"Digital Evidence and Forensic Investigation"

Scott Greene
Evidence Solutions, Inc.

Evidence Solutions, Inc.
Complex Electronic Evidence
In PLAIN English.

Over 30 Years Experience

EvidenceSolutions.com
866-795-7166

Scott@EvidenceSolutions.com

"I think there is a world market for maybe five computers."

-- Thomas Watson, chairman of IBM, 1943

Why look at the data?

Almost all documents are now ‘word processing’ documents.

Nearly all business activities are now computerized

E-mail communications have surpassed telephone and postal (snail mail) communication.

Electronically Stored Information in Litigation

Frequently we are presented with data that appears perfectly normal and supports a particular side to a case. Unfortunately software, by its very nature, displays data not in its natural form but rather in a sorted and organized form.

Electronically Stored Information in Litigation

What you don't see:

- **Data that has been manipulated will not be evident when looking at reports generated by the reporting system.**

Metadata:

- Data about (the) Data
- Information stored inside the electronic evidence that tells you more about the information that is presented than meets the eye.
- Who entered the data
- Who last edited the data
- How many versions of the document have there been
- Where the photo was taken
- What kind of camera took the photo
- What version of AutoCAD created the document
- What version of Outlook created the email

How am I going to get there?

Review a Civil Case where data was manipulated in a medical billing system

Show how data can be manipulated in EMR systems

Review a Civil Case where Email was Fabricated.

And various other subjects

Case Background

Plaintiff Company:

Contracted to bill for a high end medical specialist with his own surgical facility.

Maintained:

- That they properly billed for all services.
- The did so in a timely manner.

Case Background

Defendant Doctor/Surgical Facility

- Maintained that the Plaintiff did not bill timely
- Determined that the Plaintiff chose to concentrate on the large ticket bills

Case BS (Before Scott)

Procedural issues of the billing dispute

Discovery disputes – billing company claimed that it didn't have certain data

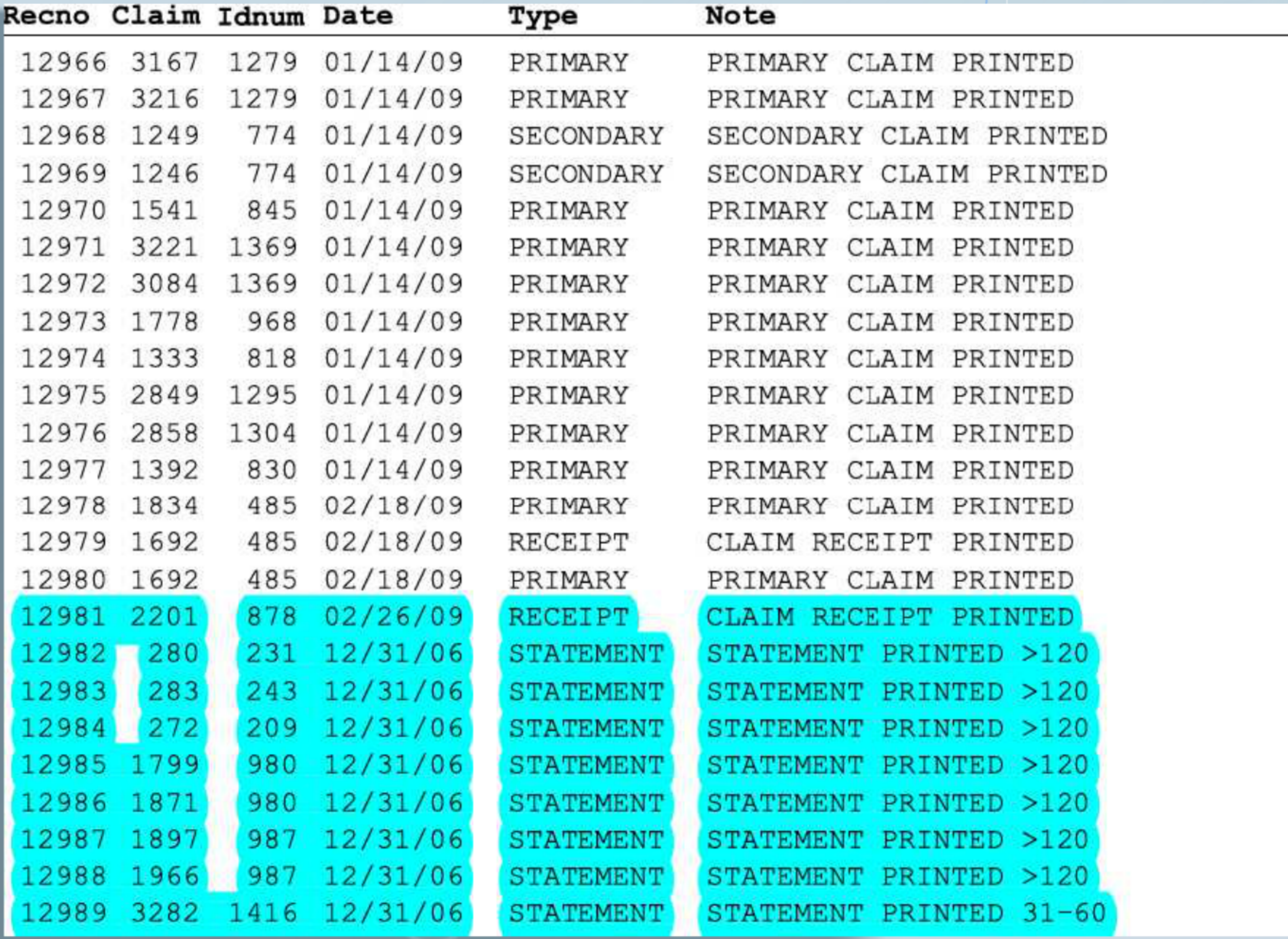
Arbitrator failed to order production of billing software until eve of arbitration

Special Master Tasks

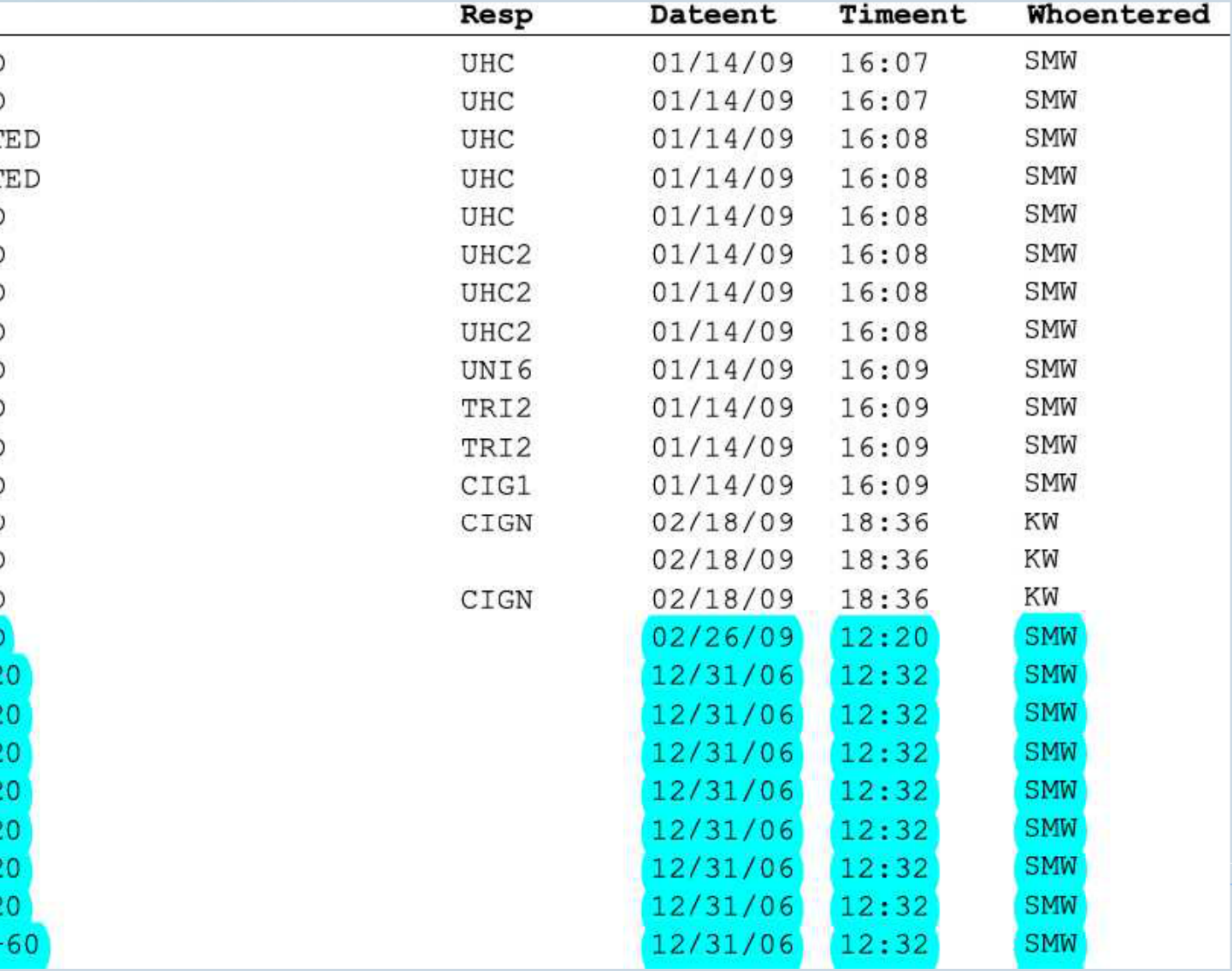
Evidence Solutions was tasked with analyzing the software and determining what standard reports were available from the system

