THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 10 | Number 3 Article 1

2015

Computer Forensic Projects for Accountants

Grover S. Kearns
University of South Florida, St. Petersburg

Recommended Citation

Kearns, Grover S. (2015) "Computer Forensic Projects for Accountants," *Journal of Digital Forensics, Security and Law*: Vol. 10 : No. 3 , Article 1.
DOI: https://doi.org/10.15394/jdfsl.2015.1203
Available at: https://commons.erau.edu/jdfsl/vol10/iss3/1

COMPUTER FORENSIC PROJECTS FOR ACCOUNTANTS

Grover S. Kearns
University of South Florida St. Petersburg
Program of Accountancy
St. Petersburg, FL 33701
gkearns@mail.usf.edu

ABSTRACT

Digital attacks on organizations are becoming more common and more sophisticated. Firms are interested in providing data security and having an effective means to respond to attacks. Accountants possess important investigative and analytical skills that serve to uncover fraud in forensic investigations. Some accounting students take courses in forensic accounting but few colleges offer a course in computer forensics for accountants. Educators wishing to develop such a course may find developing the curriculum daunting. A major element of such a course is the use of forensic software. This paper argues the importance of computer forensics to accounting students and offers a set of exercises to provide an introduction to obtaining and analyzing data with forensics software that are available free online. In most cases, figures of important steps are provided. Educators will benefit when developing the course learning goals and curriculum.

Keywords: Computer forensics; forensic accounting; accounting education

1. INTRODUCTION

Increased reliance on both technological and accounting skills has been recognized in research (Albrecht & Sack, 2000; Cory & Pruske, 2012). The increase of digital fraud has led many accountants to acquire advance information technology (IT) skills and certifications in order to qualify as IT auditors and forensic accountants (Davis, Schiller & Wheeler, 2007). As routine accounting tasks are becoming highly automated an accountant's value is more likely to be determined by higher order skills such as those needed in forensic analysis (Hunton, 2002).

A data breach can result in extensive losses in both profits and reputation. The Target data breach that affected as many as 110 million customers received substantial adverse publicity and the total dollar loss is expected to be high (Tsu, 2014). In 2014, hacks were perpetrated on a large number of companies including Neiman Marcus, AT&T, J.P. Morgan and Home Depot (Walters, 2014). In most cases, the attacks compromised confidential and financial information.

Companies may be legally obligated to provide confidentiality. Failure to protect personally identifiable information (PII) may subject the organization to fines and other

penalties. The Gramm-Leach-Bliley Act (GLB) and Health Insurance Portability and Accounting Act (HIPPA) of 1996 stipulate that financial and health organizations are accountable for the safe guarding of PII (Pearson, 2008) and firms that operate abroad may be subject to the European Union Data Protection Directive which places stringent rules on the protection of private information.

Professional and regulatory bodies recognize the value of IT to accountants. The American Institute of Certified Public Accountants (AICPA) recognizes the importance of technology to the organization and to accountants. In its 2013 List of Top 10 Technology Initiatives the AICPA listed Securing the IT Environment, Ensuring Privacy and Preventing and Responding to Computer Fraud as top priorities (AICPA, 2013). The Public Company Accounting Oversight Board (PCAOB) has recommended that auditors receive IT training (O'Donnell and Moore, 2005). An analysis of 595 job listings for IT auditors found that a large percentage specifically mentioned technical skills/abilities including networking, security, database, experience with IT controls, and computer-assisted audit tools and techniques (Merhout & Buchman, 2007). The Sarbanes-Oxley Act of 2002 and Statement on Auditing Standards No. 99 (SAS 99, 2002), "Consideration of Fraud in a Financial Statement Audit," extended expectations for auditors stating that,

> "Electronic evidence often requires extraction of the desired data by an auditor with IT knowledge and skills or the use of an IT specialist ... it may be necessary for the auditor to employ computer-assisted audit techniques ... to identify the journal entries and other adjustments to be tested."
>
> Source: AICPA (2012), p. 6.

The increased sophistication and complexities of information systems have created vulnerabilities that can be exploited to damage organizations by compromising confidential personal information, allowing unauthorized access to sensitive projects and intellectual property, and by concealing financial statement frauds and misappropriation of assets. In order to assess the nature and extent of these threats, to acquire and analyze evidence and to maintain a proper chain of custody, forensic accountants must possess a basic understanding of computer forensic techniques. This paper presents a set of exercises and projects that will be useful to educators creating an introductory course in computer forensics for accountants. This provides an important element in curriculum development and allows students to learn these skills in a hands-on environment. The exercises and projects use widely recognized software that is freely available.

2. COMPUTER FORENSICS FOR ACCOUNTANTS

Nelson, Philips & Steuart (2010) define computer forensics as "The process of applying scientific methods to collect and analyze data and information that can be used as evidence." Thus, computer forensics addresses the methods and procedures necessary to investigate possible criminal and non-criminal conduct involving digital data. From an organizational perspective, investigations should initially proceed with the assumption that the case may be of a criminal nature so that all steps meet the statutory rules for admission of evidence. An

understanding of computer forensics allows the accountant to make knowledgeable decisions regarding what steps to take and how to proceed during an investigation and not taint the evidence.

Computer forensics is considered by some to be dominated by IT and law-enforcement. Although both play important roles, accountants can also be a vital forensic resource. Accountants, in particularly auditors, are highly familiar with corporate information systems (IS), policies and internal controls, and often possess advanced analytical skills. They possess a broad understanding of the overall systems and databases, access rights, organizational roles and responsibilities which are critical to an effective forensic investigation. They are in a positon to recognize the normal routines of organizational agents and to recognize suspicious and unusual activities. IT specialists are primarily concerned with establishing defenses against external attacks and in maintaining and securing the internal environment through authorizations and access rights. Regardless of technical knowledge, organizational agents who inspect digital evidence must be forensically trained or they could taint evidence by opening and inspecting suspect files without first creating a mirror image and following chain-of-evidence procedures. Law-enforcement agents may have priorities that do not parallel and could even conflict with organizational goals. While the organization is most interested in identifying attacks and protecting digital assets, law-enforcement agents are primarily interested in apprehending the perpetrator. They may even seize the organization's computer as evidence. For these reasons, accountants, when properly trained, can provide another forensic asset through a combination of accounting and computer forensics skills that provide a special capability to investigate, analyze and report on suspicious patterns and anomalies and to follow the trail of unauthorized activities (Kearns, 2010).

Larger firms will usually have one or more internal auditors with forensic skills who are responsible for fraud detection and investigation (Pearson & Singleton, 2008). Evidence in most organizational fraud cases is in digital form. With the need for increased vigilance it is imperative that these professionals be able to obtain, manage, and analyze digital forensic data in an effective manner. These accountants need, at minimum, training in the basics of computer forensics.

3. COMPUTER FORENSIC TRAINING

IT is now considered a basic skill for accountants (Hurt, 2007) and most undergraduate accounting students acquire an intermediate level IT competency. Schools accredited by the Association to Advance Collegiate Schools of Business (AACSB) usually include three courses in computer related knowledge and skills. First is an introductory computer class that covers productivity software including word processing, spreadsheets, database, email and slide presentation software. Second is a management information systems (MIS) class that covers the foundations of information resources, system management and security techniques, database concepts and IS management principles. Third is a course in accounting information systems (AIS) that focuses on internal controls for IS, transaction systems, systems design and documentation, system security, computer fraud, and IT governance. The AIS class may also cover advanced spreadsheet and database knowledge and generalized audit

software such as Audit Control Language (Coglitore & Matson, 2007).

Some accounting programs now offer courses in forensic accounting and a few colleges have full programs in forensic accounting. Graduate programs may offer an emphasis or track in forensic accounting in the Masters of Business Administration or Masters of Accountancy programs. The composition of the courses varies depending upon the number of courses offered. Schools that offer a full program or major will have a broader offering than those that only offer an emphasis or track in forensic accounting. Acquiring these skills can increase market appeal particularly for accounting students who wish to work as internal auditors or as IT or fraud auditors or as agents for the FBI, IRS or ATF who are important employers of accounting students. As a result of the increasing need for digital security and the importance of uncovering corporate fraud many universities are also creating courses in computer forensics (Busing, Null & Forcht, 2005/2006).

Forensic accounting represents an integration of accounting, auditing and investigative skills that support the acquisition, maintenance, and analysis of relevant information in a manner that would be acceptable for judicial review and meet the requirements of professional oversight. It also extends to the formulation and presentation of findings in formal reports and court testimony as an expert witness. Forensic accountants command a set of skills that transcends the traditional expectations of accountants. These skills are acquired and enhanced through audit experience and increased investigative training. This allows the forensic accountant to analyze and interpret more complex business and non-business issues in a manner that meets the highest requirements of reliability and integrity. As such, forensic accountants may be employed in a public or private capacity and play important roles in internal auditing departments of banks and insurance companies, governmental and law enforcement agencies, and as self-employed contractors for individuals and attorneys. Thus, the market for forensic accountants and the required skill sets are very well defined.

