



Evidence Solutions, Inc.

And the

2018 Cruise to Learn
hosted by
Mississippi Legal Professionals Association

Present:

You Can do that?

February 08, 2018

Presented by:

Scott Greene, SCFE, CEO

Evidence Solutions, Inc.

A Digital Forensics Firm

866-795-7166

Scott@EvidenceSolutions.com



Biography

Scott Greene

Scott is the CEO of Evidence Solutions, Inc. Scott Greene has been doing Data Recovery, Computer, Technology and Digital Forensics, and EDiscovery work for over 35 years.

Directly out of high school, Scott went to work for IBM as a programmer.

In 2008 he created Evidence Solutions, Inc., a full service Computer, Technology & Digital Forensics firm, from the Technology Forensics department of Great Scott Enterprises.

Scott has developed and presented strategic planning seminars, taught numerous classes in database design & optimization, cyber security and technology forensics. Scott's extensive knowledge draws clients to him from all over the United States as well as Internationally for consulting and expert witness services in the field of Technology, Computer & Digital Forensics. His extensive and diverse experience allows him to be an expert in many facets of computer & digital technology.

Scott and Evidence Solutions have been involved in Civil & Criminal Cases, for Plaintiff, Defense and Special Master in Justice, Superior & District Courts as well as Internationally.

He is a sought after speaker and educator and travels throughout the country presenting to local, regional, national and International organizations.

Computer, Technology, and Digital Forensics for Over 35 Years.

www.EvidenceSolutions.com

Scott@EvidenceSolutions.com

Box 42047;Tucson, Az 85733

866-795-7166

You Can Do That? 2019 Cruise to Learn hosted by Mississippi Legal Professionals Association

Faculty:

Scott Greene

Evidence Solutions, Inc.

Scott@EvidenceSolutions.com

www.EvidenceSolutions.com



Evidence Solutions, Inc. Digital Forensics Expert Witness

Famous Quote

- ▶ "I think there is a world market for maybe five computers." -- *Thomas Watson, chairman of IBM, 1943*
- ▶ Today there are: over 1 billion PC type machines.



Evidence Solutions, Inc. Digital Forensics Expert Witness

GENERAL COMPUTER FORENICS



Evidence Solutions, Inc. Digital Forensics Expert Witness

Digital Forensics Expert Witness

Presented by Scott Greene, Senior Digital Forensics Examiner

Evidence Collection Sources of Evidence:

- ▶ Storage Media includes:
 - Hard Disk Drives
 - Backup tapes
 - DVD / CD Rom disks
 - E-prom and Memory chips
 - Thumb Drives
 - iPods, iPads & MP3 Players
 - Cell Phones
 - The Cloud
 - Infotainment Systems



Evidence Solutions, Inc. Digital Forensics Expert Witness

Evidence Collection

- ▶ Storage Media
 - Because data is easily destroyed, when the data arrives at the lab, the first priority of the investigator is to preserve integrity of the evidence.
 - Just turning on the machine and allowing the system to boot, will cause irreparable changes to the data.....



Evidence Solutions, Inc. Digital Forensics Expert Witness

Evidence Collection

- **Hard Drive Image**
or
Mirror Image
or
Forensic Image:
- This is a bit-by-bit copy of storage media. (i.e., an exact copy of a physical Hard Drive).



Evidence Solutions, Inc. Digital Forensics Expert Witness

Evidence Collection

▶ Hash or Digital Fingerprint:

- ▶ A hash value is a unique hexadecimal value identifying lines of text, a file or Hard Drive Image. The value serves as an identifying fingerprint, and is even more unique than human DNA. The value is generated via mathematical algorithm; the de facto algorithm still used is Message Digest-5, or MD5 for short. Others include SHA-1, SHA-256, etc.



Evidence Solutions, Inc. Digital Forensics Expert Witness

Evidence Collection / Hashes

- ▶ “The quick brown fox jumps over the lazy dog”
 - 9e107d9d372bb6826bd81d3542a419d6
- ▶ “The quick brown fox jumps over the lazy cog”
 - ffd93f16876049265fbaef4da268dd0e



Evidence Solutions, Inc. Digital Forensics Expert Witness

How Data is Stored

▶ Slack Space or File Slack:

- ▶ Slack space refers to portions of a hard drive that are not fully used by a current file and which may contain data from a previously deleted file.



Evidence Solutions, Inc. Digital Forensics Expert Witness

How Data is Stored

▶ **Free Space or Unallocated Space:**

- The area of a data storage device that is available for more data storage. Unallocated space is where deleted but recoverable data may be found



Evidence Solutions, Inc. Digital Forensics Expert Witness

File Dates

▶ **Date Created:**

- The date and time that this file was created on this machine, this would include the date downloaded from the Internet.

▶ **Date Modified:**

- The date and the time the file was last modified. This may also include downloading from the Internet. This date normally follows the file around and doesn't change unless the file changes.

▶ **Date Accessed:**

- This is the last date that the file was accessed for reading by the machine or user.



Evidence Solutions, Inc. Digital Forensics Expert Witness

INFOTAINMENT SYSTEMS



Evidence Solutions, Inc. Digital Forensics Expert Witness

Infotainment Systems



Evidence Solutions, Inc. Digital Forensics Expert Witness

Infotainment Systems

- ▶ BMW
- ▶ Buick
- ▶ Cadillac
- ▶ Chevrolet
- ▶ Chrysler
- ▶ Dodge
- ▶ FIAT
- ▶ Ford
- ▶ GMC
- ▶ HUMMER
- ▶ Jeep
- ▶ Lincoln
- ▶ Maserati
- ▶ Mercury
- ▶ Pontiac
- ▶ Ram
- ▶ Saturn
- ▶ SEAT
- ▶ Skoda
- ▶ SRT
- ▶ Toyota
- ▶ Volkswagen



Evidence Solutions, Inc. Digital Forensics Expert Witness

Infotainment Systems

- ▶ **Vehicle/System Information**
 - Serial Number
 - Part Number
 - Original VIN Number
 - Build Number
- ▶ **Installed Application Data**
 - Weather
 - Traffic
 - Facebook
 - Twitter
- ▶ **Connected Devices**
 - Phones
 - Media Players
 - USB Drives
 - SD Cards
 - Wireless Access Points
- ▶ **Navigation Data**
 - Tracklogs and Trackpoints
 - Saved Locations
 - Previous Destinations
 - Active and Inactive Routes
- ▶ **Device Information**
 - Device IDs
 - Calls
 - Contacts
 - SMS
 - Audio
 - Video
 - Images
 - Access Point Information



Digital Forensics Expert Witness

Evidence Solutions, Inc. Digital Forensics Expert Witness

Presented by Scott Greene, Senior Digital Forensics Examiner

Infotainment Systems

▶ Events

- Doors Opening/Closing
- Lights On/Off
- Bluetooth Connections
- Wi-Fi Connections
- USB Connections
- System Reboots
- GPS Time Syncs
- Odometer Readings
- Gear Indications



Evidence Solutions, Inc. Digital Forensics Expert Witness

CELL PHONES



Evidence Solutions, Inc. Digital Forensics Expert Witness

▶ Cell Phones & Tablets

- Text messages
- Photos?
 - GeoTagging
- Calendars
- Phone Books
- Call Logs
- Complete information about where the phone has been....

• Digital Evidence: Cell Phone Forensics



Evidence Solutions, Inc. Digital Forensics Expert Witness

Digital Forensics Expert Witness

Presented by Scott Greene, Senior Digital Forensics Examiner

- ▶ Cell Phones & Tablets
 - Browsing History
 - Documents
 - Email accounts
 - Online data storage accounts

Digital Evidence: Cell Phone Forensics



Evidence Solutions, Inc. Digital Forensics Expert Witness

03/01/12 0709 SMS-Inbox
03/01/12 0710 SMS-Inbox
03/01/12 0714 Texting
03/01/12 0715 SMS-Sent
03/01/12 0717 SMS-Inbox
03/01/12 0718 SMS-Sent
03/01/12 0719 SMS-Inbox
03/01/12 0759 In Service
03/01/12 0813 Texting
03/01/12 0814 SMS-Sent
03/01/12 0905 In Service
03/01/12 0915 Driving
03/01/12 0958 SMS-Inbox
03/01/12 1008 In Service
03/01/12 1042 Driving
03/01/12 1125 In Service
03/01/12 1225 In Service
03/01/12 1240 SMS-Inbox

