



Evidence Solutions, Inc.

And the

Arizona Judicial Conference

Present:

You Can do that?

June 21, 2017

Presented by:

Scott Greene, SCFE, CEO

Evidence Solutions, Inc.

An Arizona Digital Forensics Firm

520-795-7166

866-795-7166

Scott@EvidenceSolutions.com

You Can Do That?

2017 Arizona Judicial Conference

Faculty:

Scott Greene

Evidence Solutions, Inc.

Scott@EvidenceSolutions.com

www.EvidenceSolutions.com



Evidence Solutions, Inc. Arizona Computer 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. Cell Phone Forensics Expert Witness

Disclaimer

- ▶ Scott Greene, & Evidence Solutions, Inc. are not supplying legal advice.
- ▶ Because, well, I'm not an attorney.
- ▶ But I do play one on TV.



GENERAL COMPUTER FORENICS



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

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. Arizona Cyber 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. Cyber Evidence 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. Arizona Computer 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. Arizona Hard Disk Drive 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. Computer Forensics Expert Witness Arizona

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. an Arizona Computer 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. an Arizona Computer 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. an Arizona Computer Forensics Expert Witness

INFOTAINMENT SYSTEMS



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

Infotainment Systems



Evidence Solutions, Inc. an Arizona Computer 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. an Arizona Computer 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



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

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. an Arizona Computer Forensics Expert Witness

CELL PHONES



Evidence Solutions, Inc. an Arizona Computer 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. an Arizona Computer Forensics Expert Witness

Cell Phones & Tablets

- Browsing History
- Documents
- Email accounts
- Online data storage accounts

Digital Evidence: Cell Phone Forensics



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

Time	Status	Description
12:00A	OFF	(500)
01:07A	DUTY	(500)
01:12A		State: TX
01:12A		Driver
01:12A	DUTY	(500)
01:14A	DRIVE	(500)
02:00A	DUTY	(TX-2083)
02:13A	DRIVE	(TX-2083)
03:14A	DUTY	(295) C/P
03:38A	DRIVE	(295) C/P
04:16A	DUTY	(TX-2083)
04:50A	DRIVE	(TX-2083)
05:32A	DUTY	(295) C/P
05:37A	DRIVE	(295) C/P
06:47A	DUTY	(TX-2083)
07:15A	DRIVE	(295) C/P
08:22A	DRIVE	2.7 mi S of
09:05A	DRIVE	(TX-4298)
09:35A	DRIVE	(TX-4298)
10:18A	DUTY	(295) C/P
10:42A	DRIVE	(295) C/P
11:25A	DUTY	(TX-4298)
11:55A	DRIVE	12.6 mi N
12:35P	DUTY	(295) C/P
01:01P	DRIVE	(295) C/P
01:28P	DUTY	(500)
01:31P		Driver Leave(500)
01:31P	DUTY	(500)

03/01/12 0709	SMS - Inbox
03/01/12 0710	SMS - Inbox
03/01/12 0716	Driving
03/01/12 0727	SMS - Inbox
03/01/12 0728	SMS - Sent
03/01/12 0728	SMS - Inbox
03/01/12 0759	In Service
03/01/12 0823	Driving
03/01/12 0946	SMS - Sent
03/01/12 0905	In Service
03/01/12 0935	Driving
03/01/12 0955	SMS - Inbox
03/01/12 1018	In Service
03/01/12 1042	Driving
03/01/12 1125	In Service
03/01/12 1143	Driving
03/01/12 1230	SMS - Inbox
03/01/12 1235	In Service
03/01/12 1240	SMS - Inbox



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

1329977.002
06/12/2013
SCAMP

MOBILITY USAGE

Run Date: 06/12/2013
Run Time: 17:41:35
Voice Usage For: (480) [REDACTED]
Account Number: 8134 [REDACTED]

Item	Conn. Date	Conn. Time	Seizure Time	Originating Number	Terminating Number	Elapsed Time	Number Dialed	IMEI	IMEI	Description
1	01/01/11	05:36A	0:22	[REDACTED]	[REDACTED]	0:00	[REDACTED]	35349104165148	310410366057466	m2M_DTR
2	01/01/11	05:37A	0:02	[REDACTED]	[REDACTED]	0:06	[REDACTED]	310410366057466	[REDACTED]	m2M
3	01/01/11	05:37A	0:27	[REDACTED]	[REDACTED]	0:06	[REDACTED]	310410366057466	[REDACTED]	m2M
4	01/01/11	09:09A	0:10	[REDACTED]	[REDACTED]	4:42	[REDACTED]	35349104165148	310410366057466	m2M_DTR
5	01/01/11	09:31A	0:08	[REDACTED]	[REDACTED]	3:22	[REDACTED]	35349104165148	310410366057466	m2M_DTR
6	01/01/11	09:35A	0:05	[REDACTED]	[REDACTED]	1:05	[REDACTED]	35349104165148	310410366057466	M2O_DTR
7	01/01/11	09:38A	0:05	[REDACTED]	[REDACTED]	0:47	[REDACTED]	35349104165148	310410366057466	M2O_DTR
8	01/01/11	09:40A	0:23	[REDACTED]	[REDACTED]	0:06	[REDACTED]	35349104165148	310410366057466	M2O_DTR
9	01/01/11	09:42A	0:08	[REDACTED]	[REDACTED]	0:31	[REDACTED]	35349104165148	310410366057466	M2O_DTR
10	01/01/11	09:45A	0:01	[REDACTED]	[REDACTED]	0:00	[REDACTED]	35349104165148	310410366057466	M2O_DTR