Unable to get the software running we decided to look at the data.

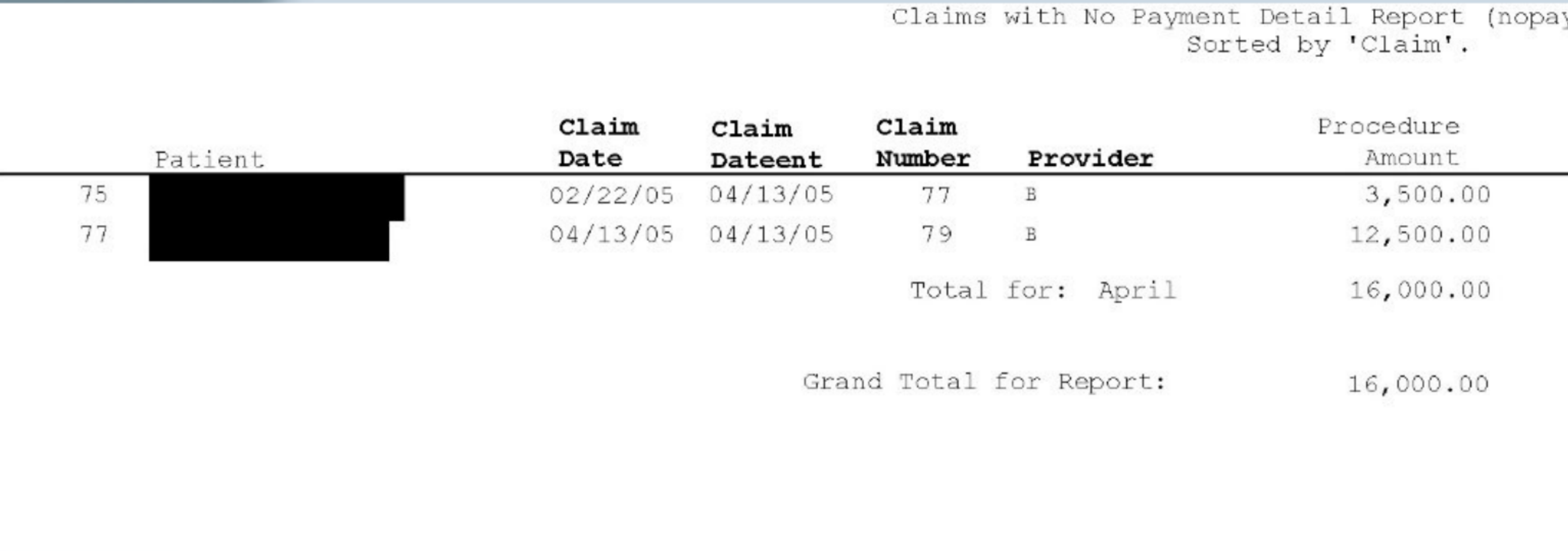
The first report from the database.



Recno	Claim	Idnum	Date	Type	Note
12966	3167	1279	01/14/09	PRIMARY	PRIMARY CLAIM PRINTED
12967	3216	1279	01/14/09	PRIMARY	PRIMARY CLAIM PRINTED
12968	1249	774	01/14/09	SECONDARY	SECONDARY CLAIM PRINTED
12969	1246	774	01/14/09	SECONDARY	SECONDARY CLAIM PRINTED
12970	1541	845	01/14/09	PRIMARY	PRIMARY CLAIM PRINTED
12971	3221	1369	01/14/09	PRIMARY	PRIMARY CLAIM PRINTED
12972	3084	1369	01/14/09	PRIMARY	PRIMARY CLAIM PRINTED
12973	1778	968	01/14/09	PRIMARY	PRIMARY CLAIM PRINTED
12974	1333	818	01/14/09	PRIMARY	PRIMARY CLAIM PRINTED
12975	2849	1295	01/14/09	PRIMARY	PRIMARY CLAIM PRINTED
12976	2858	1304	01/14/09	PRIMARY	PRIMARY CLAIM PRINTED
12977	1392	830	01/14/09	PRIMARY	PRIMARY CLAIM PRINTED
12978	1834	485	02/18/09	PRIMARY	PRIMARY CLAIM PRINTED
12979	1692	485	02/18/09	RECEIPT	CLAIM RECEIPT PRINTED
12980	1692	485	02/18/09	PRIMARY	PRIMARY CLAIM PRINTED
12981	2201	878	02/26/09	RECEIPT	CLAIM RECEIPT PRINTED
12982	280	231	12/31/06	STATEMENT	STATEMENT PRINTED >120
12983	283	243	12/31/06	STATEMENT	STATEMENT PRINTED >120
12984	272	209	12/31/06	STATEMENT	STATEMENT PRINTED >120
12985	1799	980	12/31/06	STATEMENT	STATEMENT PRINTED >120
12986	1871	980	12/31/06	STATEMENT	STATEMENT PRINTED >120
12987	1897	987	12/31/06	STATEMENT	STATEMENT PRINTED >120
12988	1966	987	12/31/06	STATEMENT	STATEMENT PRINTED >120
12989	3282	1416	12/31/06	STATEMENT	STATEMENT PRINTED 31-60



