INSTITUTE FOR CRIMINAL JUSTICE EDUCATION

January 2013 In the News - Our Take on What it Means to You

IN THIS ISSUE

Steganography
Decoding Messages with Camera Phone
Hiding Messages in Mutimedia
Preserving Evidence
If Your are Going to Search
Going Dark and the FBI
APTA - Instructor Development
True Hero
Training

**Greetings!**

At the risk of offending those of you who are not Alabama fans, "Congratulations" to the Tide for their decisive win over Notre Dame! My daughter was fortunate enough to get a student ticket (which then became a Christmas gift from good ole Mom and Dad) and she said that while the Alabama fans were outnumbered by Notre Dame fans, they got the last laugh, and laugh it was.

My wife and I were fortunate to attend a much better game, weeks before, when the Tide defeated the Dawgs in the SEC championship game. What a game it was, as the clock ticked away on Georgia and the ticker tape fell on a victorious Tide team.


*Bryant - Denny Stadium*

But as fun as the game was, the conversation I had before the game really got me thinking. As some of you may know, a very good friend (who was my roommate at the FBI Academy) is a football official in the SEC, and my wife and I attended the game with him. Prior to the game our conversation turned to the expectation that officials perform their duties to perfection, to include the use of more and more technology to achieve perfect calls. And with every introduction of new technology, it moves the bar of expectations of perfection higher and higher.

I wondered out loud if we fans were carrying the expectation of "a perfect call on every play" to an extreme that was destroying the game. It was a rhetorical question, but I sometimes wonder why we expect so much more of football officials than we do of ourselves.

I sat through one game this year in which the first quarter lasted one hour and 15 minutes because of so many "the previous play is under review" calls. One touchdown call was reviewed for 8 minutes! All trying to determine if an official, who had a great view of the pile of players, was correct when he ruled that the ball carrier, who was buried somewhere in the pile, had made it across the goal line.

I would suggest that it is not perfection that we should look for in other people's decisions, but instead we should look for individuals who place honesty and integrity in the decision making process as the foundation with which they make decisions.

Perfection is not possible, honesty and integrity are.

Sometimes we just need to trust the decisions of those around us. Don't require perfection, for only one person attained that while on this earth. Surround yourself with people that place honesty and integrity on the compass that directs their life, we'll all be better off.

As always, Roll Tide Roll, and I hope this month's newsletter provides information, and food for thought.

Jim Rechel - Newsletter Editor


## "What is Steganography?"

I was in New York last week surrounded by attorneys in a conference room for two days, all of us involved in a mediation process regarding a multi-million dollar fraud case.

During one of the long intervals as both sides made their case to a mediator who shuttled between distant conference rooms, one of the participants asked me if criminals could disguise or hide text in a document in such a way that it could not be seen.

I thought for a second, and told them that terrorists use steganography to embed hidden text into jpg images, and that while I had never worked a financial fraud case in which the perpetrators used this method, I presumed that it would be easy to do with the right knowledge and software.

Of course the next question was, "What is steganography?"

I know of steganography, but I am far from being proficient in explaining how it actually works, so I started my research. From that basic question, I found an eye opening amount of information, much of which is probably way out of what you would see in daily interactions, but I

found some additional information that is useful in the everyday world of investigating and preventing fraud in everyday life. So this month we will explore the world of hidden data.

## Using a Camera Phone to Decode Messages

Steganography-the practice of concealing data within a carrieri-may be used to obscure malicious or criminal information and activity from law enforcement. While steganography dates to the fifth century BC, it has long been regarded as, and remains, one of the most advanced forms of clandestine communication.

In modern usage, the Internet allows accessibility to, and broad dissemination of, steganography tools, and its application continues to evolve with technology. Understanding steganography in its current state is essential to its identification and detection.

Using a camera phone and secret messages: Secret Messages in Photos

## Steganography: How al-Qaeda Hid Text in Porn Videos


When a suspected al-Qaeda member was arrested in Berlin in May of 2011, he was found with a memory card with a password-protected folder-and the files within it were hidden. But, as the German newspaper Die Zeit reports, computer forensics experts from the German Federal Criminal Police (BKA) claim to have eventually uncovered its contents-what appeared to be a pornographic video called "KickAss."

Within that video, they discovered 141 separate text files, containing what officials claim are documents detailing al-Qaeda operations and plans for future operations-among them, three entitled "Future Works," "Lessons Learned," and "Report on Operations."

Find more in an ars technicia article at: Hidden Text

## Preserving Evidence in Our Digital World

An important part of the acquisition of evidence in connection with cases involving the use of the Internet for terrorist purposes concerns the recovery of stored digital data. The two primary goals in this data recovery exercise are the retrieval of relevant evidence for the purposes of effective investigation and prosecution and the preservation of the integrity of the data source and the chain of custody to ensure its admissibility in court proceedings.

In order to identify the best method of evidence preservation, it is important to distinguish between volatile data, which stored on devices, such as the random access memory (RAM) of devices, and may be irretrievably lost if there is a disruption in the power supply, and non-volatile data, which is maintained independently of the power supply to the device.

For example, the act of switching off a computer may alter the data contained on the storage discs and RAM, which may contain important evidence of computer programs used by the suspect or websites visited. Volatile data may provide information relating to current processes on an active computer which may be useful in an investigation, such as information relating to users, passwords, unencrypted data or instant messages. Examples of storage devices for non-volatile data include internal/exter- nal hard disks, portable disk drives, flash storage devices and zip disks.

From the DHS:

Best practices for data preservation

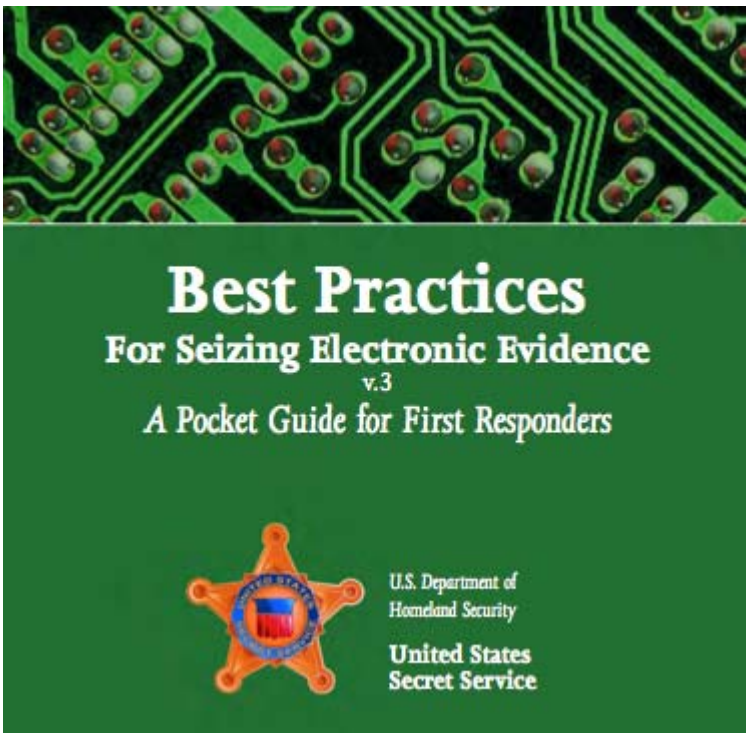
- Do not use the computer or attempt to search for evidence
- If the computer is connected to a network, unplug the power source to the router or modem
- Prior to moving any evidence, photograph the computer as found, including the front and back, as well as any cords or connected devices and the surrounding area
- If the computer is "off", do not turn it "on"
- If the computer is "on" and something is displayed on the monitor, photograph the screen
- If the computer is "on" and the screen is blank, move the mouse or press the space bar (this will display the active image on the screen); after the image appears, photo- graph the screen
- For desktop computers, unplug the power cord from back of the computer tower
- For laptop computers, unplug the power cord; if the laptop does not shut down, locate and remove the battery pack (the battery is commonly placed on the bottom, and there is usually a button or switch that allows for its removal); once the battery is removed, do not return it to or store it in the laptop (this will prevent the accidental start-up of the laptop)
- Diagram and label cords to later identify connected devices
- Disconnect all cords and devices from the tower or laptop

- Package and transport components (including the router and modem, if present) as fragile cargo
- Where permitted pursuant to the terms of any applicable search warrant, seize any additional storage media
- Keep all media, including the tower, away from magnets, radio transmitters and other potentially damaging elements
- Collect instruction manuals, documentation and notes, paying particular attention to any items that may identify computer-related passwords or pass phrases
- Document all steps involved in the seizure of a computer and its components.

***With regard to mobile devices such as smart phones and personal digital assistants, similar principles apply, except that it is recommended <u>not</u> to power down the device, as this may enable any password protection, thus preventing access to evidence. The device should therefore be kept charged, to the extent possible, or undergo specialist analysis as soon as possible before the battery is discharged to avoid data loss.***

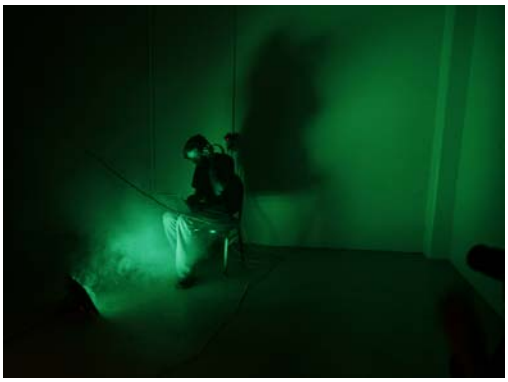
For more details: UN Report on Use of Internet by Terrorists

## Best Practices for Seizing Electronic Evidence




For more information: First Responders - Best Practices for Seizing Electronic Evidence

## The FBI and Losing the Ability to Intercept Communications



For the last few years, the FBI's been warning that its surveillance capabilities are "going dark," because internet communications technologies - including devices that connect to the internet - are getting too difficult to intercept with current law enforcement tools.

So the FBI wants a more wiretap-friendly internet, and legislation to mandate it will likely be proposed this year. But a better way to protect privacy and security on the internet may be for the FBI to get better at breaking into computers.

Whoa, what? Let us explain.

For the complete article: The FBI Needs Hackers

## APTA

### 2013-A Certified Instructor Development Course

The next Five Day Law Enforcement Instructor Development Course will be held in Montgomery at the Alabama Criminal Justice Information Center, from February 11, 2013 through February 15, 2013. Registration link appears below.

This course will only be open to the first 15 law enforcement trainers who register. Those registering after the class is full will be placed on the standby list. If there is enough interest, ICJE will hold another class in October, 2013.

The training is free to all Alabama law enforcement trainers.

To register for the APTA 2013-A Instructor Development Course, click the Registration Link below:

To Register: Instructor Development Registration

To view IDC Course Topics: IDC Course Topics

To view participant comments: Previous Attendee Comments

For more information about this class, contact training@apta.us

## Auburn Student Rescues Bridge Jumper from Alabama River

If you have ever questioned yourself, wondering if you should get involved to help someone, Doug Bacon, an Auburn grad student, wasted no time while driving through Selma, Alabama recently.

Noticing a car stopped on the side of the bridge as he drove eastbound across the Edmund Pettus Bridge, he spotted a woman standing on the side of the bridge, staring over the edge.

When he looked back in his rear view mirror, she was gone.

He wasted no time, didn't hesitate to help. He parked his car on the opposite side of the bridge, took off his jeans and shirt, and with the help of a fisherman spotted a woman bobbing in the river. He swam out, grabbed her by the arms and swam her back to shore.

The despondent woman from Opelika survived, and was flown to Montgomery for medical treatment.

These are the unsung heroes in our communities!

For the Selma Times Journal Article: Unsung Heroes

## ICJE / AUM Training

Law Enforcement Training

List of Classes and Registration Link: ICJE / AUM Seminar List and Registration

ICJE, Inc.
P.O. Box 293
Montgomery, Alabama 36101
334-280-0020