Item	Date	Time	Origination	Termination	Elapsed Time	Number	IMEI	IMEI	Description
1	01/01/11	05:30A	0:22		0:00	35349104165348	310410366057466		m2W_DTR
2	01/01/11	05:37A	0:42		0:04		310410366057466		m2W
3	01/01/11	05:37A	0:27		0:06		310410366057466		m2W
4	01/01/11	09:09A	0:10		4:42	35349104165348	310410366057466		m2W_DTR
5	01/01/11	09:31A	0:08		3:22	35349104165348	310410366057466		m2W_DTR
6	01/01/11	09:35A	0:05		1:05	35349104165348	310410366057466		M2O_DTR
7	01/01/11	09:38A	0:05		0:47	35349104165348	310410366057466		M2O_DTR
8	01/01/11	09:40A	0:23		0:06	35349104165348	310410366057466		M2O_DTR
9	01/01/11	09:42A	0:08		0:31	35349104165348	310410366057466		M2O_DTR
10	01/01/11	09:45A	0:01		0:00	35349104165348	310410366057466		M2O_DTR



Evidence Solutions, Inc. Digital Forensics Expert Witness

Artifacts From Web Browsing

- ▶ The value of seeing what a person is searching for in the Internet can be key.



Evidence Solutions, Inc. Digital Forensics Expert Witness

Artifacts From Web Browsing

- ▶ http://wiki.answers.com/Q/How_can_you_help_a_sociopath?#slide=59
- ▶ How can you help a sociopath? – Answers.com



Evidence Solutions, Inc. Digital Forensics Expert Witness

Artifacts From Web Browsing

- ▶ <http://www.subito.it/appartamenti/appartamento-a-grutti-di-gualdo-cattaneo-rif-301-perugia-77278016.htm>
- ▶ Appartamento in castello di Grutti – Appartamenti In vendita a Perugia



Digital Forensics Expert Witness

Evidence Solutions, Inc. Digital Forensics Expert Witness

Presented by Scott Greene, Senior Digital Forensics Examiner

Artifacts From Web Browsing

- ▶ http://mysecurewallet.nl/payment/islive/isliveeu/?p=199&pi=typein_isliveeu&flash=1&mbellaluna
- ▶ My Secure Wallet



Evidence Solutions, Inc. Digital Forensics Expert Witness

SOCIAL MEDIA



Evidence Solutions, Inc. Digital Forensics Expert Witness



LinkedIn



Evidence Solutions, Inc. Digital Forensics Expert Witness


Digital Forensics Expert Witness

Presented by Scott Greene, Senior Digital Forensics Examiner

The statistics of need In 30 seconds.....

- LIKES AND COMMENTS ON FACEBOOK: > 1,185,186
- APPLE AND ANDROID APP DOWNLOADS: > 493,827
- TWEETS SENT ON TWITTER: > 64,814
- VIDEOS WATCHED ON YOU TUBE: > 831,928
- SEARCHES MADE ON GOOGLE: > 940,741
- PHOTOS UPLOADED TO FACEBOOK : > 111,110
- EMAILS SENT GLOBALLY : > 106,888,890

...and they're all DISCOVERABLE!



Evidence Solutions, Inc. Digital Forensics Expert Witness

The statistics of need


- There are over:
 - 800 million Facebook users
 - 300 million people using Twitter
- Evidence from social media sites can be relevant to almost every litigation dispute and investigation matter.



Evidence Solutions, Inc. Digital Forensics Expert Witness

The statistics of need:

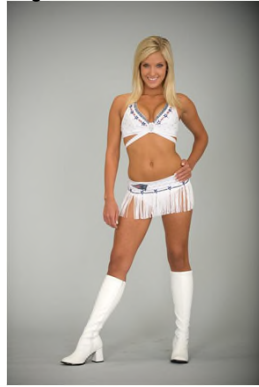
- Social media evidence is:
 - widely discoverable
 - generally not subject to privacy constraints when established to be relevant to a case, particularly when that data is held by a party to litigation or even a key witness.



Evidence Solutions, Inc. Digital Forensics Expert Witness

Here is what is out there

- ▶ New England Patriots Cheerleader, Caitlin Davis, 18



Evidence Solutions, Inc. Digital Forensics Expert Witness

Here is what is out there

Caitlin lost her job after photos appeared on Facebook showing her holding a Sharpie marker up to a passed out man with offensive graffiti all over him. Davis was booted from the Patriots squad.



Evidence Solutions, Inc. Digital Forensics Expert Witness

Here is how they use it...

Charlie Barrow's Profile Oxford



Charlie Barrow	Oxford Alum '06 London Share ↕
Sex:	Male
Birthday:	May 24, 1984
Hometown:	London, England
▶ Mini-Feed	
▼ Information	
Contact Info	
Current Address:	Soho
Website:	http://www.cant-touch-this.co.uk/morning...
Personal Info	
Favorite Quotes:	"Hey Slim, I just drank a fifth of vodka, dare me to drive?"
	"per sidora kuro, per superos et si qua fides telure sub ima est, invitus, regno, tuo de libere ceso!"

"Hey Slim, I just drank a fifth of vodka, dare me to drive?"



Evidence Solutions, Inc. Digital Forensics Expert Witness

Here is how they use it....



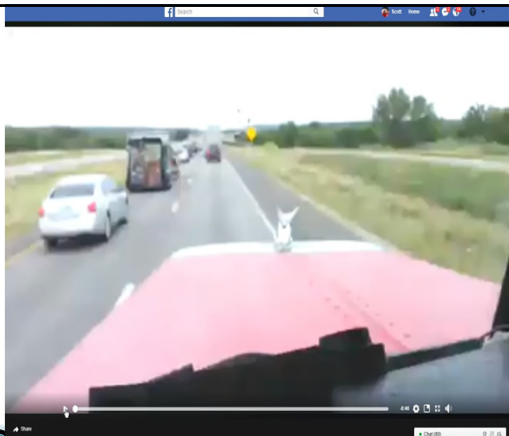
- ▶ A juror posted details of the case she was serving on. The she wrote, "I don't know which way to go, so I'm holding a poll."
- ▶ An anonymous tip resulted in the woman being immediately dismissed from the jury.



Evidence Solutions, Inc. Digital Forensics Expert Witness



Evidence Solutions, Inc. Digital Forensics Expert Witness



Digital Forensics Expert Witness

Evidence Solutions, Inc. Digital Forensics Expert Witness

Presented by Scott Greene, Senior Digital Forensics Examiner

STALKERWARE



Evidence Solutions, Inc. Digital Forensics Expert Witness

Stalkerware

▶ What kinds of spyware and stalkerware apps are out there?

- **-SpyPhone Android Rec Pro:** Offers "full control" over a smartphone's functions, including listening in to the background noise of calls and recording them in their entirety; intercepting and sending copies of SMS and MMS messages sent from the victim's phone, sending activity reports to the user's email address, and more.



Evidence Solutions, Inc. Digital Forensics Expert Witness

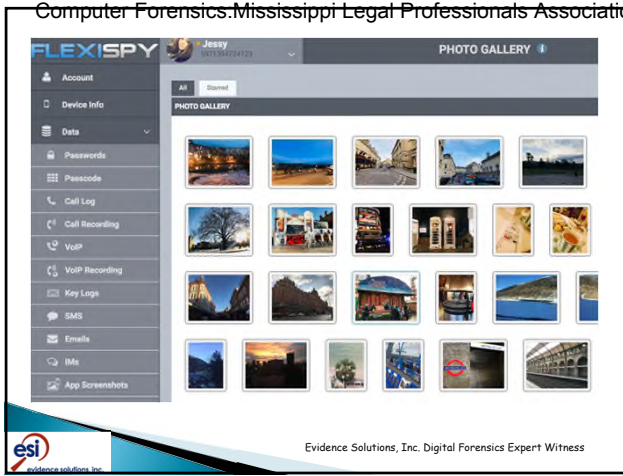
Stalkerware

▶ What kinds of spyware and stalkerware apps are out there?

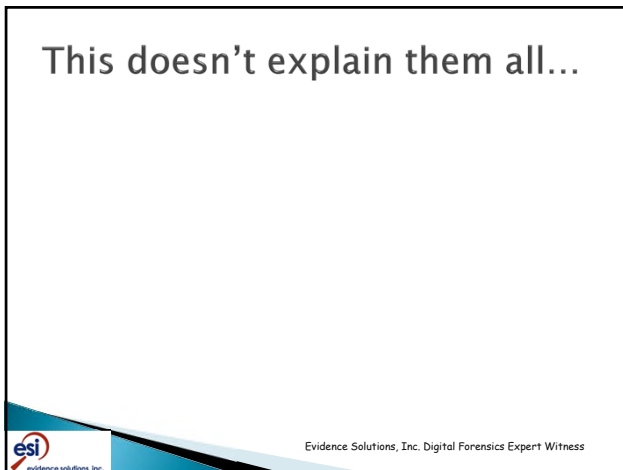
- **-FlexiSpy:** Claims: "It takes complete control of the device, letting you know everything, no matter where you are." This product includes Android Smart phones as well as PCs. It can listen in on calls, spy on apps including Facebook, Viber, and WhatsApp, turn on the infected device's microphone covertly, record Android VoIP calls, exfiltrate content such as photos, and intercept bot SMS messages and emails.



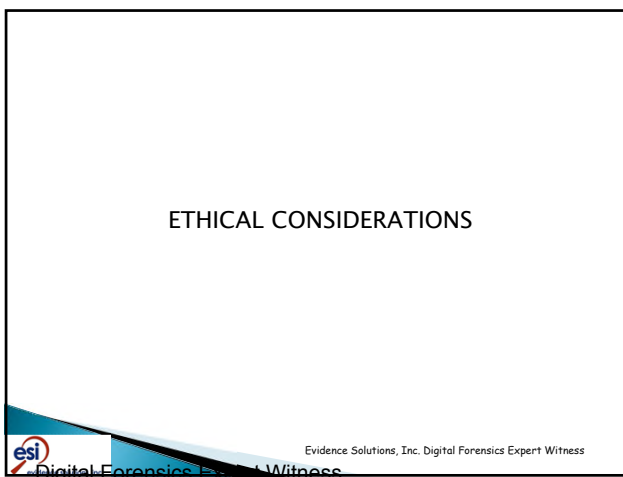
Evidence Solutions, Inc. Digital Forensics Expert Witness



This doesn't explain them all...



ETHICAL CONSIDERATIONS



Ethical Considerations

- ▶ The Non-discovery Context: when lawyers send or receive information (i.e., “communications”) containing metadata.
- ▶ The Discovery Context: when lawyers send, produce or receive electronically stored information (ESI) containing metadata in response to a discovery request or subpoena.
- The Sedona Principles, Second Edition: Best Practices Recommendations & Principles for Addressing Electronic Document Production (2007), <https://thesedonaconference.org/download-pub/81>.



Evidence Solutions, Inc. Digital Forensics Expert Witness

Metadata

- ▶ **Metadata:** Metadata is “data about data.” Metadata can be attached or associated with various types of ESI including: Document Files, Photos, SMS Messages, Messages, as well as physical items such as CDs and DVDs.



Evidence Solutions, Inc. Digital Forensics Expert Witness

Metadata

- ▶ Photographs
- ▶ Electronic Medical Records
- ▶ Vehicles
- ▶ Email
- ▶ Documents / Spreadsheets
- ▶ File System Metadata



Evidence Solutions, Inc. Digital Forensics Expert Witness

Confidentiality

- ▶ Attorneys (and others) should not reveal metadata.

- ▶ Exercise reasonable care
 - Erase / eliminate data from shared documents
 - Print to PDF to prevent metadata transmission
 - (not save to pdf)



Evidence Solutions, Inc. Digital Forensics Expert Witness

Competence

- ▶ Lawyers should be competent to represent their clients.



Evidence Solutions, Inc. Digital Forensics Expert Witness

American Bar Association

- ▶ ABA Ethics 20/20 revision of the model ethics rules. Rule 1.1 Competence.
 - "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."



Evidence Solutions, Inc. Digital Forensics Expert Witness

Preservation

- ▶ This means metadata should be preserved and disclosed.
- ▶ If litigation is reasonably anticipated, care should be taken to prevent the routine deletion of certain metadata, especially embedded metadata in potentially relevant Electronically Stored Information (ESI).



Evidence Solutions, Inc. Digital Forensics Expert Witness

Preservation

- ▶ Deletion of metadata may constitute spoliation.
- ▶ Removing metadata from certain evidentiary files may even be illegal.



Evidence Solutions, Inc. Digital Forensics Expert Witness

IMPERSONATION



Evidence Solutions, Inc. Digital Forensics Expert Witness

Security is paramount

- ▶ Spammers & Scammers account for as much 40 percent of the accounts on social-media sites!



Evidence Solutions, Inc. Digital Forensics Expert Witness

Scammers are Everywhere

Robin Sage
@robinsage
Sorry to say, I'm not a Green Beret! Just a cute girl stopping by to say hey! My life is about info sec all the way!

Follow



Evidence Solutions, Inc. Digital Forensics Expert Witness

Scammers are Everywhere

- ▶ Graduate of Massachusetts Institute of Technology
- ▶ Cyber Threat Analyst - US Navy Network Warfare Command
- ▶ She had
 - 141 Twitter Followers
 - 110 Facebook Friends
 - 148 LinkedIn Connections
 - Including: Joint Chiefs of Staff, NSA, US Marines, US House of Representatives, Pentagon, DoD, Lockheed Martin, Northrup Grumman, Boos Allen Hamilton.



Digital Forensics Expert Witness

Evidence Solutions, Inc. Digital Forensics Expert Witness

Presented by Scott Greene, Senior Digital Forensics Examiner

- ▶ Hospital Paging Systems
 - Was the Doctor Onsite?
- ▶ Electronic Medical Record Systems
 - Don't just believe what the give you
- ▶ Vehicle Maintenance Systems
 - Records of what happened when & by whom

• "Digital Evidence is Everywhere!"



Evidence Solutions, Inc. Digital Forensics Expert Witness

- ▶ Email Systems
 - Data is Easily Fabricated
- ▶ Telematics / Electronic Logging Devices
 - They aren't the end
- ▶ Self Driving / Automation in Cars
 - Safer.... eventually

• "Digital Evidence Is Everywhere!"



Evidence Solutions, Inc. Digital Forensics Expert Witness

Faculty:

Scott Greene
Evidence Solutions, Inc.

Scott@EvidenceSolutions.com
www.EvidenceSolutions.com

[866-795-7166](tel:866-795-7166)

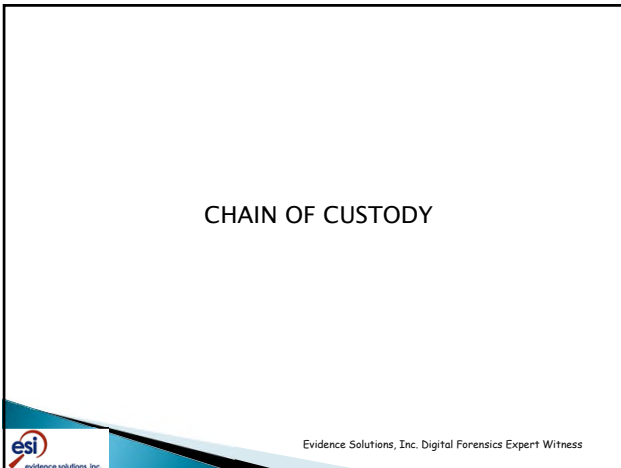


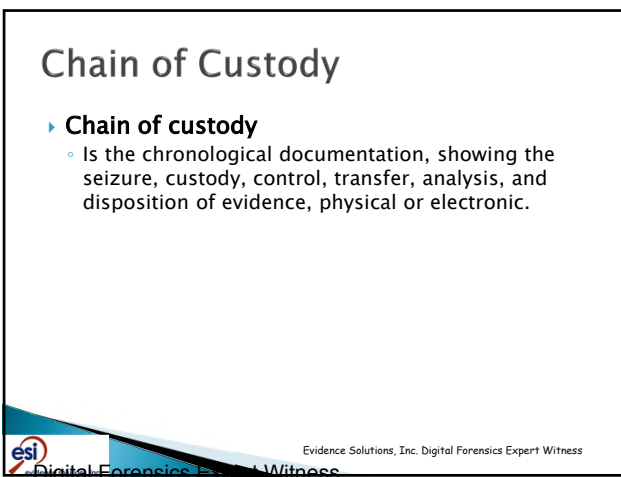
Evidence Solutions, Inc. Digital Forensics Expert Witness

Digital Forensics Expert Witness

Presented by Scott Greene, Senior Digital Forensics Examiner







What is Chain of Custody

- ▶ Evidence which can be used in court to convict persons of crimes, must be handled in a very careful manner to avoid later allegations of tampering, altering, or misconduct.



Evidence Solutions, Inc. Digital Forensics Expert Witness

What is the Chain of Custody?

- ▶ Recording the chain of custody ensures that evidence is in fact related to the alleged case or crime – and has not, for example, been planted fraudulently to make someone appear guilty.



Evidence Solutions, Inc. Digital Forensics Expert Witness

General Rules for Chain of Custody

- ▶ An identifiable person must always have the physical custody of the evidence.
- ▶ This means that an investigator will take charge of a piece of evidence, document its collection, and hand it over to an evidence clerk for storage in a secure place.



Evidence Solutions, Inc. Digital Forensics Expert Witness

Evidence Collection

- ▶ Seizing the original
 - Should be bagged and documented
- ▶ Copying the original
 - Date copied
 - Location copied
 - Type of copy
 - Hash of original



Evidence Solutions, Inc. Digital Forensics Expert Witness

General Rules for Chain of Custody

- ▶ Transactions start with collection and end with court (or later)
- ▶ Transactions should be documented chronologically
- ▶ Transactions should be able to withstand legal challenges to the authenticity of the evidence.



Evidence Solutions, Inc. Digital Forensics Expert Witness

General Rules for Chain of Custody

- ▶ Documentation should include:
 - The conditions under which the evidence is gathered
 - The method with which the evidence is gathered
 - The identity of all evidence handlers
 - The length of time of evidence custody by each handler
 - The conditions, including the Security conditions while handling or storing the evidence
 - The manner in which evidence is transferred to subsequent handler each time such a transfer occurs
 - Signatures for each person involved at each step



Evidence Solutions, Inc. Digital Forensics Expert Witness

What is Unique about Electronically Stored Evidence?

- ▶ Original data
 - Create a digital fingerprint (hash) that continually verifies data authenticity
- ▶ Storage Media includes:
 - Hard Disk Drives
 - Backup tapes
 - DVD / CD Rom disks
 - E-prom and Memory chips
 - Thumb Drives
 - iPods, iPads & MP3 Players
 - Cell Phones
 - The Cloud
 - Infotainment Systems



Evidence Solutions, Inc. Digital Forensics Expert Witness

What is Unique about Electronically Stored Evidence?

- ▶ Servers
 - Most companies intend for data to be stored on servers
- Ha!
- Workstations, Laptops are an incredible source of information



Evidence Solutions, Inc. Digital Forensics Expert Witness

What is Unique about Electronically Stored Evidence?

- ▶ Workstations
 - When someone is doing something that they shouldn't be doing, it is more likely that you will find it on their workstation than you will find it on the server.



Evidence Solutions, Inc. Digital Forensics Expert Witness


evidence solutions, inc.


Equipment & Media Chain of Custody

Case:							
Hdd	Floppy	Tape	BlackBox	CellPhone	CD	DVD	Other
Make:				Model:			
S/N:				Jumpers:			
Additional:							
From:				To:	Evidence Solutions, Inc.		
Date:				Time:			
Location:				Signature:			
From:				To:			
Date:				Time:			
Location:				Signature:			

 Evidence Solutions, Inc. Digital Forensics Expert Witness


Rules for Electronically Stored Information, Chain of Custody

- ▶ Electronically Stored Information can be easily altered
- ▶ A chain of custody log for ESI should show:
 - The data was properly copied
 - The data was properly transported
 - The information wasn't altered
 - All media has been secure throughout the time period

 Evidence Solutions, Inc. Digital Forensics Expert Witness

Plain and Simple:

- ▶ Data must be preserved and maintained in a manner that verifies its authenticity.
- ▶ There should be a list of who has had the data and for how long.
- ▶ In a court of law each person may be required to testify as to what happened to the original media when it was in their control.

 Evidence Solutions, Inc. Digital Forensics Expert Witness



ELITE EXPERT WITNESSES IN...

- **Electronic Evidence**
- **Trucking and Commercial Motor Vehicles**
- **Sports and Fitness**
- **Police and Law Enforcement**
- **Fraternity**



evidence solutions, inc.

Presented by Digital Forensics Examiner

EvidenceSolutions.com | 866-795-7166