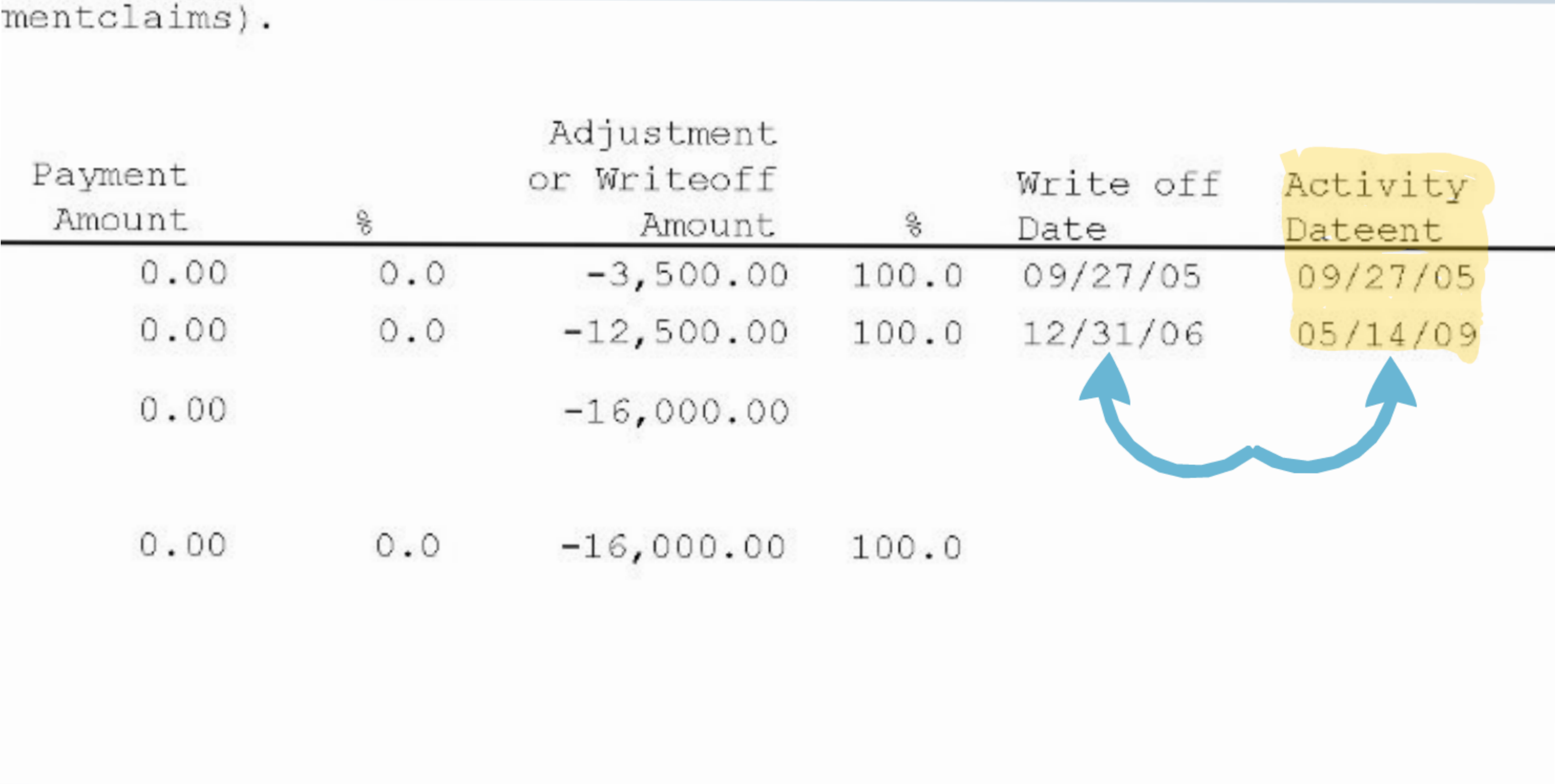
	Resp	Dateent	Timeent	Whoentered
D	UHC	01/14/09	16:07	SMW
D	UHC	01/14/09	16:07	SMW
ED	UHC	01/14/09	16:08	SMW
ED	UHC	01/14/09	16:08	SMW
D	UHC	01/14/09	16:08	SMW
D	UHC2	01/14/09	16:08	SMW
D	UHC2	01/14/09	16:08	SMW
D	UHC2	01/14/09	16:08	SMW
D	UNI6	01/14/09	16:09	SMW
D	TRI2	01/14/09	16:09	SMW
D	TRI2	01/14/09	16:09	SMW
D	CIG1	01/14/09	16:09	SMW
D	CIGN	02/18/09	18:36	KW
D		02/18/09	18:36	KW
D	CIGN	02/18/09	18:36	KW
D		02/26/09	12:20	SMW
20		12/31/06	12:32	SMW
20		12/31/06	12:32	SMW
20		12/31/06	12:32	SMW
20		12/31/06	12:32	SMW
20		12/31/06	12:32	SMW
20		12/31/06	12:32	SMW
20		12/31/06	12:32	SMW
-60		12/31/06	12:32	SMW



Claims with No Payment Detail Report (nopay

Sorted by 'Claim'.

		Claim	Claim	Claim		Procedure
	Patient	Date	Dateent	Number	Provider	Amount
75	[redacted]	02/22/05	04/13/05	77	B	3,500.00
77	[redacted]	04/13/05	04/13/05	79	B	12,500.00
				Total for:	April	16,000.00
				Grand Total for Report:		16,000.00



mentclaims).

Payment Amount	%	Adjustment or Writeoff Amount	%	Write off Date	Activity Dateent
0.00	0.0	-3,500.00	100.0	09/27/05	09/27/05
0.00	0.0	-12,500.00	100.0	12/31/06	05/14/09
0.00		-16,000.00			
0.00	0.0	-16,000.00	100.0		

Hospital systems are a focal point in many Medical Malpractice cases.
A common mis-conception is that the "Audit Log" is the gospel.

Unfortunately the "Audit Log" is just Data. It can be manipulated just like any other data.

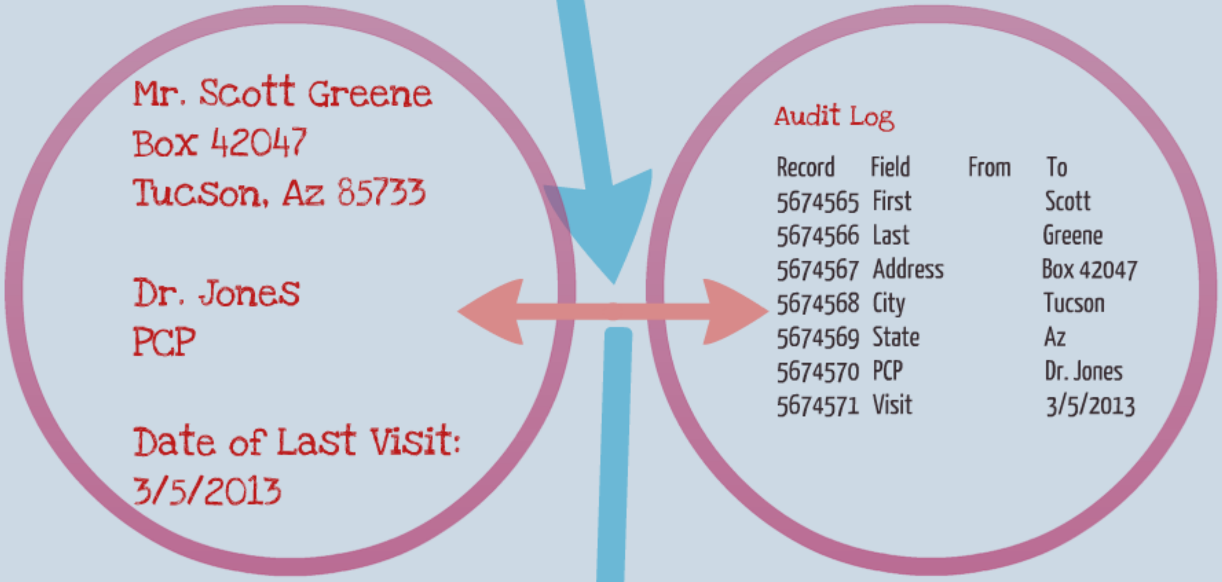
Don't trust the software.

Data Being Written to the EMR

Mr. Scott Greene
Box 42047
Tucson, Az 85733

Dr. Jones
PCP

Date of Last Visit: 3/5/2013



Mr. Scott Greene
Box 42047
Tucson, Az 85733

Dr. Jones
PCP

Date of Last Visit:
3/5/2013

Audit Log

Record	Field	From	To
5674565	First		Scott
5674566	Last		Greene
5674567	Address		Box 42047
5674568	City		Tucson
5674569	State		Az
5674570	PCP		Dr. Jones
5674571	Visit		3/5/2013

Create initial data

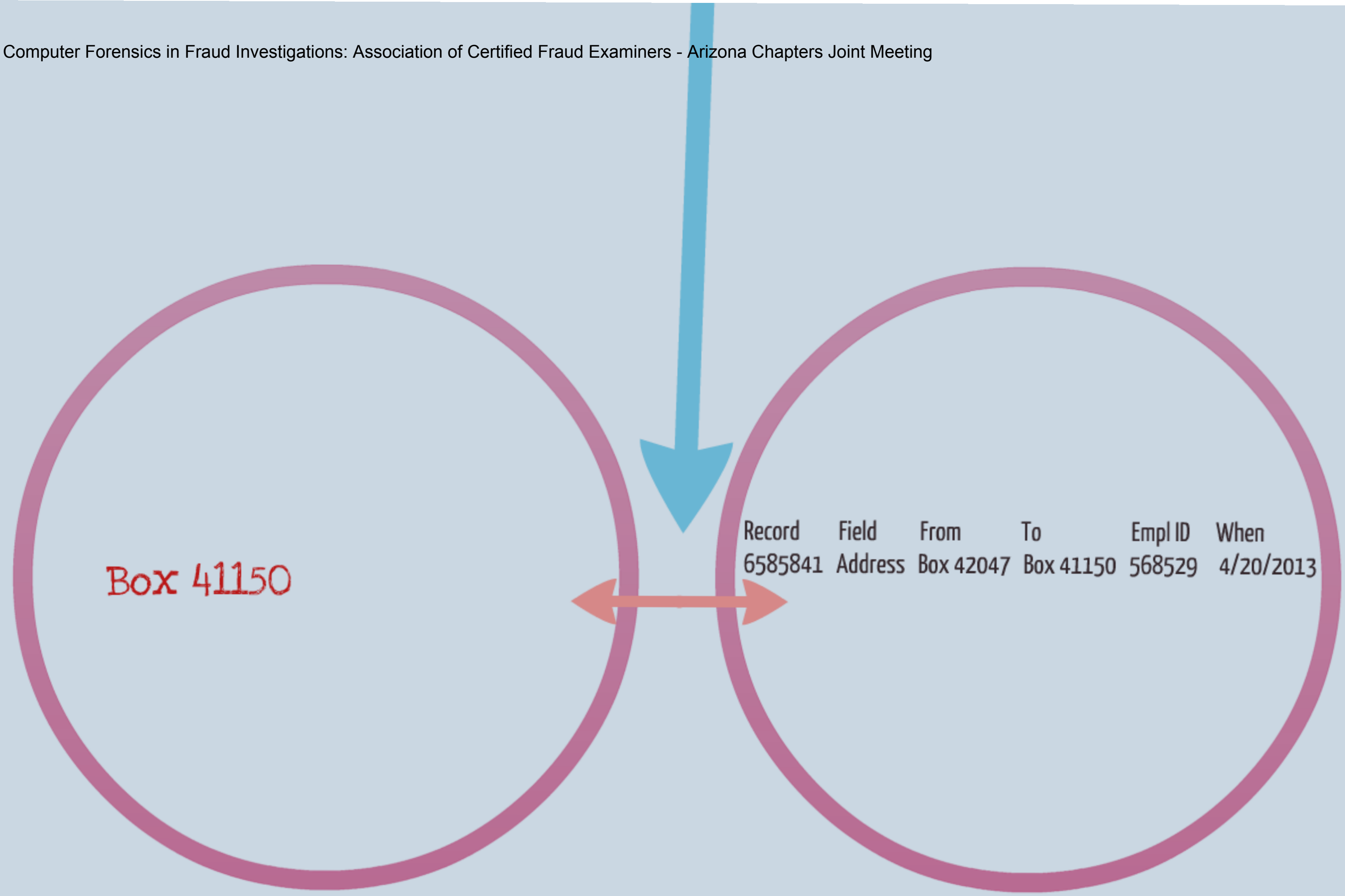
Mr. Scott Greene
Box 42047
Tucson, Az 85733

Dr. Jones
PCP

Date of Last Visit:
3/5/2013

Audit Log

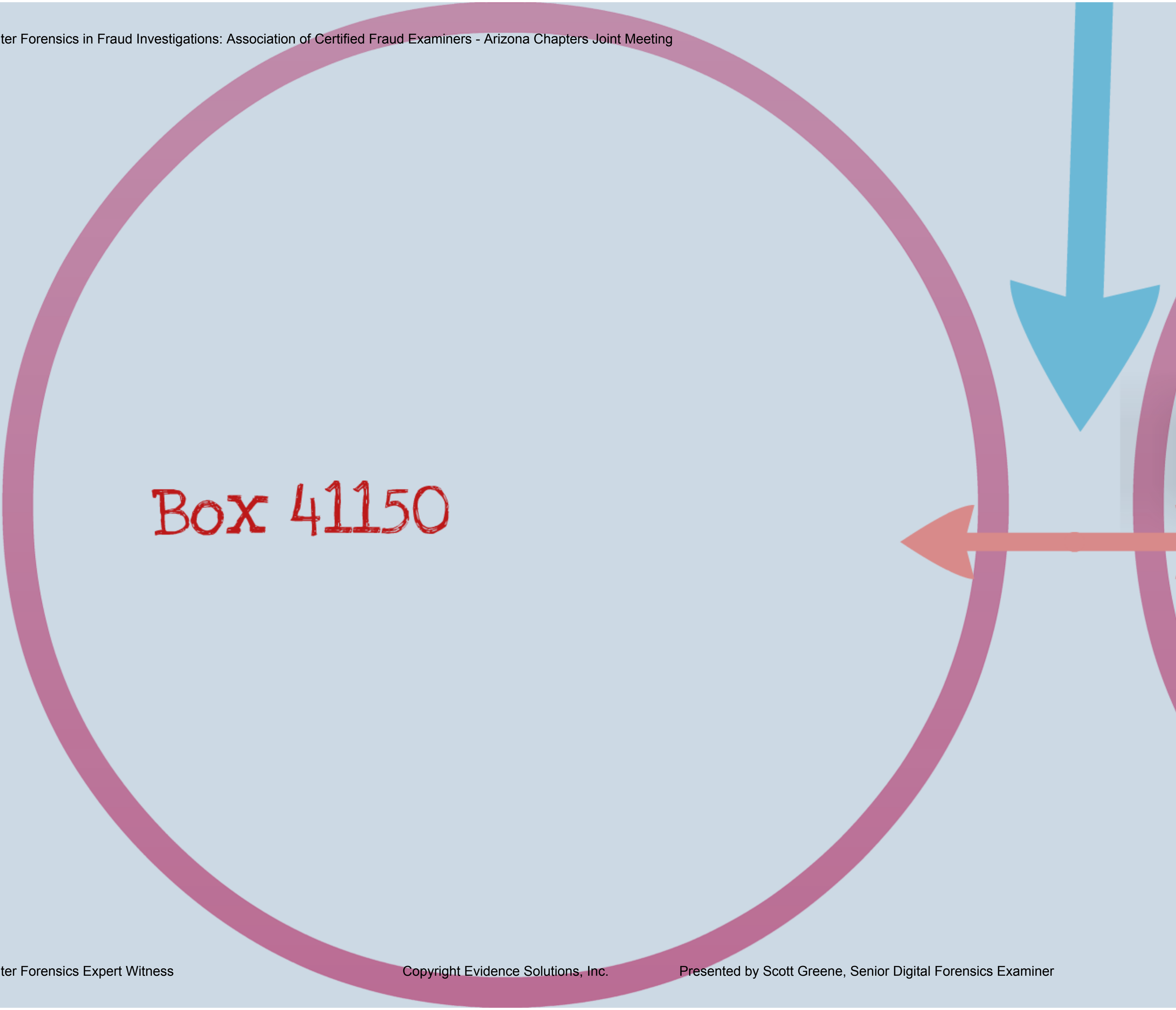
Record	Field	From	To
5674565	First		Scott
5674566	Last		Greene
5674567	Address		Box 42047
5674568	City		Tucson
5674569	State		Az
5674570	PCP		Dr. Jones
5674571	Visit		3/5/2013



Box 41150

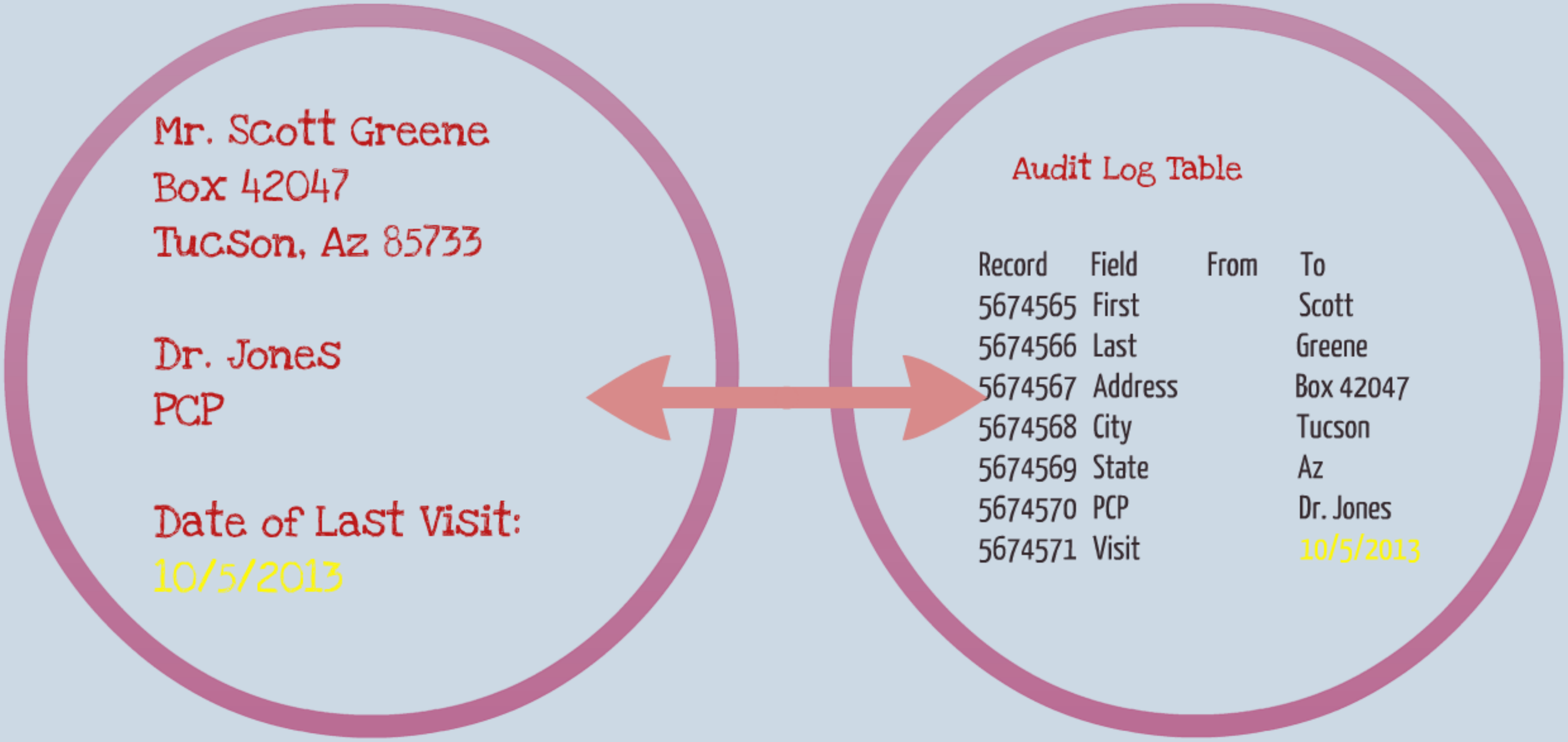
Record	Field	From	To	Empl ID	When
6585841	Address	Box 42047	Box 41150	568529	4/20/2013

Single Data Field Edit



Box 41150

Record	Field	From	To	Empl ID	When
6585841	Address	Box 42047	Box 41150	568529	4/20/2013



Mr. Scott Greene
Box 42047
Tucson, Az 85733

Dr. Jones
PCP

Date of Last Visit:
10/5/2013

Audit Log Table

Record	Field	From	To
5674565	First		Scott
5674566	Last		Greene
5674567	Address		Box 42047
5674568	City		Tucson
5674569	State		Az
5674570	PCP		Dr. Jones
5674571	Visit		10/5/2013

Edit both the patient record & the Audit Record

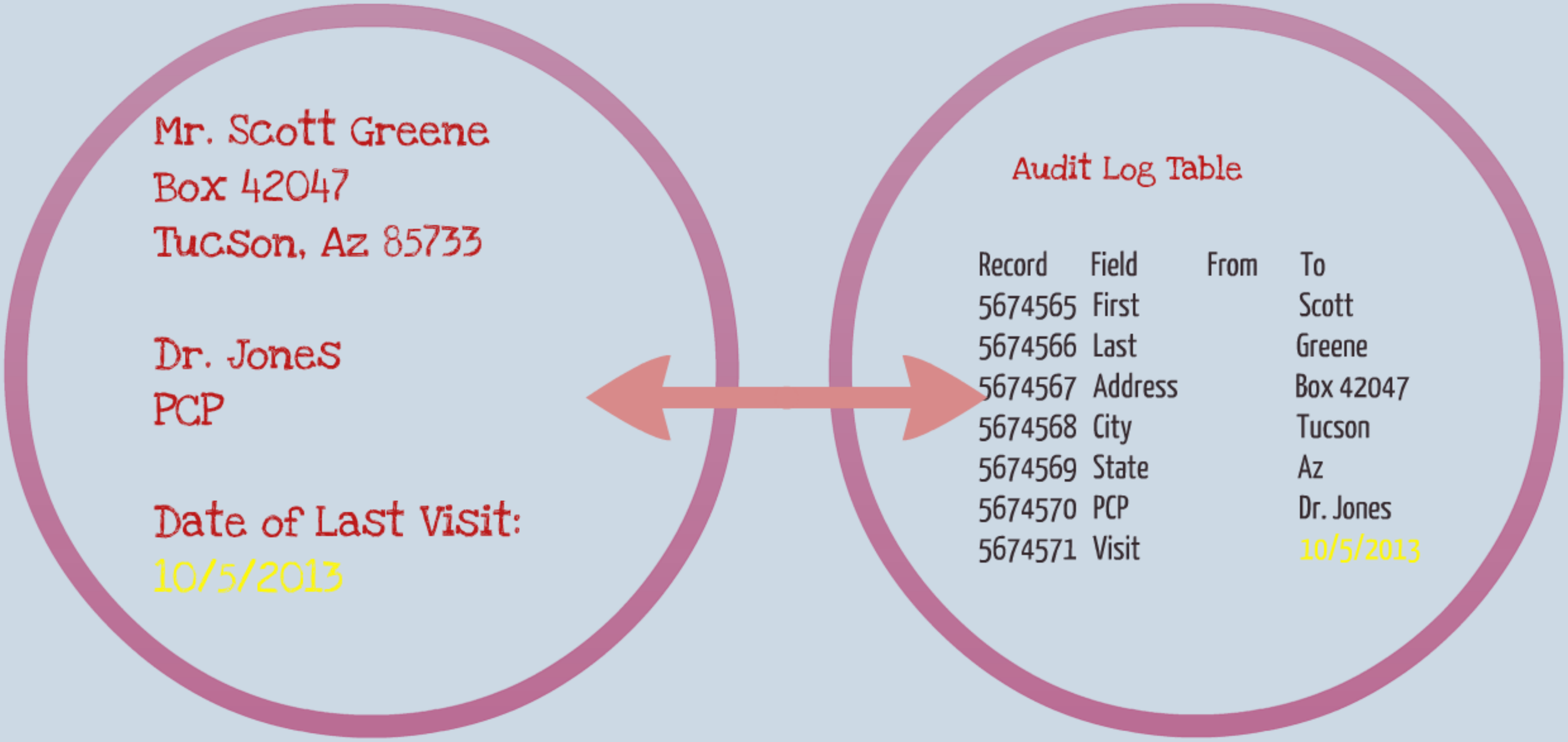
Mr. Scott Greene
Box 42047
Tucson, Az 85733

Dr. Jones
PCP

Date of Last Visit:
10/5/2013

Audit Log Table

Record	Field	From	To
5674565	First		Scott
5674566	Last		Greene
5674567	Address		Box 42047
5674568	City		Tucson
5674569	State		Az
5674570	PCP		Dr. Jones
5674571	Visit		10/5/2013



Mr. Scott Greene
Box 42047
Tucson, Az 85733

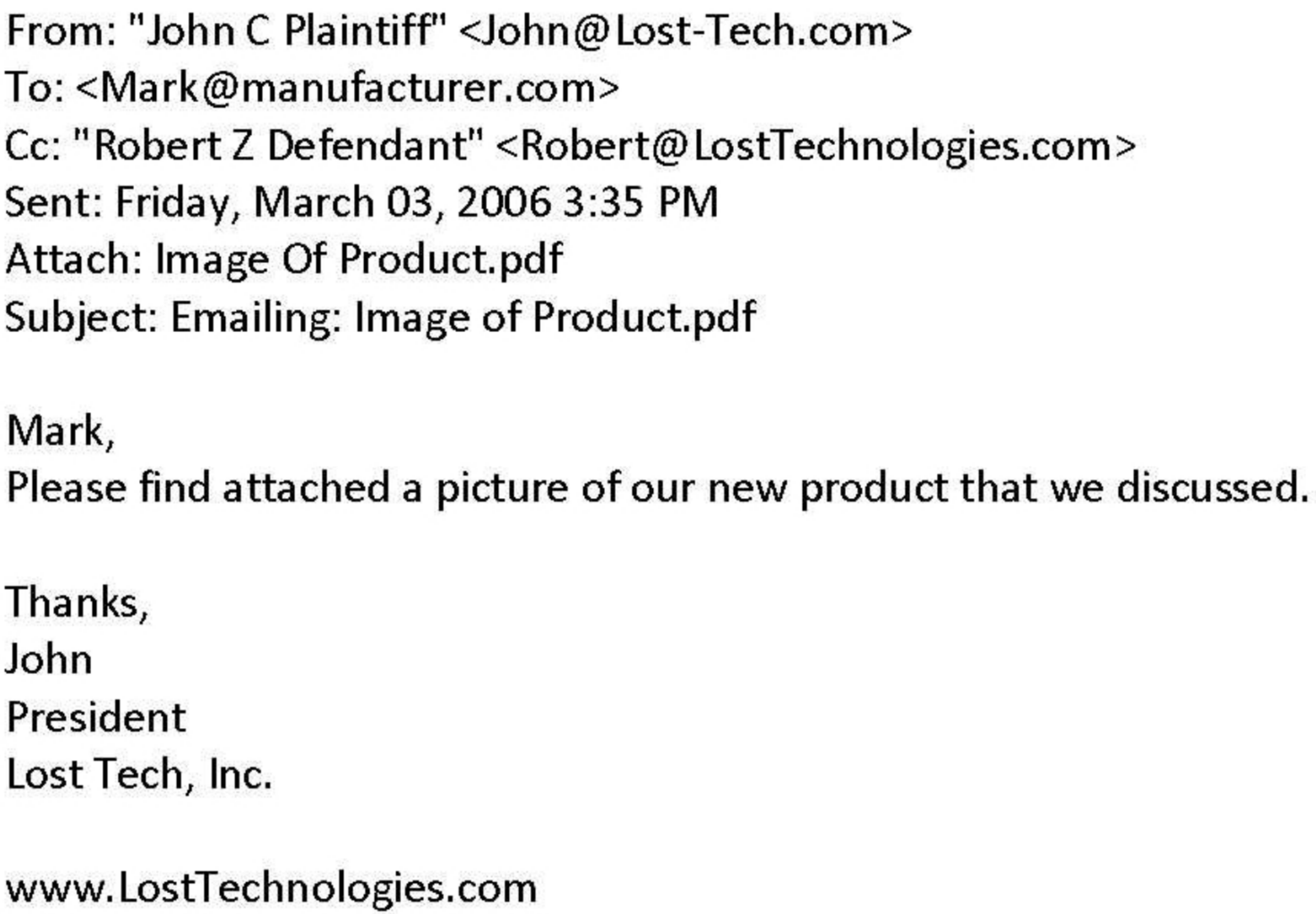
Dr. Jones
PCP

Date of Last Visit:
10/5/2013

Audit Log Table

Record	Field	From	To
5674565	First		Scott
5674566	Last		Greene
5674567	Address		Box 42047
5674568	City		Tucson
5674569	State		Az
5674570	PCP		Dr. Jones
5674571	Visit		10/5/2013

Edit both the patient record & the Audit Record

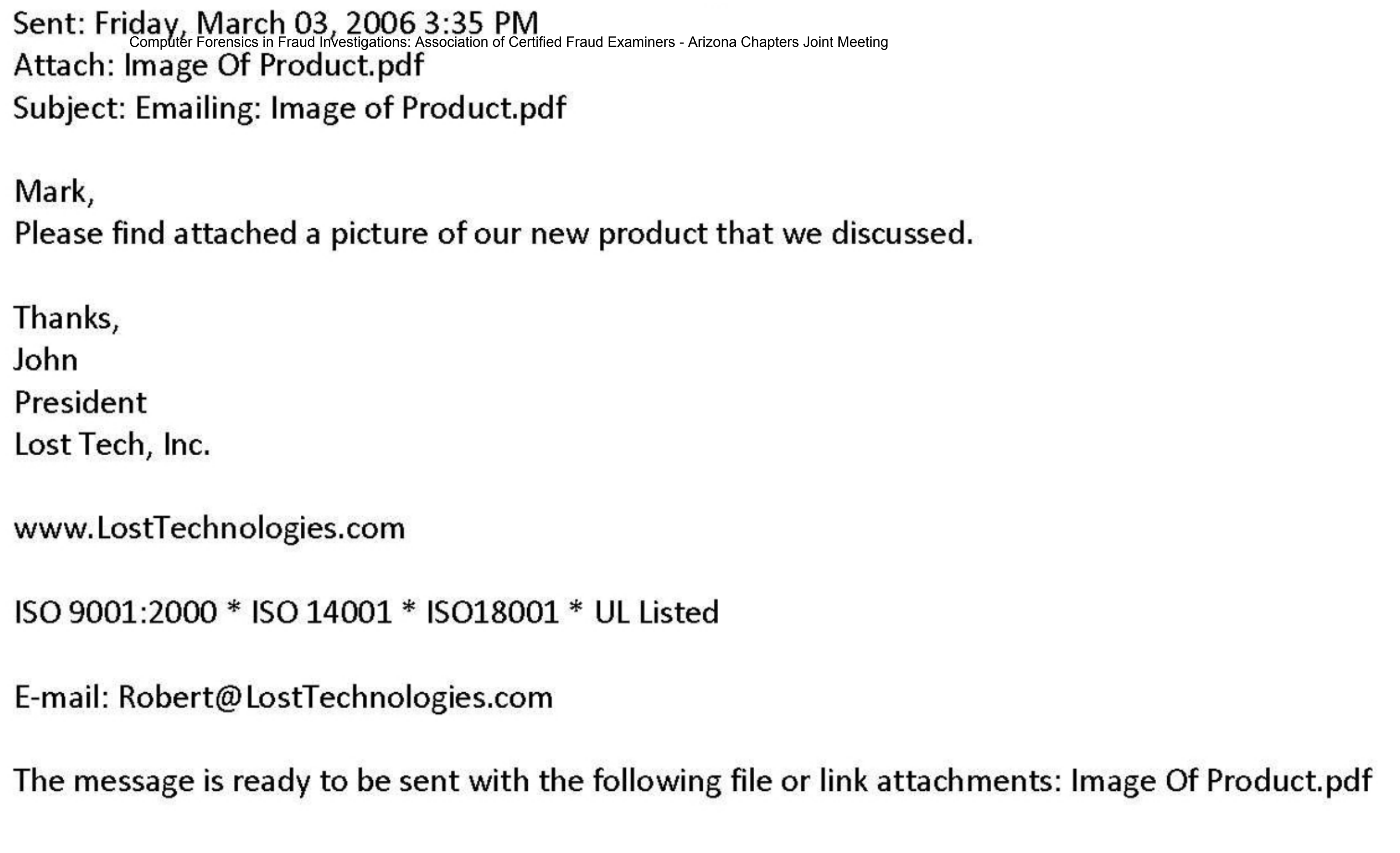


From: "John C Plaintiff" <John@Lost-Tech.com>
To: <Mark@manufacturer.com>
Cc: "Robert Z Defendant" <Robert@LostTechnologies.com>
Sent: Friday, March 03, 2006 3:35 PM
Attach: Image Of Product.pdf
Subject: Emailing: Image of Product.pdf

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

Thanks,
John
President
Lost Tech, Inc.

www.LostTechnologies.com



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: Robert@LostTechnologies.com

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

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

“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>

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

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>

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

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

The problem is:

Build:14.02

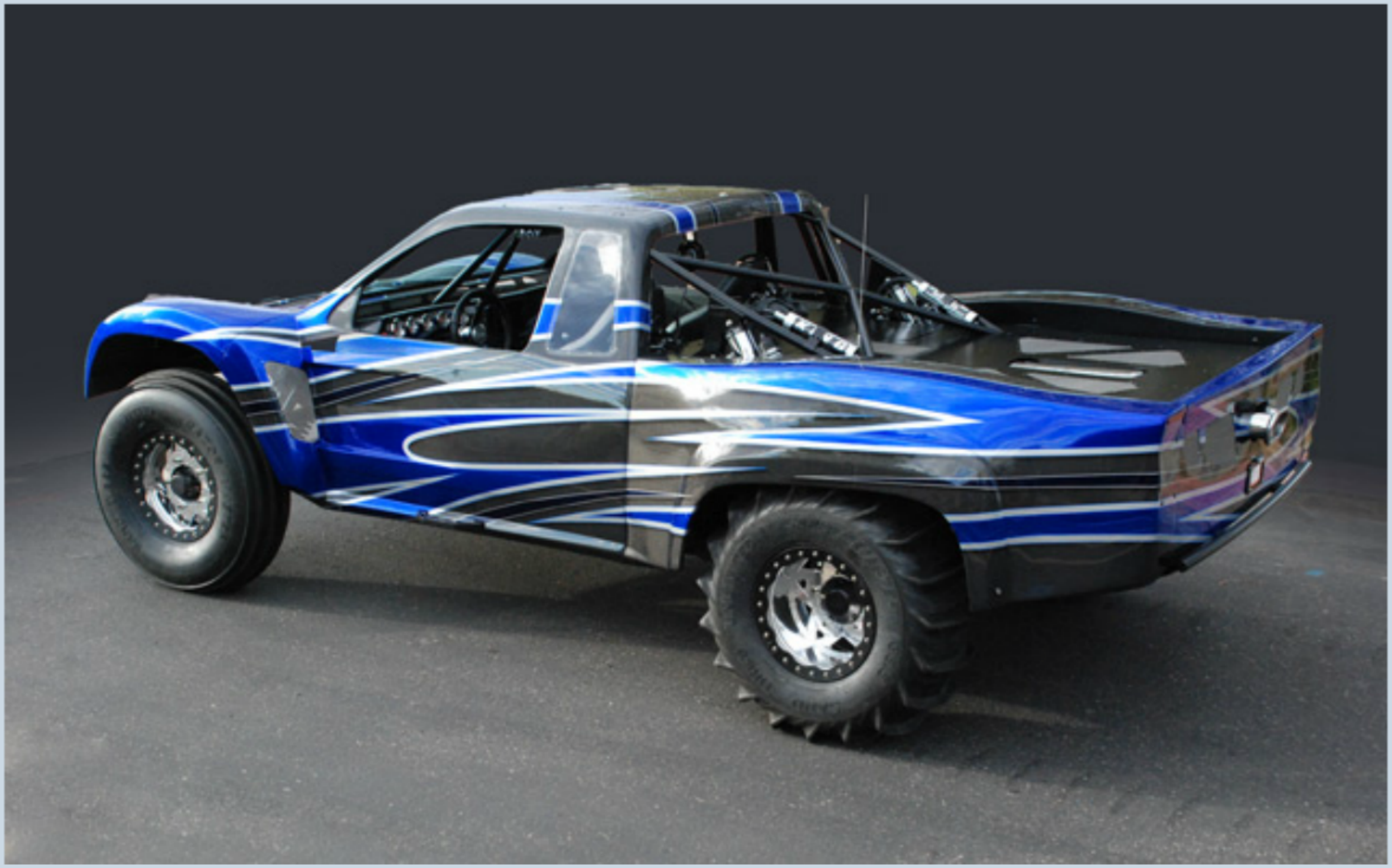
Rollup 3 for Exchange Server 2010

Service Pack 2 May 29, 2012

Exotic Handmade Cars

- Made in Phoenix Arizona
- This company builds millions of dollars of these cars every year

Just out of curiosity what do you picture?



$134,900

What happened?

The partners broke up over some significant funds

One partner managed to raise the funds to keep the company

The departing partner claimed they took nothing

What Happened?

The departing partner claimed they took nothing

After a time we were able to capture a copy of the departing partner's

Examination revealed references to previous company

Source Code Copyright Case

Game Company, Inc. writes game software

It is sold on a lease basis and Game Company receives a payment for playing of the game as well.

The market for this particular software is very lucrative.

Their software was aging

Source Code Copyright Case

We Plagiarize Stuff, LLC is a software development firm

They write programs for hire

They claim they have game knowledge

They show game knowledge

Source Code Copyright Case

Game Company, Inc. hires We Plagiarize Stuff, LLC to re-write their software.

They meet several times.

Game Company gives We Plagiarize Stuff a complete network with all of their software running on it so that We Plagiarize Stuff can see how the software is supposed to operate.

Source Code Copyright Case

Game Company, Inc. hires We Plagiarize Stuff, LLC to re-write their software.

They meet several times.

Game Company gives We Plagiarize Stuff a complete network with all of their software running on it so that We Plagiarize Stuff can see how the software is supposed to operate.

Source Code Copyright Case

Game Company gives We Plagiarize Stuff a CD of their source code

They begin to discuss a contract
They continue to discuss a contract
They continue to discuss a contract
They continue to discuss a contract

Source Code Copyright Case

Ultimately they don't reach contract fruition.

They agree to part ways

We Plagiarize Stuff gives everything back to Game Company.

Source Code Copyright Case

Fast forward to 9+/- months later

Game Company receives notice that one of their clients is not renewing it's contract with Game Company.

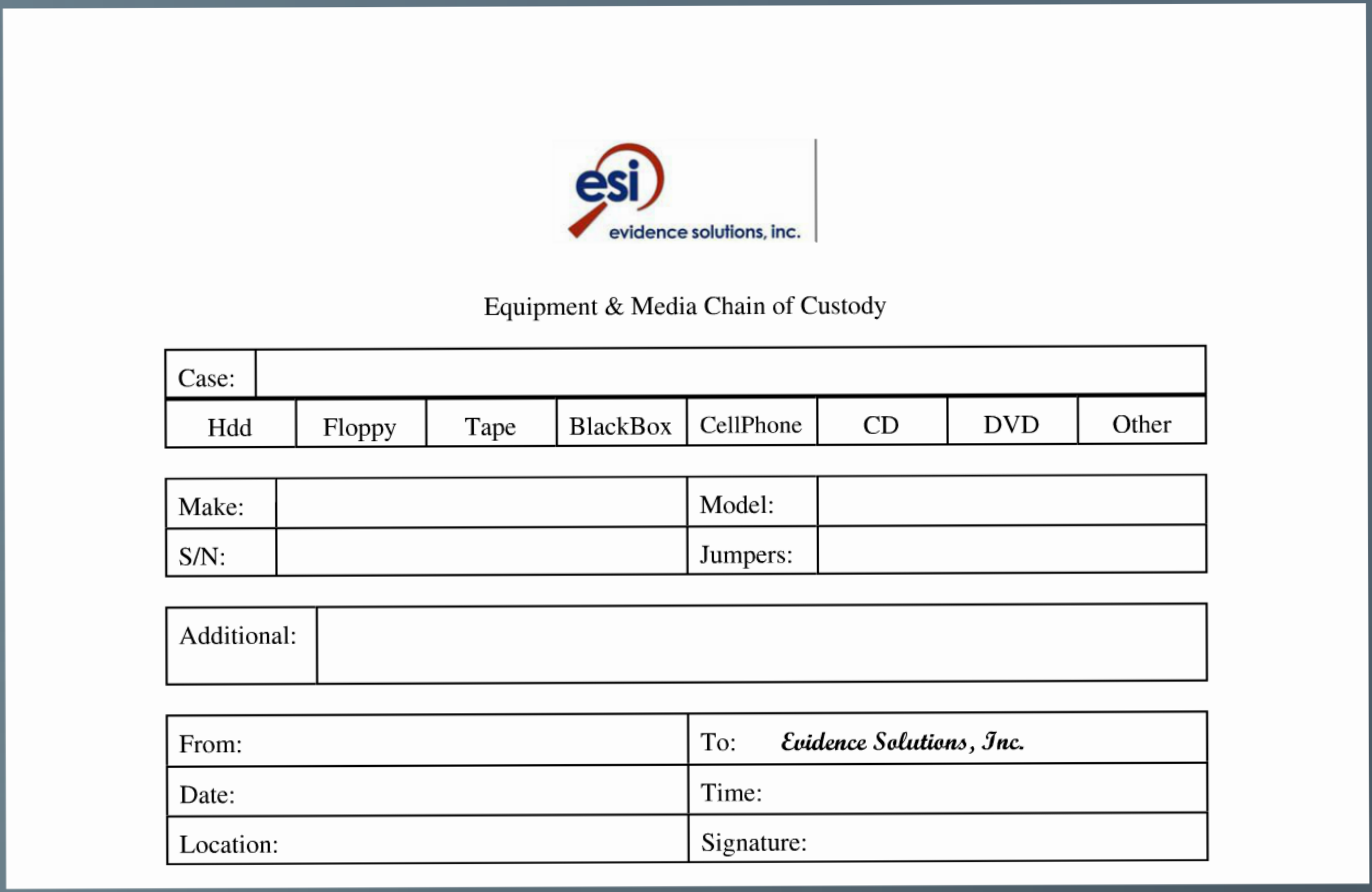
After a little while Game Company receives another notice from another client.

Source Code Copyright Case

Evidence Solutions, Inc. was hired to review the two system's source code and determine if the source code was copied.

We Plagiarize Stuff claimed they couldn't read the Source Code CD.

The screen layouts matched on many screens, almost identically...



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:

Evidence Collection

Sources of Evidence:

Storage Media includes:

Hard Disk Drives

Floppy Disks

Backup tapes

CD Rom disks

EPROM and Memory chips

Thumb Drives

iPods, iPads & MP3 Players

Cell Phones

Complex Electronic Evidence in PLAIN English.

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.....

Complex Electronic Evidence in PLAIN English.

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).

Complex Electronic Evidence in PLAIN English.

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

Complex Electronic Evidence in PLAIN English.

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.

Complex Electronic Evidence in PLAIN English.

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:

Complex Electronic Evidence in PLAIN English.

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.

Complex Electronic Evidence in PLAIN English.

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

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

Artifacts From Web Browsing

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

My Secure Wallet

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.

Complex Electronic Evidence in PLAIN English.

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

Complex Electronic Evidence in PLAIN English.

What to do / How to do it.

Meta Data is Everywhere
– it can tell a much different story than the data

How does you know when to call for help?
- upfront a consultant can steer you in the right direction
- data that looks suspicious
- if it is too good to be true, it probably is

"Digital Evidence and Forensic Investigation"

Scott Greene
Evidence Solutions, Inc.

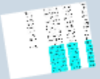
Evidence Solutions, Inc.
Complex Electronic Evidence
In PLAIN English.

Over 30 Years Experience

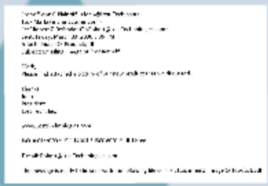
EvidenceSolutions.com
866-795-7166

Scott@EvidenceSolutions.com

How am I going to get there?



Special Master Tasks



Scott Greene

Other Sources of Data

Other Sources of Data

Scott Greene
Evidence Solutions, Inc.

Evidence Solutions, Inc.
Collects, Analyzes, & Explains complex
Electronic Evidence in PLAIN ENGLISH.

Over 30 Years Experience

EvidenceSolutions.com
866-795-7166

Scott@EvidenceSolutions.com

Other Sources of Data

Source Code Copyright Case

Game Company, Inc. writes game software
It is sold on a license basis and Game Company receives a payment for playing of the game as well.
The market for this particular software is very lucrative.
Their software was aging

Source Code Copyright Case

We Plagiarize Stuff, LLC is a software development firm
They write programs for hire
They claim they have game knowledge
They show game knowledge

Source Code Copyright Case

Game Company, Inc. hires We Plagiarize Stuff, LLC to re-write their software.
They meet several times.
Game Company gives We Plagiarize Stuff a complete network with all of their software running on it so that We Plagiarize Stuff can see how the software is supposed to operate.

Source Code Copyright Case

Source Code Copyright Case

Ultimately they don't really get along.
They agree to part ways
We Plagiarize Stuff gives everything back to Game Company

Source Code Copyright Case

Source Code Copyright Case

This manufacturer used SolidWorks
- 3D CAD
- Product Data Management

What Happened?

The partners broke up over some significant funds

One partner managed to raise the funds to keep the company

The departing partner claimed they took nothing

What to do / How to do it.

What Happened?

The departing partner claimed they took nothing

After a time we were able to capture a copy of the departing partner's

Examination revealed references to previous company

Scott Greene
Evidence Solutions, Inc.

Evidence Solutions, Inc.
Collects, Analyzes, & Explains complex
Electronic Evidence in PLAIN ENGLISH.

Over 30 Years Experience

EvidenceSolutions.com
866-795-7166

Scott@EvidenceSolutions.com