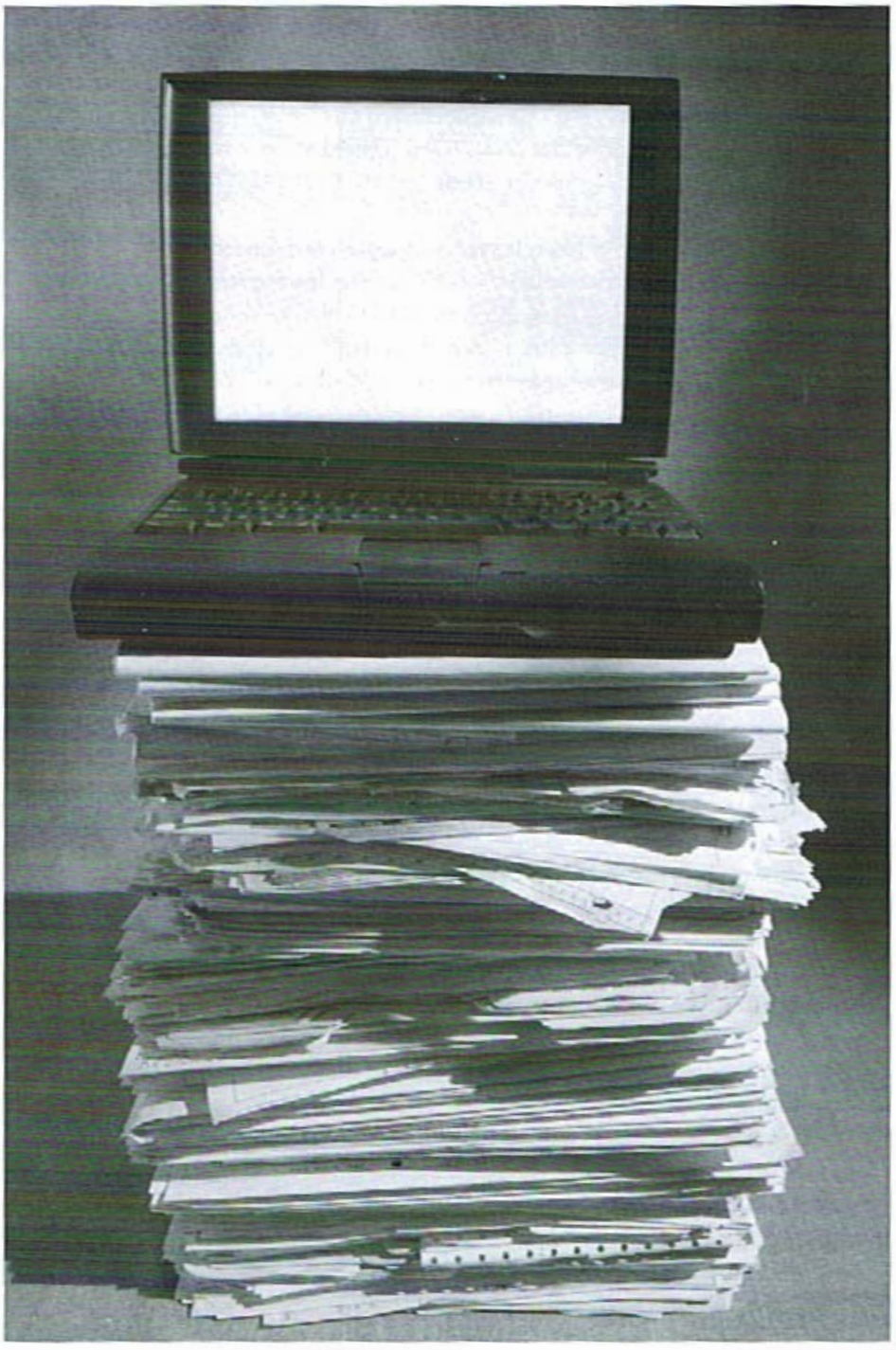

Computer Forensics: A Science or an Art

By Wayne Marney

As a retired 22 year police veteran, including eight years as a detective in a computer crimes unit, I have seen almost every imaginable crime having a computer related element. I have been an instructor in computer forensics since 1997 and a past member of the board of directors of the largest law enforcement training organization (IACIS) in the world.

Today, academia and the courts consider computer forensics a science, but is it really? This article will examine that question and discuss the current environment in which most attorneys will find themselves when defending cases involving computer evidence. The focus will be on criminal cases, but this discussion is equally applicable to civil litigation.

