Evidence Solutions, Inc.

And the

Arizona Public Defenders Association

Present:

Cell Phone Evidence: Tweets, Snapchats, and Messaging

June 22, 2017

Tempe Mission Palms Hotel and Conference Center
60 E 5th St, Tempe, AZ 85281, USA

Presented by:

Scott Greene, SCFE, CEO
Evidence Solutions, Inc.

An Arizona Computer & Cell Phone Forensics Company

520-512-5001
866-795-7166

Scott@EvidenceSolutions.com

Messages, Email, Tweet & More

Arizona Public Defender's Association

Faculty:

Scott Greene
Evidence Solutions, Inc.
Scott@EvidenceSolutions.com
www.EvidenceSolutions.com

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.

Today is the holiday called:

"Damn It's Hot in Arizona Day"

Sponsored by Hallmark

Great Stuff

- "Where a calculator on the ENIAC is equipped with 18,000 vacuum tubes and weighs 30 tons, computers in the future may have only 1,000 vacuum tubes and weigh only 1.5 tons." -- *Popular Mechanics, 1949*

The laws

- States are still grappling with electronic discovery rules
  - Example of the struggle:
    - Employee in office uses computer, who owns the data?
    - Employee takes work home and uses a company laptop to do his work. Who owns the data?
    - Employee takes work home, accesses the corporate network via VPN but uses his own PC. Who owns the data?

- Email

Reasons to examine electronic data

- E-mail communications have surpassed telephone and postal (snail mail) communication.
- And e-mail has entered the shadow of Instant Messaging, Texting (SMS) etc.
- Cell phones have 100,000 times as much computer power as put us on the moon.

Evidence Collection Sources of Evidence:

- E-mail
  - People tend to write things in email that they would never consider writing in a memorandum or letter.
  - Email has been used successfully in criminal cases as well as civil litigation.

Evidence Collection Sources of Evidence:

- E-Mail (continued)
  - Email is often backed up on tapes that are generally kept for months or years or perhaps permanently.
  - Privacy and Ownership laws and ramifications

Evidence Collection Sources of Evidence:

- E-Mail (continued)
  - With one unintended click in the e-mail system's address book, a message intended for one recipient will be sent to the entire organization or to an entire Internet discussion group.

Evidence Collection Sources of Evidence:

- ISP servers
  - How does e-mail get from one place to another?
  - E-mail generally passes through ISP mail servers. Copies of e-mail may remain on their servers for quite some time. This information can be subject to subpoena.

- Received: from server45.appriver.com ([69.20.58.226])
- by 10.0.0.4 with ESMTP; Mon, 13 Oct 2008 15:26:47 -0700
- Received: from [10.238.8.138] (HELO inbound.appriver.com)
- by server45.appriver.com (CommuniGate Pro SMTP 5.1.9)
- with ESMTP id 510030976 for spg@great-scott.com; Mon, 13 Oct 2008 18:17:41 -0400
- Received: by inbound.appriver.com (CommuniGate Pro PIPE 5.1.7)
- with PIPE id 934012320; Mon, 13 Oct 2008 18:17:41 -0400
- Received: from [208.109.78.209] (HELO smtpoutwbe07.prod.mesa1.secureserver.net)
- by inbound.appriver.com (CommuniGate Pro SMTP 5.1.7)
- with SMTP id 934012226 for spg@great-scott.com; Mon, 13 Oct 2008 18:17:36 -0400
- Received: (qmail 6678 invoked from network); 13 Oct 2008 22:17:33 -0000
- Received: from unknown (HELO gem-wbe09.prod.mesa1.secureserver.net) (64.202.189.48)
- by smtpoutwbe07.prod.mesa1.secureserver.net with SMTP; 13 Oct 2008 22:17:33 -0000
- Received: (qmail 9092 invoked by uid 99); 13 Oct 2008 22:17:33 -0000

- Received: from server45.appriver.com ([69.20.58.226])
- by 10.0.0.4 with ESMTP; Mon, 13 Oct 2008 15:26:47 -0700
- Received: from [10.238.8.138] (HELO inbound.appriver.com)
- by server45.appriver.com (CommuniGate Pro SMTP 5.1.9)
- with ESMTP id 510030976 for scott@EvidenceSolutions.com; Mon, 13 Oct 2008 18:17:41 -0400

- Received: by inbound.appriver.com (CommuniGate Pro PIPE 5.1.7)
- with PIPE id 934012320; Mon, 13 Oct 2008 18:17:41 -0400
- Received: from [208.109.78.209] (HELO smtpoutwbe07.prod.mesa1.secureserver.net)
- by inbound.appriver.com (CommuniGate Pro SMTP 5.1.7)
- with SMTP id 934012226 for scott@EvidenceSolutions.com; Mon, 13 Oct 2008 18:17:36 -0400

