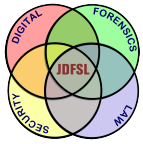

THE JOURNAL OF
DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 1 | Number 2 Article 2

2006

Computer Forensics Field Triage Process Model

Marcus K. Rogers
Computer and Information Technology, Department Purdue Universit, rogersmk@purdue.edu

James Goldman
Computer and Information Technology Department, Purdue University

Rick Mislan
Computer and Information Technology Department,Purdue University

Timothy Wedge
National White Collar Crime Center

Steve Debrota
U.S. Attorney's Office, Southern Indiana

Recommended Citation

Rogers, Marcus K.; Goldman, James; Mislan, Rick; Wedge, Timothy; and Debrota, Steve (2006) "Computer Forensics Field Triage Process Model," *Journal of Digital Forensics, Security and Law*: Vol. 1 : No. 2 , Article 2.
DOI: https://doi.org/10.15394/jdfsl.2006.1004
Available at: https://commons.erau.edu/jdfsl/vol1/iss2/2

Computer Forensics Field Triage Process Model

Marcus K. Rogers
Computer and Information Technology Department
Purdue University
rogersmk@purdue.edu

James Goldman
Computer and Information Technology Department
Purdue University

Rick Mislan
Computer and Information Technology Department
Purdue University

Timothy Wedge
National White Collar Crime Center

Steve Debrota
U.S. Attorney's Office – Southern Indiana

ABSTRACT

With the proliferation of digital based evidence, the need for the timely identification, analysis and interpretation of digital evidence is becoming more crucial. In many investigations critical information is required while at the scene or within a short period of time - measured in hours as opposed to days. The traditional cyber forensics approach of seizing a system(s)/media, transporting it to the lab, making a forensic image(s), and then searching the entire system for potential evidence, is no longer appropriate in some circumstances. In cases such as child abductions, pedophiles, missing or exploited persons, time is of the essence. In these types of cases, investigators dealing with the suspect or crime scene need investigative leads quickly; in some cases it is the difference between life and death for the victim(s). The Cyber Forensic Field Triage Process Model (CFFTPM) proposes an onsite or field approach for providing the identification, analysis and interpretation of digital evidence in a short time frame, without the requirement of having to take the system(s)/media back to the lab for an in-depth examination or acquiring a complete forensic image(s). The proposed model adheres to commonly held forensic principles, and does not negate the ability that once the initial field triage is concluded, the system(s)/storage media be transported back to a lab environment for a more thorough examination and analysis. The CFFTPM has been successfully used in various real world cases,

and its investigative importance and pragmatic approach has been amply demonstrated. Furthermore, the derived evidence from these cases has not been challenged in the court proceedings where it has been introduced. The current article describes the CFFTPM in detail, discusses the model's forensic soundness, investigative support capabilities and practical considerations.

Keywords: Computer forensics, process model, triage, computer crime, cyber crime, digital evidence

1. INTRODUCTION

Computer crime is an unfortunate artifact of today's wired and global society. It is no surprise that individuals involved in deviant and or criminal behavior have embraced technology as a method for improving or extending their criminal tradecraft. With the proliferation of technology, our notions of evidence and what constitutes potential sources of evidence are drastically changing. Gone are the days when evidence was primarily document based. Today, and going forward, evidence is becoming more electronic or digital based. This is true for all investigations, not just those we commonly associate with crimes that use or are directed toward a computer, network or IT infrastructure.

There have been several investigative models developed to assist law enforcement in dealing with the shift from document based to digital based evidence (cf. Carrier & Spafford, 2003; Beebe & Clarke, 2004; Reith, Carr, & Gunsch, 2002; Rogers, 2006; Stephenson, 2003). These various models have assumed that the entire investigative process for computer forensics would be undertaken (see Figure 1). This can be extremely time consuming given the volume of data to examine and in most cases it involves the transfer of the system(s) or a forensic copy(s) of the data located on the storage media to a lab environment for a thorough examination and analysis. While this method may work in situations where time is not overly critical, it is not sufficient in time critical situations. Examples of these time critical situations include child abductions, missing persons, death threats etc. In these situations the need for quick information and investigative leads outweighs the need for an in-depth analysis of all the potential digital evidence back in a laboratory environment.

In order to meet the demand for timely information derived from digital sources a different process model is proposed that is based on forensically sound principles and at the same time is sensitive to time constraints (i.e., critical investigative information can be derived in a short timeframe). The proposed model can be conducted on scene which provides the added benefit of having a feedback loop with the investigators; this allows the computer forensics analyst to modify their searches based on input from the primary investigators and those in direct contact with the suspect.

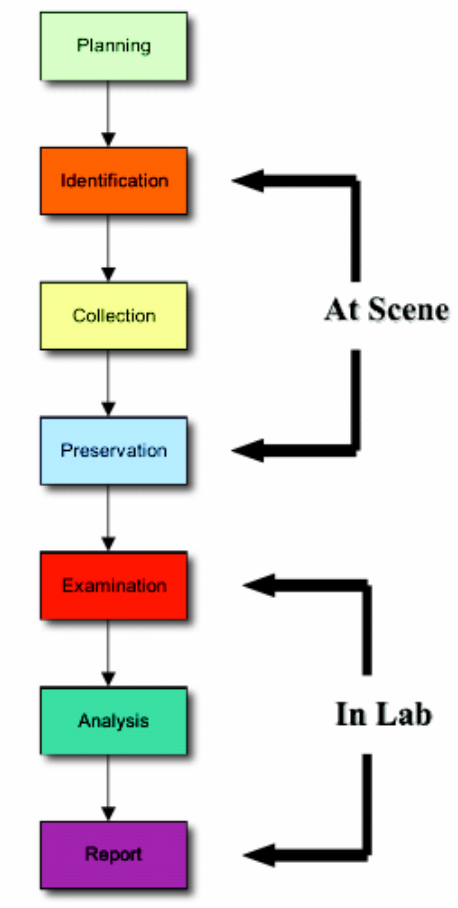

Figure 1 – Traditional Process Models

2. BACKGROUND

The development of the current process model was guided not only by the perceived need by the law enforcement community, but also from the formalization of a novel investigative approach that was being used in real investigations by agents working with the Southern Indiana Assistant U.S. Attorney's office – USADA Steve Debrota. This office had been involved in several cases where the quick and efficient examination of digital evidence was crucial to the case and the investigative leads that were generated on site (at the suspect's dwelling) were critical to the success of the operation, in securing a conviction of the offender and to protecting future victims. The USADA's office approached the Cyber Forensic Program housed in the Computer and Information Technology Department at Purdue University and the National White Collar Crime Center for assistance. The successful and pragmatic approach needed to be articulated and structured into a formal process model in

order for it to be replicated in other jurisdictions, and in order for it to be properly evaluated and matured. The approach has been formalized into the computer forensics field triage process model.

The formalization of the model was evaluated by 20 State and Local Law Enforcement Officers from Indiana who took part in a two-day seminar offered at Purdue University during the fall of 2005. The model was presented to the officers over the course of two days and the feedback was overwhelmingly positive.

3. PROCESS MODEL

The computer forensics field triage process model (CFFTPM) is defined as:

Those investigative processes that are conducted within the first few hours of an investigation, that provide information used during the suspect interview and search execution phase. Due to the need for information to be obtained in a relatively short time frame, the model usually involves an on site/field analysis of the computer system(s) in question.

The foci of the model are to:

1. Find useable evidence immediately;
2. Identify victims at acute risk;
3. Guide the ongoing investigation;
4. Identify potential charges; and
5. Accurately assess the offender's danger to society.

While at the same time protecting the integrity of the evidence and/or potential evidence for further examination and analysis.

Being able to conduct an examination and analysis on scene, in a short period of time and provide investigators with time sensitive leads and information provides a powerful psychological advantage to the investigative team. Suspects are psychologically more vulnerable within the first few hours of their initial contact with police, especially when this contact occurs in their place of business or dwelling (Yeschke, 2003). They tend to be more cooperative and open to answering questions even after being "Mirandized". This cooperation can be critical in certain cases such as abductions, sexual predatory offenses etc. What is crucial to the investigator during this initial time period is the knowledge of the full extent of the crime and/or involvement of the suspect and "triggers" that further increase the suspect's willingness to talk and cooperate. These triggers may be found in the digital evidence located on the suspect's system(s) (e.g., email correspondence, digital maps, pictures, chat logs).

The CFFTPM uses phases derived from the Carrier and Spafford (2002) Integrated Digital Investigation Process model (IDIP) and the Digital Crime

Scene Analysis (DCSA) model as developed by Rogers (2006). The phases include: planning, triage, usage/user profiles, chronology/timeline, Internet activity, and case specific evidence (see Figure 2). These six phases constitute a high level of categorization and each phase has several sub-tasks and considerations that vary according to the specifics of the case, file system and operating system under investigation, etc. The use of higher order categories allows the process model to be generalized across various types of investigations that deal with digital evidence. The need for a general model has been identified in several studies as a core component of a practical/pragmatic approach for law enforcement investigations (ISTS, 2004; Rogers & Seigfried, 2004; Stambaugh, H., Beaupre, D., Icove, D., Baker, R., Cassaday, W., & Williams, W., 2001).

Before discussing each of the model's phases it is important that qualifications be placed around the use of the CFFTPM, as the model is not appropriate for all investigative situations.

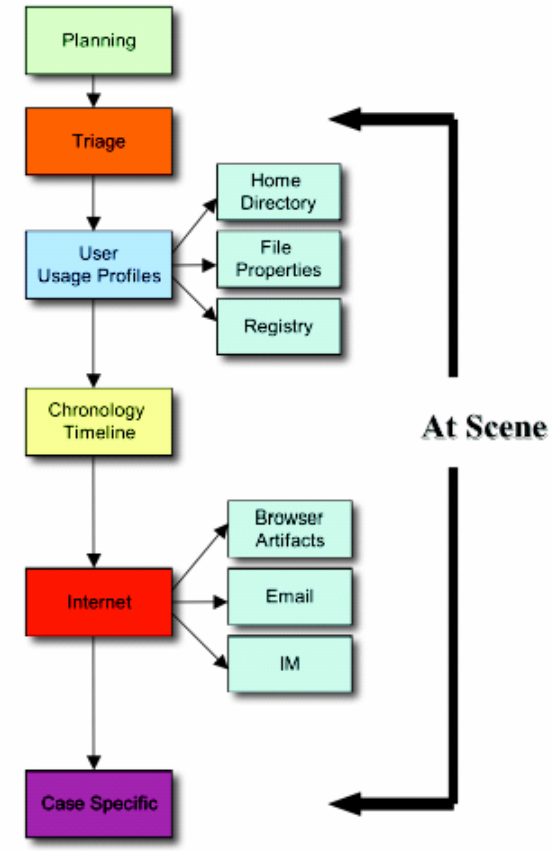

Figure 2 - CFFTPM Phases

3.1 Considerations

As with any other type of investigation there are several considerations that must be made prior to deciding the most effective and efficient method. Two primary areas of consideration are legal and technical/operational considerations. Legal considerations include the scope and particulars of the warrant or order. Does the warrant allow for the seizure and removal of the system(s)? Is there sufficient particularity in the warrant and application for the warrant that allows for an onsite or *in situ* examination? Are there any 4th Amendment issues that need to be addressed? What are the reporting obligations to the issuing magistrate or judge? Are there particular discovery issues present or anticipated? Another important consideration is whether conducting an onsite examination affects the integrity of the original evidence. It is only when these and other potential legal issues are sorted out that the feasibility of using the CFFTPM can be determined. These legal considerations obviously necessitate that investigators and legal counsel work together throughout the entire case.

Technical/operational considerations include but are by no means limited to: The type of case? How critical is the time factor? What are the skills and abilities of the computer forensic examiners? What type of technology is involved (standalone systems, complex networks etc.)? Can the scene be safely and effectively controlled? Can the systems in question be powered off or must they remain "live"? What is the technical skill and knowledge level of the suspect? Do the computer forensic examiners have the proper equipment for onsite examinations? As was stated with legal considerations, these questions need to be considered before deciding to use the CFFTPM approach.

It is also important to understand that the CFFTPM does not preclude transporting the system(s) or storage media back to a lab environment for a more thorough and exacting examination and analysis. The procedures used in the CFFTPM adhere to the forensic principles of minimizing the contamination of the original scene and evidence, maintaining the integrity of digital evidence, maintaining the chain of custody of evidence, and complying with rules of evidence for admissibility at the Federal and State levels. In many cases a two step process is appropriate and prudent, where step one is the CFFTPM conducted at the scene to provide time sensitive investigative and interview leads and then step two being a secondary more traditional examination and analysis back at the lab in order to make a more exact determination of events and evidentiary locations in a more controlled environment.

4. PHASES

Due to length constraints the discussion will only provide a brief description of the six phases and key sub-tasks. The primary investigative/examination considerations that are pertinent for each of the phases will also be presented.

4.1 Planning

The first phase in the CFFTPM is proper prior planning. Ideally, a lead investigator will have a matrix that *quantifies* the various possibilities of the crime scene, the suspect and the digital evidence and *qualifies* the expertise of the various investigators on the investigation team. For the lead investigator, this matrix is used to define what is known and what is not known thus aiding in determining what is wanted to be known. Similar to a Situation paragraph of a military Operations Order (OpOrd), this matrix identifies the "enemy" and "friendly" situations providing preemptive case intelligence. In the OpOrd, the enemy is defined characteristically by collecting intelligence through the acronym SALUTE: Strength, Activity, Location, Uniform, Time, and Equipment. This same acronym can be used in gathering case intelligence about the enemy/suspect prior to arriving at the crime scene.

Strength initially determines the suspect count and any other involved cohorts (specific numbers can be helpful), but could also include known or possible capabilities of the suspect. Activity defines the specific actions of the suspect (even small details could later be important). Location is not only the physical location of the scene, but also the virtual possibilities of cyberspace. Uniform relates more to the military, but in terms of cyberspace it can include email addresses, Uniform Resource Locators (URLs), usernames, passwords, network domains and other related deterministic markings, symbols, or corporate or agency identifiers. Time obviously builds upon other previously gathered case intelligence providing the chronological scope for investigative searches. Finally, Equipment covers the various types of wired and wireless hardware devices and software applications that can be expected when approaching the digital crime scene. Dependent upon the case intelligence determined from the SALUTE, the lead investigator will have many specific decisions to make prior to arriving at the crime scene.

Once the enemy/suspect elements of the SALUTE matrix are determined, the lead investigator can then identify friendly information for *attacking* this crime scene. From the OpOrd, this section of the matrix includes the mission of the investigation, the identification of the necessary personnel to provide the expertise for the investigation, and the knowledge of how to handle the unexpected. The mission of the investigation is normally determined by the type of crime committed in turn determining the level of investigation and the level of expertise necessary for the investigation. If the crime warrants expertise in multiple physical and virtual locations, multiple wired and wireless networks, multiple OS, personal digital technologies, or other specific technical needs, the investigator can plan accordingly. However, if there are unknowns in the investigation, it is imperative that the lead investigator determines who else can be contacted to aid in the investigation. With this compiled situational case intelligence, both about the suspect and the

investigative team, the lead investigator can then formulate a plan of attack for determining what evidence is to be sought after and used to further the investigation.

4.2. Triage

Once the appropriate planning has been completed, the investigative process moves to those phases that deal more directly with the actual suspect or crime scene (depending upon the case). For the sake of our discussion it is assumed that the scene has been properly secured and controlled. Here the scene refers to both the physical and the digital (cf. Carrier & Spafford, 2003; Lee, Palmbach, & Miller, 2001; Rogers, 2006).

Since time is a crucial factor in the CFTTPM, it is extremely important that some sort of initial prioritization be undertaken. An effective and time-tested approach is to follow the medical triage model. In the medical field triage refers to:

> "A process for sorting injured people into groups based on their need for or likely benefit from immediate medical treatment. Triage is used in hospital emergency rooms, on battlefields, and at disaster sites when limited medical resources must be allocated." (AHD, 2000)

For our purposes triage can be distilled down to:

> ***A process in which things are ranked in terms of importance or priority.*** Essentially, those items, pieces of evidence or potential containers of evidence that are the most important or the most volatile need to be dealt with first.

The triage phase is fundamental to the process model and along with proper planning it is the foundation upon which the other phases are built. The investigator needs to re-verify that the CFFTPM approach is still valid. Potential containers of evidence (e.g., computer systems, storage media and devices) need to be identified and prioritized based on the criteria of potential relevant evidence that can be obtained in a reasonably short time frame, and/or evidence with a short time to live (e.g., data in volatile memory, process tables, routing tables, temporary files systems). The investigators and interviewers who are dealing directly with the suspect or witnesses need to be providing direct input to the computer forensic examiner at this stage. This ensures that correct prioritizations and assumptions are being made.

For the remainder of the discussion it will be assumed that the computer forensic examiner has access to a forensic examination workstation or laptop that they have brought, a hardware write blocker to ensure that any storage media that is examined is done so in read only mode (thus ensuring that no contamination is occurring), and the computer forensic examiner has access to software tools that allow them to conduct field examinations (e.g., EnCase,

FTK, ProDiscover, Sleuthkit, Filehound).

4.3 Usage/User Profiles

Once a system or storage media has been identified and prioritized during the triage phase, the actual examination and analysis are conducted. When compelling evidence is found on digital media, it is essential to show a link between that evidence and a specific, identifiable suspect[1]. In some cases, this is almost a fait accompli; for example, when it can be clearly shown that only one person had physical access to a PC. In many cases, multiple persons have access to a PC, making it necessary to find and examine digital artifacts and their properties to ascertain which individual or individuals are responsible for, or even had knowledge of, incriminating data found on the storage media. Often it is necessary to place artifacts in context with verifiable real world events. The payoff can be significant. A suspect presented with clear evidence indicating that he or she, and no other person is responsible for evidence recovered during an interview may feel compelled to admit their guilt.

This challenge has always existed, and is an essential element of most "traditional" examinations of digital evidence. In the context of the computer forensics field triage process model, the challenge is not only to do this quickly, but to expeditiously determine if it can even be done within the time constraints. (In some cases, the specifics of the evidence can obviate the need for this evaluation, for example when contraband files are found only in a specific user's home directory). A thorough knowledge of user profiles and artifacts relating to usage, are essential to accomplishing this goal.

It is not always necessary or fruitful to evaluate user profiles. In determining the need and the most time efficient approach, several questions need to be asked: How many people use (have access to) the PC? How many user accounts are there? The answers to the first two are often not the same, leading to a third question, how many or which accounts are shared by more than one individual? Obviously in any case where more than one individual is able to log in to the same account, evaluating user profiles in and of itself, will not be sufficient to establish culpability for, or even a suspect's knowledge of incriminating artifacts. It may be necessary to use the dates and times associated with incriminating artifacts and put them in context with the dates and times a suspect had access to the PC, or could reliably said not to have had access to a PC. Special care must be taken when attaching significance to dates and times recovered from digital evidence. This will be discussed further in the "Timeline" section of this paper. At the other extreme, if it can be firmly established that only one individual had access to a PC, the examiner can

[1] The discussion will be constrained to standalone systems running a Microsoft Windows environment, since this represents the majority of the training and systems encountered by law enforcement investigators (Rogers & Scarborough, 2006).

dispense with evaluating user profiles, and allocate the time budgeted to more fruitful avenues of search.

Loosely put, a user profile is a collection of files, folders, registry keys, and file properties that are exclusively associated with a unique user account. The value of, and speed at which these items can be evaluated will vary widely depending on case specifics, available tools, and specific knowledge and experience of the examiner.

4.3.1 Home Directory

In Microsoft Widows operating systems, the most obvious user related artifact is the "Home Directory". By default, the home directory is only accessible only by the associated user account. Also by default, the location of stored files associated with various applications is set to a subfolder inside the home directory. The presence of incriminating files in the suspect's home directory or one of it's subfolders (Including such notables as "desktop" "my documents" and "favorites") is a reliable indicator that only the suspect (or anyone who could log onto that account) had access to those files. Additionally, the creation of a subdirectory structure with unique subfolder names can go a long way towards showing knowledge of and culpability for evidentiary objects found in the subdirectory structure (DeBrota, 2005).

4.3.2 File Properties (security)

It may be useful and time-efficient to check ownership and security properties of objects with known evidentiary value. The ability to set and read security permissions is not available in FAT, and is off by default in Windows XP (National White Collar Crime Center, 2003), even when the NTFS file system is used. When NTFS is used, and the feature turned on, a file's security properties, most notably "owner" and "permissions" may be useful in establishing which account had access to, or even created that particular file (National White Collar Crime Center, 2003). When a file is created, the user account logged on is recorded as the "owner" as part of the file's security descriptor (This can be changed only if an Administrator "takes ownership" of the file, in which case the Administrator is recorded as the owner). Permissions may also be of limited usefulness in establishing culpability. Only those accounts with the permission to do so may access an object, however this can be one or more user accounts, and the accounts that have permission to the object may change over time. An account that had "read" access on the 25th of January might not have had that same access on the 24th.

4.3.3 Registry

The registry can be a trap, causing the needless expenditure of valuable time, if the examiner does not have a precise idea of what they are looking for and exactly where to go to find it. On the other hand, a knowledgeable examiner with a clear vision of what information they want to recover can find several

highly valuable items in less than a few minutes (National White Collar Crime Center, 2005). For example, the HKEY_USERS*suspect's SID*\Software\Microsoft\Windows \CurrentVersion\Explorer\RecentDocs key and associated sub-keys contain a fairly comprehensive list of files that were opened while that account was logged on. This is a strong indicator that a suspect had knowledge of all files that were viewed, but requires that the examiner knows or can quickly and reliably identify the NTUSER.DAT file associated with the user's account.

Depending on the circumstances and resources available, examining the user profile may be the most costly part of the examination in terms of time expended, however it is often an indispensable operation as well.

4.4 Chronology/Timeline

The chronological scope of the investigation can be defined by the case intelligence. In an investigation, digital evidence is defined by its temporal value, known as MAC times (Casey, 2004). Without going into a detailed narrative of the specifics of MAC times specifically to each OS, the following are some general guidelines for Windows MAC Times. Windows MAC times are defined in the FAT32 and NTFS file systems as:

- Modification is defined by when a file contents has been changed
- Access time is defined by when a file was viewed
- Created time is defined by when a file was created

Although MAC times appear simple, it is well-documented (Casey, 2004; Farmer & Venema, 2005;Vacca, 2002) that there are many inconsistencies with MAC times and there are various other vulnerabilities when describing other vendor specific operating systems, such as those used on personal digital technologies devices (e.g., PDAs, Cellphones, MP3 players).

Once an investigator gains access to the files in question and their individual MAC times, they can start to qualify their searches, thus quantifying their evidence (Casey, 2004). For the CFFTPM, several quantifications should be examined by sorting the files on their various MAC times within the chronological scope of the investigation. The first such quantification includes the time periods of normal use by the suspect and other known users of the computer or device (Casey, 2004; Farmer & Venema, 2005). This can be obtained by correlating known users accessing the computer with files that have been modified, accessed or created during those times. Organization by user or by time period helps to quantify who was doing what during what time periods. Such organization may also provide time periods that stand out or look unique. These types of unique time periods could be studied outward in an attempt to find other significant relationships or value.

Another quantification includes the identification and analysis of software applications and data files used or accessed during qualified times of interest (Casey, 2004; Farmer & Venema, 2005; Vacca, 2002). Again, this can be obtained by correlating known users with MAC times possibly providing unique time periods that could be of significant value. Organization of applications or files within a certain time period quantify activities that occurred during these time periods. An application or file that is accessed prior to, during or after a criminal incident can be a major indication of involvement or intent.

Finally, the third quantification includes the identification and analysis of recent shortcuts and stored information (Casey, 2004; Farmer & Venema, 2005; Vacca, 2002). These could include, but are not limited to items on the desktop, commonly used software applications, and the various locations of Internet browser cookies, cache, and the index.dat file. Note that various Internet structures (cookies, cache and the index.dat file) can be very useful in determining chronological intelligence in that these provide much more time-based evidence than just MAC times. Specifically, each Index.dat file provides date-time stamps for each Internet server request.

For clarification, it should be noted that time is maintained differently in different operating systems and versions, system clocks do drift and are easily corrupted, and knowledge of time zones and time changes is essential to any digital investigation (Casey, 2001; Casey, 2004; Farmer & Venema, 2005; Vacca, 2002). Finally, in defining the case through chronology, there is a need to establish a provenance of the information and correlate events based on an absolute time determined by some piece of physical evidence (Casey, 2004; Vacca, 2002).

4.5 Internet

Almost every case will require an examination of artifacts associated with Internet activity, such as instant messaging (IM), e-mail and web browsing. The value, time cost, and time criticality will vary widely, depending on circumstances including the specific applications involved, type of activity being examined, and whether the PC being examined belongs to a suspect or a victim (e.g., in a missing persons case). An effective practice is for the computer forensic examiner to evaluate what type of Internet activities they believe the suspect (or victim) was involved in, and to evaluate if and how each of those activities relates to the case. Types of activities may include web browsing, e-mail, instant messaging, reading or posting to USENET newsgroups, trading files.

4.5.1 Browser Artifacts

While the specifics vary, most web browsing applications store some method for storing “cookies”, either as a file or as separate files, some means of storing

temporary Internet files, and some means of storing user information and preferences, such as typed Uniform Resource Locator (URLs) and "favorites". The specific content of individual cookies is determined by each individual website and is rarely of evidentiary value. In most cases, the evidentiary value of a cookie is limited to its name. Typically, the name of a cookie will match the URL of the site that deposited the cookie, indicating that the PC had visited that site at some point in the past. This does not go to show intent as the cookie will be created whether the browser was redirected from another site, or intentionally pointed to the site with a typed URL. Dates and times associated with cookies may help to determine when a site was visited and can be useful in creating investigative timelines.

Temporary Internet files are essentially cached copies of web page components (often graphics) stored on the local PC. The investigative value is that these files are stored locally without the intent or intervention of the user, and that some files, for example contraband images, are of evidentiary value in and of themselves. An investigator must keep in mind that these files are easily cleared out by most browsing applications, or with third party tools. Most importantly, investigators must weigh the potential value against the time it will take to search through even a moderately populated cache. Examiners should expect a search of temporary Internet files to take hours or days. In many cases, that requires more time than the examiner has.

A web browser's storage of user information and preferences can be a quick source of useful information. In cases where "Internet Explorer" is the browser, the index.dat file can contain a running record of sites visited, including access to web based e-mail (but not e-mail content), and even local files. The examples below (some information has been redacted) all represent data pulled from an index.dat file in less than five minutes, using a free third-party tool (see Figure 3). The "User Name" in each case, indicates the name of the windows account that "owned" the index.dat file in question.

4.5.2 E-mail Artifacts

E-mail artifacts may be of enormous evidentiary value, but can require a very expensive investment in time. Procedures for examining e-mail and extracting useful data are usually specific to the particular e-mail client, and can be time consuming to implement. If extraction of e-mail is successful, even a cursory screening of all the e-mail in a suspect's mailbox could take many hours. If web-based e-mail is used, there is often no local storage of e-mail artifacts.

==========
URL : http://www.XXXXXX.com
Title : New Page 1
Hits : 17
Modified Date : 10/4/2005 9:05:35 PM
Expiration Date : 10/30/2005 9:05:36 PM
User Name : xxxxxx
==========
This example shows a user visiting a site 17 times, most recently on 10/4/2005

==========
URL : http://images.google.com/images?q=kitties&hl=en
Title : kitties - Google Image Search
Hits : 7
Modified Date : 10/4/2005 9:09:46 PM
Expiration Date : 10/30/2005 9:02:38 PM
User Name : xxxxxx
==========
This example shows that a user performed a google image search on the term "kitties" 7 times, most recently on 10/4/2005

==========
URL : http://us.f307.mail.yahoo.com/ym/ShowFolder?rb=Inbox&reset=1&YY=85059
Title : Yahoo! Mail - xxxxxxxx@yahoo.com
Hits : 21
Modified Date : 10/4/2005 9:06:37 PM
Expiration Date : 10/30/2005 9:06:38 PM
User Name : xxxxxx
==========
This example shows a user accessing their yahoo account for the 21st time on 10/4/2005.

==========
URL : file:///D:/Program%20Files/mIRC/logs/%23Beginner.EFnet.log
Title :
Hits : 1
Modified Date : 10/4/2005 9:44:39 PM
Expiration Date : 10/30/2005 9:37:32 PM
User Name :xxxxxx
==========
This example shows the user accessing a file (in this case, an IRC chat log, but could be any type file) on the local drive for the first time on 10/4/2005.

Figure 3 - Index.dat Examples

4.5.3 Instant Messaging Artifacts

Most instant messaging clients maintain some type of contact information, and have the capability to record and store logs of the conversations that take place between the user and his or her online contacts. In most cases, this logging capability is off by default but can, and often is, turned on by the user. Contact information for most IM applications is maintained at the server, and may not be found on the local PC. Chat logs can contain a wealth of data, including the

conversation itself, as well as the screen names of other parties. A single chat log may contain hours of conversation. A thorough examination of multiple logs may bear a prohibitive cost in time. If it is necessary to examine chat logs, it is important for the examiner to have a clear idea of what he or she is looking for. String search tools should be implemented as much as possible.

A "traditional" examination would likely involve a thorough examination of all of these, and many other artifacts. The mandates of the CFFTPM require that the examiner judiciously evaluate the potential benefit of examining each of these artifacts with the time cost of doing so.

4.6 Case Specific Evidence

It is important for the computer forensic examiner to be able to adjust the focus of every examination to the specifics of that case. This is a skill set in and of itself, and requires the ability to reconcile a number of conflicting requirements in the manner most appropriate not just to a type of case, but to each specific set of circumstances. There are several practices that can facilitate an effective optimization of resources. A computer forensic examiner should be able to evaluate time resources, utilize pre-raid intelligence, customize search goals, and prioritize search goals.

Of all the resources available to the examiner, time is usually in shortest supply. One consideration when taking stock is whether the time requirement is "bounded" or "unbounded". Is there a defined deadline ("bounded") beyond which the search is halted, or the evidence loses all value? Is the mandate to find evidence as soon as possible, but even if it takes days ("unbounded")? For example, a permissive search might only be allowed until the end of an interview, whereas the search of a missing person's PC might be conducted as rapidly as possible, but still go on for hours. Time is clearly of the essence in both cases, but the lack of a time limit in the unbounded case can justify some avenues of investigation that would not be feasible in a bounded situation. In all cases, time is an expensive commodity. The time cost of any examination activity must be weighed against the potential for fruitful results of that activity. As a general rule, it is usually best to perform those tasks which can be accomplished most quickly first.

The value of planning and pre-raid intelligence cannot be over-emphasized. Reliable information on search terms, contacts, types of activities, applications used, etc. in advance of the search can allow the examiner to develop at least some search strategies before arrival on scene. Every minute saved in this manner is potentially another minute available to conduct the search itself.

It is difficult to say with certainty which specific type of digital artifact is the optimum site to search for a given type of case; however some types of artifacts are *generally* more likely to produce relevant information for specific types of cases. The example cases summarized below are not intended to be a

comprehensive list of the type of case or of all recommended approaches.

5. CHILD PORNOGRAPHY

The highest priority should obviously be given to actual instances of child pornography on the drive. A graphic viewing utility that quickly displays large quantities of thumbnails from graphic and audiovisual files can help speed up the task of searching the drive directly. It may be helpful to take a quick look at the directory structure, searching for indications of cataloged, sorted storage of contraband material. If Internet activity is involved, many web browser artifacts can be searched fairly quickly to identify contact with incriminating web sites. Instances of child pornography may potentially be found in temporary Internet files, however the time required to search through these files is likely to be prohibitive. If distribution of child pornography is suspected, it may be prudent to search for artifacts associated with IRC FServes or peer to peer file sharing applications (DeBrota, 2005). E-mail and USENET newsgroup postings may also be associated with distribution of child pornography; however this is often very time-consuming and should be considered carefully.

6. DRUG ACTIVITY

A quick search of the drive for spreadsheets, documents or databases is often a sensible use of time (unless the number of files found is prohibitive). These files may contain sales records, customer information, drug-making instructions, or lists of precursor chemicals. If time can be allotted to do so, it may be fruitful to examine Internet artifacts for Internet searches on drug-related terms, and for online transactions involving purchases of precursor chemicals or equipment. It may be possible to find drug-related e-mail or instant messaging artifacts, however this will be time consuming – especially so because it will likely require manual screening of message content.

7. FINANCIAL CRIMES

A cursory search of the drive for documents and images (specifically images of checks or other potentially fraudulent financial instruments) might be at the top of the list. Documents could include invoices or other financial records. Installed financial applications, such as quicken or MS Money and their associated records may be a fruitful source of evidence.

Within the constraints of the factors previously highlighted, the examiner must efficiently prioritize the search goals from the beginning. Some considerations will be constant. Time and speed will almost always be the most important consideration. Forensically sound practices must always be observed. System date and time, and time-zone information from the suspect's system should always be examined and documented. To the extent practical, the examiner

should prioritize search goals to focus on applications the suspect is known to have used or reasonably presumed to have used in relation to the suspected illegal activity based on available intelligence.

8. CONCLUSIONS

The computer forensic field triage process model (CFFTPM) is a formalization of real world investigative approaches that have distilled into a formal process model. At the heart of the model is the notion that some investigations are extremely time sensitive; hours can literally mean the difference between life and death for a victim or the escape of the suspect. Most law enforcement cases today involve digital evidence of some kind. We are truly a digital nation and as such our lives (the good and the bad) are reflected in technology and the bits and bytes. Correspondingly, digital evidence is a primary source of critical information and investigative leads that are required within the first few hours of many investigations.

While the investigative approaches that were used to develop the model came primarily from child pornography cases, the model is general enough to be used across a wide spectrum of investigations. The six primary phases of the CFFTPM (planning, triage, usage/user profiles, chronology/timeline, email & IM, and case specific evidence) are important in such diverse cases as financial fraud, identity theft, cyber stalking and murder. The various sub-phases or tasks under each primary phase need to be modified based on the specifics of each investigation. The tasks and considerations discussed under each of the phases act as examples of the decision making process that needs to take place – sensitivity of time vs. quality and importance of the evidence derived.

The CFFTPM is consistent with the various theoretical models that have been developed within the field of digital forensic science. By following the CFFTPM a computer forensic examiner has not precluded a more thorough traditional examination and analysis back in the lab. The procedures used on site are forensically sound, maintain the chain of custody, and comply with Federal and State rules for the admissibility of evidence.

One of the biggest advantages of the CFFTPM (very practical and pragmatic) is due to the fact the model was developed in reverse of most other models in the area. The investigators in the field matured their instinctive approaches based on actual trial and error, cases, court decisions and the direction from prosecutors. The CFFTPM merely aggregated these approaches and articulated them into a more formal methodology; still maintaining the investigative essence and the key components that have been battle tested.

Just as it has been said that "one software tool does not a computer examiner make", only possessing one investigative process model is equally as limiting. Computer forensic examiners need a repertoire of tools and just as important, a repertoire of examination and investigative approaches. The CFFTPM is not

the ultimate solution for every case; it should only be used where appropriate and only after carefully weighing the legal and technical considerations that were discussed. In those instances where it has been employed it has been extremely effective!

"Education never ends, Watson. It is a series of lessons, with the greatest for the last"
(Sherlock Holmes, The Adventure of the Red Circle)

9. REFERENCES

Beebe, N. & Clark, J. (2004). *A hierarchical, objectives-based framework for the digital investigations process.* Paper presented at the DFRWS, June 2004, Baltimore, MD.

Casey, E. (2001). Handbook of Computer Crime Investigation: Forensic Tools and Technology. San Diego: Academic Press.

Casey, E. (2004). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. San Diego: Academic Press.

Carrier, B., & Spafford, E. (2003). Getting Physical with the Digital Investigation Process. *International Journal of Digital Evidence, Volume 2* (Issue 2), 20.

DeBrota, S. (2005). *Computer Forensic Analysis Checklist.* US Attorney's Office, Southern District of Indiana checklist. Updated March 28, 2005.

Farmer, D., Venema, W. (2005) Forensic Discovery. Pearson Education, Inc, Upper Saddle River, NJ Carrier, B. (2005). File System Forensic Analysis. Addison-Wesley Professional.

Institute for Security Technology Studies. (2004*). Law enforcement tools and*

technologies for investigating cyber attacks: A national research and development agenda. Retrieved Sept 9, 2004 from http://www.ists.dartmouth.edu

Lee, H., Palmbach, T, and Miller, M. (2001). *Henry Lee's crime scene handbook*. San

Diego: Academic Press.

National White Collar Crime Center. (2005). *Registry Windows NT/2000/XP*. Unpublished training presentation from Cybercop 301 course.

National White Collar Crime Center. (2003). *Windows NT/2000/XP Security and Processing issues.* Unpublished training presentation from Cybercop 301 course.

Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic

Models. *International Journal of Digital Evidence, Volume 1*(Issue 3), 12.

Rogers, M. (2006). DCSA: Applied digital crime scene analysis. In Tipton & Krause.

(Eds.). Information Security Management Handbook. (pp. 601-614) New York: Auerbach.

Rogers, M. & Scarborough, K. (2006). *Preliminary findings: 2006 law enforcement national digital evidence survey*. American Academy of Forensic Sciences Annual Conference. Seattle, Feb 20-24.

Rogers, M., & Seigfried, K. (2004). *The future of computer forensics*: A needs analysis survey. Computers and Security(Spring 2004).

Stambaugh, H., Beaupre, D., Icove, D., Baker, R., Cassaday, W., & Williams, W. (2001). Electronic crime needs assessment for state and local law enforcement. Retrieved September 1, 2005 from http://www.ojp.usdoj.gov/nij/pubs-sum/186276.htm

Stephenson, P. (2003). Modeling of Post-Incident Root Cause Analysis. *International Journal of Digital Evidence Fall 2003, Volume 2*(Issue 2), 16.

The American Heritage Dictionary of the English Language - 4th Edition. (2000). *Triage.* Boston: Houghton Mifflin.

Vacca, J. (2002). Computer Forensics Computer Crime Scene Investigations. Revere, MA: Charles River Media.

Yeschke, C. (2003). The art of investigative interviewing - second edition. Boston: Butterworth Heineman.