4. COMPUTER FORENSICS COURSE EXERCISES AND PROJECTS

Forensic accountants are often deficient in their understanding of computer forensics for several reasons. Many schools do not offer such a course because they lack qualified instructors. Also, the topics are not covered on the CPA exam and a large percentage of accounting students plan to acquire a CPA or similar certification such as Certified Management Accountant (CMA) or Certified Internal Auditor (CIA), none of which require the technical skills of computer forensics. Finally, accounting students who plan to take the CPA exam may have to meet the 150 hour rule adopted by many states and may perceive forensic skills as ones they can acquire in the future (Seda, Kramer & Peterson, 2008). Thus, they may not be highly motivated to take a course that does not lead to a professional certification.

This deficiency, however, directly impacts the ability and effectiveness of the forensic accountant and makes him or her more reliant upon IT specialists for all steps requiring computer forensic analysis. Also, students may recognize that computer forensic skills are in-demand and may lead to careers in forensic accounting and IT auditing. Educators who recognize the

importance of computer forensic skills will be interested in exercises and projects that provide the accounting student with basic computer forensic techniques. The exercises and projects that follow introduce several widely recognized software products that are important to forensic analysis. Among other things, these exercises and projects illustrate how fraudsters can hide important information in files, how to inspect files for hidden data, how to acquire images from a suspect drive, how to recover deleted files and how to calculate hash values to insure the integrity of files. A set of student files for the exercises and projects are available upon request from the author. The exercises were performed in-class while the projects were performed by the individual student outside of class.

4.1 Exercise and Project Requirements

The projects use several applications available in demo versions.

1. WinHex Hexadecimal Editor

http://www.x-ways.net/

2. AccessData Forensic Tool Kit

http://accessdata.com/product-download/digital-forensics/forensic-toolkit-ftk-version-5.5

3. ProDiscover

http://www.arcgroupny.com/products/

4. HashCalc

http://www.slavasoft.com/hashcalc/

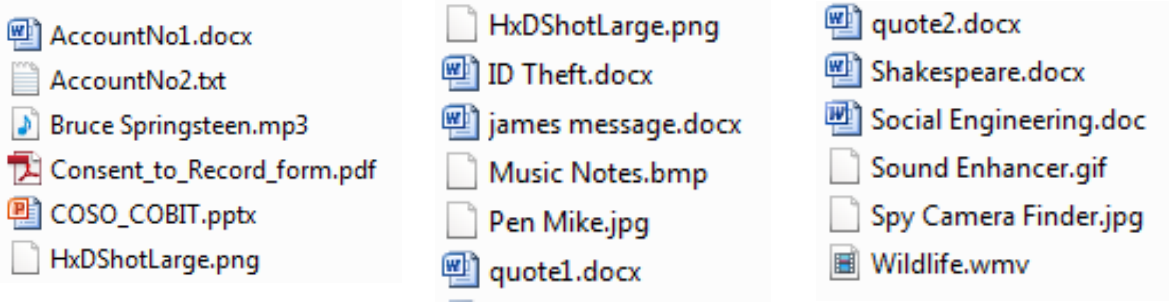
5. Eraser

http://eraser.heidi.ie/

6. OpenPuff Steganography

http://embeddedsw.net/OpenPuff_Steganography_Home.html

The following files are used in the exercises and projects and can be downloaded in zipped format. They should be placed in a work-folder named Projects. These files are available from the author although instructors may choose to create their own project files.



4.2 Computer Forensic Exercises

These exercises are intended to introduce the accounting student to knowledge and skills basic to computer forensics.

Exercise 1: Numbering Systems

Tantamount to the use of forensic software is the knowledge of the binary and hexadecimal numbering systems. All modern numbering systems have two things in common: (1) digits, and (2) placeholders. Each placeholder represents the base raised to a higher power. In the following tables, the second row is the placeholder and the third row is the power to which each value is raised.

Placeholder and Power (Rows 1 and 2 respectively) (Note that the power is always one less than the placeholder.)									
10	9	8	7	6	5	4	3	2	1
9	8	7	6	5	4	3	2	1	0

DECIMAL (Base 10 - Ten digits 0-9)

Placeholder and Power									
10	9	8	7	6	5	4	3	2	1
10^9	10^8	10^7	10^6	10^5	10^4	10^3	10^2	10^1	10^0

Thus, in base 10, the value 8,673 equals:

$8 \times 10^3 + 6 \times 10^2 + 7 \times 10^1 + 3 \times 10^0 = 8{,}000 + 600 + 70 + 3$

BINARY (Base 2 – Two digits 0 and 1)

Placeholder and Power									
10	9	8	7	6	5	4	3	2	1
2^9	2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

Thus, in base 2, the value 1100 1100 equals:

$1 \times 2^7 + 1 \times 2^6 + 1 \times 2^3 + 1 \times 2^2 = 128 + 64 + 8 + 4 = 204_{\text{base10}}$

HEXADECIMAL (Base 16 - Sixteen digits 0-F where A=10, B=11, C=12, D=13, E=14, F=15)

Placeholder and Power									
10	9	8	7	6	5	4	3	2	1
16^9	16^8	16^7	16^6	16^5	16^4	16^3	16^2	16^1	16^0

Thus, in base 16, the value 1A5F equals:

$1 \times 16^3 + 10 \times 16^2 + 5 \times 16^1 + 15 \times 16^0 = 4096 + 2560 + 80 + 15 = 6{,}751_{\text{base10}}$

Student Exercise: Binary and Hexadecimal to Decimal	**Answers (in decimal values)**
Convert each of the following to decimal values.	
1. Binary: 1111	1. 15
2. Binary: 1111 1111	2. 255
3. Binary: 1 0000 0000	3. 256
4. Binary: 1010 1010	4. 170
5. Hex: 123	5. 368
6. Hex: ABC	6. 2748
7. Hex: FF	7. 255
8. Hex: 100	8. 256

Student Exercise: Decimal to Binary and Hexadecimal	**Binary Value**	**Hexadecimal Value**
Convert each of the following to binary and hex.		
1. 88	1. 0101 1000	1. 58
2. 337	2. 0001 0101 0001	2. 151
3. 1,024	3. 0100 0000 0000	3. 400
4. 2,000	4. 0111 1101 0000	4. 7D0

(Note to instructor: Following the exercise refer students to a site that has a binary hex converter such as the one available at http://www.binaryhexconverter.com/)

Exercise 2: Creating Hash Values (Checksums)

A hash, also known as a checksum or message digest, is a value that has no real meaning. Hashes are often used as control values such as the sum of employee id numbers for payroll applications. In accounting and forensics, hash values are created by computer algorithms that create a unique key string for any size of file. In most of our projects we would hash the file before and after testing to insure that the file itself has not been modified in any way.

The file size has no impact on the string length which is determined by the algorithm. In forensics the algorithms, MD5 and SHA256 have been popular. Calculators are readily available. We use HashCalc as shown in Figure 1.

1. Open HashCalc© and note the number of hash types. Open the MS Word file ID Theft.

2. Select the MD5, SHA256 and Tiger hash algorithms. Click Enter.

3. Take a screenshot of the results and add to your Results file and save to your Project_Work folder. See Figure1.

4. Close the ID Theft file.

5. Open the ID Theft file and again select the MD5, SHA256 and Tiger hash algorithms. Click Enter.

6. Compare the results to those from your previous screenshot. They should be the same.

7. At the bottom of the file type OK. Save the file.

8. Open the ID Theft file and again select the MD5, SHA256 and Tiger hash algorithms. Click Enter.

9. Compare the results to those from your previous screenshot. They should be the different.

Note that there are a number of different hashing algorithms and different hash values (aka message digests). MD5 and SHA256 are popularly used algorithms and have been accepted in courts of law.

Exercise 3: Using Command Prompt

IP and MAC Addresses for Windows OS

IP (Internet protocol) addresses are not unique to computers. They identify the node. If you switch computers the IP address remains with the node. However, each computer has a unique identifying number called the MAC (media access control) address. In this exercise you will use the Command Prompt to find your IP and MAC addresses.

On your home computer, go to Accessories / Command Prompt

If the cursor is not on the C: directory, enter the following...

