michael Simmons, who may possibility be involved in providing confidential information to his company's business competitor concerning a *new kayak.* Michael Simmons is sending altered graphic files attached in his company's email. He is considered to be an insider threat.

1. Start the EnCase program by clicking on the icon on the desktop.
2. Next the EnCase will open to the Home Screen. ***Select start a new case*.**
3. Once you select start a new case the case wizard will begin. We want to treat this as if we were handling real evidence for a real ongoing case so we will fill out the report.

- ***Case Name***: This is where you would state the name of the case. Enter "Intellectual Property Case".
- ***Case Path:*** This is where you want all the files need for this case to be stored. Leave all the default setting and to save into the EnCase Folders.
- ***Case Number:*** This would match the case number of the court case. You can make up your own case number **double click on *"define value field "***
- Next is the forensic Examiner information. Here you are only required to enter your name. **double click on *"define value field"***
- ***Case description:*** Here you would want to enter details about the case. Remember to keep it professional because this is evidence that will be going into the court of law. **double click on *"define value field "***



Creating a new case

- **Click ok to finish.**

4. Now you have reached the New Case Home Page Screen.
    - ***Insert Thumb Drive containing michael.simmons.pst***
    - Click the ***Add Evidence***
    - Click the ***Add Local Evidence Device***
    - Check **Enable *DCO Removal*** *and* ***Next***
    - Check Thumb Drive Letter ***Box*** and ***Click Finish***
    - Double click on ***drive letter***
    - Select ***mikesimmons.pst***

- Because we are using an image of the ***Thumb Drive***, you will have to click ***Acquire***. Then click ***ok.***
- You are now back at the Add Evidence menu. **Click next**.
- From Top Menu Bar Click ***Add Evidence*** and select ***Process Evidence.***
- Select ***Acquire*** and ***Ok***
- Select ***Process*** and double click on ***Find Email***. Select ***PST (Outlook)*** *and* ***Ok***, *Ok*
- Wait for your Email Evidence Processor to complete.

5. Click on the ***search tab*** -> ***new search***.
6. In the search tab search for the keyword word **Money**, investors or any other word that would be use in an email as someone attempts to sell intellectual property. ***Click Ok***.
7. Next you select your search term then click ***View cumulative results.***
8. Double click files review content. Record Time Stamps of interest.
9. Next Click ***Evidence Tab*** and select all Time Stamps of interest emails (attachment will also be automatically be included).
10. Find the incriminating evidence needed to incriminates or de-criminates Michael Simmons, by reading his email messages and attachments ……..Use the tools inside of EnCase.
11. Once completed gathering all the necessary evidence Go the Top Menu Bar and Select ***View Reports*** and in the comments box state whether you think you have enough evidence to file a law suit or if we should seek further evidence?

Upon completion all Teachers Assistance to review your work before leaving the class.

Evaluations and Conclusions

The recovered emails and a graphic file are extremely incriminating evidence that will be used again Michael Simmons for violating the company policy of confidentially agreement. Criminal changes may also be filed.

I. Recommendation for building a Basic forensic lab, I would include the following items.

After reviewing the basics of forensic duplication and related investigation on cybersecurity techniques, on multiple platforms(Windows, Mac OS X, Linux, and *BSD). I can now outline some core requirement for lab forensics workstation, laptop and server:

1. The system must support IDE
2. The system must support SCSI
3. The system must have network connectivity
4. The system must support hardware based drive duplication
5. The system must support remote and network based drive duplication
6. The system must support duplication and analysis of these common file system types:
    a. NTFS
    b. FAT16/32
    c. Solaris UFS
    d. BSD UFS
    e. EXT2 (Linux)
    f. EXT3 (Linux)
    g. HFS & HFS+ (Macintosh)
    h. Swap
    i. Solaris
    ii. BSD
    iii. Linux

7. The system must have the ability to validate image and file integrity.
8. The system must be able to identify dates and times that files have been modified, accessed and Created.

9. System must have the ability to create file system activity timelines
10. The system must be able to identify deleted files
11. The system must be able to analyze allocated drive space
12. The system must be able to isolate and analyze unallocated drive space
13. The system must allow the investigator to directly associate disk images and evidence to a case
14. The system must allow the investigator to associate notes to cases and specific evidence
15. The system must support removable media for storage and transportation of evidence and disk images
16. Evidence collected by the system must be admissible in a court of law

Window Server System Platform, Windows Workstation and Labtop , Macintosh Workstation and MacBook Pro laptop to include the above requirements just mention.

Hardware Component	Requirement
Processor	Minimum: Single processor with 1.4 GHz (x64 processor) or 1.3GHz (Dual Core) Note: An Intel Itanium 2 processor is required for Windows Server 2008 R2 for Itanium-Based Systems
Memory	Minimum: 512 MB RAM Maximum: 8 GB (Foundation) or 32 GB (Standard) or 2 TB (Enterprise, Datacenter, and Itanium-Based Systems)
Disk Space Requirements	Minimum: 32 GB or greater Note: Computers with more than 16 GB of RAM will require more disk space for paging, hibernation, and dump files
Display	Super VGA (800 × 600) or higher resolution monitor
Other	DVD Drive, Keyboard and Microsoft Mouse (or compatible pointing device), Internet access (fees may apply)
Backups	2 Terabytes Tape Backup
Disk Space Requirements	Minimum: 32 GB or greater Note: Computers with more than 16 GB of RAM will require more disk space for paging, hibernation, and dump files

- Work Area must be a minimum of 1000 square feet, fully furish for five investigators. The average number of cybersecurity investigation is 30 per month
- Network Connectivity Required

Software	Description	License	Homepage
dd for Windows	dd but for Windows.	GPL	Download Page
Encase 4	EnCase 4 is a complete forensic toolkit that covers much of the work that the I&TM Forensic Analysts carry out. Encase is the Primary I&TM forensic tool	Commercial	Download Page
FTK	The AccessData Forensic Toolkit (FTK) is another complete forensic toolkit. FTK is recognized as one of the leading forensic tool to perform e-mail analysis.	Commercial	Download Page
Paraben Email Examiner	Paraben's E-mail Examiner is one of the most comprehensive e-mail examination tools available. E-mail Examiner claims to recover more active and deleted mail messages than the leading competitor.	Commercial	Download Page
WinHex	WinHex is a universal hexadecimal editor. WinHex is often used in forensic examinations	Freeware	Download Page

Image and Document Readers

Software	Description	Software Licence	Link
Adobe Reader	PDF reader	Freeware/ Commercial	Download Page
IrfanView	IrfanView is a very fast, small, compact and innovative FREEWARE (for non-commercial use) graphic viewer for Windows 9x/ME/NT/2000/XP/2003.	Freeware	Download Page

Data Recovery/Investigation

Software	Description	Software Licence	Link
Pasco	An Internet Explorer activity forensic analysis tool. Many computer crime investigations require the reconstruction of a subject's internet activity. Pasco, the Latin word meaning "browse", was developed to examine the contents of Internet Explorer's cache files. Pasco will parse the information in an index.dat file and output the results in a field delimited manner so that it may be imported into your favourite spreadsheet program. Pasco is built to work on multiple platforms and will execute on Windows, Mac OS X, Linux, and *BSD platforms.	Freeware	Download Page
SnapView HTML Viewer	Quick and easy way to examine recovered HTML pages from unallocated space. This little viewer is built on the same technology as used by Internet Explorer. It can load up pages very quickly. You can also toggle between page and source view by pressing F9. It not only	Freeware	Download Page

Software	Description	Software Licence	Link
	supports HTML but a number of other formats. It can also use any Internet Explorer plug-ins, already available within the operating system, giving it quite a large selection of supported file formats. The following is not the full list, but a flavour of the file formats possibly available: HTML, JPEG, GIF, ICO, Flash Move, Adobe Acrobat, Office Documents such as Word, Excel, PowerPoint, Bitmap, PNG, ART etc.		
StegHide	StegHide is a steganography program which embeds a secret message in a cover file by replacing some of the least significant bits of the cover file with bits of the secret message. After that, the secret message is imperceptible and can only be extracted with the correct pass phrase. Features: support for JPEG, BMP, WAV and AU files encryption of plain data before embedding (blowfish encryption algorithm) pseudo-random distribution of hidden bits in stego file embedding of a crc32 checksum of the plain data.	FreeWare	Download Page

Password Cracking

Software	Description	Software Licence	Link
Accent Access Password Recovery 2.01	Software to recover forgotten or lost passwords for Microsoft Access documents	Shareware	Download Page
Accent Excel Password Recovery 2.10	Software to recover forgotten or lost passwords to open for Microsoft Excel documents	Shareware	Download Page

Network Investigation

Software	Description	Software Link	Link
FavURLView	This utility will decode Internet Shortcut (*.URL) files to allow you to compare the Shortcut Description with the actual link. It will also decode the Modified time and date. The software can be run as an External Viewer within Encase, iLook or any forensic application that supports external viewers. It has also been designed to accept data from Encase by sending data via the command line.	Freeware	Download Page
Putty	PuTTY is a free implementation of Telnet and SSH for Win32 and Unix platforms, along with an xterm terminal emulator.	Freeware	Download Page

Phone Investigation

Software	Notes	Software Licence	Link
Chip-it	Another program to strip out phone numbers from a variety of mobile phones – Freeware	Freeware	Download Page
Oxygen	A forensic analysis tool for analyzing mobile phones. The software does not change any data on the phone and does not write data to the phone. Oxygen requires a Windows OS.	Freeware	Download Page
Paraben Cell Seizure	Cell phone forensics is not to be compared with traditional bit stream forensics. Cell phone data storage is proprietary, based on the manufacturer, model, and system. Paraben's Cell Seizure was designed to allow forensic acquisition of user entered data and portions of unallocated storage on some devices. Each device is unique and should be dealt with caution as each phone has unique considerations. Continual advances will be made to Paraben's Cell Seizure in reference to acquiring of proprietary data. Paraben's Cell Seizure currently supports certain models of Nokia, Sony-Ericcson, Motorola, & Siemens. Paraben's Cell Seizure also supports GSM SIM cards with use of a SIM card reader (which can be found in Cell Seizure Toolbox).	Commercial	Download Page
PDU spy	Another mobile phone examination program. The site has a number of interesting recovery programs and useful bits for investigating phones – Freeware.	Freeware	Download Page

PDA Investigation

Software	Description	Software Licence	Link
Paraben PDA Seizure	The only forensic tool designed to capture data and report on data from a PDA. As an examiner you know better than anyone that the difference between making a case and losing a case is hard evidence. And with more bad guys going high tech, obtaining that evidence is becoming more difficult than ever. Paraben's PDA Seizure is a comprehensive tool that allows PDA data to be acquired, viewed, and reported on, all within a Windows environment. Now with USB support.	Commercial	Download Page
Pilot-Link	Used to get contents of ROM and RAM from Palms. Additionally *pilot-xfer* allows acquisition	Freeware	Download Page
POSE	Emulator for Palms that runs on the desktop. Behaves exactly as the palm would do when a palm image is loaded into it	Freeware	Download Page

Lab Tools

Software	Description	Software Licence	Link
Black Bag Macintosh Forensic Software	BlackBag offers customers a suite of forensic solutions, as well as a Macintosh Boot CD, which boots any systems capable of running OS X	Commercial	Download Page
WinRAR	Compression tool	Shareware	Download Page
WinZip	Compression tool	Shareware	Download Page
Wipe	Wipe is a secure file wiping utility. It is based on work by Peter Gutmann.	Freeware	Download Page

Operating System Software

Software	Description	Software Licence	Link
Windows	The last three versions workstation and server versions	Commercial	
Macintosh	The last three versions workstation and server versions	Commercial	
Unix	The last three versions workstation and server versions	Shareware	
Linux	The last three versions workstation and server versions	Freeware	

Desktop Software

Software	Description	Software Licence	Link
Browsers Internet Explorer Safari Netscape Navigator Mozilla Firefox Opera SeaMonkey	The last three versions	Commercial	
Database	Microsoft SQL Server 2005 or higher, mixed mode authentication	Commercial	
Microsoft Office 2010	Complete Office Suite	Commercial	
Aniti-Virus	MacAfee Aniti-Virus 8.7.i	Commercial	
Aniti-Spyware	MacAfee Aniti-Spyware 8.5	Commercial	

References

- **U.S. Department of Justice**
  https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

- EnCase Essentials Training Manual (hyperlink)

- EnCase was tested using Retina Network Security Scanner, which is an NIST validated FDCC scanner ***http://nvd.nist.gov/fdcc/download_fdcc.cfm***

Guideline for Digital Forensics

- **U.S. Department of Justice**
  Office of Justice Programs
  National Institute of Justice

- **Forensic Examination of Digital Evidence: A Guide for Law Enforcement**

- **ENCASE® FORENSIC V7 ESSENTIALS TRAINING ONDEMAND**

- FBI Cyber Investigation
  http://www.fbi.gov/cyberinvest/cyberhome.htm
- Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors
  http://www.ojp.usdoj.gov/nij/pubs-sum/211314.htm
- Forensic Examination of Digital Evidence: A Guide for Law Enforcement
  http://www.ojp.usdoj.gov/nij/pubs-sum/199408.htm