Collecting Legally Defensible Online Evidence:

December 2007

Creating a standard framework for Internet Forensic Investigations

Todd G. Shipley, CFE, CFCE
CEO and President
Detective Sergeant (Retired)
Reno, Nevada Police Department
# Table of Contents

BACKGROUND ........................................................................................................................................4

WHO CONDUCTS INVESTIGATIONS ON THE INTERNET? .........................................................4

CURRENT INVESTIGATIVE METHODOLOGIES ........................................................................6

LEGAL BACKGROUND FOR CONDUCTING INVESTIGATIONS ON THE INTERNET ............9

LAW ENFORCEMENT INTERNET INVESTIGATIVE COSTS ......................................................12

CONCLUSION ..................................................................................................................................19

APPENDIX A - PERTINENT U. S. CASE LAW REGARDING INTERNET INVESTIGATIONS ....21

REFERENCES ......................................................................................................................................24
BACKGROUND
Collecting evidence from computers, networks, cellular telephones and assorted digital storage devices has rapidly become a standard practice in law enforcement investigations commonly referred to as digital forensics. The collection of digital evidence from the Internet or Internet forensics is a discipline of digital forensics that deals with the securing of data as evidence from the Internet. Investigating alleged criminal activity committed on the Internet has been conducted almost since the Internets’ inception. The investigation and collection of online evidence has been an ongoing challenge for those tasked with that collection. The factors that contribute to the challenge include:

- the rapid changes in technology and the ability of investigators to keep up with that technology,
- the investigators lack of education on the Internet and the techniques required to investigate it,
- the inability to properly collect Internet based evidence,
- the lack of tools specifically designed for this purpose,
- and, the inability to present the evidence collected in an understandable manner to those not familiar with the specifics behind the Internet.

Internet forensics is a unique discipline within digital forensics. The uniqueness comes from the geographic location of the crime scene. Internet investigators access data on computers without knowing the physical location of that data. This makes Internet forensics singularly unique amongst the forensic disciplines.

WHO CONDUCTS INVESTIGATIONS ON THE INTERNET?
Conducting investigations on the Internet has generally been thought of as the sole domain of law enforcement. Certainly there are enough crimes to investigate from child exploitation to auction fraud. Law enforcement has taken an aggressive role in the lead to stop child exploitation online as evidenced by continued funding from the Department of Justices’ Office of Juvenile Justice and Delinquency Prevention (OJJDP) of the Internet Crimes Against Children’s (ICAC) Task Forces nationwide. Millions of dollars from the federal budget has been dedicated to these task forces and additional millions have been specifically dedicated to the National Center for Missing and Exploited Children (NCMEC) and its important programs.¹

¹ www.icactraining.org and www.ncmec.org
Many additional law enforcement investigators, from local agencies to the highest levels of the federal government, are investigating a variety of crimes committed on the Internet, from prostitution to network hacking. Still, law enforcement investigators are not the only ones conducting investigations online. Many other fields require the collection of evidence either for a judicial function or merely need to verify their actions to a superior.

The legal system in the United States and elsewhere in the world has certain requirements for the introduction of information as evidence in any civil or criminal proceeding. According to Wikipedia “Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial”. With more and more information stored on the Internet, and accessible to the average user, more and more information of “probative” value will be located there. That being said, information from the Internet will be used by attorneys needing to conduct due diligence investigations for their clients. Anyone conducting any type of research for a civil proceeding of any kind uses the Internet. Research conducted by licensed private investigators for a client is commonly accomplished through the use of tools found on the Internet. Companies conducting investigations into Intellectual Property (IP) theft commonly use the Internet to track the misuse of their companies IP. Additionally, those conducting competitive intelligence find much of what they need through the use of the Internet. These are only a few examples of the kind of occupations who use the Internet to conduct their investigations, quite a few of them being non-law enforcement or crime oriented investigations. In fact, the larger use of the Internet as an investigative tool is probably done by many personnel other than those in law enforcement.