CD\

Then enter ... ipconfig /all

Partial results of the ipconfig /all command appear below. Note the physical address (MAC address) and the IPv4 address. Write down your MAC and IPv4 addresses.


```
Host Name . . . . . . . . . . : client1.microsoft.com
DNS Servers . . . . . . . . . : 10.1.0.200
Description . . . . . . . . . : 3Com 3C90x Ethernet Adapter
Physical Address. . . . . . . : 00-60-08-3E-46-07
DHCP Enabled. . . . . . . . . : Yes
Autoconfiguration Enabled . . : Yes
IP Address. . . . . . . . . . : 192.168.0.112
Subnet Mask . . . . . . . . . : 255.255.0.0
```

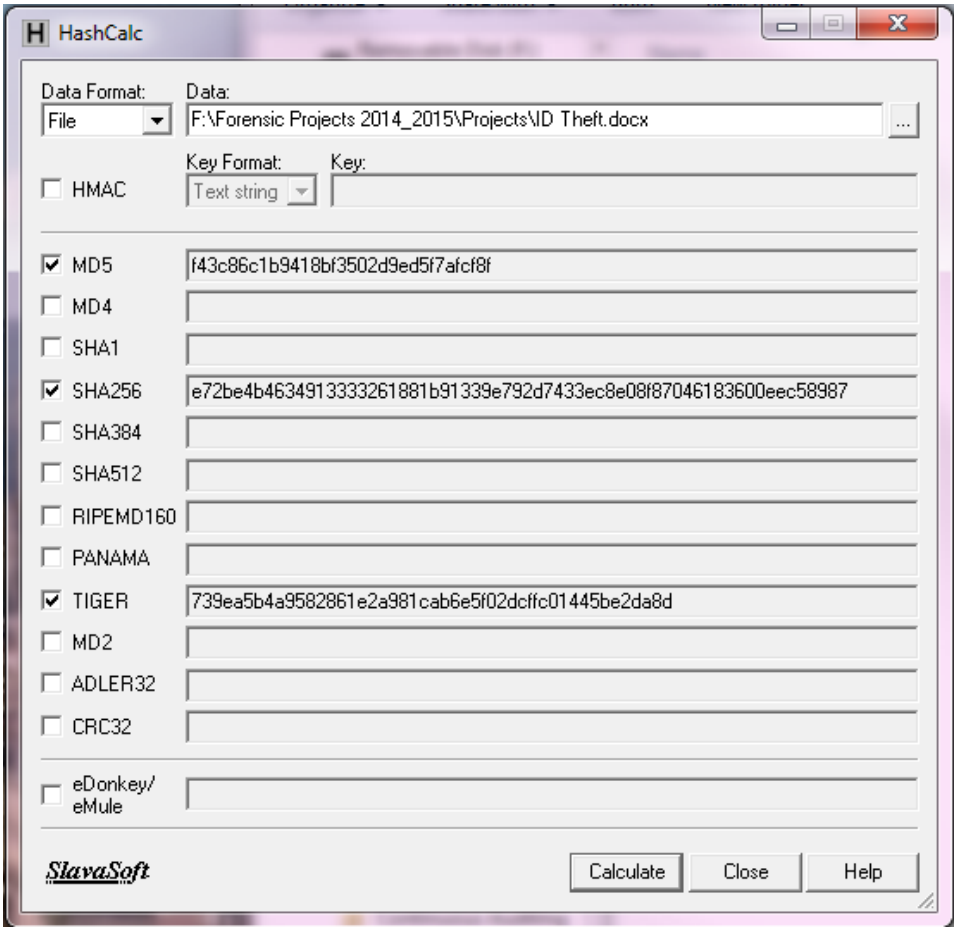


Figure 1. Original Hash Values for ID_Theft.doc

Command Prompt and DOS Commands

At the command prompt attempt the following commands. [ ] is for annotation only.

This assumes the file is on your C: drive. If not, then insert the full path to the file.

Enter the following commands (commands are shown in uppercase to separate them from the file names. Commands can usually be entered in upper or lower case).

C:	[this will take you to the c: drive]
TYPE C:\ Shakespeare.txt	[this will type out the contents of the file]
RENAME C:\ Shakespeare.txt WilliamShakespeare.txt	[renames the file]
MD Projects	[creates a new folder name Projects]
DIR *.*	[lists all files in the current folder: note new folder]
RD Projects	[removes folder named Projects]
DIR *.*	[lists all files in the current folder]
DIR C:\Projects\ *.doc	[lists all .doc files in the Projects folder]

PrintScreen the CommandPrompt window and enter the following command to clear the screen: CLS

Print System Information

Click Start \ Run

type msconfig

In the System Configuration table select Startup and examine what programs are opened when you start your computer. Do you want all of these to open? If not, then deselect the box for unwanted applications.

In the System Configuration table select Tools \ Security Center and click Launch. Click Internet Options and explore the trusted certifications.

PrintScreen the System Information for your computer.

Exercise 4: ASCII and HEX Codes

ASCII (American Standard Code for Information Interchange) is used for storage of all text values in personal computers. In ASCII each letter, digit and special character is represented in eight bits or one byte and a total of 128 different characters can be represented. From the table in Figure 2, insert the code for each item in the table below in its hexadecimal equivalent. Leave a space between each byte. (An extended code, Unicode, is often used in place of ASCII because it allows for more than the 128 characters. However, the right-most 8 bits in Unicode are the same as for ASCII.)

ITEM	ASCII VALUE IN HEX
MI 5	
Microsoft Word	
123 Oak Ave.	
(555) 123-1234	
$50.46	

4.3 Computer Forensic Projects

Forensic Project 1: File Headers and Image Files

Opening files in either NotePad or a hexadecimal (hex) editor provides initial information for examination of files. The investigator can also determine if the file

type is correct. For each file, you will open it in both NotePad and WinHex. In WinHex you will note the first eight bytes in positions 0-7. Each byte will be two characters ranging from 00-FF. These eight bytes often are the signature for the filetype. However, for MS Windows, the signature is the same for Word, Excel and PowerPoint but different for Access. To determine the Microsoft Office filetype you can go to offset hex 512 (200) for doc, xls and ppt files. Figure 3 shows the different signatures for MS Office files. For a more extensive list of file signatures visit Professor Gary Kessler's site at *http://www.garykessler.net/library/file_sigs.html.*

Step 1: Create a work-folder on your personal computer c: drive named Projects.

Step 2: Download and extract the projects.zip from the instructor's web site.

Step 3: Open the following files in both Notepad and WinHex. Determine the file type for each and indicate how you could identify the file type in Notepad and the hex editor. Simply copy the identifying information into the table. If it does not appear to be identifiable then type NI.

ASCII	Hex	Symbol	ASCII	Hex	Symbol	ASCII	Hex	Symbol	ASCII	Hex	Symbol
0	0	NUL	16	10	DLE	32	20	(space)	48	30	0
1	1	SOH	17	11	DC1	33	21	!	49	31	1
2	2	STX	18	12	DC2	34	22	"	50	32	2
3	3	ETX	19	13	DC3	35	23	#	51	33	3
4	4	EOT	20	14	DC4	36	24	$	52	34	4
5	5	ENQ	21	15	NAK	37	25	%	53	35	5
6	6	ACK	22	16	SYN	38	26	&	54	36	6
7	7	BEL	23	17	ETB	39	27	'	55	37	7
8	8	BS	24	18	CAN	40	28	(	56	38	8
9	9	TAB	25	19	EM	41	29	)	57	39	9
10	A	LF	26	1A	SUB	42	2A	*	58	3A	:
11	B	VT	27	1B	ESC	43	2B	+	59	3B	;
12	C	FF	28	1C	FS	44	2C	,	60	3C	<
13	D	CR	29	1D	GS	45	2D	-	61	3D	=
14	E	SO	30	1E	RS	46	2E	.	62	3E	>
15	F	SI	31	1F	US	47	2F	/	63	3F	?

ASCII	Hex	Symbol	ASCII	Hex	Symbol	ASCII	Hex	Symbol	ASCII	Hex	Symbol
64	40	@	80	50	P	96	60	`	112	70	p
65	41	A	81	51	Q	97	61	a	113	71	q
66	42	B	82	52	R	98	62	b	114	72	r
67	43	C	83	53	S	99	63	c	115	73	s
68	44	D	84	54	T	100	64	d	116	74	t
69	45	E	85	55	U	101	65	e	117	75	u
70	46	F	86	56	V	102	66	f	118	76	v
71	47	G	87	57	W	103	67	g	119	77	w
72	48	H	88	58	X	104	68	h	120	78	x
73	49	I	89	59	Y	105	69	i	121	79	y
74	4A	J	90	5A	Z	106	6A	j	122	7A	z
75	4B	K	91	5B	[	107	6B	k	123	7B	{
76	4C	L	92	5C	\	108	6C	l	124	7C	|
77	4D	M	93	5D	]	109	6D	m	125	7D	}
78	4E	N	94	5E	^	110	6E	n	126	7E	~
79	4F	O	95	5F	_	111	6F	o	127	7F	

Figure 2. ASCII Code Source http://ascii.cl/
Tables with extended binary information are available at http://www.ascii-code.com/

Instructions: Insert the identifying code and the hex signatures for each of the files.

