The Journal
Private Investigator's Association of Utah, Inc.

October 2007
Mel B. Ashton
Editor

Searching For the Truth

By Mark Nosack

I was a police officer for over thirty years. I've worked virtually every type of investigation that you could imagine. I've gotten thousands of confessions from people who never dreamed they would tell me the truth when they walked through the door. Remember though, the truth is the most important part of our profession. Our job is not to find the defendant innocent; our purpose is to determine the truth of the matter. The easiest and most common way to gather valuable information is through the interview process.

Interviewing people is both an art and a science. There has been significant research done over the past forty years concerning deception detection. A well trained investigator can conduct interviews with numerous people concerning a single event and determine who is telling the truth and who is lying. I don't need a polygraph to tell me that a person is lying. I simply interview and learn the truth. It's called a Behavioral Analysis Interview.

During the polygraph, the interviewer asks what are called control questions. Those are questions which the interviewer knows the answer to. *"Is your name Mark Nosack?"* The polygrapher compares the responses of the control questions to the responses of the subject questions concerning the event.

During the Behavioral Analysis Interview, the interviewer first asks questions about school, work, family, etc. that have no threat to the subject. That initial phase of the interview allows the interviewer to analyze the subject's behavior and how they act when being honest. Once the interviewer moves into the phase that concerns the event, the interviewer pays close attention to verbal and non-verbal behaviors and analyzes any changes in the subject's conduct.

A trained interviewer can determine whether the subject is telling the truth, 85-95% of the time. I have gone into businesses and interviewed 25 employees concerning an internal theft and narrowed the field down to two or three in Just a few hours. Then I conduct follow-up interviews and narrow the field to one. Then I go in and get a confession.

Remember, interview and interrogation are two totally separate animals. The interview is designed to illicit information and also helps the interviewer to determine who is telling the truth and who is lying. During the interview, the questions are designed to get the subject to talk.

The interrogation, on the other hand, is designed to get a confession. The conversation is 90% the interrogator and there is typically only one question asked during the interrogation phase. The question, often called the Alternative Question, is designed to illicit a confession.

continued on page 3

The Journal is the official publication of the Private Investigator's Association of Utah. It is published quarterly. The opinions expressed herein are those of the authors and do not necessarily represent the view of PIAU nor its individual members.

1780 West 9000 South,
Suite 221
West Jordan, Utah 84088
Phone: (801) 467-9500
FAX: (801) 253-0578

As the year ends, I look back on the good things that have happened for private investigators. We have has some good Quarterly Meetings and the Annual Conference was a success. We elected a new president and have some new board members for 2008. I think that it is exciting to have some new leadership and watch PIAU move ahead in the upcoming year. There are some concerning bills that are currently in the US congress that as written would make it a felony to obtain or sell a social security number without the authorization of the person whose social security number it is. If any of these bills pass, as written, it would be a terrible blow to the private investigators. I am glad that NCISS is there fighting for us to see that private investigators are exempt from these proposed laws.

We have has some of our former members not rejoin with us but it has been a good year for new members joining our ranks. We are only as strong as our membership. There is always a lot to be done to keep the privileges that we have and try to stay on top of our profession. I want to sincerely thank our membership for supporting me as president for the past two years. I really missed the assistance of Kelly Madsen in planning for the Annual Conference.

We recently suffered a blow from a decision of the Department of Public Safety. A meeting of their attorney, the Director of the Driver's License Division and some staff members resulted in a decision to deprive private investigators of the privilege to get Drivers License and Photos. They determined that although the Drivers Privacy Protection Act (federal law) classified private investigators as a permissible user we are not permitted to receive Highly Restricted Personal Information which includes individual's photographs, images, social security number, medical or disability information. I have received several calls from our members on this issue and we plan take the matter up with the Director of the Driver's License Division. After reviewing the Drivers Privacy Protection Act, I feel that we have a good position to ask for the return of this privilege. The Utah Code gives us the privilege but if DPS continues to maintain their position, Utah Law does not supersede Federal Law.

I have enjoyed serving at your president and I will enjoy working in 2008 as a member of the Board of Directors with the new president and board members.

Mel Ashton

SEARCHING FOR THE TRUTH continued from page1

"Did you plan this out, or did it just happen on the spur of the moment?"

Folks, seek out good interview and interrogation training. Outside of surveillance, interviewing people is 90% of what we do.

When you write your final investigative report, make certain that it ends with the truth. If you do any less, you're doing both yourself and your client a disservice.

CIVIL OR CRIMINAL

By Tim Penney

Typically, private investigators handle a variety of cases. Of course, a criminal case is the violation of a statute that involves jail, imprisonment, a fine or both; so the investigator working a criminal case is likely to proceed with a great deal of vigilance, especially if (s)he is working a field assignment in a metropolitan area with a high rate of crime; but do private investigators proceed judiciously if they are working a civil case that takes them into the streets?

For Example, if a private investigator is serving a summons and complaint in a civil cause of action, at the defendant's place of residence, does the investigator work alone or use a colleague for cover? Does (s)he have some form of communication with a local police agency? Does the private investigator employ "door tactics" when approaching the residence? Does the investigator understand the "Fatal Funnel" concept? Does the investigator have an understanding of the "Kill Zone?" Does the investigator wear concealable body armor? These are all valid questions.

Years ago, there was a South Ban (San Jose California) attorney that utilized me to serve as many as sixty papers a day at one of the local HUD housing complexes. Although the legal documents were civil actions, the geographical locations mandated that I have a security detail, housing officers, the projected the same image as any tactical squad or emergency services unit, escort me through the maze of urban concrete that occupied four city blocks. The reason for the backup was clear. At best, the named defendants could have dropped a TV set from the third floor on my head; and at worse they could have literally shot the messenger.

In the jurisdiction where my firm is located a "TRO" (temporary restraining order) is technically a civil action. However, most of us know that the reason for seeking court intervention in a "TRO" is anything but civil. Usually the moving party has received some type of credible threat, and in a lot of cases, great bodily injury. On the "TRO" the petitioner indicated the reason for the restraining order and if the respondent has any weapons. The late "TRO" I served, the respondent had a propensity to carry weapons and made overt death threats to the moving party and family members.

Since the subject resided in an area known for gang activity, I proceed with a great deal of due vigilance and contacted the local police department and requested a marked unit.

Keep in mind that some agencies may not respond to this type of call for a variety of reasons; and if they do not dispatch a unit, it could be priorities and placed at the bottom of the list. Therefore, you could be waiting for several hours; and it is not unusual for this kind of call to be passed onto the next shift.

When working field assignments, it is paramount to work safely and within the parameters of the law, irrespective of your experience or the type of training you have been through. It is equally imperative to always be attentive, constantly alert and always remember; **safety takes precedence over billable hours and margin of profit.**

ISOTOPE RATIO MASS SPECTROMETER (And What It Might Mean to Private Investigators)

By Michael D. Myers II

What is IRMS

Many of us may have heard of a mass spectrometer. Newer to the field of science is the stable mass spectrometer. It is used to separate the heavy isotopes from the light ones.
We are not talking about elements or radioactive isotopes which have a half life and decay over time. Probably the easiest way to illustrate this is the illuminated sights on a modern firearm. Numerous companies have used for many years 3H, also called tritium, to give that green radioactive glow in the dark to pistol sights (and to rifles). These types of elements decay over time (or with tritium go dark) and this decay can take from nanoseconds to thousands of years. 14C, or carbon 14, is widely known because of its use in dating biological materials that are less than 50,000 years old. They are also used as a tracer in metabolic studies. [1 (pg.401)]

How Does the Test Work

For the purposes of our discussion, think of the mass spectrometer in the new and old configuration. Maybe even a VCR. The old VCRs had 1 head and produce a good, but not super defined picture on the TV. Later versions had 3 heads, which make the picture much clearer.

The old mass spectrometer has one receptor cup which can detect one element at a time. The isotope ratioing mass spectrometer (IRMS), can detect three elements.

The substance to be tested, TNT, hair, perfume, etc, must first be turned into a gas form and then introduced into the isotope ratioing mass spectrometer. The gases are blown or carried down a tube by an ion beam. A magnet is used to deflect or separate the ions from the elements being tested. At the end of the flight tube the elements are deflected into separate detector cups.

The traditional mass spectrometer might be able to identify or detect a 0.05% difference in the abundance of an isotope. The isotope radio mass spectrometer can identify a 0.0002% difference.