The online investigative situation is no different around the world. According to Abhaya Induruwa, Department of Computing, Canterbury Christ Church University, UK, in a presentation during the Second International Workshop on Digital Forensics and Incident Analysis, Samos, Greece, 27 – 28 August 2007, “of around 140,000 police officers in the UK, barely 1,000 have been trained to handle digital evidence at the

---

basic level and fewer than 250 of them are currently with Computer Crime Units or have higher level forensic skills.” With that being said, in the UK according to the Association of Chief Police Officers (ACPO) Good Practice Guide for Computer-Based Electronic Evidence, “As a result, many bodies actively engage in proactive attempts to monitor the Internet and to detect illegal activities.”

CURRENT INVESTIGATIVE METHODOLOGIES

Current law enforcement investigative methodologies for the Internet are varied and many. Some agencies have dedicated the necessary resources to conduct investigations and still many others have ignored the Internet and the crime conducted there, either out of ignorance or negligence. No standard process currently exists to guide an investigator, at any level within the government (local, state or federal), military or those investigating the Internet for a corporation. This has caused a lack of understanding among those assigned these tasks, and has caused the development of a variety of practices within this community. To add to the lack of consistent practices, the lack of specialized tools in this area has driven the adoption of tools specifically designed for other purposes. These tools have sometimes provided the investigator with insufficient support for Best Evidence practices. However, investigators ever adapting to their changing world, proceeded ahead and have put many criminals in prison based on their ability to collect evidence from the Internet with tools not designed for evidence collection.

The most significant adoption of standardized investigative methods for Internet evidence collection is with the Internet Crimes Against Children (ICAC) Task Forces (TF’s). Since their inception in the late 1990’s, The ICAC TF’s have grown from a few task forces to over 46 across the United States. The managing working group of the task forces has standardized the methods they use for investigating child exploitation on the Internet. These standards guide the task force members and dictate appropriate actions during on line child predator investigations.

The law enforcement guide “Electronic Crime Scene Investigation, A Guide for First Responders” is the first in a series of guides funded by the National Institute of Justice (NIJ), U.S. Department of Justice
Many federal agencies invest personnel resources in the investigation of crime committed on the Internet. For example the Federal Trade Commission (FTC) investigates identity theft, the Federal Bureau of Investigation investigates terrorism, the Secret Service investigates credit card fraud and the Immigration and Customs Enforcement investigates counterfeit pharmaceutical sales over the Internet. Amongst all of these agencies, no common standard methodology exists for these online investigations.

The National Institute of Justice (NIJ), a division of the Office of Justice Programs (OJP), Department of Justice, through the Office of Law Enforcement Standards (OLES) at NIST (the National Institute of Standards and Technology) started producing guides for law enforcement regarding the investigation of technology. The first in the series “Electronic Crime Scene Investigation, A Guide for First responders” was an initial guide that exposed many in law enforcement to basic techniques for dealing with computers at crime scenes. The project began in May 1998, and the technical working group met, reviewed, and compiled material until the guide was published in 2001. Subsequent texts in the series include “Investigations Involving the Internet and Computer Networks”, “Digital Evidence in the Courtroom: A Guide for Law Enforcement Prosecutors” and “Forensic Examination of Digital Evidence: A Guide for Law Enforcement”.

In the United Kingdom the Association of Chief Police Officers has looked at digital evidence from the computer forensic perspective and outlined in their pamphlet entitled “Good Practice Guide for Computer-Based Electronic Evidence”, four basic principles for the handling of digital evidence:

Principle 1: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

Principle 2: In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Principle 3: An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Principle 4: The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

The APCO guide discusses the collection of online evidence in its section entitled “Crime scenes on the Internet”. However, unlike the previous clear guidance on how to handle digital evidence from computers, APCO gives less than clear direction on the actual collection of evidence from the Internet. They recognize that the Internet is essentially a large computer network and that data of interest resides on computers but that some volatile data may require capturing live website content. The use of undercover investigation techniques is governed by the National Standards in Covert Investigations, which are detailed in the “Manual of Standards for the Deployment of Covert Internet Investigators.” The general advice in the guide for an investigator wishing to collect evidence from the Internet is to consult their force’s Computer Crime Unit.