File	Filetype	NotePad	Hex Editor
Consent_to_Record_F	.pdf		

orm			
HxDShotLarge	.png		
Sound Enhancer	.gif		
Social Engineering	.doc		
Pen Mike	.jpg		
AccountNo2	.txt		
Bruce Springsteen	.mp3		
Wildlife	.wmv		

Step 4: Open the Social Engineering file in WinHex and change the first eight bytes to resemble a .jpg file. Save the file and then try to open it. What happens? Open it again in WinHex and change the first eight bytes back to their correct values. Save and re-open. It is now back to its original state. This process allows fraudsters to conceal files in plain sight.

Offset	0	1	2	3	4	5	6	7
00000000	D0	CF	11	E0	A1	B1	1A	E1

The above file signature is the same for MS Office doc, xls, and ppt

00000200	EC	A5	C1	00	0F	C0	09	04
00000210	00	00	00	10	00	00	00	00

Signatures for doc, xls, and ppt can be found at offset hex 512 (200). The above is the .doc signature.

Offset	0	1	2	3	4	5	6	7
00000000	50	4B	03	04	14	00	06	00

MS Office docx, xlsx, and pptx all have the file signature shown above.

Figure 3. File Signatures for MS Word, Excel and PowerPoint

Working with Image Files

A basic tenant of forensic investigations is to never work on the original file. First create a mirror image (bit-by-bit copy) and work on the copy. The student will image the contents of a USB drive (the suspect drive) and perform a search on the image file.

Learning Goal(s): Wiping Disks, Creating a USB Image File; Searching an Image File

Software: Eraser, ProDiscover Basic (this can also be performed with FTK Imager)

Files: Shakespeare, james message, ID Theft, quote1, quote2, AccountNo1, AccountNo2, COSO_COBIT, Social Engineering, Sound Enhancer, Pen Mike, Spy Camera Finder,

Instructions: First, you will delete the files on your USB drive and then add the files you wish to have in your image file. Be sure that you have saved your USB files to another drive.

1. Start Eraser and be sure that the correct drive is selected. In settings, choose those for **Pseudorandom 1 Pass** (see Figure 4). Run Eraser.

2. Copy the above files to your USB drive.

3. Start ProDiscover Basic and click **Run Administrator**. In the Launch Dialog box, click the **New Project** tab and enter the project number **Proj01**, and project name **Proj01**.

4. Click **Action** and click **Capture Image**. For Source Drive, select your USB drive. For Destination also select your USB drive. Name the destination file **ForensicProject**. Use your initials for Technician Name and 01 for image number. Click **OK**. This may take several minutes. An image file (**ForensicProject.eve**) will be created which will be a bit-by-bit copy of your USB.

5. Start ProDiscover Basic and click **Run Administrator**. In the Launch Dialog box, click the **New Project** tab and enter the project number: Proj01, and project name:

6. Click **Action** from the menu, point to Add and click **Image File**.

7. In your work folder, click the file **ForensicProject.eve** and then click **Open**. If the Auto Image Checksum message box opens, click **No** (we will not calculate a checksum on this project).

8. In the tree view, click to expand **Content View**, click to expand **Images**, and then click the **pathname** containing your image file. (Files are listed in the work area. See Figure 5).

9. Right-click any file and click **View** – this will start the associated program such as MS Word or Excel. View the file and then exit the program. Try this with several types of files.

10. To search for the keyword "bank" click the **Search** toolbar button (the binoculars icon) to open the Search dialog box.

11. Click the **Content Search** tab. If necessary, click the **ASCII** button and the **Search for the Pattern(s)** option button. Type **bank** in the list box for search keywords. Under Select the Disk/Image(s) click the drive that you are searching and then click **OK**.

12. In the tree view, click to expand **Search Results** and then click **Content Search** results to specify the search type and note the search results in Figure 6.

13. To search all clusters, click the **Cluster Search** tab and search for **bank**. This will take more time because all clusters are being searched. Note the results.

14. Save the project. Click **File, Save Project** from the menu.

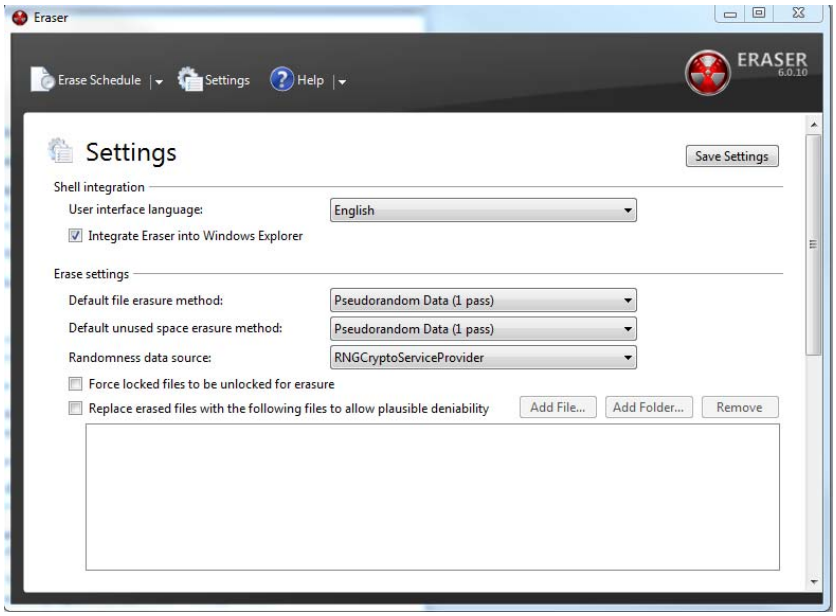


Figure 4. Eraser Settings

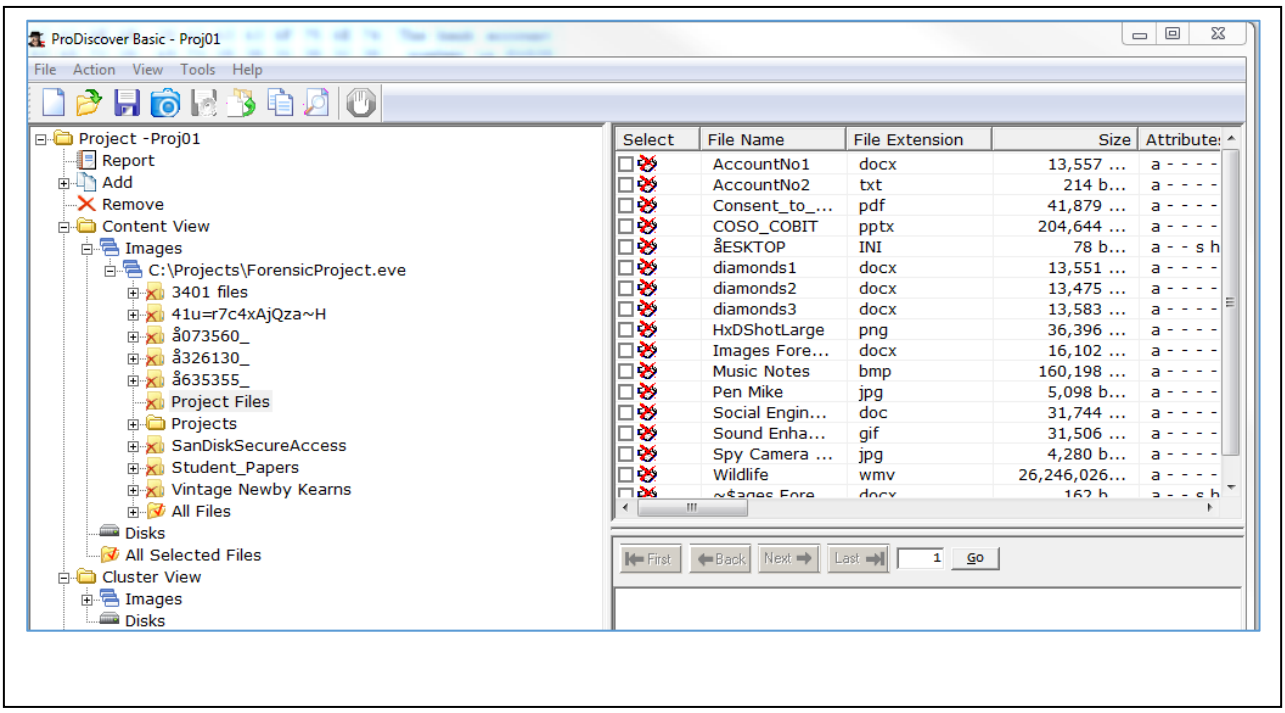


Figure 5. Expanded Path in Content View

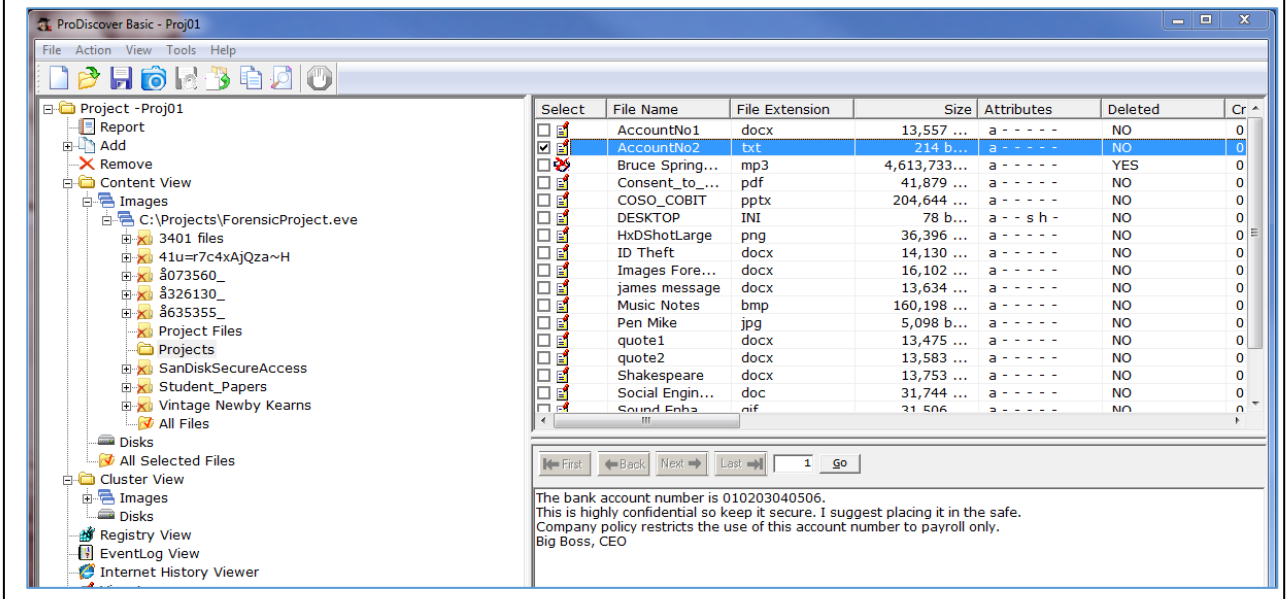


Figure 6. Search for the Term “Bank”

Forensic Project 2: Searching Unix Image Files

Learning Goals: Search a Unix .dd image file for hidden account numbers

Software: ProDiscover Basic (this can also be performed with FTK Imager)

Files: RawFormat.dd

Raw format files are non-proprietary and are often used because they can be viewed in a number of tools.

1. Start ProDiscover Basic and click **Run Administrator.** In the Launch Dialog box, click the **New Project** tab and enter the project number Proj02, and project name Proj02. Click **File, Save Project**.

2. Click **Action** from the menu, point to **Add** and click **Image File**.

3. In your work folder, click the file **RawFormat.dd** and then click **Open**. If the Auto Image Checksum message box opens, click **No** (we will not calculate a checksum on this project). Note that this is a Unix .dd image file.

4. In the tree view, click to expand **Content View**, click to expand **Images**, and then click the pathname containing your image file. (Files are listed in the work area.)

5. Click **View, Gallery View**. Scroll through the graphics files on the drive image. To discover the account numbers you will have to inspect each of these files. In the Add Comment dialog box enter a brief comment and click **OK**. This will add your case notes to the ProDiscover reports.

6. For each file of interest, open the file click the **Search** toolbar button (the binoculars icon) to open the Search dialog box.

7. Click the **Content Search** tab. If necessary, click the **ASCII** button and the Search for the Pattern(s) option button. Type the account number **0102030405** in the list box for search keywords. Under Select the Disk/Image(s) click the drive that you are searching (see Figure7) and then click **OK**.

8. In the tree view, click to expand **Search Results** and then click **Content Search** results to specify the search type and note the search results.

9. To search all clusters, click the **Cluster Search** tab and repeat the search using the account number 0102030405 as the search keyword. Enter notes in the Add Comment dialog box when your search is successful.

10. Click **Report** in the tree view and review the report to insure it is complete. A complete and concise report is critical to the forensic investigation.

11. Click the **Export** toolbar button. In the dialog box click the **RTF Format** button (for rich text) and type **Bank Account Report** in the File Name text box, and then click **OK**. You have now saved the project report.

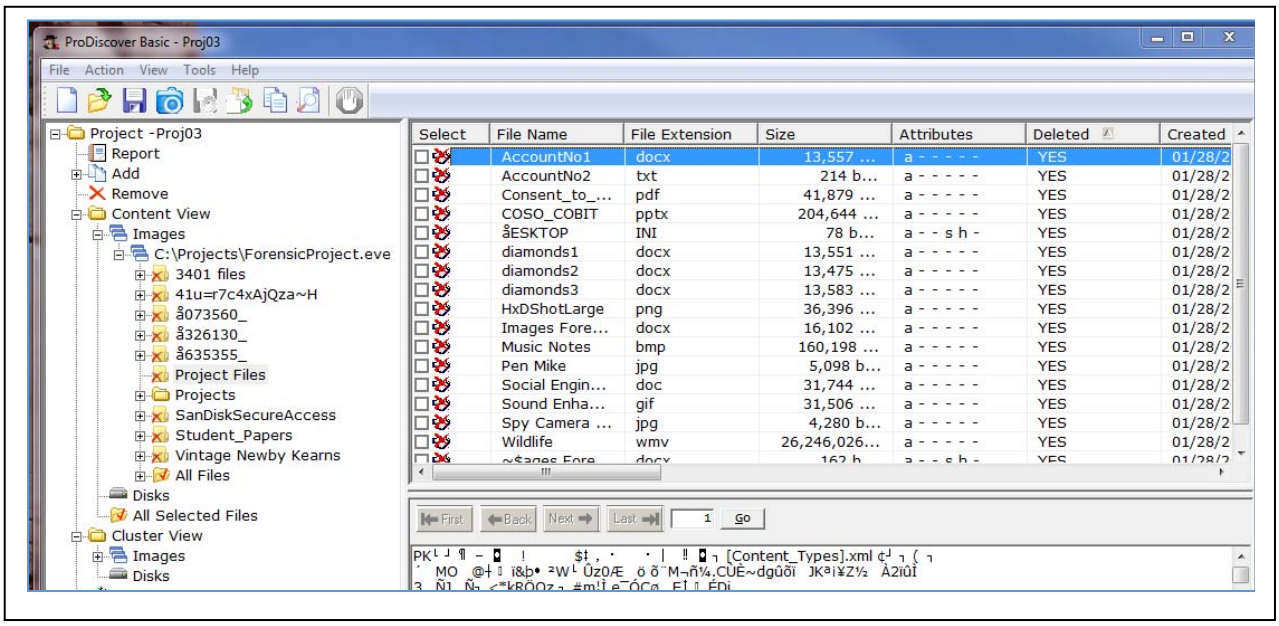


Figure 7. Image File Displayed in Work Area

Forensic Project 3: Extract Allocated and Unallocated Files

Learning Goals: Extract allocated files and unallocated files separately

Software: ProDiscover Basic

Files: ForensicProject.eve

1. Start ProDiscover Basic and click **Run Administrator.** In the Launch Dialog box, click the **New Project** tab and enter the project number **Proj03** and project name **Proj03** . Then click **Open**.

2. In the tree view, click to expand **Add**, click **Image File**. In your work folder, click the **ForensicProject.eve** file and then click **Open** and click **No** in the Auto Image Checksum message box. Save the project to your folder.

3. In the tree view, click to expand **Content View**, click to expand **Images**, and then click the pathname containing the image file. Examine the files displayed in the work area. Under the column heading **Deleted** note that the files are either YES (indicating deleted or unallocated files) or NO (indicating active or allocated files).

4. Sort on the Deleted column by clicking the **Deleted header**.

5. To extract the **allocated files**, right-click each of the files designated as NO in the Deleted Column and click **Copy File**. In ProDiscover Basic this must be performed for each separate file.

6. To extract the **unallocated files**, right-click each of the files designated as YES in the Deleted Column and click **Copy File**. As you click a check-box, the Add Comment dialog box appears. Note the filename and type that has been deleted. (In practice, you would first examine each of these files and add a meaningful comment.)

Forensic Project 4: Creating a USB Write-Blocker

This project creates two desk-top icons that enable or disable writing to USB devices. Students are advised to create a

system restore point before attempting this project.

Learning Goals: Modify the MS Windows Registry; Create a USB Write-Blocker

Software: MS Windows Regedit

1. In the MS Windows Start Search text box, type **regedit** and press **Enter**. This opens the Registry Editor from which you can access system folders and files.

2. In the editor, browse to and click to expand the **\HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet** key.

3. Right-click the **Control** subkey, click **New**.

4. The Registry Editor prompts the user for a key name. Enter **USBDevicePolicy** and press **Enter**. This creates a descendant key.

5. Right-click the **USBDevicePolicy** key, point to **New**, and click **DWORD Value**. If you have an option for 32-bit or 64-bit, click **32-bit**.

6. In the prompt, type **WriteProtect** and press **Enter**.

7. In the key data area, right-click **WriteProtect DWORD** (or just WriteProtect) and click **Modify**.

8. In the Edit DWORD Value dialog box, change the Value Data setting from 0 to 1, and then click **OK** to activate write-blocking to USB devices.

9. Right-click the **USBDevicePolicy** descendant key and click **Export**.

10. In the Export Registry File dialog box, click **Desktop** in the Save in list box. In the filename text box, type **Write Protect USB ON**, and click **Save**.

11. In the registry editor, click **USBDevicePolicy**. In the key data area, right-click **WriteProtect DWORD** and click **Modify**.

12. In the Edit DWORD Value dialog box, change the Value Data setting from 1 to 0 and click **OK** to deactivate write-blocking to USB devices.

13. Right-click **USBDevicePolicy** descendant key again and click **Export**.

14. In the Export Registry File dialog box, click **Desktop** in the Save in list box. In the File name text box, type **Write Protect USB OFF**, and click **Save**. Close the registry editor.

Forensic Project 5: Restoring an Image File to a Drive

Learning Goals: Restore an image file to a drive using the UNIX dd format for raw acquisition.

Software: ProDiscover Basic

Files: ForensicProject.eve

1. Transfer the data from the **ForensicProject.eve** file to the target drive (USB drive). Connect a USB drive to the workstation. Smaller USB drives work best as this exercise writes to the entire drive. I suggest 100-500 MB if available.

2. Start ProDiscover Basic and click **Tools, Copy Disk**.

3. In the dialog box click the **Image to Disk** tab.

4. From the work folder, click the **ForensicProject.eve** file and then click **Open**.

5. In the Copy source disk dialog box click in the **area below Disk Name**.

6. Click the **Disk Name list arrow** and then click the **target drive**, then click **OK**.

7. In the dialog box that opens click Write all 0's and then click **OK**. This begins the data loading and fills the remainder of the drive with 0's.

8. In the completion dialog box click **OK** to terminate loading.

Now you will use the raw acquisition format for creating an image file.

9. On your workstation click the **Write Protect USB ON** icon that you created earlier. This will protect the acquisition drive. Click **Yes** and then **OK** in the confirmation dialog boxes.

10. In ProDiscover Basic click **Action, Capture Image** from the menu.

11. In the dialog box, click the **Source Drive** list arrow and then click **PhysicalDrive1**.

12. Next to the Destination text box, click the >> button and in the Save As dialog box navigate to the work folder and click **Save**.

13. In the **Capture Image** dialog box click the **Image Format** list arrow and click **UNIX style dd** format (for a raw acquisition). Click **OK** to start the acquisition and then click **Proceed** in the warning box. When the acquisition is complete click **OK** in the message box. The raw format creates the acquired file (.dd), a log file (.pds) and a hash file (.md5).

14. Click the **Write Protect USB OFF** button on the workstation desktop and remove the USB. Exit ProDiscover Basic. The suspect files are now imaged on the workstation in UNIX dd format.

Forensic Project 6: Time and Date Information in MetaData

Learning Goals: (a) How to locate time and date information from metadata, (b) How to identify file fragments found in the MFT records which could be found in unallocated disk space or the Pagefile.sys.

Software: ProDiscover Basic

1. Open Notepad and create a text file with the message: Not even computers will replace committees because committees buy computers. Save the file in the work folder as **ForensicProj06A.txt**. Exit Notepad.

2. Start ProDiscover Basic and begin a new project ForProj01A. Click **Action** and then **Add**.

3. In the Add Disk to Project dialog box click **PhysicalDrive0**. Type **c-drive** in the text box and click **Add**. If there is a warning message, click **OK**.

4. In the tree view, click to expand **Content View, Disks, and PhysicalDrive0**. Then click the **C** drive.

5. If necessary scroll down in the work area and right-click **$MFT** and click **Copy File**. In the Save As dialog box, save the file to the work folder. Exit ProDiscover Basic.

6. Start the WinHex hex editor by clicking **Start, All Programs, WinHex**. If there is a warning message box, click **OK**.

7. On the toolbar click **Open** and navigate to the workfolder. Click the **$MFT** file and then **Open**.

8. On the menu, click **Search, Find Text**.

9. In the text box for specifying a search string type **ForensicProj06A.txt**. Click the

Format Code arrow, click **Unicode** and then click **OK**.

10. Right-click the **Data Interpreter** window and click **Options**. In the dialog box, click the **Win32 FILETIME** (64 bit) check box and then click **OK**.

11. Scroll up so that the MFT record label FILE for **ForensicProj06A.txt** is the first line at the top of the hexadecimal and text displays.

12. Click at the beginning of the record, on the letter **F in FILE**, and then drag down and to the right while you watch the hex counter in the lower-right corner. When the counter reaches 50 release the mouse button.

13. Move the cursor to the next byte (one position to the left) and record the date and time of the Data Interpreter's FILETIME values.

14. Exit WinHex.

Forensic Project 7: Conducting a Keyword Search

Learning Goals: Conducting a keyword search

Software: AccessData FTK

1. Start AccessData FTK. Create a new case called **ForProj07** for the case name and number. Click **Next** until the **Add Evidence** and **Case** dialog box appear.

2. Click **Add Evidence**, click **Local Drive** and then click **Continue**.

3. Insure that your USB drive (or local disk drive) and **Logical Analysis** are selected and then click **OK**.

4. In the Evidence Information dialog box click to select your **time zone** and then click **OK**. Click **Next** and then click **Finish**. FTK will process the files and then indicate the evidence items.

5. Click **Search, Tools, Analysis Tools** from the menu, click to select the **Full Text Indexing** check box and then click **OK**.

6. In the search term text box type **Diamond** and then click **Add**. Click the **View Cumulative Results** button and then click **OK** in the Filter Search Hits dialog box. Repeat the search for the terms **Gold**, and **Silver**. The number of hits or occurrences of the search terms will appear under Search Items. (This will not include the items in the file slack space.)

7. Click **Overview, Documents** and then **click**. Scroll the upper-right pane until you see the word '**Diamond**'. Note the logical sector position at the bottom of the upper-right pane.

8. Click the **Search** tab and then click **Live Search**. In the text box, type Diamond and make sure that **ASCII** and **UNICODE** are selected. Click **Add** and then the **Search** button, select **All Files** option and then click **OK**. When the search is complete click **View Results** to see the information displayed at the upper-right.

9. Click the **expand (+) buttons** to find the search results. Scroll in the middle pane until you find 'Diamonds'.

10. Repeat steps 8 and 9 for '**Gold**'.

11. The bottom pane displays details about the data FTK found including each occurrence of the word. Close FTK.

Forensic Project 8: Bit Rotation

One way of hiding information is to place the information in a file using a hex editor and corrupt the file so that it cannot be opened or, when opened, presents garbled data. This can be performed by simply rotating the bits in the file. To repair the file, simply rotate the bits back to their previous position.

Learning Goals: Bit shifting and rotation.

Software: AccessData FTK

Files: AccountNo2.txt

1. Start WinHex and open the file codes.txt.

2. Move the cursor over the toolbar buttons for Shift Left, Shift Right and note that Rotate Left, Rotate Right, Block Shift Left and Block Shift Right are also available. Click **Rotate Right** and **create a screen print** of the results for later comparison. Assume that the data is ordered in little endian. Then click **OK**.