esi
Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness



1329977.002
06/12/2013
SCAMP

MOBILITY USAG

Run Date: 06/12/2013
Run Time: 17:41:35
Voice Usage For: (480) [REDACTED]
Account Number: 8134 [REDACTED]

Item	Conn. Date	Conn. Time	Seizure Time	Originating Number	Terminating Number	Elapsed Time	Number Dialed
1	01/01/11	05:36A	0:22	[REDACTED]	[REDACTED]	0:00	[REDACTED]
2	01/01/11	05:37A	0:02	[REDACTED]	[REDACTED]	0:06	[REDACTED]
3	01/01/11	05:37A	0:27	[REDACTED]	[REDACTED]	0:06	[REDACTED]
4	01/01/11	09:09A	0:10	[REDACTED]	[REDACTED]	4:42	[REDACTED]
5	01/01/11	09:31A	0:08	[REDACTED]	[REDACTED]	3:22	[REDACTED]
6	01/01/11	09:35A	0:05	[REDACTED]	[REDACTED]	1:05	[REDACTED]
7	01/01/11	09:38A	0:05	[REDACTED]	[REDACTED]	0:47	[REDACTED]
8	01/01/11	09:40A	0:23	[REDACTED]	[REDACTED]	0:06	[REDACTED]
9	01/01/11	09:42A	0:08	[REDACTED]	[REDACTED]	0:31	[REDACTED]
10	01/01/11	09:45A	0:01	[REDACTED]	[REDACTED]	0:00	[REDACTED]

esi
Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness



1329977.002
06/12/2013
SCAMP

MOBILITY USAGE

Run Date: 06/12/2013
Run Time: 17:42:47
Data Usage For: (480) [REDACTED]
Account Number: 8134 [REDACTED]

Item	Conn. Date	Conn. Time	Originating Number	Elapsed Time	Bytes Up	Bytes Down	IMEI	IMEI	Access Pt	Description
6374	05/26/11	10:00A	[REDACTED]	13:13	6677	111991	3534910416514804	310410366057466	acds.voicemail	_MOBILE_DATA_1
6375	05/26/11	10:14A	[REDACTED]	5:08	0	0	3534910416514804	310410366057466	acds.voicemail	_MOBILE_DATA_1
6376	05/26/11	10:31A	[REDACTED]	13:14	9271	49317	3534910416514804	310410366057466	BLACKBERRY.XE	_MOBILE_DATA_7
6377	05/26/11	10:31A	[REDACTED]	2:13	2639	8417	3534910416514804	310410366057466	NAP_CINGULAR	_MOBILE_DATA_
6378	05/26/11	10:44A	[REDACTED]	0:24	553	571	3534910416514804	310410366057466	BLACKBERRY.XE	_MOBILE_DATA_

esi
Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness



1329977.002
06/12/2013
SCAMP

Run Date: 06/12/2013
Run Time: 17:42:47
Data Usage For: (480) [REDACTED]
Account Number: 81342 [REDACTED]

Item	Conn. Date	Conn. Time	Originating Number	Elapsed Time	Bytes Up	Bytes Dn
6374	05/26/11	10:00A	[REDACTED]	13:13	6677	111991
6375	05/26/11	10:14A	[REDACTED]	5:08	0	0
6376	05/26/11	10:31A	[REDACTED]	13:14	9271	49317
6377	05/26/11	10:31A	[REDACTED]	2:13	2639	8417
6378	05/26/11	10:44A	[REDACTED]	0:24	553	571



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

1329977.002
06/12/2013
SCAMP

MOBILITY USAGE

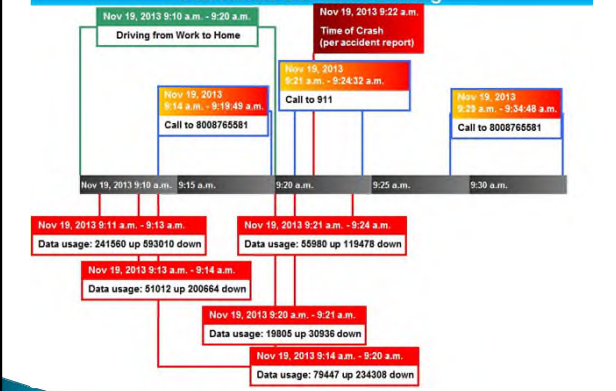
Run Date: 06/12/2013
Run Time: 17:44:11
SMD Usage For: (480) [REDACTED]
Account Number: 81342 [REDACTED]