The current methods of collecting digital evidence are based on law enforcements early experiences in collecting evidence from hard drives. Over the past decade, a standard in that process has been developed and refined. Early in the digital evidence process development, the NIJ Technical Working Group on Digital Evidence (TWGDE) that produced the document “Electronic Crime Scene Investigation, A Guide for First responders” outlined a four stage process for dealing with digital evidence. Those four stages are collection, examination, analysis and reporting of the digital evidence.

![FIGURE 1 DIGITAL FORENSIC FOUR STAGE PROCESS](image)

This process was later enhanced with the Abstract Digital Forensics Model⁴ which increased the stages to nine (see figure 2):

---

⁴ http://www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf
Several attempts have been made to further define this process, but few have gained the acceptance that the listed processes have in the digital forensic community. The commonality of all of the digital forensic processes harkens back to the NIJ’s TWGDE’s four stages, the collection, examination, analysis and reporting of the digital evidence. Current online investigations should follow these four basic stages in a similar manner.

LEGAL BACKGROUND FOR CONDUCTING INVESTIGATIONS ON THE INTERNET

Since the Internet went public in 1994, law enforcement officers have investigated and collected evidence of crimes online. The collection of digital evidence has morphed from an uncommon concept to a topic of daily discussion. Digital evidence is as common today as any other “standard” evidence. Digital evidence exists anywhere that there is electronic devices, from cellular telephones to the global positioning systems in many of the newer automobiles. Computers have become the standard electronic device where most digital evidence is commonly collected. A large industry has arisen to support the emerging science of computer forensics⁵. The area of digital discovery of electronic evidence alone has grown immensely as businesses rely on computers to store company data and rely on email as an everyday means of communication.

The legal system in the United States has been looking at the changing landscape of legal cases by the inclusion of digital evidence as a normal part of civil and criminal cases. The U.S. Federal Court system instituted changes in the Federal Rules of Civil Procedures (FRCP) during December, 2006, to clarify

---

⁵ Computer Forensics “… is the art and science of applying computer science to aid the legal process. Although plenty of science is attributable to computer forensics, most successful investigators possess a nose for investigations and a skill for solving puzzles, which is where the art comes in”. - Chris L.T. Brown, Computer Evidence Collection and Preservation, 2006
“electronically stored information” and its place in the courts as evidence. A large body of case law is building around digital evidence and its introduction in both criminal and civil cases in the United States. Recently the most significant case in the area of digital evidence has been the Lorraine v. Markel American Insurance Co. In this case, the magistrate denied the admission of electronic stored information (ESI), but outlined how the evidence should have been properly admitted. The decision outlines more than any other existing case, clear guidance for the admission of electronic evidence in a Federal civil case. What this does for law enforcement and those collecting data as evidence from the Internet is to layout a partial roadmap for development of a standard methodology for Internet forensics and its successful admission in court. In the decision, Judge Grimm acknowledges “The process is complicated by the fact that ESI comes in multiple evidentiary “flavors,” including e-mail, website ESI, internet postings, digital photographs, and computer-generated documents and data files.” Of particular note is Judge Grimms discussion of ESI authentication including the use of Hashing (digital fingerprints), ESI meta-data, as well as the collection of the data in its “native format”.

The United States Department of Justice (DOJ) early in this field developed guidelines for dealing with digital evidence. The DOJ Computer Crime and Intellectual Property Section produced the reference guide “Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.” This has been the basis for law enforcement across the U.S. when dealing with digital evidence. In addition, Guidance Software has maintained a running text of the applicable case law as a reference tool for everyone in this digital evidence field entitled the “Encase® Legal Journal”.

A review of the current applicable case law reveals a complicated field that has developed around certain concepts of evidence collection and preservation. Basic premises of digital evidence collection include the collection of the data in a manner consistent with the law, verification of the data collected and maintenance of a proper chain of custody of evidence collected. Digital evidence, although electronic bit and bytes on some storage media, is extremely important to the average law enforcement investigation.

---

9 www.guidancesoftware.com
Specialized tools for its collection and examination have become the standard in the field of digital evidence.

Guidance Software’s “Encase®”, a digital evidence examination and collection software program, is an example of an evidence collection tool accepted by courts (as exampled in recent prosecutions in Ohio State v. Anderson and Texas State v. Willard 10). Additional tools in this field are regularly used to automate and simplify the evidence collection process. These tools include AccessData’s Forensic ToolKit (FTK) and Technology Pathways’ ProDiscover that are also used by many in the digital evidence collection process. In the Ohio case State v. Anderson, the conviction of the defendant was upheld using Encase® and the Texas case State v. Willard, the court specifically validated the reliability of Encase® as used in the case.

Each of these tools collect a variety of digital evidence based generally around data at rest on hard drives or removable media. Data at rest is generally referred to as data that is saved to a computer storage device and not moving through a network or residing in a computer’s memory. While Encase and ProDiscover are both capable of collecting data across networks including volatile data contained in their memory, none of these tools focus themselves on the collection of data specifically from the Internet. This is due to the current theory that in order to use these digital evidence collection tools, access and control of the suspect system to some degree is required.

The collection of information on the Internet outside of the control of the user (observer of the data) is unaddressed by these tools. A variety of commercial and freeware tools have done the historical collection of Internet based data. The tools used by law enforcement and others conducting investigations online vary from off the shelf (OTS) software designed for other purposes to tools designed by an agency for its individual investigators use. Numerous tools have been adopted to collect evidence from various parts of the Internet. Many freeware (no cost to the user) and shareware programs have been used to capture

10 http://www.guidancesoftware.com/support/legalresources.aspx
11 http://www.accessdata.com
12 http://www.techpathways.com
webpage’s as well as commercial products. Adobe\textsuperscript{13} and Techsmith\textsuperscript{14} provide tools that have been moderately successful for law enforcement and others to capture images, video and webpage’s. These tools save their captures in a normal electronic file used for general use such as a PDF\textsuperscript{15}, jpg\textsuperscript{16} or mpg\textsuperscript{17}.

For the purpose of collecting evidence from the Internet, law enforcement has adopted these tools for these purposes, none of which were originally intended for the collection, preservation and presentation of the data in court. As a result, their use has caused court challenges. The concept and process of evidence collection from the Internet, most especially in the area of child exploitation investigations, has been validated in a number of legal cases where convictions have occurred, (References to pertinent case law is presented in Appendix A).

**LAW ENFORCEMENT INTERNET INVESTIGATIVE COSTS**

Choosing to conduct investigations or collect information for evidentiary purposes from the Internet requires an investment. That investment includes hardware costs, software costs, personnel costs, training costs, and physical location costs. Each of these requires a commitment of resources to the task that often is more than an agency will want to allocate.

![Diagram](image)

**FIGURE 3 COSTS ASSOCIATED WITH CONDUCTING INVESTIGATIONS ON THE INTERNET**

\textsuperscript{13} www.adobe.com
\textsuperscript{14} www.techsmith.com
\textsuperscript{15} .PDF is a document file format designed by Adobe
\textsuperscript{16} .jpg is an image format standard
\textsuperscript{17} .mpg is a movie format standard
• Personnel Costs: These are the actual costs associated with assigning personnel to conduct investigations online. These costs include the hourly wage of the employee and any benefits associated with that salary.

• Hardware Costs: These are the actual costs associated with providing the assigned personnel with the computers and equipment required to investigate crimes on the Internet.

• Software Costs: These are the actual costs associated with providing the assigned personnel with the software needed to conduct investigations on the Internet.

• Training Costs: These are the actual costs associated with providing the assigned personnel training needed to conduct investigations on the Internet.