- Received: (qmail 6678 invoked from network); 13 Oct 2008 22:17:33 -0000
- Received: from unknown (HELO gem-wbe09.prod.mesa1.secureserver.net) (64.202.189.48)
- by smtpoutwbe07.prod.mesa1.secureserver.net with SMTP; 13 Oct 2008 22:17:33 -0000
- Received: (qmail 9092 invoked by uid 99); 13 Oct 2008 22:17:33 -0000

Evidence Collection Sources of Evidence:

- E-mail Logs
  - What was done when and by whom
    - Most software used to operate networks, including web servers, mail servers and gateways, logs transactions and communications.
    - These logs will normally include the e-mail addresses of senders and recipients of e-mail and the time of transmission.

Evidence Collection Sources of Evidence:

- The content of e-mails themselves would not normally be logged but may be stored on mail servers.
- System administrators are also capable of reading the contents of e-mails sent and received by the corporate network.

Email Case Example

- Case Background:
  - Intellectual property case. The two parties were fighting over a patent.
  - Some of the evidence supplied by the plaintiff was email.

From: "John C Plaintiff" <JohnP@Lost-Tech.com>
To: <Mark@manufacturer.com>
Cc: "Robert Z Defendant" <Robert@LostTechnologies.com>
Sent: Friday, March 03, 2006 3:35 PM
Attach: Image Of Product.pdf
Subject: Emailing: Image of Product.pdf

Mark,
Please find attached a picture of our new product that we discussed.

Thanks,
John
President
Lost Tech, Inc.

www.LostTechnologies.com

ISO 9001:2000 * ISO 14001 * ISO18001 * UL Listed

E-mail: JohnP@LostTechnologies.com

The message is ready to be sent with the following file or link attachments: Image Of Product.pdf

Electronic Version

From: "John C Plaintiff" <JohnP@Lost-Tech.com>
To: "<Mark@manufacturer.com>" <Mark@manufacturer.com>
Cc: "Robert Z Defendant" <Robert@Lost-Tech.com>
Sent: Friday, March 03, 2006 3:35 PM
Attach: Image Of Product.pdf
Subject: Emailing: Image of Product.pdf

Mark,
Please find attached a picture of our new product that we discussed.
John

Lost Tech, Inc.
www.LostTechnologies.com
ISO 9001:2000 * ISO 14001 * ISO18001 * UL Listed
E-mail: JohnP@LostTechnologies.com
The message is ready to be sent with the following file or link attachments: Image Of Product.pdf

Electronic Metadata

"MS Exchange Server version 6.5.7638.1"
Emailing: Image of Product.pdf
Return-path: <>
From: "John C Plaintiff" <JohnP@Lost-Tech.com>
To: "<Mark@manufacturer.com>" <Mark@manufacturer.com>
Cc: "Robert Z Defendant" <Robert@Lost-Tech.com>

Second Email

From: “Robert Z Defendant” <Robert@LostTechnologies.com>
To: robertzdefendant@yahoo.com;
Sent: Thursday, March 30, 2006 9:29 AM
Subject: FW: Check This out?
funny mpeg

Second Email Metadata

From: Robert Defendant
To: robertzdefendant@yahoo.com
Return-Path: < Robert@LostTechnologies.com>
Subject: FW: Check This out?
Produced By Microsoft Exchange V6.0.6249.0
Date: Thu, 30 Mar 2006 08:29:26 -0800
From: "Robert Defendant“ <Robert@LostTechnologies.com>
To: <robertzdefendant@yahoo.com>

Third Example Email Body

From: <Jose McCormick>
To: <“John C Plaintiff”>
Date: Monday, October 02, 2006 1:14 PM
Subject: new product status
CC: <Mrs Plaintiff>

John,
We’ve started on new product. It isn’t perfect yet.
Jose

Third Example Email Metadata

"MS Exchange Server version 14.02.5004.000"
Subject: new product status

The only problem is:
Build:14.02
Rollup 3 for Exchange Server 2010
Service Pack 2 May 29, 2012

SnapChat

Snapchat:
This is a social media application that allows users to exchange images, videos and more. In addition, the application allows users to communication via video chat.

Snapchat originally centered around self-deleting media and messages which disappeared after a short time. Newer versions allow users to save media and messages.

