THE PICA INVESTIGATIVE REPORTER

THE OFFICIAL PUBLICATION OF PROFESSIONAL INVESTIGATORS OF CALIFORNIA, INC.

Spring 2010

this issue

www.pica-association.org

P.I.C.A.
P.O. Box 568
Verdugo City, CA 91046
(800)-765-7422

President's Message

David Herrera, President

Welcome to PICA,

Thank you for supporting PICA as we celebrate PICA's 9th year in business. We've grown stronger financially and we've increased in membership and in popularity.

Why join PICA? Our network members care for one another, our association, and we contribute to strengthen the private investigator industry. Plus, PICA's annual dues are the lowest in the industry!

By actively listening to our members, PICA distinguishes itself with pride. Everything we do in PICA is member-driven; we poll our members to know their desires. Aside from numerous membership rights, we offer educational opportunities that are accessible online or through our regional training seminars. Statewide, PICA holds bi-monthly meetings featuring outstanding educational speakers who provide extended learning and networking opportunities.

We provide fantastic free Listserv and WorkServe; these are interactive online boards where members can post questions and answers. If you need copies of contracts, specialized forms or if you want to know more about how to conduct specific types of investigations, just ask and receive results. Further, members can use the boards to advertise and to respond to job offers.

If you can't attend a meeting to vote, use our secure online voting system. Concerned with what is happening in the P.I. legislative world? Our Legislative Committee monitors state and federal legislation affecting the P.I. industry. Want to know about current investigative tools? Read our informative PICA Newsletters. Check out member benefits such as affordable dental and vision plans and other discounted services.

PICA's relationship with the Bureau of Security and Investigative Services has never been better. As PICA president, I am a member of the BSIS Advisory Board where I have an excellent working relationship with the BSIS chief and his staff. I am here to represent your concerns and needs.

This year PICA expanded its business operations to 10 statewide chapters resulting in immediate growth. Additionally, PICA is expanding its membership nationwide. Our goal is to gain more national recognition through national representation.

PICA is being represented at this year's World Investigators' Conference in Dallas, Texas and joins over 700 attendees from 18 countries. Our Legislative Day in Sacramento happens March 15, 2010 and all PICA members are encouraged to join us as we meet and greet many of our legislators inside the Capitol. Our Unlicensed Activity Committee has its fingers on the legislative pulse.

Please remember, PICA is your association. Your direct comments and emails are always welcome and appreciated. Enjoy this year's ride!

Legislation:

The chief goal of your PICA Legislative Committee is to identify and inform so that PICA members are made aware of issues facing our profession. Clearly, our state budget deficit creates a hurdle for many new bills. California simply doesn't have the money to pay for new programs and laws. Likely, we'll see bills that deal with identification theft and efforts to reduce the availability of public information, as well as bills limiting sources and access to personal identification information. Additional legislation may involve the requirement of private investigator employees to register with BSIS and the exemption of surveillance operatives from mandatory breaks.

Rick von Geldern,
Legislative Chair - Northern CA

Raymond Guillermo,
Legislative Chair - Southern CA

***About the Author** (Featured Article): Rick Albee is the president of Data Chasers, Inc. He holds a master's degree, is a BAR associate member, and is certified through multiple disciplines in computer forensics. Rick has served in law enforcement for 29 years. He is an expert witness in several jurisdictions and sits as Special Master in Federal Court. Additional Information about Rick can be found at www.DataChasersInc.com.*

Featured Article:

By: Rick Albee © 2010 Richard L. Albee, excerpt

Computer Forensics: When Do You Need It?

COMPUTER FORENSICS

Computer forensics is the science of identifying, recovering, extracting, preserving, and documenting ESI (Electronically Stored Information) so that it can be presented as evidence in a court of law. Although relatively new to the private sector, computer forensics has been an evidence gathering tool of technology-related investigations and intelligence gathering in law enforcement and in military agencies since the mid-1980s. However, tools making the examination process comprehensive, expedient, and financially feasible have only been around since 1999.

E-DISCOVERY

Electronic discovery for ESI differs from computer forensics, although your case may require both. **E-discovery** is the science of turning a mountain of paperwork into searchable electronic data that can then be examined for keywords, redacted, de-duped, and produced in a manageable format. Consider this: You have 150 boxes of paper that need to be examined for specific data. You either hire a team of paralegals to slave over the documents, which takes several months and yields questionably accurate results, or you use the E-discovery process, which takes about a week, and results in guaranteed accurate findings.

COMPUTER FORENSICS VS DATA RECOVERY: MAKING THE DECISION

When deciding if a case calls for a computer forensics expert, it is important to distinguish computer forensics from data recovery. Data recovery, as the name implies, is the recovery of information after events affect the physical data (such as a hard drive crash). Computer forensics goes much further; it involves a complete computer examination with analysis as the ultimate goal. Computer forensics involves both recovering deleted files and searching the slack (data remaining in the unused portion of each cluster) and unallocated space (space not assigned a File Allocation Table) on the hard drive. These are places where a plethora of evidence resides.

Computer forensics requires tracing Windows artifacts, those tidbits of data left behind by the operating system, for clues as to what the computer has been used for. Forensics experts know how to find these artifacts and evaluate the importance of the information discovered. Forensics exams allow the processing of hidden files that contain past usage data. Forensics experts reconstruct and analyze the date codes for each file to determine when the file was created, last modified, last accessed and/or deleted.

Computer forensics allows investigators to run string-searches for e-mail when an e-mail client isn't obvious. Analysis can reveal Internet usage and full data recovery even after a computer has been defragged or formatted. In using industry-standard methodology, forensics experts can supply concise reports with demonstrable and organized results. If your case calls for intricate data recovery and analysis, it's time to call a forensic computer expert.

WHAT'S IT WORTH

In the vast majority of cases, a forensic analysis is moderately to highly successful. However each case is different and sometimes the desired evidence is not on the computer. In this situation, you have the right to be informed, and an experienced examiner will advise you regarding the possibility and probability of finding what you're looking for.

In assessing the value of a case, I use the analogy of a poker game. If it's a small pot, and you have a great hand, you'll call the raise with little risk. If it's a big pot, even if you have a poor hand, you might still call the raise because there is much to be gained. But if it's a small pot, you've got a mediocre hand, and it's a large raise, you'll probably fold. It's not worth the risk. This is much the same for a forensic computer exam. If there is a lot at stake, it's worth taking a chance to recover those instant messages. If it's a small pot, let it go.

FROM AN EXPERT: 3 STEPS TO MAINTAIN COMPUTER DATA INTEGRITY

1. If the computer is ON, leave it on. If it's OFF, leave it off. Each time an operating system boots up, it writes to several hundred files and overwrites data that is crucial to the investigation. We use tools specifically designed to acquire the data without booting into Windows. This data is retrievable if it isn't over-written by the boot process.

2. Never allow company personnel to access the computer. This changes the date that files were last accessed or written to, stores contaminated data in files that are only accessible by forensic experts, and taints the evidentiary value of all data. We never boot into Windows; there is no way to do so while insuring the hard drive's integrity as Windows writes to several hundred files during each boot process.

3. Never allow a copy of the hard drive to be made. A forensic copy differs from Windows and DOS copies which only copy existing, logical files and not the entire physical hard drive. We make a bit-copy of the entire physical hard drive, including slack and unallocated spaces where much of the needed data resides.

By following these simple suggestions, you allow us to ensure a thorough forensic examination that can be used for testimony.

Technology: Cellular TelephoneData Recovery

By: Frank Zellers

Over the last few years, cellular telephones have become an increasingly popular source of investigative intelligence. Investigators recovering evidence from a variety of different cellular telephones continually face challenges. The level of difficulty in recovering information from cell phones depends on the digital media and type of data being recovered.

RECOVERABLE INFORMATION

Some of the recoverable information from cell phones includes:

- Address books
- Call logs (i.e. incoming, outgoing, and missed calls)
- SMS messages (Short Message Service)
- MMS messages (Multi-media Message Service i.e. picture, video, and audio/music messages)
- Images and pictures
- Device specifics and network information: IEMI, ESN, MEID, phone number, carrier, etc.

POPULAR CELLULAR RETREIVAL SOLUTIONS

There are several forensic solutions used to retrieve data from cellular telephones. Here, I highlight two of the more popular tools, the Susteen Secure View 2 and the CelleBrite UFED System.

The Susteen Secure View 2 is a PC-based cellular telephone forensic solution. Data cables are used to connect the cellular telephone to a laptop or desktop computer running Secure View 2 software. Cellular telephones can also be examined using a blue tooth connection. The Secure View 2 currently supports 2,203 different phone models. Susteen provides online customer support and their Secure View 2 is touted for its mobility and its capacity to acquire cell phone data through several methods such as USB and IrDA. Other features include the MD5 hash software which verifies and validates the integrity of the data acquired and a SIM (Subscriber Identity Module) card reader.