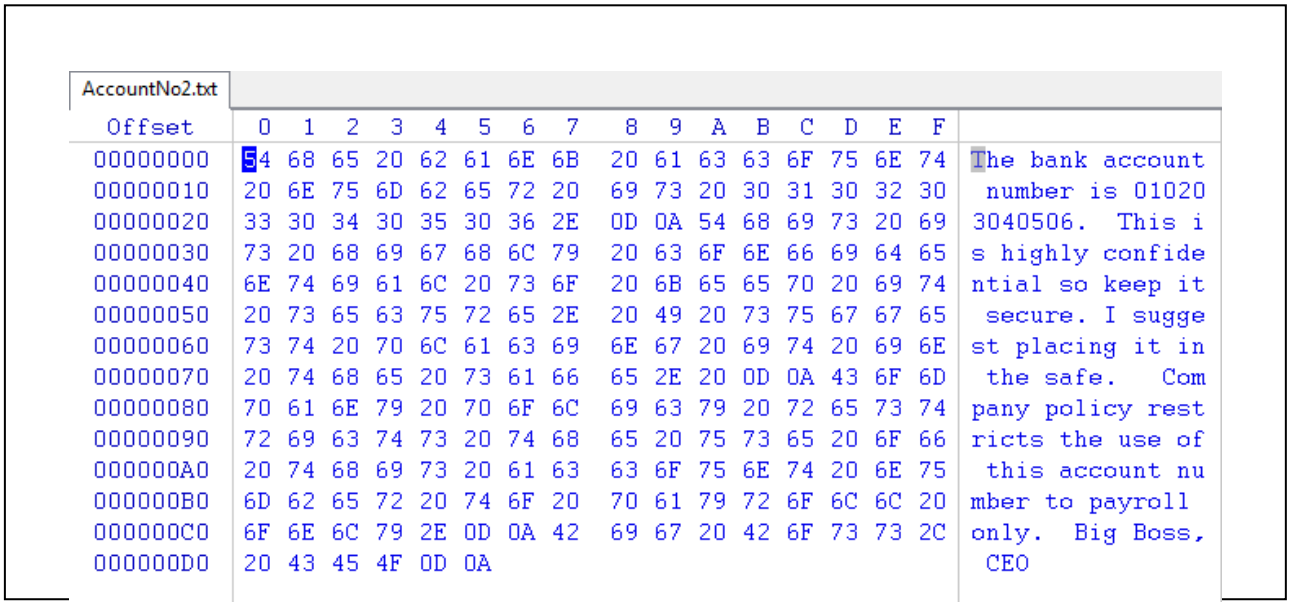
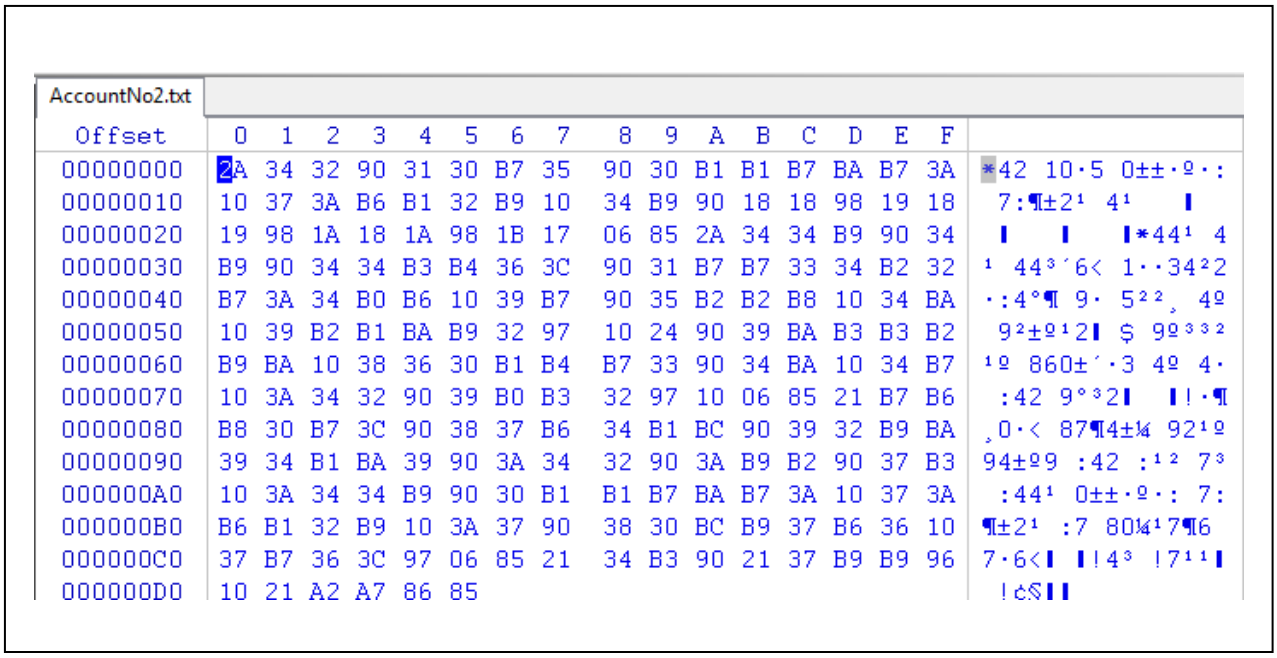


Figure 8. File Before Bit Shifting



AccountNo2.txt

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	2A	34	32	90	31	30	B7	35	90	30	B1	B1	B7	BA	B7	3A
00000010	10	37	3A	B6	B1	32	B9	10	34	B9	90	18	18	98	19	18
00000020	19	98	1A	18	1A	98	1B	17	06	85	2A	34	34	B9	90	34
00000030	B9	90	34	34	B3	B4	36	3C	90	31	B7	B7	33	34	B2	32
00000040	B7	3A	34	B0	B6	10	39	B7	90	35	B2	B2	B8	10	34	BA
00000050	10	39	B2	B1	BA	B9	32	97	10	24	90	39	BA	B3	B3	B2
00000060	B9	BA	10	38	36	30	B1	B4	B7	33	90	34	BA	10	34	B7
00000070	10	3A	34	32	90	39	B0	B3	32	97	10	06	85	21	B7	B6
00000080	B8	30	B7	3C	90	38	37	B6	34	B1	BC	90	39	32	B9	BA
00000090	39	34	B1	BA	39	90	3A	34	32	90	3A	B9	B2	90	37	B3
000000A0	10	3A	34	34	B9	90	30	B1	B1	B7	BA	B7	3A	10	37	3A
000000B0	B6	B1	32	B9	10	3A	37	90	38	30	BC	B9	37	B6	36	10
000000C0	37	B7	36	3C	97	06	85	21	34	B3	90	21	37	B9	B9	96
000000D0	10	21	A2	A7	86	85										

Figure 9. File After Bit Shifting

3. Click **Rotate Left**. In the **Rotate Left Operation** dialog box insure that the settings are the same as in the **Treat Data As for Rotate Right**. Otherwise, the bits will not be shifted equally. Save the file but do not close.

4. Click **Shift Right** and click **OK** twice and note what is happening with the data.

5. Click **Block Shift Left**. Attempt to reverse the procedure by clicking **Block Shift Right**, click **Shift Left** twice and click **OK** as needed.

6. Note that the data is garbled and the procedure has not been reversed. A shift (nonrotated) operation simply drops the bits as they are moved to the right or left and they cannot be recovered. Close the file but do not save. See Figures 8 and 9.

Forensic Project 9: Steganography

Learning Goals: Hide a secret message using steganography.

Software: OpenPuff

Files: chihuly.jpg

1. Copy the chihuly.jpg file and rename chihuly_original.jpg

2. Start the OpenPuff software and click **Hide** (see Figure 10)

3. **Uncheck** boxes **Enable [B] [C]** and enter an **8 bit password** in box [A] (see Figure 11)

4. In (2) browse to the Projects folder and select AccountNo2.txt (this contains your secret message)

5. In (3) click **Add** and browse to the chihuly.jpg file (this will be the carrier file)

6. In (3) click **Hide Date** (the contents of AccountNo2.txt is hidden in the chihuly.jpg file)

7. Save to another location as chihuly.jpg and then rename chihuly2.jpg.

8. Close OpenPuff and click **Unhide** and enter your password. In (3) open the chihuly2.jpg file.

9. A text file containing the hidden message will appear on the desktop.

10. You may wish to open both the original and converted jpg images to see if you can discern a difference. They look exactly the same. One, however, contains a hidden message.

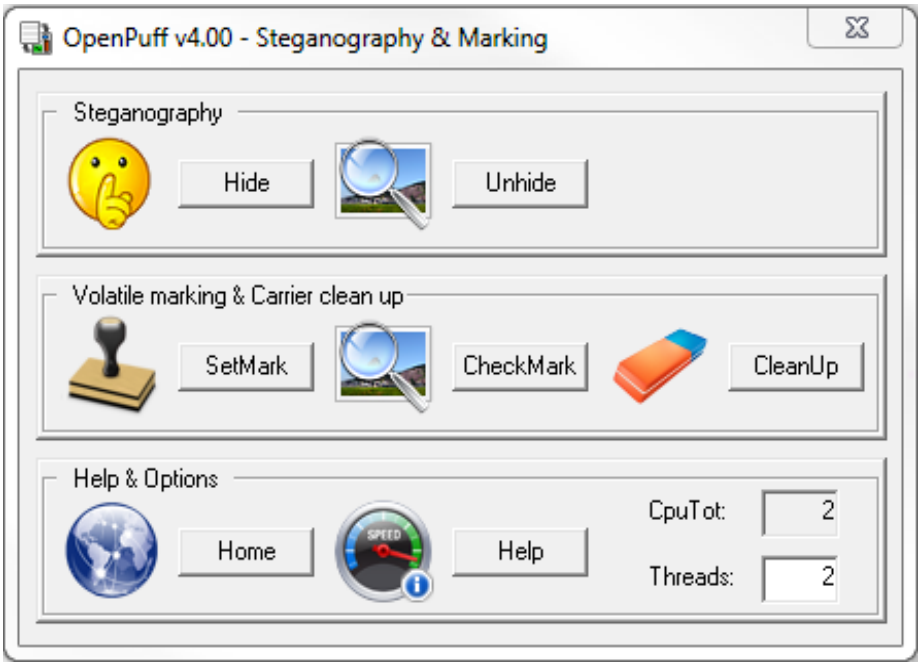


Figure 10. Chihuly.jpg file before Encoding

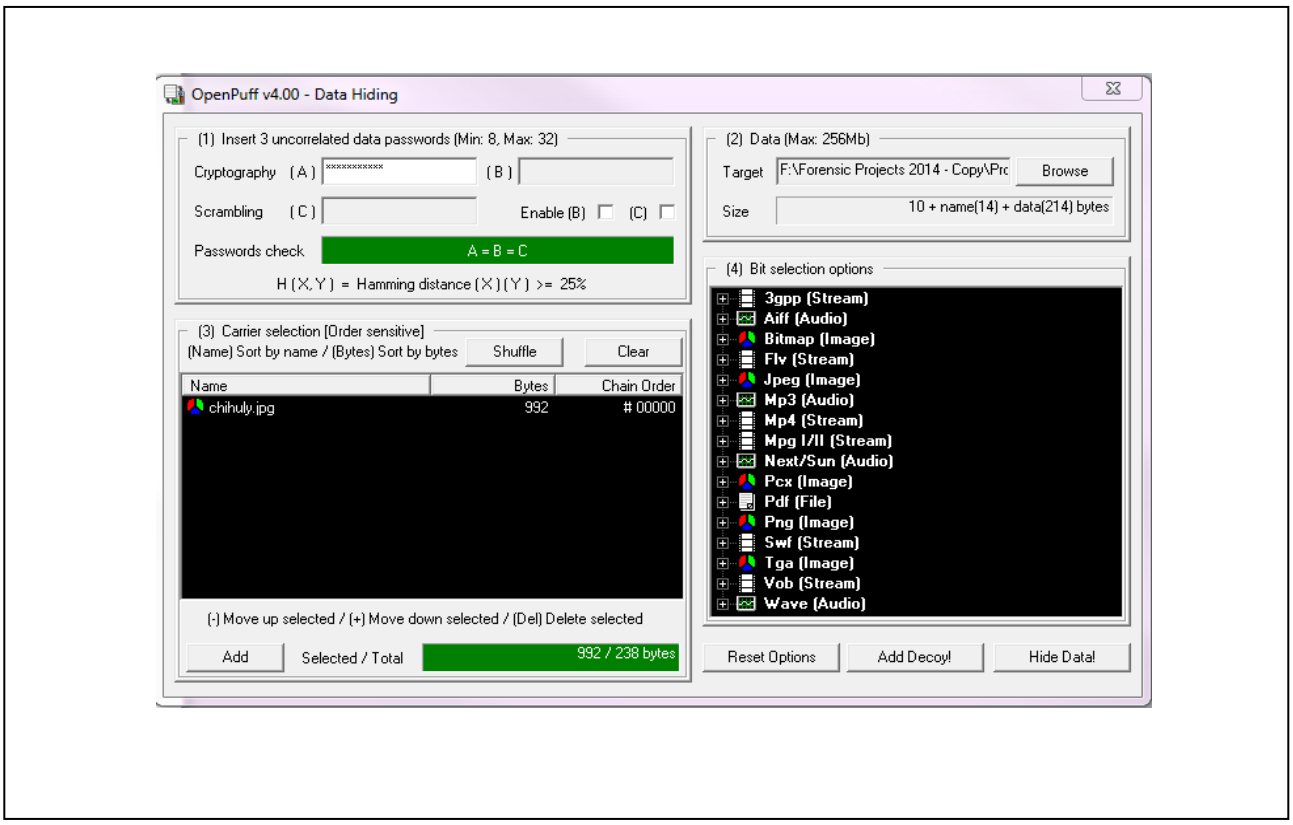


Figure 11. Adding Message to the File

Figure 12. Chihuly.jpg File Containing Hidden Message

5. DISCUSSION AND CONCLUSIONS

This paper addresses the need for computer forensics education for accounting students. While the forensic accounting profession continues to grow, most accounting students do not have exposure to a class in computer forensics. To be effective, it is essential that forensic accountants be knowledgeable of and

able to apply basic computer forensic skills. Forensic knowledge increases the ability to recognize and uncover fraud and helps meet the increased expectation for auditors in recognizing and uncovering fraud. These skills are important to accountants considering a career in auditing and especially IT auditing. They should also be useful in gaining entry-level positions with federal agencies such as the FBI, IRS and ATF that often use accountants to analyze computer files and digital devices.

The purpose of this paper is to present the educator with a number of exercises and projects that provide the accounting student with skills important to careers as forensic accountants and IT auditors. While students may not emerge from this course as experts in computer forensics they will develop a competence that is important to the organization. These skills can be extended in a variety of ways through pursuing advanced education in college courses, workshops and self-study tutorials.

REFERENCES

American Institute of Certified Professional Accountants (AICPA) (2013). AICPA top 10 tech. Retrieved from http://www.accountingtoday.com/gallery/AICPA2012-Top-10-Technology-Initiatives-62024-1.html

AICPA Forensic and Valuation Services Section Task Force (2012) Computer Forensic Services and the CPA Practitioner, p. 6. Retrieved from http://www.aicpa.org/InterestAreas/ForensicandValuation/Resources/PractAidsGuidance/DownloadableDocuments/Computer%20Forensic%20Services%20and%20the%20CPA_Final.pdf

Busing, M.E., Null, J.D. & Forcht, K.A. (2005/2006). Computer forensics: the modern crime fighting tool. The Journal of Computer Information Systems, 46(2), 115-119.

Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, (3rd ed.). Maryland Heights, MO: Elsevier Science & Technology/Syngress.

Coglitore, F.J. & Matson, D.M. (2007). The use of computer-assisted auditing techniques in the auditing course: further evidence. Journal of Forensic Accounting, VIIII, 201-226.

Cory, S.N. & Pruske, K.A. (2012). Necessary skills for accounting graduates: an exploratory study to determine what the profession wants. Proceedings of the American Society of Business and Behavioral Sciences Conference, Las Vegas, NV, 19(1), 208-218.

Davis, C., Schiller, M. & Wheeler, K. (2007). IT Auditing. New York, NY: McGraw-Hill.

Hall, J. & Singleton, T. (2005). Information Technology and Assurance, (2nd ed.). Thomson South-Western, Mason, OH.

Hurt, B. (2007). Teaching what matters: a new conception of accounting education. Journal of Education for Business, 82(5), 295-299.

Kearns, G. (2010). Computer forensics for graduate accountants: a motivational curriculum approach. Journal of Digital Forensics, Security and Law, 5(2), 63-83.

Merhout, J. W. & Buchman, S. E. (2007). Requisite skills and knowledge for entry-level IT auditors. Journal of Information Systems Education, 18(4), 469-477.

Nelson, B., Phillips, A., & Steuart, C. (2010). Guide to Computer Forensics and Investigations, (4th ed.). Boston, MA: Cengage/Course Technology.

O'Donnell, J. & Moore, J. (2005). Are accounting programs providing fundamental IT control knowledge? The CPA Journal, 75(5), 64-66.

Pearson, T. A. & Singleton, T. W. (2008). Fraud and forensic accounting in the digital environment. Issues in Accounting Education, 23(4), 545-559.

Sammons, J. (2012). The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. Maryland Heights, MO: Elsevier Science & Technology/Syngress.

SAS 99 (Statement on Audit Standards 99: Consideration of Fraud in a Financial Statement Audit) (2002). Retrieved from

http://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AU-00316.pdf

Seda, M., Kramer, B. & Peterson, K. (2008). The emergence of forensic accounting programs in higher education. Management Accounting Quarterly, 9(3), 15-23.

Tsu, T. (January, 2014). Target traces data breach to credentials stolen from vendor. Los Angeles Times. Retrieved from http://www.latimes.com/business/money/la-fi-mo-target-data-breach-vendor-20140129,0,8026.story#axzz2rzEFEbhQ

Walters, R. (2014). Cyber attacks on U.S. companies in 2014. The Heritage Foundation. Retrieved from http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014