Is computer forensics a scientific inquiry or an art? *Texas House Bill 1068, Section 2. Article 38.35* states a forensic analysis "does not include: (C) digital evidence." As you will see, once an exact image of the electronic media has been made, scientific standards assume a limited role and the art begins. The data found and conclusions drawn can vary dramatically completely dependant on the skill and or agenda of the examiner. Computer forensics can and does provide answers to key issues in criminal and civil litigation. Results from such an exam have to be vetted because they also commonly tar individuals with incomplete exams and inaccurate findings.

Some relevant factors that affect the results of an exam are:

(a) Investigative experience, e.g., does the examiner have enough background to know the elements of the offense, experience with human behavior, what culpable mental state needs to be proven, if necessary, recognize a conspiracy, recognize improper evidence handling procedures;

(b) Most examiners do proceed with ethics and attempt to be impartial in their exams. Unfortunately, peer pressure and the "thin blue line" mentality does exist. Computer Forensics is not a discipline that embraces open peer review, but keeps things very proprietary/trade secret. Does the examiner have a vested interest in the outcome of the case; is s/he the case agent or is s/he evaluated on how many cases are indicted versus not filed? As you will see, this leads to fixation on the indictments and not a scientific impartiality looking for the truth, and includes both inculpatory and exculpatory facts. Or are examiners just advocates, shading things for the home team?

(c) Knowledge of the rules of evidence;

(d) Forensic computer training and certification is only the beginning; it doesn't make the examiner an expert as case studies show.

Computer evidence rarely stands on its own merit; it requires a thorough human based investigation. Without a good "gumshoe" investigation, the forensic examiner can rarely say who was sitting at the keyboard. Unless physical custody of the computer removes other people as suspects, only a solid investigation can establish culpability. Is scene documentation haphazard? This is a major weakness with many cases. Finally, confirming the chain of custody is the most crucial element in a defense. Once the computer evidence is admitted at trial, it then becomes an issue of "what is, is."

Certified computer examiners are required to adhere to a code of ethics that requires an honest review and portrayal of the evidence. It is improper to mislead the unwary or computer-illiterate person about the nature of computer evidence or the weight that should be given to one piece of evidence over another. A forensic computer examiner does not have the luxury of speculation because (1) the computer hard drive either has the data on it or it does not, and (2) either the forensic examiner makes the correct conclusion based on reproducible testing or s/he does not. Computer evidence by itself isn't all that conclusive (other than the obvious). There are so many ways that the condition of the data can change. Conclusions from just the data are restricted. However, once a person makes a statement as to his or her actions, then the computer evidence can rise up and empirically prove or disprove that statement.

We will now leave the perfect world and enter today's world of computer forensics. A computer leaves behind all the elements that most people associate with a common crime scene, e.g., the body, finger prints/DNA, trace evidence, the smoking gun, confessions, witness statements, neighborhood canvasses, etc. On a computer hard drive these elements take the form of user files, log files showing actions or accesses to web sites, IP addresses, file fragments, intellectual property (where the mere presence of certain files is the smoking gun), email and email address books of other contacts. Almost all examiners try to be fair and accurate, but many times, they miss the mark.

An Expert or Just an Investigator? Issues with Certifying Forensic Computer Examiners

Unlike traditional crime labs, there are few certification programs for computer forensics. Moreover, none are accredited by an outside organization. The overarching issue is, where does the science stop and the investigation begin? Traditional crime lab technicians know in advance what they are testing for, e.g., blood spatter, shell casing mark identification, controlled substance testing. For example, ASCLAD[2] testing follows stringent testing procedures using specific order of occurrence of testing, reagents, equipment, etc. As they try and apply standards computer forensics only chain of custody procedures translates from standard forensic labs.

My experience has been that a majority of all examiners claiming to do computer forensics are investigators without being experts. They are similar to the homicide detective who finds a shell casing on the floor. He can testify as to when and where he found the shell casing, but he cannot testify about any extractor marks, firing pin marks, ballistic comparisons, etc. The same logic extends to the person conducting the forensic examination. That person must demonstrate that s/he is in fact an expert; otherwise s/he must be limited to testifying only as to where data was found.

Part of what makes a forensic examiner an expert is training. A person claiming to have received training needs to be *voir dired* to determine if s/he possesses the necessary functionality knowledge about the operating system or program involved before an opinion is given. Here we come full circle, because without this knowledge how can you look for *Brady* material? When I refer to *Brady* material, I mean reasonable alternatives or conditions that change the focus of the evidence. I do not mean the electronic equivalent to a "bushy-haired stranger," the omnipresent "unknown network hacker." Courts have

dismissed the defense's attempts to present mere possibilities or theories of third party responsibility without a showing of actual occurrences.

