Hands on Demonstration

Cybercrime Training Lab 1 Symposium on Cybersecurity & Information Assurance at FDU May 1st 2013 30 minutes Elly Goei (3 PM -3:30PM)

30 minutes (3:30 PM- 4 PM) Professor Eamon P. Doherty Ph.D., CPP, CCE, SSCP

Disclaimer

 This set of slides is for academic purposes only. The techniques showed in this slide set are only one possible set of methods that could be done during an investigation and should only be done in an authorized policy investigation or a law enforcement investigation by qualified authorized individuals.

Eamon Doherty Ph.D., CCE, CPP, SSCP

- Dr. Eamon Doherty is the Cybercrime Training Lab Director as well as an associate professor in Petrocelli College of Continuing Studies at Fairleigh Dickinson University (FDU).
- Dr. Doherty has also created three 1/2 day classes for law enforcement officers and security practitioners and published a variety of those class materials made during a Department of Justice grant. These classes are "PDA Forensics", "Cell Phone Forensics", and "Introduction Electronic Eavesdropping Device and Wiretap Detection."

Eamon P. Doherty Ph.D., CCE, CPP, SSCP Why Get Certifications?

- CCE is Certified Computer Examiner
- SSCP Systems Security Certified Practitioner
- CPP Certified Protection Professional

• Certifications are important for when you go to court and a jury needs to be able to believe you know what you are talking about with regard to digital forensics.

Welcome to Today's Presentation

• I will demonstrate and speak about the following:

- 1. Metadata in Pictures
- 2. Permission to Examine Computers
- 3. Chain of Custody
- 4. Recovering a Password
- 5. Creating a Forensic Image of a Drive

Permission is Needed

We cannot just take a camera and look at its contents. We need to have permission or authority to view the contents.

1. Search Warrant is needed in law enforcement investigation

2. Policy investigation – camera is owned by school or corporation, no expectation of privacy by person using camera

3. Consent – Consent was given by camera owner

Chain of Custody Form

• Any investigation could result in findings that lead to a criminal investigation so it is best to:

- Document everything,
- Don't allow evidence out of your sight
- Use a chain of custody form
- Use a Paraben Faraday Bag

Consultants

- If you are not sure of how to do this, get a consultant and get advice from:
- IACIS
- HTCIA
- ASIS International
- Kroll Ontrack

Report Writing

• Please be objective on your reports.

 Please look for evidence to find people innocent (exculpatory evidence) and evidence for use in supporting an allegation.

Digital Picture Forensics Dr. & Mrs. Doherty – Where?



View Meta Data Inside Picture X

Albany-20120623-00632.jpg Properties

eneral Security Deta	ails Novell Version Previous Version	s
Property	Value	*
Flash maker		
Flash model		
Camera serial number		
Contrast		
Brightness		
Light source	Unknown	
Exposure program		
Saturation		
Sharpness		
White balance		
Photometric interpretat	tion	
Digital zoom		Ξ
EXIF version	0220	
GPS		-
Latitude	42; 38; 32.39999999999398	
Longitude	73; 44; 59.099999999765	
Altitude	48	
-		Ŧ
Remove Properties and	Personal Information	
	OK Cancel Ap	olv

MetaData – Right Click on Picture, Select Properties – Camera Details

neral Security Details	Novell Version Previous Versions	l.
Property	Value	*
Image		
Image ID		
Dimensions	1792 x 1344	
Width	1792 pixels	
Height	1344 pixels	111
Horizontal resolution	72 dpi	100
Vertical resolution	72 dpi	
Bit depth	24	
Compression		
Resolution unit	2	
Color representation	sRGB	
Compressed bits/pixel		
Camera		
Camera maker	Research In Motion	
Camera model	BlackBeny 9700	
F-stop	enzana di kemperatakan badalakan dikerdan terdikan ker	
ISO speed		
Exposure bias		Ŧ
amova Properties and Pr	monal Information	
lemove Properties and Pe	sisonal momation	

Create Map with www.gpsvizualizer.com



A Password Protected File May Need to Be Opened in an Investigation

• <u>Brute Force Attack</u> Can Be Used (every combination of characters and numbers) it is good if your computer uses an NVDIA Card which acts like another CPU or computer

<u>Dictionary Attack</u> – Tries every word in the dictionary. Hundreds of languages are available.

Advanced Office Password Recovery From Elcomsoft Can Be Used

			5120	10400	
			Pages	6	
	Permissions Anyone can open, copy, and change any part of this document.		Words	2784	
			Total Editing Time	0 Minutes	
Protect			Title	UNIT 2 – Com	
Document *		Encrypt Document	_? <mark>_</mark> >	🛀 i a tag	
		Encrypt the contents of this file		d comment	
Check for Issues • Before sharing this Document pro Characters for Content that c		Password:			
	Prepare for Sharing	•••			
	 Before sharing this file, be aware that it contains: Document properties and author's name Characters formatted as hidden text Content that cannot be checked for accessibility 	Caution: If you lose or forget the password, it cannot be recovered. It is advisable to keep a list of passwords and their corresponding document names in a safe place. (Remember that passwords are case-sensitive.)			
	current file type		OK Cancel	ulty	
	Versions				
	3 There are no previous versions of this file		Last Modified By	FDUUSER	

Forensic Image of a Drive

We need to make an exact byte for byte copy and verify it with an MD5 Hash.

1. The forensically wiped drive goes inside the Logic Cube Device.

2. The suspect's drive connects on the outside of the Logic Cube.

3. The investigator creates an exact copy of the suspect's drive and the drives are verified to be the same with an MD5 Hash.



Use Helix to Image a Drive

- 1. Please put the CD with Helix in the live system.
- 2. Please Run Helix and connect an external USB Drive.
- The destination is the external USB SSD Flash drive and the source is the suspect's hard drive.
- 4. Please select "Acquire" and create the image of memory or a disk drive.
- 5. The original drive is preserved, the copy is examined.



The End

Thank you for attending the presentation.