As with many testing procedures, there is used what one might call a control or calibration. This is done right before and right after a test. It not only ensures the machine is working accurately, buts gives one a known benchmark to compare your working sample to.

Daily calibration is not done. Different laboratories exchange information on working samples with each other. These samples are identified by the stable isotope community and exchanged in order to determine the best estimate of actual stable isotope composition of the working standard.

Under the best conditions, there will be many working standards or 'data bases' from which tested evidentiary type samples can be compared. [1 (pg.403)]

Forensics

In the world of 'knock-offs' or black market goods, which are sold in many back alleys of big American Cities, perfumes have always been popular.

One possible use of the IRMS would be to take known (fake) samples of confiscated perfume and have it tested and entered in to a database. If possible, to include where the confiscated sample was originally manufactured (i.e.; Mexico, China, etc).

After the authenticated sample from the original manufacturer was tested (benchmark or standard) the suspect perfume could be tested and compared to past samples for the purposes of similarity (trying to identify the geographic origins of the suspect sample).

The IMRS may also be able to identify the geographic origins of elements (including but not limited to, water) used in the making of the perfume.

Where the current data bases may be lacking in ability to compare a new sample to a bench mark from an existing geographic location, new computer modeling and programs may lead the way. The computer programs may be able to project to a geographic location the origins of a sample even though no sample from that location has been tested or entered into a data base previously (Geographic Information Systems, spatial maps of predicted stable isotope ratios can be constructed).

Fingerprints revolutionized law enforcement. Isotope testing may do the same thing, possibly extending its effective reach beyond law enforcement and intelligence communities to the private sector, especially as databases grow. [1 (pg.405)]

After the authenticated sample from the original manufacturer was tested (benchmark or standard) the suspect perfume could be tested and compared to past samples for the purposes of similarity (trying to identify the geographic origins of the suspect sample).

The IMRS may also be able to identify the geographic origins of elements (including but not limited to, water) used in the making of the perfume.

Where the current data bases may be lacking in ability to compare a new sample to a bench mark from an existing geographic location, new computer modeling and programs may lead the way. The computer programs may be able to project to a geographic location the origins of a sample even though no sample from that location has been tested or entered into a data base previously (Geographic Information Systems, spatial maps of predicted stable isotope ratios can be constructed).

Fingerprints revolutionized law enforcement. Isotope testing may do the same thing, possibly extending its effective reach beyond law enforcement and intelligence communities to the private sector, especially as databases grow. **1 (pg.405)**

What About What We Eat

IRMS testing can be used to not only test where a sample of honey came from (country of origin or area of origin) but to test to see if it has been 'watered' down with low-cost fructose corn syrup. Although traditional testing may not distinguish between real and adulterated samples of honey, IRMS can.

This type of testing can also spot the use of inferior quality ingredients in the manufacturing process of things like beer and wine allowing a company or government to stay vigilant.

Concerns over illnesses such as mad cow disease, testing compliance with food production regulations, and verification of claims of origin, especially for high-value products such as cheeses or wines, are all contributing to an increased use of stable isotope analysis in food authenticity (see also http://trace.eu.org).

This type of testing can and has been applied to many different types of food, including testing meat for steroids, similar to the protocols used in human doping.

Examination of food can go beyond light isotope testing. By this I mean researchers and scientists can go farther that just trying to pin down a geographic point of origin.
Looking at hydrogen, oxygen, nitrogen and sulfur isotopes has been explored for the specific purposes of detecting methods used to farm or raise the beef, in addition to narrowing down its geographic source.

Combining light isotope ratio analysis with heavy isotope analysis (ratios) (for example lead or strontium), as well as other chemical analysis or elemental analysis, may yet be a profound source of information about food sources and process methods. **1 (pg.407)**

Drugs and Drug Abuse

Being that there are four major / primary poppy growing areas in the world, ease of identification through IRMS is probable. If and when new sample (most likely contraband/evidence) are tested and show no similarity to existing known sources in the database, further testing can begin to unravel the mystery of the sample's origin.

This takes us back to the importance of Geospatial Modeling Software. This software is able to predict or project possible locations of manufacture, until verification can be had. Once confirmed, it would probably be added to the database for use in future investigations.

Of course the same techniques can and are used by local, state and federal law enforcement agencies for investigations to include, but not limited to marijuana and cocaine. In fact, the D.E.A.'s Cocaine Signature Program does just that, allowing them to narrow down cocaine samples, large and small, to more specific points of origin.

Recently, Australian Police seized 50 kilograms of heroin from the freighter Pong Su, a ship which sailed under North Korean registry. Another 75 kilograms was seized at the Australian off load site. Authorities were suspicious that North Korea was venturing into the heroin trade. Later analysis through IRMS testing excluded all known major heroin producing areas, SE Asia, SW Asia, Mexico and South America.

This type of testing can also alert law enforcement that existing drug trafficking routes might be changing.

When synthetic drugs like ecstasy enter into an investigation, testing will less likely reveal points of origin than matching batch to batch or batch to cook. [1 (pg.410)]

Humans

Because scientists can identify variations of differences in the hydrogen and oxygen isotopes from different bodies of water, they are then able to identify those variations in humans or animals. Whether it is a migrating human or migrating elephant, through testing, it can be possible to track a person's travels. Of course this presumes that the subject tested did in fact consume local foods.

A simple strand of hair may be all that is needed to confirm that one has been to a specific location or to multiple locations throughout the globe.

Given sufficient space from one another, scientists are able to test water and not only differentiate the different water sample sources, but, project where the samples came from if not in the existing databases.

IRMS could have been utilized in the 2001 anthrax attacks. As long as the original spores remain intact, the isotopic composition of the water that these microbes were cultured in may point to a specific location investigators can follow up on. [1 (pg.411)]

Teeth Aren't Just for Biting Any More

Although there is DNA, fingerprint or possibly dental records which can be used in many investigations, what if those are not panning out for investigators?

There might be help from IMRS. Even without dental records, if you have teeth, there might be hope of recovery of some evidentiary material.

Teeth are formed during the pre-adult stage of our lives. Meaning that even later in our lives, even if no good DNA can be recovered from a tooth, IMRS testing may show a number of trace components, like lead, strontium, and carbonates. The carbon isotopes reveal dietary information. The oxygen in the carbonate reflects the oxygen of the water in the blood, which is related to geographical variations in drinking water.

The heavier element strontium shows geographic variation related to differences in different regions and countries. Strontium is taken in by plants and makes its way into the food chain, becoming incorporated into humans as part of our diet. It seems that both teeth and bone can be used to distinguish migrants from locals in a population.

Hair and fingernails also record dietary and water source information. It has recently been shown that through IRMS testing, persons from Europe, the United States and Brazil could be distinguished based solely on the isotopes in their fingernails. [1 (pg.413)]

TNT to Packing Tape

Whether it is TNT made in the United States or abroad, or many other products like security papers, counterfeit currencies, plastic tape, packing materials, explosives, clothing or synthetic drugs, IRMS can provide substantial insight for investigators.

What About Your Investigation

It is unclear at this point whether private sector investigations can access this technology. I hope to have a definitive answer soon and will report on it.

It certainly has been embraced by law enforcement and the intelligence community.

I would like to thank University of Utah, Professor of Law, Scott M. Matheson, Jr. and University of Utah Biology Department Professor James R. Ehleringer.

This article was derived solely from a scientific paper written by James R. Ehlinger, Thure E. Cerling, and Jason B. West. (2007). "Forensic science applications of stable isotope ration analysis," in R. D. Blackledge (ed.) "Forensic Analysis on the Cutting Edge: New Methods For Trace Evidence Analysis." John Wiley & Sons, Inc: Hoboken, New Jersey.

[1]A substantial portion of this article was quoted directly from the above research article (corresponding page numbers noted at the end of each section).

PRETEXTING IS CONSTANTLY COMING UNDER FIRE AND THERE IS A PRETEXTING BILL TO OUTLAW ALL PRETEXTING THAT DIDN'T PASS in the US House of Representatives.

Mel Ashton

The password today is 'pretext'

State, federal bills might impose sentences on impostors

Dan Fost, Chronicle Staff Writer
Wednesday, September 13, 2006

The Hewlett-Packard scandal has taken a word from the film noir world of the private eye, pretexting, and put it into a bright spotlight. In the process, the affair could help criminalize the activity as well.

Pretexting, a practice long used by detectives and others, has increasingly come under fire by lawmakers and privacy advocates.

Although it has many names, from undercover work to the hacker slang "social engineering," the basic ruse is one in which someone represents him or herself as someone else, using a false pretext to obtain information.

Ten states have outlawed the activity in recent years, and a bill is on Gov. Arnold Schwarzenegger's desk that would do the same. Congress is also considering penalties.

"This little incident at HP shows that there can be abuse, not only of power, but from folks who try to gain the information," said Nick Garcia, spokesman for state Sen. Abel Maldonado, R-Santa Maria (Santa Barbara County), co-sponsor of SB202, which would make it a crime to obtain phone records through fraud or deceit.

"I want to know that my conversation is private, my records are private and no one can get them," Garcia said.

The bill passed the Senate and Assembly last month. Schwarzenegger has until Sept. 30 to act or it automatically becomes law. His press office said he has not taken a position. Garcia said he hopes that last week's apparent computer intrusion, in which someone was able to listen to tapes of Schwarzenegger's private phone calls, would help spur the governor to sign the bill.

The U.S. House of Representatives and Senate also have bills pending. A bill that passed the House in April has been stalled in the Senate. House members have cited the HP case in pressing Senate Majority Leader Bill Frist, R-Tenn., to act, according to the Wall Street Journal.

Some groups have been agitating for such action for a long time. The Electronic Privacy Information Center petitioned the Federal Communications Commission to establish stronger security requirements for customer records and had asked the Federal Trade Commission to crack down on the data-broker industry.

"We have felt for some time that it's a real risk for consumers," said Marc Rotenberg, the center's executive director. "We're hoping some of the policymakers in Washington will take some action."

Last month, AT&T also shined a light on the practice when it filed suit in Texas

against two dozen unnamed data brokers who had used false pretenses to get access to customer phone records.

AT&T spokesman Walt Sharp said the company is "strongly in favor of laws that would criminalize this activity and establish very severe penalties for it."

However, the new laws may not resolve the issue, some suggest.

"The problem is not merely about those who pretend to be someone else, but also that the companies that have our information are careless with it," Lee Tien, a senior staff attorney with the Electronic Frontier Foundation in San Francisco, said in an e-mail. "What's easier, to go after pretexters or for AT&T to be more careful?"

Kevin Mitnick, a notorious former hacker and now a security consultant, said in a phone interview that many current laws apply to pretexting or, as he referred to the practice, social engineering. He said he was convicted of wire fraud as a young man for essentially doing the same thing, calling the phone company and pretending to be someone else in order to obtain something -- in his case, phone company software.

"If the feds want to make an example of someone for making a phone call in furtherance of a scheme or a fraud, by using deception ... technically the wire fraud statute can be used to prosecute," he said.

California Attorney General Bill Lockyer and the FBI have already started criminal probes into the Hewlett-Packard case.

But Rotenberg said wire fraud laws don't go far enough because most wire fraud involves demonstrable economic harm, such as a fraudulent check. Instead, he said, the actual act of posing as someone else needs to be outlawed.

New laws aren't what's needed, Mitnick argued. Instead, he said people and companies need to be aware of how much information is readily available and how easy it is to use a false pretext to get it.

"When I used to be a private investigator, I used to use a pretext against the phone company all the time," Mitnick said. "How they verify a customer's identity is usually by the last four digits of their Social Security number or their driver's license number. And that information is really easy to obtain. ... If I was in front of a computer, in about three minutes, I could give you your Social, your driver's license and your mother's maiden name, all legally obtained."

He acknowledged that California has tougher laws regulating driver's license numbers than other states and he might not find them so easily.

With that information, Mitnick said a person might call the phone company and claim their teenager obtained a cell phone without consent. Then, using a Social Security number, the person might be able to persuade the company to reveal the phone records of an individual under investigation.

Another tactic is to call a cell phone company retail outlet, claiming to be a staff person at another store where the computers are down. That's how hackers were able to get Paris Hilton's cell phone information, he said.

"The milk is already spilt," he said. "The key is, don't have any level of confidence. Just assume that all of that is public and don't use it for authentication."

.