Many examiners are neither able to articulate how their forensic software creates its image nor have they personally validated the accuracy of what it displays. Many have not taken the steps to validate their forensic software even though they are trained in how to validate their methodology. Many can only describe how the forensic program displays an item, but not how the item was originally created or stored. In one case on the East Coast, a federal prosecutor painfully pointed out that the defense examiner didn't know what was taking place with the data and was nothing more than a "script kiddie." This is a derogatory term originating from the hacking community and applied to people who only know how to push the Enter key to run a "script (is a set of actions)" but who in fact do not understand the underlying functionality.

These types of examiners are no different from any other investigator and should not be allowed to give opinions.

Utilizing these automated forensic tools often masks the limited skill of an examiner. Attorneys focus on specific areas of the law to practice; the forensic computer field is no different and has its own specialties. Anyone can "find things;" however, it takes a detailed understanding of what artifacts are left behind when a computer operator uses a computer in order to prove intent or to find *Brady* material. It takes a detailed understanding of this functionality to accurately explain what steps occurred for the data to be in the condition in which it is found.

Forensic Certification Process Isn't Always the Same

Mellon v. IACIS, Case No. 03-10171 (2003), Benton County Circuit Court, Oregon. This case highlights the need to thoroughly vet a person's qualifications as listed on his or her Curriculum Vitae. Obtaining a certification does not automatically qualify someone as an expert. This court hearing brought to light the perceptions of special treatment when seven people with the older DOS Processing Certification were awarded the new CFCE certification without doing the same level of work. The board voted to award the newer CFCE certification to the seven with two of the seven being board of directors. The hearing also brought out an act of alleged cheating by a member of the board of directors in the first upgrade to CFCE certification process.

Disclosure of *Brady* Material

Under *Brady v. Maryland* 373 U.S. 83(1963), the prosecution is required to disclose to the defense any evidence of an exculpatory or impeaching nature as it relates to guilt or punishment. Does this turnover of *Brady* material actually occur in practice? Yes, but is not consistently addressed as case studies show. My experience has been that the fabled "Cops vs. the Dark Side (defense)" mindset of many in law enforcement does play a role that results in overlooking or minimizing *Brady*. Where *Brady* material is concerned, it is irrelevant as to whether the omission is unintentional or deliberate. On a number of occasions I have heard the statement that referred to a certain forensic examiner who left law enforcement as having gone to the "Dark Side." Several years ago, one of the original board members of IACIS attempted to get a member removed from the organization when it was discovered that the individual was doing defense work (the attempt was not successful).

As I approached retirement and began informing people that I was going to accept defense work, not only was I the recipient of similar accusations, but I was pointedly asked in one conversation if I would "take a bite out of an IACIS member?" When I replied "yes, if they did a poor job," the person expressed disbelief that I would do such a thing; bad job or not. It is this mentality: the focusing so fiercely on a predetermined outcome (the indictment), that results in *Brady* material being overlooked by many examiners.

The following are a few examples:

***State of Florida v. Lem Eng*, No. 04-CF-15354, 9th Jud. Circ. Orlando, FL**

Orange County Sheriff's office responds to Circuit City where Mr. Eng attempted to get his computer repaired. Employees surfed the files on the drive and found 68 images of true child pornography. The sheriff's office examiners confirmed the presence of the child porn but made no effort to address *Brady* material in their exam; Mr. Eng is indicted. A defense review reveals clear exculpatory facts that Mr. Eng:

1. Was at work when the files were saved to his hard drive at home.

2. The porn did not come from Internet activity, but was saved via networked media as part of a mass copy of six directories and more than 300 other files.

3. None of the 68 images of child porn were viewed prior to the store employees' custody and actions. *See United States v. Romm* No. 04-10648 D.C. No. CR-04-00216-PMP(PAL). Opinion states in substance that child porn found only in the Internet browser cache folders can be proof of knowledge and possession when those accesses can be shown as deliberate acts.

4. The examiner failed to identify the password

protected user profile (not Mr. Eng) that was being used at the time the files were saved to the hard drive. There was no evidence of knowledge or viewing by Mr. Eng. He was found not guilty.

***State of Florida v. Steven Shurgard*, Case No. 02CF009008A, 02CF010675, Division II**

The city of Temple Terrace police department went to Steven Shurgard's home on a pretext "knock n talk" when the brother came from Illinois with a restraining order regarding Shurgard's months old threats to kill his father over childhood molestation. Only the Sherriff's Office can serve restraining orders. They used this pretext to take Mr. Shurgard into custody on a police officer hold, over something that happened over six months prior, to be evaluated for danger to the public. They seized his computer under "exigent circumstances." While Temple Terrace PD had his computer for eight days, the officers (not being trained in forensics) conducted an exam on the original hard drive, then deleted the recent "link files" that documented their actions causing severe spoliation/tampering before sending the computer to the Florida Department of Law Enforcement computer section. The state examiner then failed to mention in her report about the spoliation\tampering of Mr. Shurgard's computer.

***United States v. Jeffery Tobin*, No. 05-20529-CR-JLG Southern District of Florida**

The tragedy of Mr. Tobin begins when a search warrant in San Diego revealed that his roommate's email address was identified as the source of sent child pornography. At the time of seizure at Mr. Tobin's home in Florida, he admitted being responsible for any child porn on the computer in order to protect his dying partner. His partner was originally the only person indicted. When the partner died of AIDS, the government no longer had an indicted person, so they indicted Mr. Tobin for possession and transmission of the child porn. They noted that the partner was out of town on the date the email was sent with child porn.

At trial, the FBI examiner admitted he wasn't aware that Mr. Tobin's computer had no computer activity of any type on the date the email (AOL) was sent to San Diego. They also failed to obtain the AOL records to show the point of access to the account. He was found not guilty of transmittal and guilty of possession due to the initial admission. During this time he was diagnosed with terminal bone cancer.

***State of Oregon v. Randall Cole*, Multnomah County Circuit Court Feb 2005**

Mr. Cole was indicted for filming three teenage boys engaged in sex acts. The Portland Police Bureau computer forensic examiner presented evidence that out of more than 200 movie clips of adult pornography, only one file was that of real child pornography. At time of discovery when asked about any *Brady* material on the hard drive, the police examiner, Sgt. Jones stated "it wasn't his job to find defense stuff." The forensic exam failed to note:

1. There was no evidence that the movie clip was ever viewed by a user.

2. The CP movie clip was part of a mass peer to peer network download of 20 other files that took more than nine hours.

3. Was deleted in a block of 10 files. This established the user was working with blocks of files. He was found not guilty on the Internet downloaded child pornography charge.

Chain of Custody Issues

For the purposes of the following discussion, the probable cause issues prior to the forensic examiner's involvement will be omitted. Depending on the type of case the players, in order of appearance, are as follows:

Prosecution: law enforcement investigator, forensic examiner, prosecutor
Defense: defendant, defense counsel, forensic examiner

This order of appearance causes different kinds of problems in litigation. It is common knowledge that the defense is playing a catch-up game after the indictment and discovery begins. This brings us to the first area needing close scrutiny: chain of custody.

As an attorney, how do you know if a demur to the search or seizure exists? Only by examining the original evidence and chain of custody documents can this be determined. Normally, photo copies of evidence transmittal forms are discovered that are created early in the case and frequently don't have all the current accesses to the evidence. Accepting a government's proffer of examining only a forensic copy of the defendant's computer prevents discovery of improper evidence handling and/or malfeasance during the forensic examination.

Doing the Discovery Two-Step: Adam Walsh Act Is a Federal Court Trial Procedure

One of the ways the "Cops versus the Dark Side" resistance manifests itself is at the time of discovery. Across the country, it is common for local law enforcement to resist discovery, particularly in child pornography cases. The discovery two-step is the systematic attempts to frustrate legitimate review of the evidence by the defense team. Since the passage of the Adam

Walsh Child Protection Act of 2006 police are withholding direct discovery to the defense and in practical terms limits the examination to a few days. They are requiring a defense expert to go to the police station to conduct the exam. The cost of the forensic exam goes up dramatically and prevents indigent clients from receiving a fair trial caused by the government-created obstacle of restricting access to the defense expert. Even state agencies are now using this act to refuse discovery of hard drives in child pornography cases.

The Adam Walsh Act provision is a federal trial procedure and doesn't apply to state courts as ruled in the Missouri Appeals Court — *State of Missouri ex rel. Matthew Tuller, Relator, v. The Honorable William C. Crawford*, Respondent.

A defense attorney is an officer of the court, whose expert being involved in a court proceeding with no criminal intent is no more susceptible to inappropriate use of evidence than the prosecution team. Until the Adam Walsh act, a protective order and the reasoning of *United States v. HILL*, 322 F. Supp. 2d 1081; D.C. AK 2004 which clearly articulates all the reasons why a defense team should be given full discovery, ruled the day and addressed the concerns of those involved.

On the federal side, the January 2007 decision *United States v. Knellinger*, US DIST CT, EASTERN DIST. OF VIRGINIA, Criminal No. 3:06cr126 found that requiring defense experts to conduct their analysis within the police station was not "reasonable access" and ordered the discovery of a copy of the forensic image with an executed protective order to the defense expert.

The next move towards fairness with computer evidence is the case *United States v. Kuchinski*, US 9th Circuit, No. 05-30607 D.C. No. CR-04-00149-RFC in limiting what evidence can be used to increase the score on the Federal Sentencing Guideline matrix. In the past, once a plea or conviction was obtained involving child pornography, the prosecution would count up all the files located on a hard drive (even though not presented at trial) and use them to increase the sentencing guidelines. *Kuchinski* curbs this practice by restricting evidence that had been deleted or in the Internet cache where no facts demonstrate the defendant was (a) aware of their existence or (b) attempts were made to access them, unlike *United States v. Romm* where such knowledge was established.

Forensic Computer Specialties

In general, there are two different disciplines within computer forensics that require different skills. The first is system intrusions (network attacks, e.g., hacking). The second is data recovery based. In order to prove intent, the examiner must find deliberate acts by the computer operator with *Brady* material being ruled out. The latter has been an afterthought and occur infrequently only when forensic findings are vetted for accuracy as we have seen with a few case studies.

Testifying in Regards to Computer Evidence

Many people are taking minimal computer forensic training and begin conducting forensic exams of computer evidence with little or no peer review. *Daubert* hearings are not being conducted to determine if the examiner does have the functionality knowledge about the issues involved in the case before they are allowed to give an opinion as an expert. Courts are accepting people as experts with only the most minimal training and experience by showing that some form of forensic training has been taken. In the case of *State of Washington v. Degroff*, Case no. 02-1-960-7 (2003), a child sex abuse/pornography trial, the defense expert used EnCase™ in her examination of a Macintosh computer. Testimony demonstrated that she was unfamiliar with the Macintosh environment, file system and used Windows terminology.

Beware of the "data dump" examination that is common within the law enforcement community caused by inexperience or over-worked examiners who resort to just finding things without providing proof of intent. Their case loads have created a policy to do superficial evidence searches betting that few cases will be contested. On the civil side, just because you find an examiner working for a large accounting firm or other business doesn't mean that person has the necessary investigative skills for a case. They rely on the attorney to tell them what evidence to collect rather than the forensic examiner taking the issues of the case and finding the relevant evidence. Attorneys have been at the mercy of their own misconceptions of what evidence is available to prove their cases and relying on their own computer skills to guide them. Consequently, *Brady* material is frequently missed, as well as other possible suspects. The examiner's ignorance of rules of evidence can lead to sanctions from the court. Conversely, if the forensic examiner is a strong investigator, he must understand what he does not know about computer science so he can seek answers.

Conclusion

Computer forensics is a complex issue and I am stretching the bounds of brevity in this paper. I'll close with some steps that would have rescued many cases. Current discovery laws, including the new changes to the federal discovery procedures, do not prevent the defendant from continuing to use the computers after they become a target of discovery. Remember, eDiscovery does not take into consideration forensic issues, it is an active file data dump and can very well not collect the evidence you need to win. In a civil case, at the time of first filing, obtain a protective order that stops the use of suspected

computer equipment until it has been forensically imaged or protected. This freezes in time the condition of the data and prevents destruction of that one piece of data that might make your case by continued use. Create forensic images of everything relevant; you don't have to examine all the images in a case, but at least you have protected the data from destruction. Always involve a forensic examiner at the first hint that there may be computer-related evidence.

endnote

1 ASCLAD – American Society of American Crime Laboratory Directors

Wayne Marney recently retired from the Oregon State Police were he was a detective in computer crimes for eight years. He is recognized nationally as an expert in Texas, Florida, Oregon, Washington, New York and US District Court, having performed more than 600 examinations in both the criminal and civil arenas, as well as having served as a trainer, speaker and author of manuals discussing technical aspects of electronic evidence. Mr. Marney has a national practice and can be reached at 214.605.1338; his email address is wmarney@cfsiusa.com.