The costs of a project drive government’s response to most any issue. The response to Cybercrime is no different. What has occurred nationally in the Cybercrime arena is varied among law enforcement agencies at the local, state and federal levels. The Federal government has responded to portions of the Cybercrime problem with large amounts of funding. The State and local response has been more sporadic. The cost of conducting investigations on the Internet is actually relatively small when compared to the financial impact to the community. Many agencies that accept the need for conducting Internet investigations have absorbed the cost into their normal investigations budgets as a cost of doing business. However, many law enforcement administrators still lack the overall understanding of the need for a response to Internet based crime.

This has caused a general tendency to ignore the communities victims, despite the public acknowledgement of the amount of crime being conducted. This is evident by the International Association of Chiefs of Police “Identifying Critical Technology Needs Technology Survey Results”\(^\text{18}\) study conducted in 2005. The survey’s respondents identified five technology priorities: communications, patrol cars, management, forensics, and video cameras. None of the reported priority needs by the respondents reflected the actuality of their need to respond to Cybercrime. A search on the IACP website offers little direction for law enforcement managers and/or advice on how to deal with Cybercrime investigations other

than from an IT perspective. All too often there would appear to be a consensus in law enforcement that Cybercrime investigations are someone else’s problem or jurisdiction.

Whole industries and professions have sprung up in response to the Cybercrime dilemma to address its daily impact on everyone including those who do not use the Internet. Everyday companies, from the banking industry to the newly formed “Identity Theft Protection” industry use the Cybercrime threat in their marketing campaigns. Millions of dollars in the U.S., let alone the rest of the world, are being spent by Americans to protect themselves from Cybercrime which, according to an FBI survey, cost Americans approximately 67 billion dollars in 2005. The fact is that more funds are being spent by the average citizen to protect themselves from online crime than governments are spending in total to protect its own residents from these crimes. Government’s response, although in the millions of dollars, has been ineffective when dealing with the overall problem of Cybercrime. It isn’t just a matter of the need to have more money being thrown at the Cybercrime problem. The need is a realization within government and law enforcement that:

- The Internet permits criminals easy access to every locked home and business online,
- Cybercrime is here to stay,
- Cybercrime is an activity that affects citizens on a daily basis more than any other crime category, and
- Everyday law enforcement needs to incorporate the Internet into their investigations, either as its focus or as a tool.

**Changing the Current Internet Investigation Paradigm**

Clearly, the need exists to investigate crimes on the Internet and equally the need to collect evidence in support of those crimes. The question becomes how is that best achieved and under what protocol. The guidance for the proper collection of evidence from the Internet is not as well defined as that for the general computer forensic field. Computer forensics has been establishing the digital evidence collection process related to computers in general since the early 1990’s. Clear guidance and established practices have been developed and are followed routinely throughout the world when dealing with digital evidence as it applies to computer forensics. Not so clear are the procedures for the online collection of evidence
from the Internet. The complication for this comes from the real time interaction that the Internet gives the users. Data is transmitted over the Internet through various methods. Some of these methods intentionally use volatile data space as the transfer method, such as Instant Messaging and Chat applications. The use of volatile memory space for these interactions allows the data not to be recorded on any computer or server along the path of the conversation. This kind of data cannot generally be obtained through traditional computer forensic examinations. The capture of this kind of data clearly needs to be accomplished by the user initiating the connection. Law enforcement investigators have adopted several commercial tools for this purpose. All are valuable tools for each intended purpose, but still adopted and used for an unintended purpose, the collection of Internet based evidence.

The collection of evidence from the Internet needs fundamental structure to properly document the veracity and defensibility of the data collected. Bruce Nikkel in *Domain Name Forensics: A Systematic Approach to Investigating an Internet Presence*, describes the forensic advantages of collecting evidence using command line tools. The advantages he describes are:

- Each file containing evidence has a system generated time-stamp showing the exact time of evidence collection.
- Collected evidence is transferred from the collection tools directly to the files without human intervention.
- The Whois and DNS server names are explicitly defined and logged, showing that the evidence was collected from authoritative sources.
- A complete transcript log of the evidence collection procedure is available for scrutiny.

Nikkel’s “forensic advantages” detail the collection and verification of Internet based evidence. The collection process uses tools to collect the evidence without human intervention. This allows for a consistent and repeatable collection of evidentiary items. He describes the use of time-stamping and logging the evidence collected to make the evidence authoritative. The use of automated collection tools and the addition of verification methods such as logging add multiple layers of verification to the data collected. “There is no single way to enforce chain of custody in digital forensics, but the use of techniques
such as time-stamping and hashing algorithms are central to all methods.” Øystein E. Thorvaldsen, Geographical Location of Internet Hosts using a Multi-Agent System

Examining Nikkel’s “forensic advantages” and the processes detailed in the NIJ guide Electronic Crime Scene Investigation, A Guide for First Responders” as well as the forensic investigative models, there are clearly three steps to the proper collection of Internet based evidence; the collection of the evidence, its preservation, and its presentation.

3. Presentation
2. Preservation
1. Collection

FIGURE 4 PROPER INTERNET EVIDENCE COLLECTION STEPS

Collection of Internet based evidence includes the actual capture of content viewed by the user. This can be a webpage or items on a webpage such as image files, music files, or documents. It can also be instant message conversations or chat conversations using a variety of applications designed for that purpose.

Preservation of the Internet based evidence includes the treatment of this digital evidence using the concepts and principles learned from computer forensics when dealing with digital evidence.

1. Don’t change the evidence if possible.

2. Collect the evidence in a verifiable manner.

3. Maintain a proper chain of custody of the evidence.
**Presentation** of the Internet based evidence means the actual viewing offline of the evidence in a manner simulating its real time collection. This could include viewing chat logs or video files of the websites visited or the real time chat sessions.

Currently, the lack of standards for the proper collection of Internet based evidence has led the average investigator to make up collection standards locally. Some organizations such as the Internet Crimes Against Children Task Forces nationwide, have, through their federal funding, developed standards for implementation by the task force members. Due to the nature of the crimes investigated those standards, are not public. The average investigator interested in the collection of evidence from the Internet has a great challenge in front of him. The current thought process would be to seek out training specifically designed for law enforcement regarding the investigation of Internet based crime. This training occurs through federally funded programs (such as SEARCH and the National White Collar Crime Center) or through a variety of colleges and universities currently offering digital investigations programs, such as Champlain College’s Center for Digital Investigation¹⁹.

---
¹⁹ [http://c3di.champlain.edu/](http://c3di.champlain.edu/)
Each program offers technical detail in the collection of evidence from the Internet. Each program has developed its own standard for the curriculum and the process of the collection of evidence from the Internet. All of the programs are valuable and go a long way to bettering law enforcements attempts at grasping the problem at hand. However, each program has some drawbacks. The federally funded programs usually last a week and offered only a few times each year in various locations, which in turn makes them almost inaccessible by the average investigator. The post secondary programs are offered for credit within an associate or bachelorette degree program. Champlain College is moving to on line program which will make the training more accessible to the average investigator. The challenge remains a standard approach to the training and evidence collection methodology. Dr. Robert DeYoung, St. Thomas University, in a paper titled *A Triad of Collaboration: Internet-Related Investigative Considerations Prior to the Computer Forensic Application* said “A single piece of evidence is important; a second associative reference is significant; and third occurrence is compelling.” The significance of this for the Internet investigator is the ability to corroborate the collection of evidence from the Internet. Multiple occurrences of associative references can substantiate a collected piece of evidence as authentic. Those associative references to a piece of Internet based evidence could include, Hash values of the evidence collected, date and time stamps of the occurrence, log files of tool actions, key logging of investigator actions, and a collection process that is repeatable and reproducible.

The collection of Internet evidence has long been a process rift with undefined process and completed using tools that collect data but not evidence. Adding a reproducible process and associative references to the methodology makes the data collected as a defensible evidentiary item.

“A single piece of evidence is important; a second associative reference is significant; and third occurrence is compelling.”

Dr. Robert DeYoung, St. Thomas University
CONCLUSION

In the United States the collection of digital evidence has become a standard in many criminal investigations. The collection of evidence from both computers and the Internet has become a regular event. Only the digital evidence collection from computers has evolved a standard process that has become generally accepted by the courts. Internet based evidence collection has emerged as a regular environment for investigators to seek out evidence of crimes. However, the use of invalidated processes for the collection of online evidence will cause challenges to the evidence.

1. Collection
   • Evidence not collected in defensible manner.

2. Preservation
   • Chain of custody dependent on investigators written notes.
   • Not an evidence file.
   • Internet data has potential for alteration.

3. Presentation
   • Invalidated Internet data turned over to prosecutor and defense.
   • Reports prepared about unvalidated evidence collection process.

Following the lessons learned from the field of computer forensics a standard can be developed for the collection of Internet based evidence. The process outlined above to collect, preserve and present Internet based evidence is a simple standard to follow.
Utilizing a defined, repeatable and verifiable process law enforcement, and any other field wishing to verify and validate information collected on the Internet, can be assured that they will have collected defensible online evidence.
APPENDIX A - PERTINENT U. S. CASE LAW REGARDING INTERNET INVESTIGATIONS

Tracing Internet Protocol Addresses


Tracing Internet Protocol addresses back to a suspect using automated tools even when the suspect is attempting hide himself, does not violate the suspects “reasonable expectation of privacy”,

U.S. v. Perez (5th Cir. April 11, 2007) 484 F.3d 735

Law enforcement obtained a search warrant based on the transmission of child pornography which was traced back to a particular IP address registered to defendant.

Validation of Undercover Communications with Defendants


That def., unbeknownst to him, was communicating with an adult posing as a minor is immaterial since factual impossibility is not a defense.


Whether the defendant was unable to complete the crime of 2423(b) because the victim was fictitious is irrelevant in addressing guilt.

U.S. v. Crow (5th Cir. 1999) 164 F.3d 229.

Motion to quash denied where individual defendant attempted to exploit [a § 2251(a) charge] was an undercover detective.

Email Authentication


E-mails introduced into evidence over defendant hearsay and improper authentication objections. Court analyzed the authentication issues under traditional evidentiary standards. (FRE 901(a) and 901(B)(4).) Contains good discussion of circumsstantial evidence of authenticity but no discussion as to the technical aspects of e-mail. As to hearsay objection, the e-mails were considered admissions of a party. (FRE 801(d)(2)(A).)


Defendant laid an inadequate foundation of authenticity to admit, in prosecution for assault with a
deadly weapon, hard copy of e-mail messages (Instant Messages) between one of his friends and the victim’s companion, as there was no direct proof connecting victim’s companion to the screen name on the e-mail messages.

**On line Evidence Admissibility**


Chat transcript of AOL instant messages admissible since it was sufficiently similar to the charged conduct.


Where the victim testified that she was an ‘actual participant’ in the IM conversation and confirmed its contents, the IM ‘transcript’ was properly authenticated.

*U.S. v. Burt* (7th Cir.,July 26, 2007) 495 F.3d 733

Logs of a Yahoo! chat were admissible when properly authenticated.


Case provides a comprehensive analysis of how to authenticate digital evidence such as digital photos, email and text messages.


Court addresses California Evidence Code section 1552 [printed representation of computer information or a computer program is presumed to be accurate]. Court noted "the true test for admissibility of a printout reflecting a computer’s internal operations is not whether the printout was made in the regular course of business, but whether the computer was operating properly at the time of the printout."

*EEOC v. E.I dupont de Nemours & Co.,* 2004 WL 2347559, 65 Fed. R. Evid. Serv. 706,

Printout from Census Bureau web site containing domain address from which image was printed and date on which it was printed was admissible in evidence.


Archived versions of web site content, stored and available at a third party web site, were admissible into evidence under Federal Rule of Evidence 901. The contents of the web site could also be considered an admission of a party opponent, and thus are not barred by the hearsay rule.

*U.S. v. Tank* (9th Cir. 2000) 200 F.3d 627.
Authentication of screen name.


Defendant laid an inadequate foundation of authenticity to admit, in prosecution for assault with a deadly weapon, hard copy of e-mail messages (Instant Messages) between one of his friends and the victim’s companion, as there was no direct proof connecting victim’s companion to the screen name on the e-mail messages.

**Admission of Duplicate Digital Evidence**

*State v. Morris*, 2005 WL 356801 (Ohio App. 9 Dist.)

During forensics analysis using EnCase a copy of the hard drive was made. Before returning the computer the expert erased all data on the original drive. At trial the copy was used as evidence. The court found that the rules of evidence permit admission of duplicates, that appellant was unable to show what type of exculpatory evidence may have been lost during the copying procedure, and that the original was not destroyed in bad faith.

**Use of Automated Tools in Digital Evidence Collection**


Upholding the use of EnCase as a forensic tool.

**Introduction of Web Sites**

*EEOC v. E.I dupont de Nemours & Co.*, 2004 WL 2347559, 65 Fed. R. Evid. Serv. 706,

Printout from Census Bureau web site containing domain address from which image was printed and date on which it was printed was admissible in evidence.


Archived versions of web site content, stored and available at a third party web site, were admissible into evidence under Federal Rule of Evidence 901. The contents of the web site could also be considered an admission of a party opponent, and thus are not barred by the hearsay rule.
REFERENCES

1) Setting up an Online Investigative Computer: Hardware, Connectivity and Software Recommendations - Daniels, Keith  

2) An Examination of Digital Forensic Models, International Journal of Digital Evidence Fall 2002, Volume 1,  
   Issue 3- Reith, Mark; Carr, Clint; Gunsch, Gregg

3) Good Practice Guide for Computer-Based Electronic Evidence, Association of Chief Police Officers’ (ACPO)

4) CIOIM Supplement: Digital Officer Safety, 2000, Parmar, S.K., Cst, N. Cowichan Duncan RCMP Det.,  
   Duncan, BC

5) Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, July  
   2002, Computer Crime and Intellectual Property Section Criminal Division United States Department of Justice

6) LAW ENFORCEMENT TOOLS AND TECHNOLOGIES FOR INVESTIGATING CYBER ATTACKS, A NATIONAL  
   NEEDS ASSESSMENT, June 2002, Vatis, Michael A., Institute for Security Technology studies at  
   Dartmouth College

7) LAW ENFORCEMENT TOOLS AND TECHNOLOGIES FOR INVESTIGATING CYBER ATTACKS GAP ANALYSIS  
   REPORT, February 2004, Institute for Security Technology studies at Dartmouth College

8) INTERNET CHILD SEX PREDATORS: BUILDING A CASE FOR CONVICTION, August 2004, Sarah Elizabeth  
   Smith, Liberty Business Review Volume II Number 2, Liberty University

9) Domain Name Forensics: A Systematic Approach to Investigating an Internet Presence, August 2005,  
   Bruce J. Nikkel, The International Journal of Digital Forensics and Incident Response, Vol. 1, No. 4

10) Geographical Location of Internet Hosts using a Multi-Agent System, November 2006, Øystein E.  
    Thorvaldsen, Department of Computer and Information Science Norwegian University of Science and Technology

11) Investigation of Cybercrime and Technology-related Crime, March 2002, Dan Koenig, National  
    Executive Institute, www.neiassociates.org/cybercrime.htm

12) E-Evidence & Internet crimes Against Children California case Digest and Commentary, December  
    2007, Robert Morgester, Deputy Attorney General, Office of the Attorney General, State of California,  
    www.cdaa.org

13) Encase Legal Journal, April 2007, Guidance Software,  
    http://www.guidancesoftware.com/support/legalresources.aspx


16) **Identifying Critical Technology Needs Technology Survey Results**, Fall 2005, International Association of Chiefs of Police