Item	Conn. Date	Conn. Time	Originating Number	Terminating Number	IMEI	IMEI	Description
913	01/14/11	09:37P	[REDACTED]	[REDACTED]	35349104165148	310410366057466	OUT
914	01/14/11	09:37P	[REDACTED]	[REDACTED]	35349104165148	310410366057466	OUT
915	01/14/11	09:41P	[REDACTED]	[REDACTED]	35349104165148	310410366057466	IN
916	01/15/11	08:06A	[REDACTED]	[REDACTED]	35349104165148	310410366057466	OUT
917	01/15/11	08:16A	[REDACTED]	[REDACTED]	35349104165148	310410366057466	IN
918	01/15/11	08:32A	[REDACTED]	[REDACTED]	35349104165148	310410366057466	OUT
919	01/15/11	08:32A	[REDACTED]	[REDACTED]	35349104165148	310410366057466	IN



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

Cell Phone Use While Driving



WEB BROWSING ARTIFACTS



Evidence Solutions, Inc. an Arizona Computer 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. an Arizona Computer 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. an Arizona Computer 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



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

Artifacts From Web Browsing

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



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

SOCIAL MEDIA



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness



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!

ESI Evidence Solutions, Inc. an Arizona Computer 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.

ESI Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

The statistics of need:

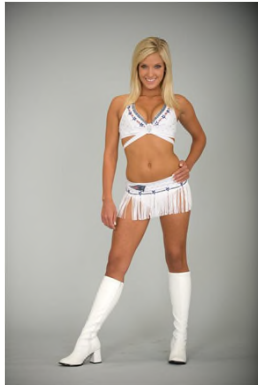
- Social media evidence is:
 - widely discoverable
 - generally not subject to privacy constraints when established to be relevant to a case, particularly when that data is held by a party to litigation or even a key witness.



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

Here is what is out there

- ▶ New England Patriots Cheerleader, Caitlin Davis, 18



Evidence Solutions, Inc. an Arizona Computer 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. an Arizona Computer Forensics Expert Witness

Arizona Computer Forensics Expert Here is how they use it....



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



Evidence Solutions, Inc. an Arizona Computer 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. an Arizona Computer Forensics Expert Witness



FACEBOOK

Making stupidity more accessible.



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

ETHICAL CONSIDERATIONS



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

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>.



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.



Metadata

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



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)



Competence

- ▶ Lawyers should be competent to represent their clients.



Competence

- ▶ The Minnesota Lawyers Professional Responsibility Board says: "Competence requires that lawyers understand that:
 - metadata is created in the generation of electronic files
 - transmission of electronic files will include transmission of metadata
 - recipients of the files can access metadata
 - actions can be taken to prevent or minimize the transmission of metadata."



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. an Arizona Computer 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).



Preservation

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



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

CHAIN OF CUSTODY



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

What is Chain of Custody

- ▶ **Chain of custody**
 - Is the chronological documentation, showing the seizure, custody, control, transfer, analysis, and disposition of evidence, physical or electronic.



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.



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.



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 Collection

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



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.



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



What is Unique about Electronically Stored Evidence?

- ▶ Original data
 - Create a digital fingerprint (hash) that continually verifies data authenticity
- ▶ Copied data
- ▶ Sources
 - Workstations
 - USB & Thumb Drives
 - Servers



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



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 that you will find it on the server.




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.


Rules for Electronically Stored Information, Chain of Custody

- ▶ Electronically Stored Information can be easily altered
- ▶ A chain of custody log for ESI must 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.

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.

 Computer & Digital Forensics

HOW NOT TO DO THINGS



How not to do things....

▶ The law firm overwrote the data!!!!

- The machine was on when we arrived.
- The owner of the machine had rigged the machine with some pretty sophisticated software that automatically overwrote key data files when the machine was booted and a question was either skipped or answered wrong in the boot process.
- The data that the law firm sought was completely destroyed.



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

How not to do things....

▶ The IT department overwrote the data!!!

- Employee deleted data from hard disk drive
 - but didn't delete it from the recycle bin
- Technology department recovered the data using some standard data tools
 - but destroyed the evidence that proved the employee deleted the data in the first place
 - this made our job much much harder than it had to be



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

IMPERSONATION



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

Security is paramount

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



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

Scammers are Everywhere



Evidence Solutions, Inc. an Arizona Computer 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.



Evidence Solutions, Inc. an Arizona Computer 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. an Arizona Computer Forensics Expert Witness
