A Triad of Collaboration: Internet-Related Investigative Considerations Prior to the Computer Forensic Application

Dr. Robert DeYoung

St. Thomas University

Forensic Recovery, LLC
Davie, FL 33331-2964
rdeyoung@forensicrecovery.com

Abstract

This article discusses the importance of the initial investigative process in Internet-related investigations where there is a receipt, transmission, or exchange of electronic data between law enforcement and a prospective offender(s). The dependence on computer forensic analysis to collaborate the evidentiary exchange will create numerous prosecutorial obstacles in that the forensic process can only recover evidence that exists and is recoverable. In terms of electronic evidence, one can only speculate as to what is not, or may have at one time, existed. The author proposes that, based on experiential substantiation, that the use of the Triad of Collaboration in all Internet-related criminal investigations provides a cross-referenced, detailed record of any and all activity where there is a receipt, transmission, or exchange of electronic data between law enforcement and a potential offender(s).

A Triad of Collaboration: Internet-Related Investigative Considerations Prior to the Computer Forensic Application

Historically reactive in nature, law enforcement once again finds itself ill prepared to effectively confront the criminal element operating in our technologically advancing society. The very technology, which has made life easier for each of us, has opened the door for offenders of crimes against persons and property to proliferate at an unprecedented rate. Federal agencies dealing with tremendous caseloads are in a position to offer local law enforcement limited support. Local law enforcement response is often sporadic and outdated.

Today’s society has become increasingly dependent upon computers for both personal and business use. “Computers have revolutionized the way we store information and communicate. The Internet has revolutionized the way we obtain information” (Read, 2001). It is not surprising to note that in 2000, there were a reported 153.2 million computers in use and 135.7 million Internet users in the US (Hendrick, 2000) (see Figure 1). The global figures only add to the potential for criminal activity. Technology itself creates an environment through which exploitation is facilitated, allowing the victimization of individuals, organizations and entire societies.

The list of crimes occurring on the Internet is extensive and growing. The familiar offenses include the sexual exploitation of children, identity theft, stalking, fraud, malicious destruction of data, and the proliferation of virus attacks.

Figure 1. Results from research reports by eTForecast

YEAR END	**2000**	**2002**	**2005**
USA (millions):			
Web/Internet Appliances-in-use	3.2	23.6	115.4
Web Share of Internet Users	2.3%	14.2%	55.4%
PCs-in-use	153.2	178.9	221.9
Internet Users	135.7	165.7	208.3
Worldwide (millions):			
Web/Internet Appliances-in-use	21.5	139.8	596
Web Share of Internet Users	5.7%	25.7%	71.0%
PCs-in-use	521	695	1008
Internet Users	375	544	840

Hendrick, V. (2000). TechOnLine. Retrieved January 8, 2004 from http://www.techonline.com/community/ed_resource/ feature_article/7285.

Our own arrogance in believing our society somehow possesses exclusive rights to Internet rules of use, was dumbfounded to discover the extent to which terrorists utilized electronic mail messaging to fulfill the tragic outcome of September 11, 2001.

As profound an event as September 11, 2001 was, individuals are still more likely today than ever to become a direct victim of technology. A clear example of this is noted in newspapers across the country every week. My initial Internet crimes against children investigation occurred in 1994, when I posed as a child victim in an online chat room. It seemed at the time that so many potential offenders approached me for illicit purposes that it was sometimes difficult to keep track of who was who. It was imperative to investigate a few and let the rest go, fully realizing the possibility that those individuals let go might ultimately contact and victimize a real child. The numbers of offenders has not diminished but have, in fact, continued to increase as the criminal element educates itself with technology. Further adding to the problem is the realization that offenders often possess a better understanding of the technology’s capabilities and limitations while typically being better equipped then law enforcement.

In 1994, legislation lagged behind the proliferation of technology, posing serious problems for both the investigator and the prosecution. Fortunately, many laws have been enacted that address the cyber-environment directly, assisting the prosecutorial efforts. “Electronic evidence is one of the fastest developing legal frontiers. The Federal Rule of Evidence provides enough latitude to allow admissibility of electronic evidence in nearly every form for every possible document. A sound document retention policy, consistently applied, can be a party's best defense to an assertion of spoliation. Given the immense number of examples of what electronic evidence could constitute, it more often falls within several general categories: data, electronic mail, offline storage, voice mail, applications, hardware, networks and peripherals” (Kridel, 2001).

Additionally, significant advances have been made in forensic recovery software and the training demanded of computer forensic examiners. “Law enforcement agencies are scrambling to hire and train officers skilled in computer forensics, the discipline of collecting electronic evidence” (Tobias, 2001).