Established in 1999 by a group of seasoned telecom and mobile telephony professionals, the CelleBrite Corporaton offers its UFED system. This system is a standalone unit that connects to the target cellular telephone via a USB cable. Currently the UFED supports approximately 2,000 phone models as well as CDMA, GSM, IDEN, and TDMA technologies, and it's compatible with any wireless carrier. It's noted for its user-friendly interface. Like the Secure View 2, CelleBrite UFED System has the ability to examine SIM cards, but only the CelleBrite UFED System has the functionality to clone SIM cards. Customer support includes online manuals, contact information, and an FAQ section.

To date, there are no systems that have the capacity to examine every type of phone. Also, each cellular telephone system examines phones differently. For example, a particular system may only be able to retrieve call logs and address books.

By using a combination of cellular telephone forensic systems, investigators may retrieve the SMS messages, the address book, and the call logs from the same phone. It's important for cellular telephone examiners to use different forensic solutions to cross-check their results and findings.

APPLYING THE TECHNOLOGY

The telephone pictured below was shot with an AK-47.The round went through the back of the telephone and exited through the front display.

The AK-47 (7.62 X 39mm) round creased the phone battery. The phone still powered on and off although the display screen was nonfunctional. I examined the cell phone using Susteen Secure View 2 to recover pertinent information which assisted investigators with their case.

For those who might find investigative cellular phone technology intimidating, professional training is available. The analyzing capacities and efficiency of these forensic systems are too valuable to pass up.

It's important for cellular telephone examiners to use different forensic solutions to cross-check their results and findings.

About the author: *Frank Zellers is a Senior Detective with the Corona Police Department assigned to the High Technology Crimes Unit. Detective Zellers has over 10 years of experience in the area of computer forensics and high technology crimes. He is also a licensed private investigator and owns and operates Inland Direct, a small consulting company located in Corona, CA.*

Cell Phone Shot By AK-47

Welcome New Members:

- L.R. Hughes
- Lew Abramson
- Andrew L. Saucedo
- Gary Hughes
- Jonathan Robinson
- Diane Parker
- Bert Friedman
- William R. Ditmars
- Jeff Ogden
- Joseph Travers
- Christopher Spicer
- Mark Eskridge
- Ralph Swenson
- John Moore
- Steve Youmans
- Darryl Ellis
- John Chadwell
- John Clausen
- Michael Johnson
- Kris Buckner
- Mike Hermann
- Richard Hofmann
- Douglas Newton
- Jeffrey Wells
- Louis Laurenti
- Dan Alvarez
- Mary Beth Fleming
- Reginald Stewart
- Ernest Pineda
- Lowell Glover
- Peter Psarouthakis
- Wayne Ketaily
- Riley Parker
- Nicole Friel
- Mary Joe Holloway
- Joe Chavez
- Jeremiah Jones
- Mario Maldonado
- James Newberry
- Robert Kraft
- William Courtice
- Michael Lee
- Sarah Rodriguez
- Daniel Santana
- David Rowan
- Richard Kelso
- Samuel Gurwin
- Francie Koehler
- Randal Hecht
- Michelle St Claire
- Conrad Cota
- Hector Diaz Colon
- Clayton Steacker
- Douglas Newton
- John Gavello
- Scott Whyte
- Merrilee Riley
- David Elsebusch
- Morgan Jenner
- Mark Neyer
- Lori Johnson
- William Black
- Ed Lopez
- Roy Howat
- John Facchin

Quotable:

"We have a criminal jury system which is superior to any in the world; and its efficiency is only marred by the difficulty of finding twelve men every day who don't know anything and can't read."

-Mark Twain

Upcoming Events:

- World Investigators' Conference

  March 11th - 13th in Dallas, Texas. Visit PICA at our confernce booth!

- Legislation Day in Sacramento

  March 15th. Annual legislation day. Walk the legislative halls of the California State Capitol Building and familiaize yourself with the legislative process.

- District Meetings and Educational Opportunities

  Please contact your local PICA director for upcoming events.

Advertising Info:

Published by PICA. Editors: Rick von Geldern & Ryan Tyler-Ramirez

Front page photo: Santa Barbara County Courthouse, by Melanie Kroon

P.I.C.A.
Professional Investigators Of California
P.O. Box 568
Verdugo City, CA 9104
800.765.7422 ph
555.543.5433 fax
www.pica-association.org

TO: