



Evidence Solutions, Inc.

And the

Maricopa County Bar Association

Present:

Ethics in Digital Evidence Collection:
How to get it and have it admissible

June 9, 2017

Maricopa County Bar Association
303 E. Palm Lane
Phoenix, Arizona 85004

Presented by:

Scott Greene, SCFE, CEO
Evidence Solutions, Inc.

Digital Forensics Firm

520-512-5001
866-795-7166

Scott@EvidenceSolutions.com



Ethics in Digital Evidence Collection: How to get it and have it admissible

1.5 CLE Ethics Credit Available



This CLE will cover the nuts and bolts of digital evidence collection and any associated ethical components. Topics include the types of evidence that can be collected and how they are collected, the use of technology used to collect digital evidence and discussion on how evidence is maintained including digital fingerprints and chain of custody.

PRESENTERS: Scott Greene, CEO and Senior Digital Evidence Examiner, Evidence Solutions, Inc.

Date: June 9, 2017
Time: 12:00PM to 1:30PM (Lunch Included)
Location: Maricopa County Bar Association
 303 E. Palm Lane
 Phoenix, Arizona 85004

ONLINE: www.maricopabar.org under CLE/EVENTS header
PHONE: Call Karla Durazo at 602.682.8586 M-F, 8:30am-5pm. Please have your credit card information handy.
EMAIL: Complete this form and send the PDF to: kdurazo@maricopabar.org Please state in subject line: "Registration".
FAX: Complete this form and fax to: ATTN: CLE Department - 602.682.8601
MAIL: Complete this form and mail to: 303 East Palm Lane, Phoenix, Arizona 85004
 Payment in full must be received before you are considered registered. Please see www.maricopabar.org for cancellation policy.
 Call (602) 257-4200 if you have any accommodation requirements or questions.

Early Bird ends June 2, 2017

| Early Bird Rate | Regular Rate |
|------------------------------------|--|
| <input type="checkbox"/> \$ 90.00 | \$ 105.00 MCBA Members |
| <input type="checkbox"/> \$ 65.00 | \$ 80.00 Paralegal & Public Lawyers Division members |
| <input type="checkbox"/> \$ 125.00 | \$ 140.00 Non-Members |
| <input type="checkbox"/> \$ 15.00 | \$ 15.00 MCBA Student members |
| <input type="checkbox"/> \$ Free | \$ Free MCBA Sustaining members |

Please call Karla at 602-682-8586 to register your paralegal for \$30 (early bird rate) or \$45 (regular rate).

Name (please print): _____ **E-mail:** _____

Address: _____

Method of Payment: CHECK VISA MASTERCARD AMERICAN EXPRESS

Credit Card#: _____ **Exp.Date:** _____ **CVV#:** _____

Signature: _____

Ethics in Digital Evidence Collection: How to get it and have it admissible

Maricopa County Bar Association

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.



Ethical Considerations

- ▶ “The enhanced possibility of inadvertent production of privileged or work product information, the stakes in the management of privilege reviews, and careless handling of client communications raise serious ethical issues. Similarly, the disparate views on how lawyers should treat metadata (e.g., when to delete, when to send, when to review) create additional risks for lawyers, especially in cases across different jurisdictions.”



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, and
 - actions can be taken to prevent or minimize the transmission of metadata."



Supervision

- ▶ ABA Model Rules of Professional Conduct say:
 - A lawyer must become knowledgeable about metadata, and a firm must provide for the acquisition of such knowledge.
 - Responsibilities of Partners, Managers, and Supervisory Lawyers (2009) require those with managerial authority to make reasonable efforts to ensure that the firm and its lawyers follow the Rules of Professional Conduct.
 - This may also require the implementation of a firm-wide application to scrub certain outgoing email to remove metadata.



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



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

Evidence Collection Sources of Evidence:

- ▶ Storage Media includes:
 - Hard Disk Drives
 - Floppy Disks
 - Backup tapes
 - CD Rom disks
 - E-prom and Memory chips
 - Thumb Drives
 - iPods, iPads & MP3 Players
 - Cell Phones



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 Solutions, Inc. Email Forensics Expert Witness Arizona

How Data is Stored Example

- ▶ We create a document that is stored in this allocation unit.
 - The directory entry looks like: document.doc
 - The data looks like:

```
Dear John, It was a
pleasure to meet wit
h you and to discuss
your desire to purc
hase the boat. Pleas
e let me know if you
need any thing else
. Sincerely Henry Ps
I think it is worth
$11,999.↑000000000000
```



Evidence Solutions, Inc. AZ Computer Forensics Expert Witness

```
Dear John, It was a
pleasure to meet wit
h you and to discuss
your desire to purc
hase the boat. Pleas
e let me know if you
need any thing else
. Sincerely Henry Ps
I think it is worth
$11,999.↑000000000000
```



Evidence Solutions, Inc. Cyber Forensics Expert Witness, AZ

How Data is Stored

Example

- ▶ We edit out the price, the document looks like:
 - The directory entry looks like: document.doc
 - The data looks like:

```
Dear John, It was a
pleasure to meet wit
h you and to discuss
your desire to purc
hase the boat. Pleas
e let me know if you
need any thing else
. Sincerely Henry¶Ps
I think it is worth
$11,999. 0000000000
```



Evidence Solutions, Inc. AZ Computer Forensics Expert Witness

```
Dear John, It was a
pleasure to meet wit
h you and to discuss
your desire to purc
hase the boat. Pleas
e let me know if you
need any thing else
. Sincerely Henry¶Ps
I think it is worth
$11,999. 0000000000
```



Evidence Solutions, Inc. Cyber Forensics Expert Witness, AZ

How Data is Stored

Example

- ▶ The document is erased / deleted (from the recycle bin):
 - The directory entry looks like: ~ocument.doc
 - The data looks like:

```
Dear John, It was a
pleasure to meet wit
h you and to discuss
your desire to purc
hase the boat. Pleas
e let me know if you
need any thing else
. Sincerely Henry¶Ps
I think it is worth
$11,999. 0000000000
```



Evidence Solutions, Inc. an Arizona Computer Forensics Company

How Data is Stored

Example

- ▶ A new document is created and saved in the same allocation unit:
 - The directory entry looks like: faxcover.doc
 - The data looks like:

```
Fax Cover Sheet. ¶ a
pleasure to meet wit
h you and to discuss
your desire to purc
hase the boat. Pleas
e let me know if you
need any thing else
. Sincerely Henry Ps
I think it is worth
$11,999. 00000000000
```



Evidence Solutions, Inc. An Arizona Digital Forensics Company

```
Fax Cover Sheet. ¶ a
pleasure to meet wit
h you and to discuss
your desire to purc
hase the boat. Pleas
e let me know if you
need any thing else
. Sincerely Henry Ps
I think it is worth
$11,999. 00000000000
```



Evidence Solutions, Inc. A Cyber Forensics Expert Witness Company

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



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.



Chain of Custody in Civil Cases

- ▶ Chain of custody is a familiar concept in criminal law, but until recent years it was foreign to civil litigators. In the criminal law arena, police would seize evidence, seal it in a plastic bag, label it, and sign it in to a locked evidence room. If the evidence was taken out by anyone for any purpose (for example, for laboratory examination or testing) that withdrawal would be noted on the log, as would its return. The next removal from the room would likely not be until its presentation at the trial itself.



How did Chain of Custody come about?

- ▶ It used to be enough for the officer or authority who made the collection to be able to testify that the "knife" was indeed the "knife" collected at the scene of the crime.
- ▶ It became even more important when the evidence began to consist of fungible items. Most often applied to illegal drugs, seized by law enforcement. In such cases, the defendant at times claims they had no knowledge of possession of the controlled substance in question. Accordingly, the chain of custody documentation and testimony is presented by the prosecution to establish that the substance in evidence was in fact in the possession of the defendant.



Federal Rules of Evidence Rule 901

- ▶ (a) General provision.
 - --The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.



Rule 901 Requirement of Authentication or Identification

- ▶ (b) Illustrations.--By way of illustration only, and not by way of limitation, the following are examples of authentication or identification conforming with the requirements of this rule:
- ▶ (1) Testimony of witness with knowledge.-- Testimony that a matter is what it is claimed to be.
- ▶ (2) Nonexpert opinion on handwriting.--Nonexpert opinion as to the genuineness of handwriting, based upon familiarity not acquired for purposes of the litigation.
- ▶ (3) Comparison by trier or expert witness.-- Comparison by the trier of fact or by expert witnesses with specimens which have been authenticated.



Rule 901 Requirement of Authentication or Identification

- ▶ (4) Distinctive characteristics and the like.--Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances.
- ▶ (5) Voice identification.--Identification of a voice, whether heard firsthand or through mechanical or electronic transmission or recording, by opinion based upon hearing the voice at any time under circumstances connecting it with the alleged speaker.
- ▶ (6) Telephone conversations.--Telephone conversations, by evidence that a call was made to the number assigned at the time by the telephone company to a particular person or business, if (A) in the case of a person, circumstances, including self-identification, show the person answering to be the one called, or (B) in the case of a business, the call was made to a place of business and the conversation related to business reasonably transacted over the telephone.



Rule 901 Requirement of Authentication or Identification

- ▶ (7) Public records or reports.--Evidence that a writing authorized by law to be recorded or filed and in fact recorded or filed in a public office, or a purported public record, report, statement, or data compilation, in any form, is from the public office where items of this nature are kept.
- ▶ (8) Ancient documents or data compilation.--Evidence that a document or data compilation, in any form, (A) is in such condition as to create no suspicion concerning its authenticity, (B) was in a place where it, if authentic, would likely be, and (C) has been in existence 20 years or more at the time it is offered.
- ▶ (9) Process or system.--Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.
- ▶ (10) Methods provided by statute or rule.--Any method of authentication or identification provided by Act of Congress or by other rules prescribed by the Supreme Court pursuant to statutory authority.



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





Evidence Solutions, Inc. an Arizona Computer 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.



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.



Rules for Electronically Stored Information, Chain of Custody

- ▶ Documentation should include:
 - 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
 - Location (is important to me).
 - Signatures for each person involved at each step



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.







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&mode=bellaluna
- ▶ My Secure Wallet



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

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



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