GENERAL COMPUTER FORENICS

Evidence Collection Sources of Evidence:

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

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 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 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 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 Collection / Hashes

- "The quick brown fox jumps over the lazy dog"
  - 9e107d9d372bb6826bd81d3542a419d6
- "The quick brown fox jumps over the lazy cog"
  - ffd93f16876049265fbaef4da268dd0e

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.

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

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.

INFOTAINMENT SYSTEMS

Infotainment Systems

Infotainment Systems

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

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

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

CELL PHONES

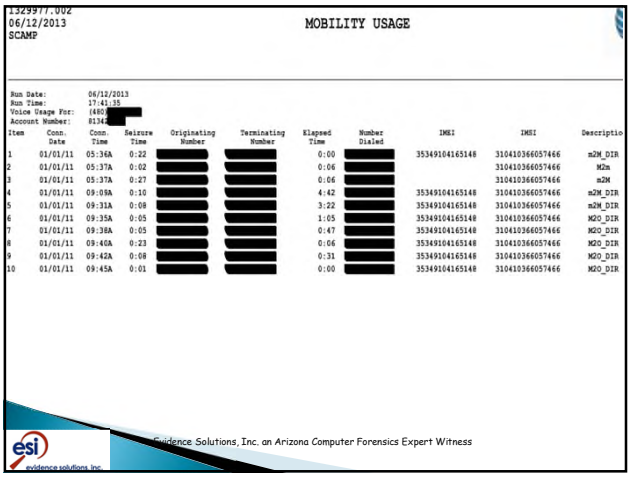
- Cell Phones & Tablets
  - Text messages
  - Photos?
    - GeoTagging
  - Calendars
  - Phone Books
  - Call Logs
  - Complete information about where the phone has been….

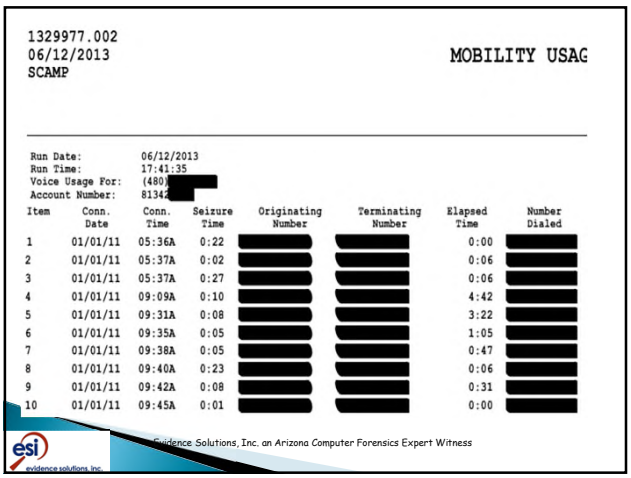
- Digital Evidence: Cell Phone Forensics

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

- Digital Evidence: Cell Phone Forensics


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)
02:33A 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
05:57A DRIVE (295) C/P
06:42A DUTY (TX-2083)
07:16A DRIVE (TX-2083)
07:59A DUTY (295) C/P
08:23A DRIVE 2.7 mi S of
09:05A DUTY (TX-4198)
09:35A DRIVE (TX-4198)
10:18A DUTY (295) C/P
10:42A DRIVE (295) C/P
11:25A DUTY (TX-4196)
11:52A DRIVE 12.8 mi NW
12:35P DUTY (295) C/P
01:01P DRIVE (295) C/P
01:28P DUTY (500)
01:33P Driver Leave(500)
01:31P DUTY (500)
01:36P OFF (500)
03/01/12 0709 SMS - Inbox
03/01/12 0710 SMS - Inbox
03/01/12 0716 Driving
03/01/12 0735 SMS - Sent
03/01/12 0737 SMS - Inbox
03/01/12 0738 SMS - Sent
03/01/12 0739 SMS - Inbox
03/01/12 0759 In Service
03/01/12 0823 Driving
03/01/12 0842 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 1152 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)
Account Number: 81342
Item | Conn. Date | Conn. Time | Seizure Time | Originating Number | Terminating Number | Elapsed Time | Number Dialed | IMSI | IMSI | Descriptio
1 | 01/01/11 | 05:36A | 0:22 | | | 0:00 | | 353491041651 48 | 310410366057466 | m2M_DIR
2 | 01/01/11 | 05:37A | 0:02 | | | 0:06 | | | 310410366057466 | M2m
3 | 01/01/11 | 05:37A | 0:27 | | | 0:06 | | | 310410366057466 | m2M
4 | 01/01/11 | 09:09A | 0:10 | | | 4:42 | | 353491041651 48 | 310410366057466 | m2M_DIR
5 | 01/01/11 | 09:31A | 0:08 | | | 3:22 | | 353491041651 48 | 310410366057466 | m2M_DIR
6 | 01/01/11 | 09:35A | 0:05 | | | 1:05 | | 353491041651 48 | 310410366057466 | M2O_DIR
7 | 01/01/11 | 09:38A | 0:05 | | | 0:47 | | 353491041651 48 | 310410366057466 | M2O_DIR
8 | 01/01/11 | 09:40A | 0:23 | | | 0:06 | | 353491041651 48 | 310410366057466 | M2O_DIR
9 | 01/01/11 | 09:42A | 0:08 | | | 0:31 | | 353491041651 48 | 310410366057466 | M2O_DIR
10 | 01/01/11 | 09:45A | 0:01 | | | 0:00 | | 353491041651 48 | 310410366057466 | M2O_DIR
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)
Account Number: 81342
Item | Conn. Date | Conn. Time | Seizure Time | Originating Number | Terminating Number | Elapsed Time | Number Dialed
1 | 01/01/11 | 05:36A | 0:22 | | | 0:00 |
2 | 01/01/11 | 05:37A | 0:02 | | | 0:06 |
3 | 01/01/11 | 05:37A | 0:27 | | | 0:06 |
4 | 01/01/11 | 09:09A | 0:10 | | | 4:42 |
5 | 01/01/11 | 09:31A | 0:08 | | | 3:22 |
6 | 01/01/11 | 09:35A | 0:05 | | | 1:05 |
7 | 01/01/11 | 09:38A | 0:05 | | | 0:47 |
8 | 01/01/11 | 09:40A | 0:23 | | | 0:06 |
9 | 01/01/11 | 09:42A | 0:08 | | | 0:31 |
10 | 01/01/11 | 09:45A | 0:01 | | | 0:00 |
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: 81342[redacted]

Item	Conn. Date	Conn. Time	Originating Number	Elapsed Time	Bytes Up	Bytes Dn	IMEI	IMSI	Access Pt	Description
6374	05/26/11	10:00A	[redacted]	13:13	6677	111991	353491041651480 4	310410366057466	acds.voicemai l	_MOBILE_DATA_
6375	05/26/11	10:14A	[redacted]	5:08	0	0	353491041651480 4	310410366057466	acds.voicemai l	_MOBILE_DATA_
6376	05/26/11	10:31A	[redacted]	13:14	9271	49317	353491041651480 4	310410366057466	BLACKBERRY.NE T	_MOBILE_DATA_
6377	05/26/11	10:31A	[redacted]	2:13	2639	8417	353491041651480 4	310410366057466	WAP.CINGULAR	_MOBILE_DATA_
6378	05/26/11	10:44A	[redacted]	0:24	553	571	353491041651480 4	310410366057466	BLACKBERRY.NE T	_MOBILE_DATA_

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

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

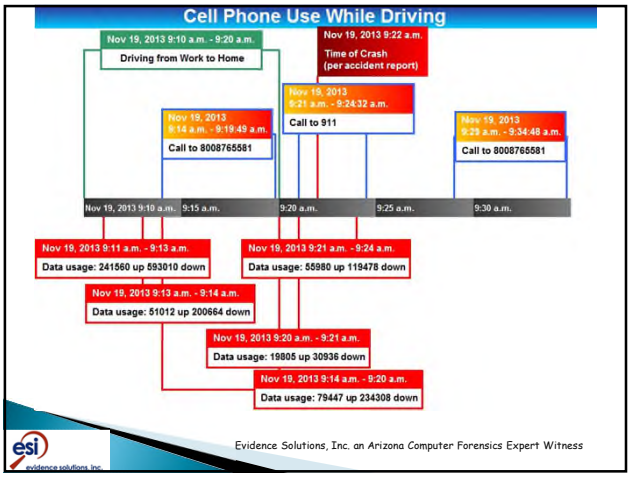
1329977.002
06/12/2013
SCAMP

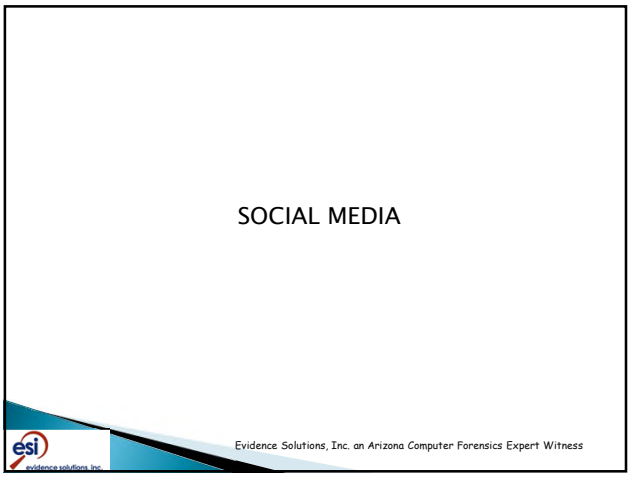
MOBILITY USAGE

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

Item	Conn. Date	Conn. Time	Originating Number	Terminating Number	IMEI	IMSI	Description
913	01/14/11	09:37P	[redacted]5660	[redacted]3109	353491041651480	310410366057466	OUT
914	01/14/11	09:37P	[redacted]5660	[redacted]3109	353491041651480	310410366057466	OUT
915	01/14/11	09:41P	[redacted]3109	[redacted]5660	353491041651480	310410366057466	IN
916	01/15/11	08:06A	[redacted]5660	[redacted]3587	353491041651480	310410366057466	OUT
917	01/15/11	08:16A	[redacted]3587	[redacted]5660	353491041651480	310410366057466	IN
918	01/15/11	08:32A	[redacted]5660	[redacted]3587	353491041651480	310410366057466	OUT
919	01/15/11	08:32A	[redacted]3587	[redacted]5660	353491041651480	310410366057466	IN

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


Cell Phone Use While Driving
Nov 19, 2013 9:10 a.m. - 9:20 a.m.
Driving from Work to Home
Nov 19, 2013 9:22 a.m.
Time of Crash
(per accident report)
Nov 19, 2013
9:21 a.m. - 9:24:32 a.m.
Call to 911
Nov 19, 2013
9:14 a.m. - 9:19:49 a.m.
Call to 8008765581
Nov 19, 2013
9:29 a.m. - 9:34:48 a.m.
Call to 8008765581
Nov 19, 2013 9:10 a.m.
9:15 a.m.
9:20 a.m.
9:25 a.m.
9:30 a.m.
Nov 19, 2013 9:11 a.m. - 9:13 a.m.
Data usage: 241560 up 593010 down
Nov 19, 2013 9:21 a.m. - 9:24 a.m.
Data usage: 55980 up 119478 down
Nov 19, 2013 9:13 a.m. - 9:14 a.m.
Data usage: 51012 up 200664 down
Nov 19, 2013 9:20 a.m. - 9:21 a.m.
Data usage: 19805 up 30936 down
Nov 19, 2013 9:14 a.m. - 9:20 a.m.
Data usage: 79447 up 234308 down
Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness


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


LinkedIn
myspace
.com
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!

The statistics of need

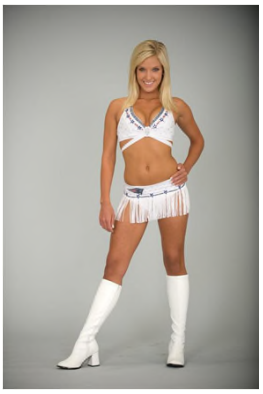
- There are over:
  - 800 million Facebook users
  - 300 million people using Twitter
- Evidence from social media sites can be relevant to almost every litigation dispute and investigation matter.

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.

Here is what is out there

- New England Patriots Cheerleader, Caitlin Davis, 18



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.

Here is how they use it....

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

Here is how they use it....

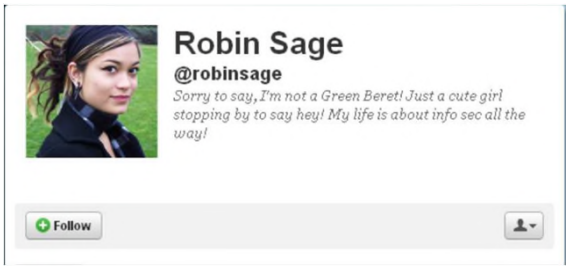
- A juror posted details of the case she was serving on. The she wrote, "I don't know which way to go, so I'm holding a poll."
- An anonymous tip resulted in the woman being immediately dismissed from the jury.

IMPERSONATION

Security is paramount

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

Scammers are Everywhere



Scammers are Everywhere

- Graduate of Massachusetts Institute of Technology
- Cyber Threat Analyst – US Navy Network Warfare Command

Scammers are Everywhere

- 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.

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.

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."

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.

CHAIN OF CUSTODY

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

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 you will find it on the server.

esi evidence solutions, inc.

esi 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:

esi 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 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

esi 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.

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.

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

Faculty:

Scott Greene
Evidence Solutions, Inc.

Scott@EvidenceSolutions.com
www.EvidenceSolutions.com

866-795-7166

Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness