



Evidence Solutions, Inc.

Arizona Attorneys for Criminal Justice

Arizona Public Defenders Association

Present:

Computer Forensics

January 8, 2015

Presented by:

Scott Greene, SCFE, CEO  
Evidence Solutions, Inc.

An Arizona Based Computer Forensics Firm

520-512-5001

866-795-7166

[Scott@EvidenceSolutions.com](mailto:Scott@EvidenceSolutions.com)

## Computer Forensics

### Arizona Public Defenders Association APDA

Faculty:

Scott Greene

Evidence Solutions, Inc.

[Scott@EvidenceSolutions.com](mailto:Scott@EvidenceSolutions.com)

[www.EvidenceSolutions.com](http://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 700 Million PC type machines.



Evidence Solutions, Inc. Cell Phone 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
  - iPpods, 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 a 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

## Evidence Collection Sources of Evidence:

- ▶ How data is stored on disk drives
  - 32,768 bytes in each allocation unit
  - A file that contains the following text: “hi” or about 2 bytes, actually consumes 32,768 bytes
  - The difference or 32,766 bytes is ‘Slack Space’. This space is not over written each time.



Evidence Solutions, Inc. Cell Phone Forensics Expert Witness Arizona

## How Data is Stored Example

- ▶ For purposes of this example, let's say that the allocation unit is 200 Characters.
  - The directory entry looks like: 00000000.000
  - The data looks like:

A grid of 200 zeros arranged in 10 rows and 20 columns, representing a 200-character allocation unit.

Evidence Solutions, Inc. Digital Forensics Expert Witness Arizona

A large grid of 2000 zeros arranged in 20 rows and 100 columns, representing a 2000-character allocation unit.

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. 00000000000
```



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. 00000000000
```



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. 00000000000
```



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  
p l e a s u r e t o m e e t w i t  
h y o u a n d t o d i s c u s s  
y o u r d e s i r e t o p u r c  
h a s e t h e b o a t . P l e a s  
e l e t m e k n o w i f y o u  
n e e d a n y t h i n g e l s e  
. S i n c e r e l y H e n r y P s  
I t h i n k i t i s w o r t h  
\$ 1 1 , 9 9 9 . 0 0 0 0 0 0 0 0 0 0



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

## 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](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&m=bellaluna](http://mysecurewallet.nl/payment/islive/isliveeu/?p=199&pi=typein_isliveeu&flash=1&m=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

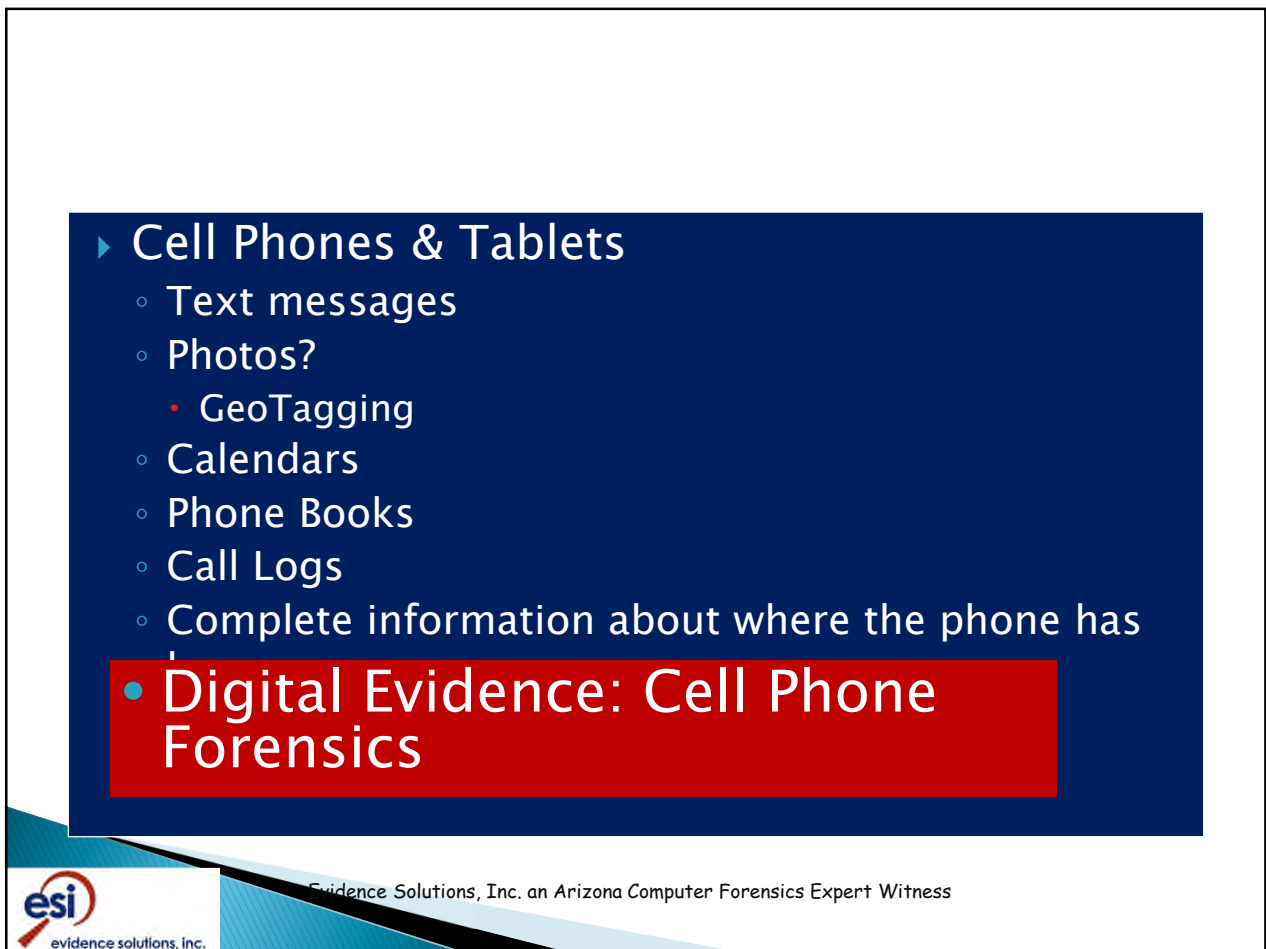
## How not to do things....

### ▶ 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



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

- Digital Evidence: Cell Phone Forensics



evidence solutions, inc.

Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness



Since 1993

“... statistics from the DOT:


- ▶ A driver who stares at his or her cell phone for just two seconds at 65 mph has traveled almost 200 feet without seeing the road. That's half the typical stopping distance, gone!
- ▶ Sending or receiving a text takes a driver's eyes from the road for an average of 4.6 seconds (or more than 500 feet of travel distance at 65 mph).
- ▶ In 2009, nearly 5,500 people were killed in crashes involving driver distraction, and an estimated 448,000 were injured.
- ▶ 16% of fatal crashes and 20% of injury crashes in 2009 involved reports of distracted driving.
- ▶ Drivers who use hand-held devices are 4 times more likely to get into crashes serious enough to injure themselves.
- ▶ Text messaging creates a crash risk 23 times worse than driving while not distracted,
- ▶ Headset cell-phone use is not substantially safer than hand-held use.
- ▶ Using a cell phone while driving, whether it's hand-held or hands-free, delays a driver's reactions as much as having a blood alcohol concentration at the legal limit of .08 percent.”




evidence solutions, inc.

Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness






Item	Conn. Date	Conn. Time	Orig. Number	Term. Number	IMEI	Description	Content	Tower Location
1	9/23/2013	11:48	Redacted	Redacted	Redacted	Incoming SMS	Wht up, lookn 4 sum peace tabs or at least sum oj, u got any?	33.30522, -111.72406
2	9/23/2013	11:49	Redacted	Redacted	Redacted	Outgoing SMS	I'll check, how much do u need?	33.30522, -111.72406
3	9/23/2013	11:50	Redacted	Redacted	Redacted	Incoming SMS	Enough 4 the weeknd, couple grams?	33.30522, -111.72406
4	9/23/2013	11:53	Redacted	Redacted	Redacted	Outgoing SMS	Meet at Pacos in 30?	33.30522, -111.72406
5	9/23/2013	11:54	Redacted	Redacted	Redacted	Incoming SMS	Tight	33.30522, -111.72406



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

04/02/12 01:54	Driving		
04/02/12 02:17	SMS - Sent	Sydney	4429788174
04/02/12 02:21	SMS - Inbox	Sydney	4429788174
04/02/12 02:21	SMS - Sent	Sydney	4429788174
04/02/12 02:21	SMS - Inbox	Sydney	4429788174
04/02/12 02:21	SMS - Sent	Sydney	4429788174
04/02/12 02:22	SMS - Inbox	Sydney	4429788174
04/02/12 02:23	SMS - Sent	Sydney	4429788174
04/02/12 02:23	SMS - Sent	Sydney	4429788174
04/02/12 02:23	SMS - Inbox	Sydney	4429788174
04/02/12 02:23	SMS - Inbox	Sydney	4429788174
04/02/12 02:24	SMS - Inbox	Sydney	4429788174



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

Driver Miles Today: 374.7 Driver Name: [REDACTED]  
 Co-Driver Miles Today: 0.0 Co-Driver Name: [REDACTED]  
 Vehicle Miles Today: 374.7

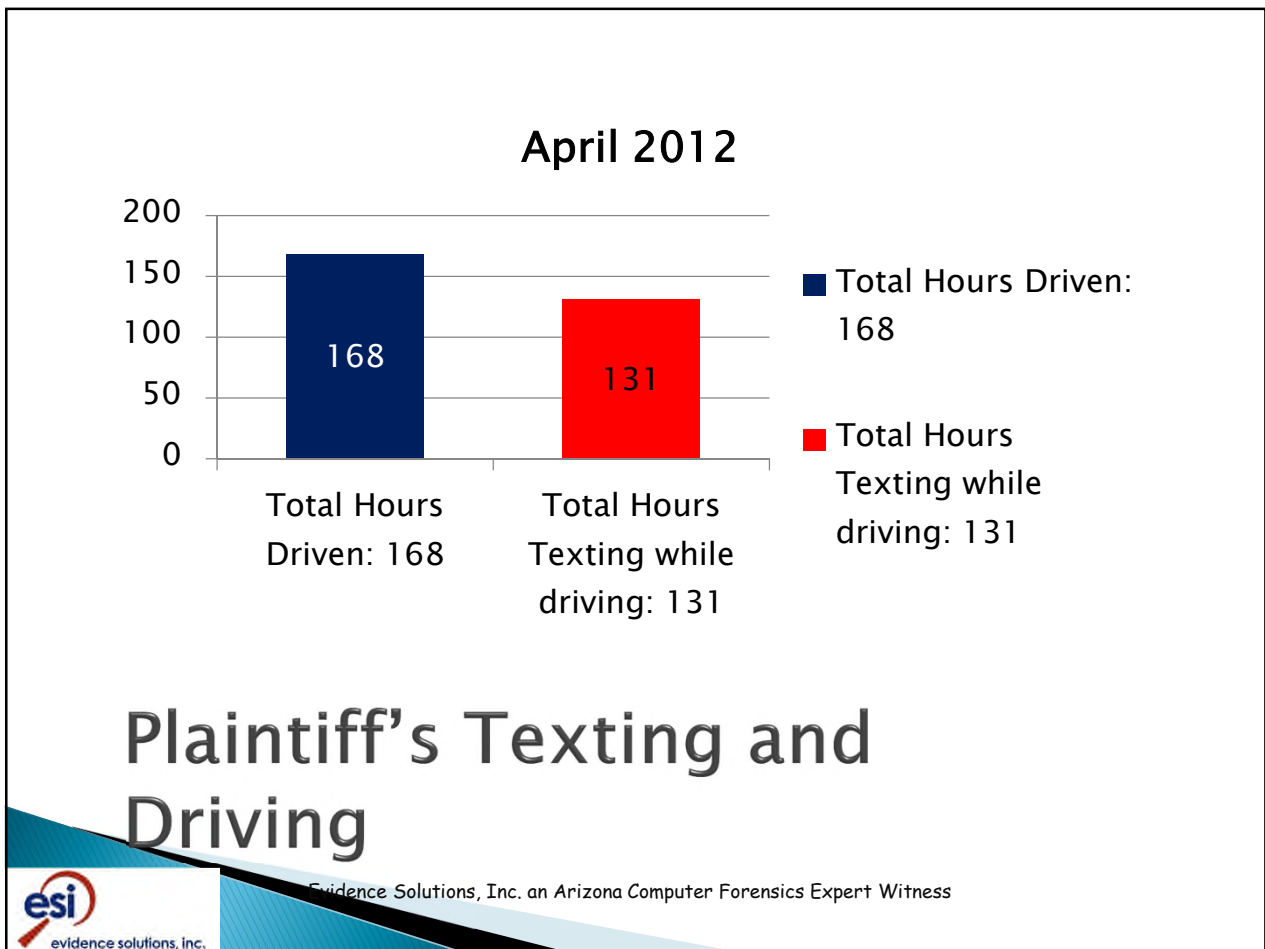
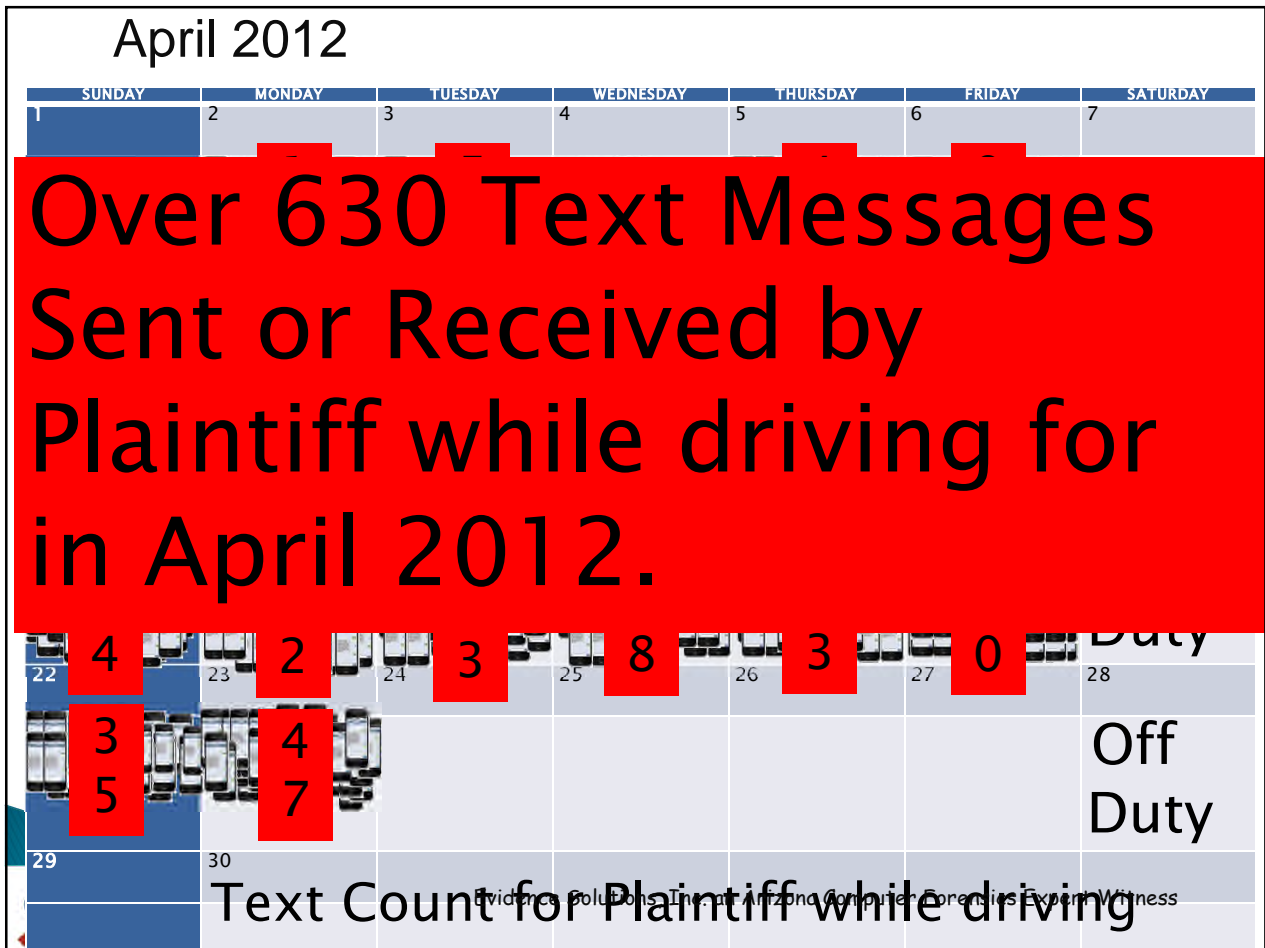
Carrier: [REDACTED] Fleet [REDACTED]

Remarks	Time	Status	Description	Inspect
PRE-TRIP @ 1:07a 00:05	12:00A	OFF	(500) [REDACTED]	
VEHICLE: 303	01:07A	DUTY	(500) [REDACTED]	
ROUTE: 0301120109	01:12A		State: TX	
POST-TRIP @ 1:31p 00:05	01:12A		Driver Join(500) [REDACTED]	
	01:12A	DUTY	(500) [REDACTED]	
	01:14A	DRIVE	(500) Odessa Yard [REDACTED]	
	02:00A	DUTY	(TX-2083) [REDACTED]	
	02:33A	DRIVE	(TX-2083) [REDACTED]	
	03:14A	DUTY	(295) C/P [REDACTED]	
	03:38A	DRIVE	(295) C/P GOLDSMITH [REDACTED]	

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

Time	Status	Description	
12:00A	OFF	(500) [REDACTED]	
01:07A	DUTY	(500) [REDACTED]	
01:12A		State: TX	
01:12A		Driver Join(500) [REDACTED]	
01:12A	DUTY	(500) [REDACTED]	
01:14A	DRIVE	(500) [REDACTED]	03/01/12 0709 SMS - Inbox
02:00A	DUTY	(TX-2083) [REDACTED]	03/01/12 0710 SMS - Inbox
02:33A	DRIVE	(TX-2083) [REDACTED]	03/01/12 0716 Driving
03:14A	DUTY	(295) C/P [REDACTED]	03/01/12 0735 SMS - Sent
03:38A	DRIVE	(295) C/P [REDACTED]	03/01/12 0737 SMS - Inbox
04:16A	DUTY	(TX-2083) [REDACTED]	03/01/12 0738 SMS - Sent
04:50A	DRIVE	(TX-2083) [REDACTED]	03/01/12 0739 SMS - Inbox
05:32A	DUTY	(295) C/P [REDACTED]	03/01/12 0759 In Service
05:57A	DRIVE	(295) C/P [REDACTED]	03/01/12 0823 Driving
06:42A	DUTY	(TX-2083) [REDACTED]	03/01/12 0842 SMS - Sent
07:16A	DRIVE	(TX-2083) [REDACTED]	03/01/12 0905 In Service
07:59A	DUTY	(295) C/P [REDACTED]	03/01/12 0935 Driving
08:23A	DRIVE	2.7 mi S of [REDACTED]	03/01/12 0955 SMS - Inbox
09:05A	DUTY	(TX-4198) [REDACTED]	03/01/12 1018 In Service
09:35A	DRIVE	(TX-4198) [REDACTED]	03/01/12 1042 Driving
10:18A	DUTY	(295) C/P [REDACTED]	03/01/12 1125 In Service
10:42A	DRIVE	(295) C/P [REDACTED]	03/01/12 1152 Driving
11:25A	DUTY	(TX-4196) [REDACTED]	03/01/12 1230 SMS - Inbox
11:52A	DRIVE	12.8 mi NW [REDACTED]	03/01/12 1235 In Service
12:35P	DUTY	(295) C/P [REDACTED]	03/01/12 1240 SMS - Inbox
01:01P	DRIVE	(295) C/P [REDACTED]	
01:28P	DUTY	(500) [REDACTED]	
01:31P		Driver Leave(500) [REDACTED]	
01:31P	DUTY	(500) [REDACTED]	
01:36P	OFF	(500) [REDACTED]	

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



(Keith) Hey you send me more pics do you have a full body pic I can see sexy

LOL no I don't .....


Will you take one for me" - "So how are thing with you and your mate

Maybe later .....and they are so so ....

"They are so so ?

Yea sometimes it seems like were just roommates LOL I have to tell u something and lets hope u don't RUN ....

37


 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: 81342 [REDACTED]

Item	Conn. Date	Conn. Time	Seizure Time	Originating Number	Terminating Number	Elapsed Time	Number Dialed	IMEI	IMSI	Descriptio
1	01/01/11	05:36A	0:22	[REDACTED]	[REDACTED]	0:00	[REDACTED]	35349104165148	310410366057466	m2M_DIR
2	01/01/11	05:37A	0:02	[REDACTED]	[REDACTED]	0:06	[REDACTED]		310410366057466	M2m
3	01/01/11	05:37A	0:27	[REDACTED]	[REDACTED]	0:06	[REDACTED]		310410366057466	m2M
4	01/01/11	09:09A	0:10	[REDACTED]	[REDACTED]	4:42	[REDACTED]	35349104165148	310410366057466	m2M_DIR
5	01/01/11	09:31A	0:08	[REDACTED]	[REDACTED]	3:22	[REDACTED]	35349104165148	310410366057466	m2M_DIR
6	01/01/11	09:35A	0:05	[REDACTED]	[REDACTED]	1:05	[REDACTED]	35349104165148	310410366057466	M2O_DIR
7	01/01/11	09:38A	0:05	[REDACTED]	[REDACTED]	0:47	[REDACTED]	35349104165148	310410366057466	M2O_DIR
8	01/01/11	09:40A	0:23	[REDACTED]	[REDACTED]	0:06	[REDACTED]	35349104165148	310410366057466	M2O_DIR
9	01/01/11	09:42A	0:08	[REDACTED]	[REDACTED]	0:31	[REDACTED]	35349104165148	310410366057466	M2O_DIR
10	01/01/11	09:45A	0:01	[REDACTED]	[REDACTED]	0:00	[REDACTED]	35349104165148	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) [REDACTED]  
Account Number: 81342 [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]

 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	3534910416514804	310410366057466	acds.voicemai 1	_MOBILE_DATA_
6375	05/26/11	10:14A	[REDACTED]	5:08	0	0	3534910416514804	310410366057466	acds.voicemai 1	_MOBILE_DATA_
6376	05/26/11	10:31A	[REDACTED]	13:14	9271	49317	3534910416514804	310410366057466	BLACKBERRY.NE T	_MOBILE_DATA_
6377	05/26/11	10:31A	[REDACTED]	2:13	2639	8417	3534910416514804	310410366057466	WAP.CINGULAR	_MOBILE_DATA_
6378	05/26/11	10:44A	[REDACTED]	0:24	553	571	3534910416514804	310410366057466	BLACKBERRY.NE	_MOBILE_DATA_

 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  
 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	35349104165148	310410366057466	OUT
914	01/14/11	09:37P	[REDACTED]5660	[REDACTED]3109	35349104165148	310410366057466	OUT
915	01/14/11	09:41P	[REDACTED]3109	[REDACTED]5660	35349104165148	310410366057466	IN
916	01/15/11	08:06A	[REDACTED]5660	[REDACTED]8587	35349104165148	310410366057466	OUT
917	01/15/11	08:16A	[REDACTED]8587	[REDACTED]5660	35349104165148	310410366057466	IN
918	01/15/11	08:32A	[REDACTED]5660	[REDACTED]8587	35349104165148	310410366057466	OUT
919	01/15/11	08:32A	[REDACTED]8587	[REDACTED]5660	35349104165148	310410366057466	IN



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness


- 
- 
- 
- 



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

## Security is paramount

- ▶ Historic method of data gathering for social engineering



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.



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

## The statistics of need:

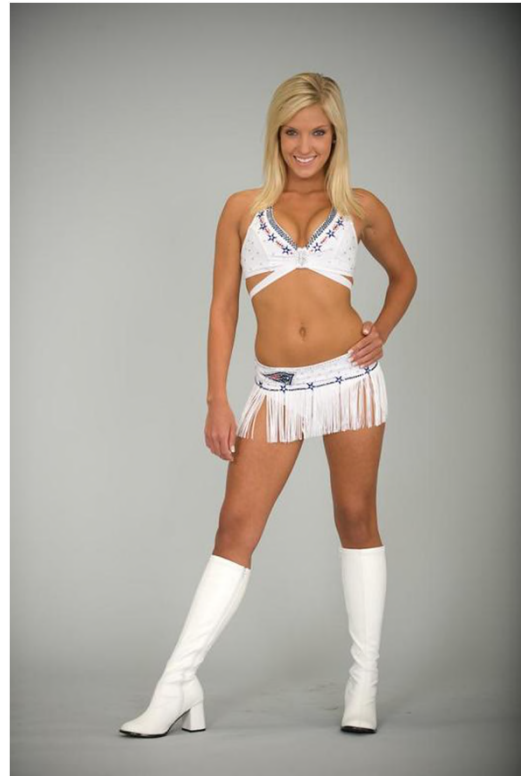
- Social media evidence is:
  - widely discoverable
  - generally not subject to privacy constraints when established to be relevant to a case, particularly when that data is held by a party to litigation or even a key witness.



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

## 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





## Security is paramount

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

## 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



## Getting it Admitted

- Many courts have applied Rule 901(b)(4) by ruling that metadata and file level hash values associated with ESI can be sufficient circumstantial evidence to establish its authenticity.



## Getting it Admitted

- ▶ Mere printouts are not enough:
  - In *State of Connecticut vs. Eleck*, the Facebook evidence in the form of a printout was rejected for failure of adequate authentication.
  - ‘it is incumbent on the party seeking to admit social media data to offer detailed “circumstantial evidence that tends to authenticate” the unique medium of social media evidence.’



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

## Getting it Admitted

- ▶ Authentication:
  - *State of Texas v Tienda* the prosecution successfully admitted key MySpace evidence over the defendant’s objection, laying a foundation through various circumstantial evidence.



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

## Getting it Admitted

- ▶ Key circumstantial evidence included:
  - relevant metadata fields
  - The username ( consistent with their commonly known nick name )
  - email addresses
  - User ID number
  - Stated location (City)
  - Posted communications with other suspects
  - Photos with associated date and time stamps.



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

## Getting it Admitted

### Metadata for Facebook includes:

- |   |                           |
|---|---------------------------|
| •Unified resource ID  | •Poster's Unique ID       |
| •Item Type <ul style="list-style-type: none"> <li>•Wall Post</li> <li>•News Item</li> <li>•Photo</li> </ul> | •User's Unique ID         |
| •Message recipients   | •User's Display name      |
| •Method used to post <ul style="list-style-type: none"> <li>•Cell phone</li> <li>•Browser</li> </ul>        | •Date & Time Created      |
|   | •Date & Time Last revised |
|   | •Number of comments       |
|   | •Etc                      |

Twitter and LinkedIn items have their own unique but generally comparable metadata.



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness



## Great Quote

- ▶ Computer Power is more than 8000 times less expensive than 30 years ago.
- ▶ “If we had similar progress in automotive technology, today you could buy a Lexus for about \$2. It would travel at the speed of sound, and go about 600 miles on a thimble of gas”

- “Randall Tobias, former Vice Chairman of AT&T, as quoted by – John Naisbitt, *Global Paradox*



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

An Arizona Computer Forensics Company,  
Evidence Solutions, Inc. provides:  
Digital Forensics  
Computer Forensics  
Cell Phone Forensics  
Electronic Medical Record Forensics  
Vehicle and Truck Forensics  
Electronic Logging Device Forensics  
Infotainment Forensics  
And  
More!



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

Faculty:

Scott Greene  
Evidence Solutions, Inc.

[Scott@EvidenceSolutions.com](mailto:Scott@EvidenceSolutions.com)  
[www.EvidenceSolutions.com](http://www.EvidenceSolutions.com)

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



Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness