

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

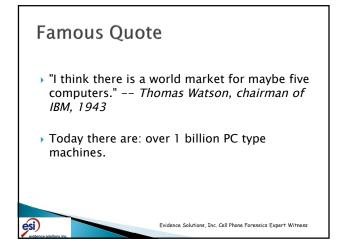
Early Bird Rate	Regular Rate
□ \$ 90.00	\$ 105.00 MCBA Members
□ \$ 65.00	\$ 80.00 Paralegal & Public Lawyers Division members
□ \$ 125.00	\$ 140.00 Non-Members
□ \$ 15.00	\$ 15.00 MCBA Student members
□ \$ Free	\$ Free MCBA Sustaining members

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

Name (please print): Address:	 E-mail:	
Method of Payment:		CAN EXPRESS
Credit Card#: Signature:	 Exp.Date:	CVV#:

Cell Phone Forensics Expert Witness - AZ





# Disclaimer

- Scott Greene, & Evidence Solutions, Inc. are not supplying legal advice.
- Because, well, I'm not an attorney.

esi)

esi)

# **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."

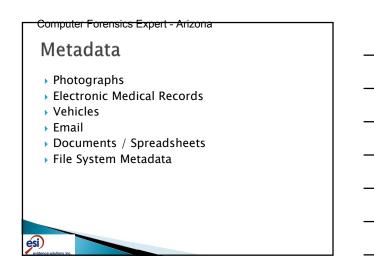
# Ethical Considerations

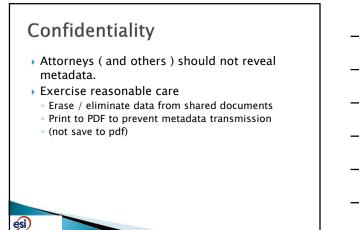
- The Non-discovery Context: when lawyers send or receive information (i.e., "communications") containing metadata.
- The Discovery Context: when lawyers send, produce or receive electronically stored information (ESI) containing metadata in response to a discovery request or subpoena.
  - The Sedona 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.

esi) Cell Phone Forensiss Expert Witness - AZ





# Competence

> Lawyers should be competent to represent their clients.



Digital Forensics, Cyber Forensics

### Computer Forensics Expert - Arizona

### Competence

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

### **Supervision**

esi)

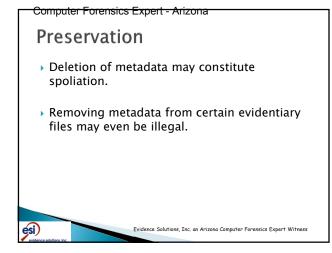
esi)

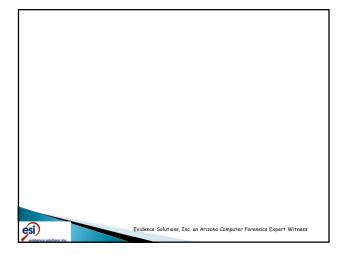
esi)

- 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).







Cell-Phone Forensist Expert Witness - AZ

### Computer Forensics Expert - Arizona

# **Evidence Collection**

### Storage Media

esi)

esi)

esi)

- 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 Solutions, Inc. Arizona Computer 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 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 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"

Evidence Solutions, Inc. Computer Forensics Expert Witness Arizona

ffd93f16876049265fbaef4da268dd0e

# Evidence Collection Sources of Evidence:

esi)

esi)

esi)

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.

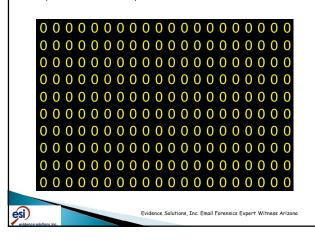
Evidence Solutions, Inc. Cell Phone Forensics Expert Witness Arizona

# 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: 0000000.000
- The data looks like:



Cell Phone Forensis Expert Witness - AZ

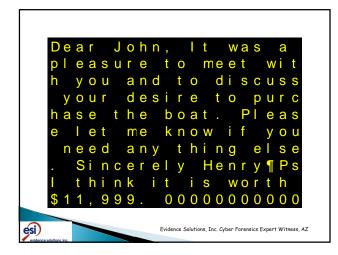


### How Data is Stored Example We create a document that is stored in this allocation unit. The directory entry looks like: document.doc The data looks like: Dear John, It was a pleasure to meet wit h you and to discuss your desire to purc hase the boat. Pleas e let me know if you need any thing else . Sincerely Henry Ps I think it is worth \$11,999. ¶00000000000

D	e	a	r		J	0	h	n	,			t		W	a	s		a	
р		е	a	S	u	r	е		t	0		m	е	е	t		W	i.	t
h		у	0	u		а	n	d		t	0		d	i.	S	С	u	S	S
	y	0	u	r		d	е	S	i	r	е		t	0		р	u	r	С
h	а	S	е		t	h	е		b	0	а	t			Ρ		е	а	S
е			е	t		m	е		k	n	0	W		i.	f		у	0	ι
	n	е	е	d		а	n	у		t	h	i.	n	g		е		S	e
		S	i.	n	С	е	r	е		у		Н	е	n	r	у		Ρ	S
I		t	h	i	n	k		i.	t		i.	s		W	0	r	t	h	
\$	1	1		9	9	9		¶	0	0	0	0	0	0	0	0	0	0	С



Computer Forensics Expert - Arizona HOW Data is Stored
Example
We edit out the price, the document looks like:
<ul> <li>The directory entry looks like: document.doc</li> <li>The data looks like:</li> </ul>
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



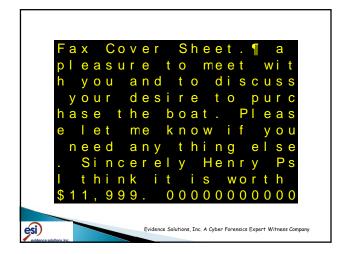
### How Data is Stored Example • The document is erased / deleted ( from the recycle bin ): • The directory entry looks like: ~ocument.doc • The data looks like: • The data looks like: Dear John, It was a pleasure to meet wit h you and to discuss your desire to purc hase the boat. Pleas e let me know if you need any thing else . Sincerely Henry [PS I think it is worth \$11,999.00000000000



### Computer Forensics Expert - Arizona 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:







## How Data is Stored

### Slack Space or File Slack:

esi)

 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

esi)

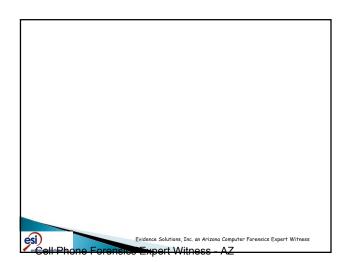
esi)

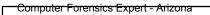
### How Data is Stored

Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

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.





# What is Chain of Custody

### Chain of custody

esi)

esi)

 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.



esi)

esi)

esi)

# 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.
- 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.

Cell Phone Forensics Expert Witness - AZ

### Computer Forensics Expert - Arizona 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.

esi)

esi)

### 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. 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
- nas 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.

esi) Expert Witness

### General Rules for Chain of Custody

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

# Seizing the original

- Should be bagged and documented
- Copying the original
  - Date copied

esi)

- Location copied
- Type of copy

esi)

• Hash of original

Evidence Solutions, Inc. on Arizona Computer Forensics Expert Witness

Cell-Phone Forensise Expert Witness - AZ

esi)

esi)

### 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:
  - $^{\circ}$  The conditions under which the evidence is gathered
  - $\,\circ\,$  The method with which the evidence is gathered
  - The identity of all evidence handlers
  - The length of time of evidence custody by each
  - handlerThe 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

esi)

Cell-Phone Forensics Expert Witness - A

### Computer Forensics Expert - Arizona What is Unique about Electronically Stored Evidence?

### Servers

- $\,^\circ\,$  Most companies intend for data to be stored on servers
- Ha!

eși)

esi)

ési )

 $^{\circ}$  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:

- $\,{}^{\circ}$  The method with which the evidence is gathered
- $^{\circ}$  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

	evidence solutions, Inc.													
	Equipment & Media Chain of Custody													
Case:														
Hdd	Floppy	Tape	BlackBox	CellPhone	CD	DVD	Other							
Make:				Model:										
S/N:				Jumpers:										
From:				To: Evide	ence Solutio	an Inc								
Date:				Time:	nce souu	ms, snc.								
Location:				Signature:										
From:				To:										
Date:				Time:										
Location:				Signature:										

### 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

esi)

esi)

• All media has been secure throughout the time period

### **Rules for Electronically Stored** Information, Chain of Custody

- Digital investigators should follow four
- µigital investigators should follow four basic steps in order to correctly maintain a digital chain of custody:
  Physically control the scene, or if conducting a remote network investigation, log all access and connectivity through an integrated and secure reporting function
  Create a binary, forensic duplication of original data in a non-invasive manner / Write Protect the original media
  Create a digital fingerprint (hach) that continuelly:

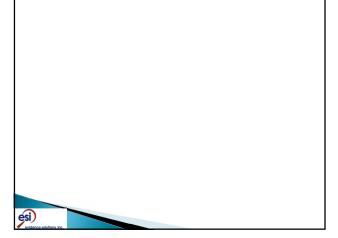
- Create a digital fingerprint (hash) that continually verifies data authenticity Log all investigation details in a thorough report generated by an integrated computer forensics software application

Expert Witness

# Plain and Simple:

esi)

- 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.





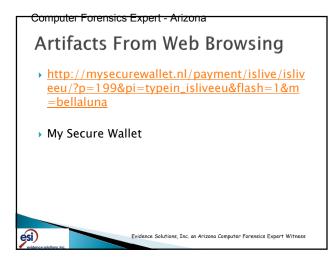
Cell-Phone Forensics Expert Witness - Az





# Artifacts From Web Browsing http://www.subito.it/appartamenti/appartamenti/appartamento-a-grutti-di-gualdo-cattaneo-rif-301-perugia-77278016.htm Appartamento in castello di Grutti - Appartamenti In vendita a Perugia

Cell Phone Forensic Expert Witness - AZ



# 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.

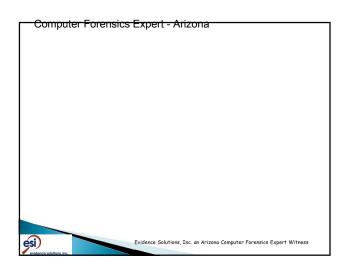
Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness

# How not to do things....

esi)

esi)

- The IT department overwrote the data!!!
  - Employee deleted data from hard disk drive
  - $\boldsymbol{\cdot}$  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



Cell	Phones & Tablets	
• Te	xt messages	
• Ph	otos?	
• 0	ieoTagging	
• Ca	lendars	
• Ph	one Books	
• Ca	ll Logs	
• Co	mplete information about where the phone has	
be	en	
- Di	sitel Evidence, Cell Phone	
	gital Evidence: Cell Phone	
FC	rensics	
	Swidence Solutions, Inc. an Arizona Computer Forensics Expert Witness	
dence solutions inc.		

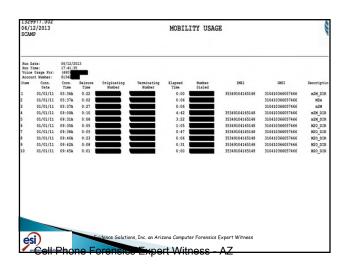
	Cell Phones & Tablets
	<ul> <li>Browsing History</li> </ul>
	<ul> <li>Documents</li> </ul>
	• Email accounts
	<ul> <li>Online data storage accounts</li> </ul>
	Digital Evidence: Cell Phone
	Forensics
	T OT CHISTCS
-	
esi	Evidence Solutions, Inc. an Arizona Computer Forensics Expert Witness
1.	Cell Phone Forence Expert Witness - A7

e	si)		Forens		pert ·	- Arizo	na	
ltem	Conn. Date	Conn. Time	Orig. Number	Term. Number	IMEI	Descriptio n	Content	Tower Location
1	9/23/2 013	11:48	Redacted	Redacted	Redacte d	Incoming SMS	Wht up, lookn 4 sum peace tabs or at lest sum oj, u got any?	33.30522, - 111.72406
2	9/23/2 013	11:49	Redacted	Redacted	Redacte d	Outgoing SMS	I'll check, how much do u need?	33.30522, - 111.72406
3	9/23/2 013	11:50	Redacted	Redacted	Redacte d	Incoming SMS	Enugh 4 the weeknd, couple grams?	33.30522, - 111.72406
4	9/23/2 013	11:53	Redacted	Redacted	Redacte d	Outgoing SMS	Meet at Pacos in 30?	33.30522, - 111.72406
5	9/23/2 013	11:54	Redacted	Redacted	Redacte d	Incoming SMS	Tight	33.30522, - 111.72406
esi	ence solutions	ins.	Suidence S	Solutions, Inc	. an Arizor	ia Computer F	Forensics Expert Witness	

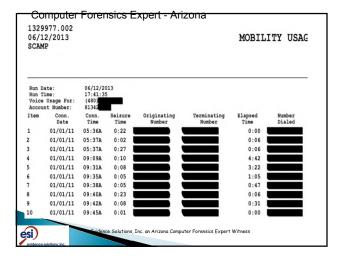
12:00A OFF	(500)	
01:07A DUTY	(500) correspondences and a	
01:12A	State: TX	
01:12A	Driver Machine and Antonio and Antonio	
01:12A DUTY	(500) determine the second	
01:14A DRIVE	(500)	03/01/12 0709 5M5 - Inbox
02:00A DUTY	(TX-2083)	03/01/12 0710 SM5 - Inbox
02:33A DRIVE	(TX-2083) ensue 2040040400 ensue 704 ensues	01/01/12 0716 Driving
03:14A DUTY	(295) C/P (200)	03/01/12 0735 SM5 - Sent
03:38A DRIVE	(295) C/P (Denuty) Construction of the	03/01/12 0737 SM5 - Inbox
04:16A DUTY	(TX-2083) with merior prevention and a state of the	02/01/12 0738 SMS - Sent
04:50A DRIVE	(TX-2083) @000785ceffer. 200	03/01/12 0739 SM5 - Inbox
05:32A DUTY	(295) C/P (1000) (200)	03/01/12 0759 In Service
05:57A DRIVE	(295) C/P (100) 500 500 500 500 500 500	03/01/12 0842 5M5 - Sent
06:42A DUTY	(TX-2083) (1840-1840-1840-1840-1840-1840-1840-1840-	03/01/12 0905 In Service
07:16A DRIVE	(TX-2083) (1000000000000000000000000000000000000	03/01/12 0935 Driving
07:59A DUTY	(295) C/P (200) CONTRACTOR (200)	03/01/12 0955 SM5 - Inbox
08:23A DRIVE	2.7 mi s of contractions	03/01/12 1018 In Service
09:05A DUTY	(1x-4198)	03/01/12 1042 Driving
09:35A DRIVE	(+x-4198) (#************************************	03/01/12 1125 In Service
10:18A DUTY	(295) C/P (1) (200) (200)	> 09/01/12 1152 Oriving
10:42A DRIVE	(295) C/P (100) (200) (200)	03/01/12 1250 SM5 - Inbox
11:25A DUTY	(TX-4196) (1000000000000000000000000000000000000	03/01/12 1235 In Service
11:52A DRIVE	12.5 mi Ny distantiana	03/01/12 1240 SMS - Inbox
12:35P DUTY	(295) C/P (	
01:01P DRIVE	(295) C/P (2000) (2000) (2000) (2000)	
01:28P DUTY	(500)	
01:31P	Driver Leave(500) (	
01:31P DUTY	(500) Contractor Evidence Solutions Inc	, an Arizona Computer Forensics Expert Witness
01:36P OFF	(500) CHINA STOCK THE BOARD	· · · · · · · · · · · · · · · · · · ·

٦

Time Status Description





		06/12/2013 17:42:47 (480) 81342	•							
Item	Conn. Date	Conn. Time	Originating Number	Elapsed Time	Bytes Up	Bytes Dn	IMEI	IMSI	Access Pt	Description
374	05/26/11	10:00A		13:13	6677	111991	3534910416514804	310410366057466	acds.voicemai l	_MOBILE_DATA
375	05/26/11	10:14A 1		5:08	0	0	3534910416514804	310410366057466	acds.voicemai l	_MOBILE_DATA
376	05/26/11	10:31A 1		13:14	9271	49317	3534910416514804	310410366057466	BLACKBERRY.NE T	_MOBILE_DATA
377	05/26/11	10:31A		2:13	2639	8417	3534910416514804	310410366057466	WAP.CINGULAR	MOBILE_DATA
378	05/26/11	10:44A		0:24	553	571	3534910416514804	310410366057466	BLACKBERRY.NE	_MOBILE_DATA

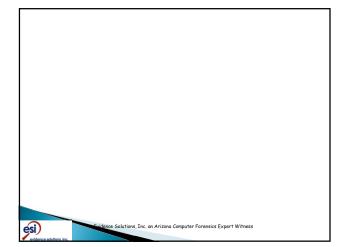


		06/12/2013 17:42:47 (480) 81342	•			
Item	Conn. Date	Conn. Time	Originating Number	Elapsed Time	Bytes Up	Bytes Dn
6374	05/26/11	10:00A		13:13	6677	11199
6375	05/26/11	10:14A		5:08	0	(
6376	05/26/11	10:31A 1		13:14	9271	49317
6377	05/26/11	10:31A		2:13	2639	841
6378	05/26/11	10:44A		0:24	553	57:

Г



Run Dat Run Tim SMS Usa Account	e: 17:44						
Item	Conn. Date	Conn. Time	Originating Number	Terminating Number	IMEI	IMSI	Description
913	01/14/11	09:37P	5660	3109	35349104165148	310410366057466	OUT
914	01/14/11	09:37P	5660	3109	35349104165148	310410366057466	OUT
915	01/14/11	09:41P	3109	5660	35349104165148	310410366057466	IN
916	01/15/11	08:06A	5660	8587	35349104165148	310410366057466	OUT
917	01/15/11	08:16A	8587	5660	35349104165148	310410366057466	IN
918	01/15/11	08:32A	5660	8587	35349104165148	310410366057466	OUT
919	01/15/11	08:32A	8587	5660	35349104165148	310410366057466	IN



Faculty: Scott Greene Evidence Solutions, Inc. Scott@EvidenceSolutions.com www.EvidenceSolutions.com 866-795-7166