What has not changed dramatically is the need for standardization in the investigative stages of Internet-related crimes, and this remains a weak link in the effort to prosecute offenders. An important investigative element is the topic of this article: A Triad of Collaboration.

A Triad of Collaboration

Most criminal and civil cases involving electronic data are won or lost in the initial investigative stages. An absence of attention to detail during the actual investigation significantly diminishes the prosecutorial effort. As a certified computer forensic examiner I dreaded most the frustrating explanations as the investigator looked to forensics to somehow materialize evidence that was not present. I cannot count the times an investigator looked to the forensic examiner to collaborate expectant testimony in the absence of electronic data. The forensic process can be the investigator’s best friend or their worst enemy in that the computer forensic report identifies both the strengths and weaknesses of the investigation. The strengths are obviously highlights for the prosecution, but the weaknesses become the soapbox for the defense.

Law enforcement investigators must come to terms with a reality that is unique to Internet-related crimes. “In the digital world, all information entered by any individual or organization leaves a digital data trail that records all communications and actions” (Yam, 2001). The receipt, transmission, and exchange of electronic data, be it in the form of emails, attachments, or text messaging is critical to the prosecution’s effort to successfully act against criminal activity.

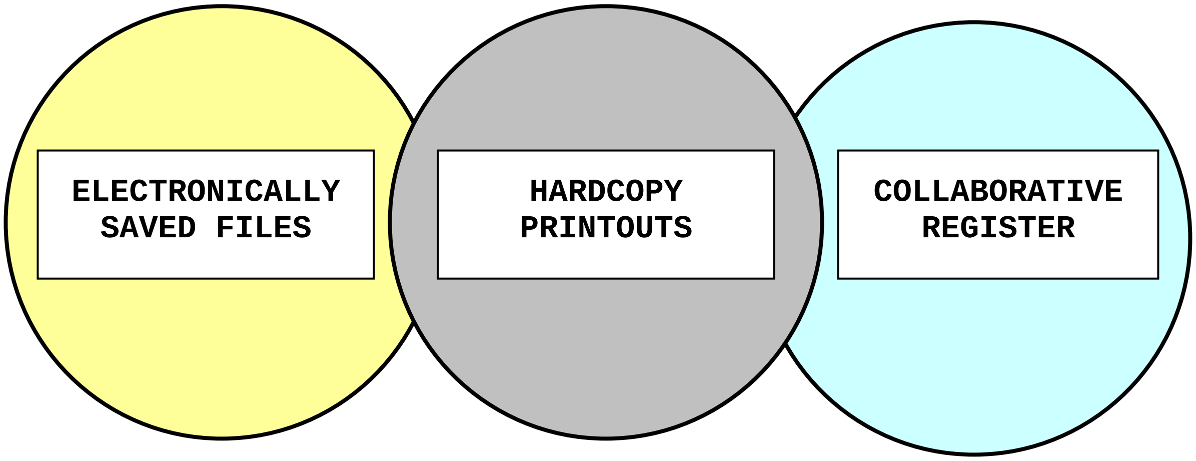
Traditional law enforcement techniques, where evidence is a process of gathering with specific attention to ensuring that nothing is added, deleted, or altered from the evidence in its original format, are inappropriate in the cyber environment. Unquestionably, it is incumbent upon the investigator to generate sufficient evidence to facilitate this endeavor. The dilemma arises when one directs law enforcement to generate evidence. But is that not exactly what is done through the exchange of electronic data?

Let me be more specific in my definition of generate evidence. The generation of evidence compels the officer to conduct a thorough investigation, one that is compelling to a jury. A single online conversation or email message is, by definition, probably sufficient to develop probable cause. Consider the implications of several, or many, or a multitude of conversations or emails that portray a predisposition or portray an unquestionable intent. I am not suggesting that investigations must be never-ending, but too many potentially strong investigations are cut short before sufficient evidence to prosecute is gathered. The generation of evidence includes any and all electronic exchanges that occur between the law enforcement officer and the offender(s). This generation of evidence is the substance of the Triad of Collaboration.

In an investigation where there is a receipt, transmission, or exchange of electronic data, it is imperative to the prosecutorial effort that three aspects of each and every electronic contact be completed. The Triad of Collaboration, used consistently, provides a cross-reference of documentation that details explicitly each electronic exchange between the investigator and the offender (see Figure 2).

The first element in the triad requires that the investigator electronically save “any and all” electronic transmissions that transpire in the course of the investigation. The term any and all refers to just that - *any and all* electronic transmissions, including extraneous information that the investigator may deem unimportant at the time but may become

Figure 2. The Triad of Collaboration



the focus of the defense to question lapses in dates, times, or what appears to be unexplainable lapses in otherwise understandable conversations. Once the investigator is on the stand it is too late to recall minor details and juries are often unsympathetic to careless investigative practices, perceived or actual.

Use consistency in deciding on a file naming convention that will be clear to you, the prosecution, the defense and a jury. This is important if the investigation consists of many transmissions that occur over days, weeks, or even months. It is highly recommended that all saved data be stored to a separate media, i.e. 3.5” diskette or CD-R. Saving the evidence to a law enforcement hard drive might open the content of that hard drive to discovery, potentially creating problems with other active investigations.

The second element in the triad is to print a copy of all data stored as a result of the ongoing investigation. This hard copy should be printed immediately after saving the data to the selected media. The file name and date/time should be included in the printout (the importance of this element will become apparent later).

The final element of the triad is simply a register. This register will identify criteria specific to the type of investigation being conducted. The register will include for each exchange the date and time, all references to saved evidence files (specifically noting the name of the file that was saved) and the investigator involved. Other important criteria should be added as deemed appropriate, i.e. one might include the criteria for file attachments or telephone contacts. It is important that the register be sufficiently detailed so as to provide a collaborative cross-reference between each of the elements.

The Triad of Collaboration provides a comprehensive, cross-referenced record of each and every electronic receipt, transmission or exchange relevant to the investigation. The electronically stored evidence file bears a file name and date and time stamp. This same information appears in the hardcopy printout and is further collaborated by the register maintained by the investigator. All three elements of the triad are now complete. A single piece of evidence is important; a second associative reference is significant; and third occurrence is compelling.

Conclusion

The use of the Triad of Collaboration in all Internet-related criminal investigations provides a cross-referenced, detailed record of any and all activity where there is a receipt, transmission, or exchange of electronic data between law enforcement and a potential offender(s). In that the federal agencies can only provide limited support, local law enforcement response must ensure thoroughness and consistency in the implementation of the investigative process.

Accepting the realization that the computer forensic process will distinguish undeniable strengths and weaknesses in the investigation, the Triad of Collaboration is one tested means to facilitate the prosecutorial effort to bring to justice those individuals predisposed to commit crimes through the use of technology.

References

Hendrick, V. (2000). TechOnLine. Retrieved January 8, 2004 from http://www.techonline.com/community/ed_resource/feature_article/7285.

Kridel, M. S. (2001). Bytes that bite: The discovery of electronic evidence. Infotech Update, May/June, Issue 3, pp. 1-4.

Read, G. C. (2001). Ticking time bomb. Defense Counsel Journal. V68(1), pp. 5-6.

Tobias, Z. (2001). Deadly pursuit. Computerworld, v35(28), p 44.

Yam, J. T. (2001). Lawyer.com: E-records: The digital data trail. Business World. August 9, 2001; p 1.

Professional Vitae

Dr. Robert DeYoung is the Master's in Management Program Coordinator and an Assistant Professor in the Department of Management at St. Thomas University, teaching across a spectrum of graduate-level managerial and research curriculum. He completed his Master's degree (MSM) at St. Thomas University, with a specialization in Human Resource Management and continued his studies, receiving a PhD in Educational Leadership from Lynn University in Boca Raton, Florida. Dr. DeYoung completed his doctoral dissertation, a naturalistic inquiry into the differences in coping strategies among parents of murdered, abducted, or long-term missing children.

Dr. DeYoung is retired from the Broward County Sheriff's Office in Fort Lauderdale, Florida. He was responsible for originating the Law Enforcement Against Child Harm (LEACH) Task Force, a federally funded, nationally recognized task force that combats Internet crimes against children. Recognized as an expert in the field of Internet crimes against children, Dr. DeYoung holds Advanced Computer Forensic Examination certifications and Advanced Computer Crimes Investigator's certification. He has instructed nationally on numerous topics related to law enforcement and management.

Dr. DeYoung is a member of the Decision Science Institute, the Southern Management Association, and the Southern Criminal Justice Association. Dr. DeYoung owns Forensic Recovery, a South Florida-based corporation providing expert computer forensic processes to the legal and corporate communities.

Dr. DeYoung owns Forensic Recovery, LLC, a corporation offering the legal and corporate communities computer forensic processes, including the collection, preservation, analysis, and presentation of electronic evidence in criminal investigations and civil litigations. The Courts recognize Dr. DeYoung as an expert in the field of computer forensic processes.