3-1-2012

Research Toward a Partially-Automated, and Crime Specific Digital Triage Process Model

Gary Cantrell

David Dampier
Marshall University, dampierd@marshall.edu

Yoginder S. Dandass

Nan Niu

Chris Bogen

Recommended Citation

Cantrell, G., D. Dampier, Y. Dandass, N. Niu, and C. Bogen, "Research Toward a Partially-Automated, and Crime Specific Digital Triage Process Model," Computer and Information Science, Volume 5, 2012, pp. 29-38.

Research toward a Partially-Automated, and Crime Specific Digital Triage Process Model

Gary Cantrell
SWRCCI, Dixie State College, 225 South 700 East, St. George, Utah 84770, USA
Tel: 1-228-342-0110 E-mail: cantrell@dixie.edu

David Dampier
Computer Science and Engineering, Mississippi State University, Mississippi State, MS 39762, USA
Tel: 1-662-325-2756 E-mail: dampier@cse.msstate.edu

Yoginder S. Dandass
Computer Science and Engineering, Mississippi State University, Mississippi State, MS 39762, USA
Tel: 1-662-325-2756 E-mail: yogi@cse.msstate.edu

Nan Niu
Computer Science and Engineering, Mississippi State University, Mississippi State, MS 39762, USA
Tel: 1-662-325-2756 E-mail: niu@cse.msstate.edu

Chris Bogen
Computer Science and Engineering, Mississippi State University, Mississippi State, MS 39762, USA
Tel: 1-662-325-2756 E-mail: chris.bogen@erdc.usace.army.mil

Received: December 5, 2011 Accepted: December 22, 2011 Published: March 1, 2012
doi:10.5539/cis.v5n2p29 URL: http://dx.doi.org/10.5539/cis.v5n2p29

Abstract

The digital forensic process as traditionally laid out begins with the collection, duplication, and authentication of every piece of digital media prior to examination. These first three phases of the digital forensic process are by far the most costly. However, complete forensic duplication is standard practice among digital forensic laboratories.

The time it takes to complete these stages is quickly becoming a serious problem. Digital forensic laboratories do not have the resources and time to keep up with the growing demand for digital forensic examinations with the current methodologies. One solution to this problem is the use of pre-examination techniques commonly referred to as digital triage. Pre-examination techniques can assist the examiner with intelligence that can be used to prioritize and lead the examination process. This work discusses a proposed model for digital triage that is currently under development at Mississippi State University.

Keywords: Digital forensics, Computer forensics, Digital triage, Process model

1. Introduction

Digital forensics involves the post-event processing of a piece of digital media for artifacts of interest. An event in this case means a crime against a computer, a crime where a computer was a tool, or a crime where the computer is incidental (Kruse & Heiser, 2002). These artifacts are digital data that can serve as intelligence for a case under investigation or serve as evidence in a court of law. Since these artifacts are to be used in a court of

law, they have to be gathered using proven, forensically sound methodologies. At present these methodologies are typically standard operating procedures created independently by each office.

Digital triage is a pre-digital-forensics process. Its primary goal is to produce intelligence not court admissible evidence. This intelligence can be useful for prioritizing before the digital forensics process. Several models have now been written to better explain digital forensics and turn in-house processes into more tested and proven methodologies (Baryamureeba & Tushabe, 2004; Beebe & Clark, 2004; Bogen & Dampier, 2005; Carrier & Spafford, 2003; Carrier & Spafford, 2004; Rogers, Goldman, Mislan, Wedge, & Debrota, 2006; Ieong, 2006; Palmer, 2001). Although some of these models mention the need for a pre-examination process like digital triage, none presently include it as a detailed phase. Thus, digital triage remains mostly un-modeled as part of existing process models. There are also very few stand-alone models that have been proposed for digital triage. One exception being (Rogers, Goldman, Mislan, Wedge, & Debrota, 2006) which is discussed further on in this work. This work describes a proposed digital triage process model that is currently be developed and tested at Mississippi State University.

The contribution this research hopes to make is the reduction of the growing labor and time problem facing digital forensic laboratories today. As digital forensics becomes better known the number of digital device analysis requests will grow. This added with the problem of the increasing sizes of typical digital storage devices is a serious problem. It is not unusual for a forensic laboratory to have a 9 to 12 month backlog. One possible way to reduce this backlog is to use digital triage in case prioritization and intelligence gathering for use in the actual examination phase.

2. Digital Triage

Digital triage is not a forensic process by definition. According to Merriam-Webster's Dictionary of Law the term forensic means, “belonging to, used in, or suitable to the courts or to public discussion and debate (Merriam-Webster's Dictionary of Law, 2011).” The information resulting from digital triage is not admissible in court, but instead serves as intelligence. It can be conducted on site during search and seizure to provide feedback to the search and seizure team, it can be conducted prior to submitting the digital evidence to a laboratory to determine if the time a complete examination will take is viable, or it can be performed in the laboratory as a tool for prioritizing case loads. Consider the extreme case of a multi-terabyte drive that has already been wiped clean. There is no reason to go through the lengthy duplication phase or send it off to a laboratory for examination if there is no information there to be found. Consider also a search and seizure of 20 multi-terabyte servers from a corporation. Would it not be better to determine which machines are the most likely to hold the evidence before undertaking the lengthy task of imaging each one?

Digital evidence is very fragile, and trust in digital evidence was, and in some sense still is, very low. Thus, the first digital forensics methodologies were created with extreme preservation in mind omitting any pre-process to examine the data. Since then there have been many improvements in hardware and software tools that can be utilized to prevent changing source media during examination or previewing. Most importantly examiners now have hardware write blockers that can be applied in conjunction with examination software that guarantee no write commands go to the source media. However, as always in the world of criminal justice and law policies are slow to change. Processes will need to be created, tested, and accepted in court before examiners can regularly veer too far from the current accepted methodology of duplicating every piece of media before examining it.

Digital triage can have many uses other than assisting with digital evidence processing once widely accepted by the law enforcement community. K. Rogers *et al.* in their work (Rogers, Goldman, Mislan, Wedge, & Debrota, 2006) point out that intelligence gathered during digital triage creates a feedback loop that can be used to guide investigators during search and seizure. For example, what about a child pornography case where no immediate contraband imagery is located, but clues found during digital triage point to external storage such as optical media or external hard drives that have not yet been found? Digital triage is certainly useful in this situation to help guide the search and seizure process. The psychological effects of immediate intelligence during suspect interviews are important to consider as well. Yeschke points out that the suspect is most vulnerable those first few hours after being apprehended (Yeschke, 2003). Perhaps the easiest way to locate the missing optical media and external hard drives in our fictitious child pornography case is to ask the suspect during their first interview where they are located.

2.1 Digital Triage Modeling

There is precedence and existing tools for doing pre-examinations but few written procedures. The FBI's image scan tool, for law enforcement use only, allows an investigator or examiner to safely scan for images prior to a full examination to determine if indeed the computer in question contains contraband imagery. More recently

commercial products have started to become available as well. IDEAL Corporation produces several hardware solutions for doing digital triage (http://www.idealcorp.com/). ADF Solutions Incorporated has developed software for digital triage (http://adfsolutions.com/). Finally, AccessData, a long time player in the world of digital forensics, has introduced a new tool for digital triage (http://accessdata.com/products/computer-forensics/ad-triage), and this list is by no means comprehensive. However much like the digital forensics process itself, even with the use of these tools the process is still mostly ad hoc or based on each office's standard operating procedures.

There have now been several published works attempting to codify a digital forensics process model. However although some mention the possibility or the need, none seem to include an actual digital triage process as part of their model. All the models typically concentrate on what happens to the digital evidence after it has been duplicated and authenticated. There have also been very few attempts to create a process model just for digital triage. One exception is the The Computer Forensics Field Triage Process Model (Rogers, Goldman, Mislan, Wedge, & Debrota, 2006).

The Computer Forensics Field Process Model, although a good model, depends greatly on user expertise to be successful. It also does not include any kind of automated process making it slow. Digital triage has to be fast if it is to be useful, and requiring the user to have large amounts of expertise to use the tool limits its usefulness. The model proposed in this paper attempts to address these weaknesses.

There are other efforts that describe using techniques to prioritize and learn about evidence, but these works are not necessarily meant to be a digital triage process. For example, Simson L. Garfinkel performs cross-drive analysis using pseudo-unique identifiers like social security numbers and credit card numbers in his work, “Forensic feature extraction and cross-drive analysis (Garfinkel, 2006).” The method he describes was not intended to be a fast process, and thus not a digital triage process. The Five Minute Forensics technique created by A. Grillo *et al.* was a work that used the extraction of specific information from drive sets in an effort to prioritize them. This is closer to the model proposed herein, but the Five Minute Forensics technique requires training of the system with manually pre-classified hard drives and was more singular of purpose intended for lab use alone. Both these processes did serve as inspiration for the model under development.

3. Semi-automated Digital Triage Process Model

The model proposed here is a semi-linear framework. The middle three phases shown in grey on Figure 1 are intended to be an automated process capable of being coded as a computer program or scripted into existing tools. Planning and Readiness is an on-going phase that occurs pre-event, and Preservation is an umbrella activity that is carried throughout all phases. The remaining phases all occur in a linear fashion. The dotted line on the left represents the information flow from the Computer Profile and Crime Potential phase into the Presentation phase where it is transformed into usable information for the digital triage examiner. The three phases in grey are the primary phases of interest as they will be implemented as software. Each phase will now be described in detail.

3.1 Planning and Readiness Phase

The planning and readiness phase is an ongoing phase involving the preparation and education of staff, and the continual upgrading of equipment. Including a phase like this in a digital triage process is particularly important as it involves the continual testing of the triage tools and the effort to stay current on all hardware that the triage examiner may have to interface with.

The need to stay current with technology as described in this phase will always be an important part of any digital forensic related process to avoid the booby traps caused by new technology that might interfere with authentication or processing. For example, in a work under taken by G. Bell *et al.* it was shown that some solid state drives will start to erase unallocated space without any user interaction potentially disrupting the authentication process just by being powered on (Bell & Boddington, 2010).

This work has minimal effect on the model described here, but it clearly demonstrates the importance of a planning and readiness phase. The digital triage examiner could wipe areas of the suspect’s hard drive that a complete examination could extract data from, regardless of the write blocking technology applied, just by applying power to the suspect's drive. If the triage exam is conducted after the evidence is seized, the triage examiner could disrupt the authentication already produced. The digital triage examiner can record their actions properly and account for the loss of authentication later if aware of the danger. If completely unaware of this danger, their findings could very easily be challenged.

3.2 Live Forensics Phase

Live forensics involves the acquisition of volatile memory, and is included as a phase of this model as an optional step dependent on need and expertise. Digital evidence should be gathered in the order of volatility to prevent the loss of any data of evidentiary value (Farmer & Venema, 2005). Thus, this step has to come before anything else in any digital forensic process to preserve volatile memory, but it is presently skipped in most investigations and the volatile memory usually ignored. It is most commonly used during incident response to attempt a determination of how a machine was compromised. However, live forensics is likely to become more important and more common as users become familiar with and operating systems come standard with full disk encryption as it can be vital to circumventing such encryption (Casey & Stellatos, 2008; Hargreaves & Chivers, 2008).

The reasoning for including it as a phase in this model is that once the digital triage process begins it is highly likely that volatile memory will be lost. A digital triage tool is either going to require a system reboot into a safe environment using boot media or the running of a program from an external drive. In either case volatile memory will have been altered. It will not be a part of the automated process, and it will require the triage examiner to have live forensics expertise. The input from this phase will not be applied to the automated process.

3.3 Computer Profile Phase

Computer profile generation will be the first phase in the automated process for the digital triage process model. In the Field Triage Process model the authors attempt to learn about the users of a system by targeting the user profiles on the computer (Rogers, Goldman, Mislan, Wedge, & Debrota, 2006). The Five Minute Forensics Technique performed a similar analysis, but used the information to categorize the users into occasional user, chat-internet user, office worker user, experienced user, and hacker user (Grillo, Lentini, Me, & Ottoni, 2009). It would be more useful to profile the computer as a whole instead of segmenting the data by user profile. After all, there is no guarantee that each user accesses just their account or indeed if the computer is set up with multiple logon accounts at all. The investigator or examiner can analyze the results and apply outside information in an effort to determine who the actual computer users are.

At a minimum this phase could create a profile based on user logon names (web accounts, email addresses, social networking sites, chat programs, and any other identifiable logons), it can create a statistical chart of the percentages of all file types on the computer, and it could attempt to determine user interests based on visited websites with some user intervention. This phase will attempt to answer who uses the computer, what is the computer used for, and what are the interests of the users of the computer.

First, the logon names on the computer should be searched for in an effort to determine who uses the computer. In 2006 Simson Garfinkel performed a series of experiments dealing with cross-drive analysis in an attempt to identify drives of interest (Garfinkel, 2006). In his work he created a histogram of all the email addresses identified in computer memory with the theory that the primary user's email address will appear most often. His goal was the rapid identification of the primary owner of the disk. This could be expanded to look for evidence of other web accounts and simplified to avoid comprehensive word searches. For example, searching for the following string in the Internet history could identify Facebook accounts: “http:www.facebook.com/profile.php.”

Email coupled with other user accounts like social networking site logons can help create a computer profile of who has been using the computer. Whereas multiple users can share a computer logon it seems less likely they would share the same web mail account or social networking page. If timestamps can also be established with these user logons, an even more detailed picture can be created. Currently research is being conducted as to the feasibility of this.

One possible organization of file statistics would be the reporting of file types by percent of total files 5% image files, 10% executables, 3% documents, 2% audio files, etc. A similar organization was proposed in the already mentioned Five Minute Forensic Technique (Casey & Stellatos, 2008). The file statistics can help determine what the computer is actually used for and large quantities of certain types of files can lend themselves to crime categories such as images in child pornography cases or financial documents in fraud cases (Electronic crime scene, 2008). A further breakdown of file types by location can also be extremely helpful in searching for information during the Triage Examination phase. For example, in a child pornography case if 90% of the images found are in the temporary Internet files folder then that is where the examiner should concentrate their search. It can decrease suspicion as they are probably web cache files, and it can increase complexity if the images are child pornography as it is harder to prosecute child porn possession when it cannot be shown the user was intentionally saving the files. In either case if the digital triage is being done in the field, it might be wise to direct the search and seizure team to look for additional media.

URL categories can help determine what the interests of the person(s) who use the computer are by grouping the URLs into categories of interest; Computer Science, Guns, Photography, Social Networking, etc. Further analysis can be done by examining how deep a person was in a website. For example, one Internet page at www.interestingLink.com could be a pop up or accidental access, but a user who has accessed www.interestingLink.com several layers deep obviously has a real interest in this site. This URL analysis could be as simple as sorting the websites and counting access levels or as complicated as grouping by interest using artificial intelligent agents. The approach used will be dependent on time and complexity issues.

Adding timestamps to both of these information sets can help establish user patterns as well. Consider a child pornography case where most of the pictures are downloaded between the hours of 2300 to 0300. If it can be established that this is also the time most web pages pertaining to specific topic were accessed, this might help establish who was downloading those images in a household with multiple users. This has very little value as court admissible evidence, but serves as good intelligence which is the primary goal of digital triage.

In the case of external storage or computers that are not connected to the Internet, the only results will be file statistics. Usernames could be searched for in the metadata of documents, stored emails, or any other file that might have metadata of interest, but this seems of limited use when compared to the profiling of an entire computer. For these reasons, at present it is suspected the profiling of external media will have limited results.

Three processing categories are mentioned here: computer logons, file statistics, and URL interests. Additional processing could be performed dependent on the crime under investigation. These additional processes could be included as part of the crime template discussed in the next phase. It is proposed here that it will always be useful to know the three sets of information described in this section, but that does not exclude the possibility of additional processing or filtering. As part of the research that is already underway a survey is planned to help determine what current practicing examiners think of these pieces of information and what other processing steps they would propose general or crime specific.

3.4 Crime Potential Phase

The Computer Profiling phase just described will be the same for every piece of media examined. In contrast, the Crime Potential phase contains those components that are dependent on a specific crime class. It will attempt to guide the triage examiner by raising red flags he or she should consider for a specific crime class. Information will be gathered from the computer profiling phase as well as gathered with word searches and known file searches. Although listed as a separate phase, it could run concurrently with the computer profiling stage to save time.

Different crimes will call for different templates. Child pornographers are likely to hoard and collect images leading to a large ratio of image files to total files on their machine (Lanning, 2010). Therefore, a large percentage of images files might be a red flag when performing triage on a piece of media. A hacker is likely to have a large number of scripts and executables, and both crime classes have certain commonly used keywords associated with each. Therefore, a set of crime templates will need to be developed different for each crime class. This template would help identify those items of particular interest in a given class of crime. This type of crime class modeling has already been identified as an important area of research at the 42nd Hawaii International Conference on System Sciences (Nance, Hay, & Bishop, 2009).

This template could become more advanced over time to include additional processes and filtering per crime class. For example, it would seem immensely useful to be able to apply flesh tone filtering to images during child pornography cases such as done by the first responder tool File Hound (Choudhury, Rogers, Gilliam & Watson, 2008; Gillam & Rogers, 2005). For initial efforts, a very simple template will be used to demonstrate the usefulness of the model. For the final project it would be beneficial to include some research on the development of these templates as a function of time. This is not, however, mission critical to proving the usefulness of the model. The simple template proposed here could be used for testing and development. Further exploration of the templates would only enhance the process. Each element from the template will now be discussed.

Some types of criminal subcultures such as child pornographers, hackers, or fraudsters have sets of commonly used words. There are also certain specific image files that are commonly collected by child pornographers that are part of sets, and certain hacker tools that might commonly be found. These files can be searched for by name or if time is available by mathematical hash value. Unless altered, these files will always produce the same hash value providing a way to red flag them no matter what they are named. These commonly used words and known file hash values are already being used by some digital forensics tools during analysis and examination. For example, the National Institute of Standards and Technologies (NIST) maintains the National Software

Reference Library which includes hash values for standard programs and those that are malicious in nature (National software reference, 2011).

A preponderance of certain file types could also be a strong indicator of certain activity. A child pornographer is likely to have a lot of image files, a hacker a lot of scripts and code, and a fraudster a lot of numerical based files and financial records. These statistics can be further divided into categories of files such as audio, video, documents, etc to help with intelligence gathering (Grillo, Lentini, Me, & Ottoni, 2009).

When choosing or designing a template a triage examiner must take into consideration the location the triage will occur. Will it take place in the field, in the office, or in the examination laboratory? The digital triage examiner must consider the time critical nature of the case. The more extensive the template the longer the automated process is likely to take. The digital triage examiner should also consider any legal ramifications. A warrant allowing the digital triage examiner to search for evidence of a murder does not allow him or her to look for child pornography as well. See tables 2, 3, and 4 for some example templates. The further development of these templates is part of the research currently being conducted. Examiners already use templates of their own making based on personal experience. The creation of standard templates would have the additional benefit of adding to the seriously lacking corpus of digital forensics (Garfinkel, Farrell, Roussev, & Dinolt, 2009; Nance, Hay, & Bishop, 2009).

3.5 Presentation Phase

In this phase the information from the User Analysis and the Crime Potential phase will be translated into a report that can quickly guide the digital triage examiner to artifacts of interest or help he or she quickly determine how the evidence should be prioritized. The results will be interpreted and applied according to need. The form this report will take will be developed as the tools are developed.

3.6 Triage Examination Phase

The Triage Examination Phase is the viewing of the evidence in a forensically safe manner using the guidance provided by the Presentation phase. This phase is optional dependent on need. If the Presentation phase produced enough information, then there will be no need for further examination.

This phase is different from a traditional examination. Typically, after the evidence is duplicated in a traditional digital forensic examination, the forensic software will assist in indexing, sorting, and categorizing all files and file fragments. One analogy is that of a filing cabinet being emptied and all the files sorted and categorized into separate stacks so the examiner can quickly locate information. The triage examination occurs prior to this duplication and sorting. Essentially the triage examiner is viewing the file system as it would be presented to the user in an explorer application. Any sorting or searching has to be done in real time by the triage examiner. In triage examination the examiner is just looking through the filing cabinet to see if anything is readily apparent guided by the information provided by the Presentation phase.

Triage examination is not a new concept, but the addition of an automated process using predefined templates specific to each crime class is. This triage examination phase would be what typically occurs when an examiner uses any tool on the suspect media for information gathering purposes prior to evidence duplication. The automation and the guidance provided by this model will, however, make this phase more successful.

3.7 Preservation Phase

Preservation is an overarching requirement for any activity involving digital evidence. During every phase of the process the triage examiner must insure that no change is made. The technology, software and hardware, exists to prevent any writing to the media being examined. If the media is being examined through the use of an examination machine, then a hardware write blocker must be in place between the source media and the examination machine. If the triage examiner is unable to remove the hard drive or a examination machine is not on site, then a tested live boot CD such as Helix (http://www.e-fense.com/products.php) can be utilized to boot the system into a safe environment.

In both cases since the original evidence was accessed, whatever process is used to do the triage will have to be recorded and that record will have to follow the evidence through the traditional forensics process if one is applied. The digital triage examiner should leave no room for challenges from the opposing council.

Digital triage and this process model both have different purposes depending on the location of the media being examined. Digital evidence is going to be in one of three places the field, the office, or the laboratory. In the field digital triage can be used to provide feedback to the search and seizure team, to gather quick information, and for use in suspect interviews.

A lot of local law enforcement agencies do not have their own digital forensics lab. If a piece of media is located at the law enforcement office waiting to be sent off, it might be wise to first perform triage to determine if it is even worth sending in. If it is determined through the use of this process that it is unlikely that evidence is present, then the investigators will want to concentrate their search for evidence in other areas and not wait on an exam.

A digital triage process that assists in prioritization would be extremely helpful in increasing efficiency for digital forensics laboratories. Working off a backlog has become the norm for most digital forensics laboratories. It is important for digital forensic labs to be able to prioritize cases based on the available evidence, and in some circumstances even to refuse to accept cases until their backlog is reduced.

4. Common Digital Triage Scenarios

A commonly mentioned use for digital triage is that of a kidnapping case due to the need for a speedy turn-around. The template for this would, perhaps, be very sparse. The search for all the logon usernames could be useful as well a list of keywords connected with the case. However, the primary intelligence needed for a kidnapping is the determination of whether the victim has been communicating via chat client, email, social networks, or any other means with an individual that might be of interest to the case. All of these items involve Internet artifacts, and getting to the Triage Examination phase as quickly as possible to look at these items directly might be preferred.

Another commonly discussed use of digital triage is that of a soldier in the theater of war. In this type of situation automation and simplicity of use is vital. The solider may have limited training in the use of the tool, and speed is always important to a soldier in combat. One scenario could be a soldier who needs to quickly locate media that was involved in a suspected terrorist activity. See Table 5 for a template that could be used in this type of situation.

5. Model Trade-Offs

The analysis performed in the Computer Profiling and Crime Potential phases calls for the search for logon usernames, analysis of URLs, a search of keywords, an analysis of file types, and a search for known files. There will need to be some trade-off analysis conducted pertaining to this research. For example, the more thorough the searches the longer the process will take.

One trade-off measured will involve whether these keywords should be searched for within all present files, just through the file names, or within certain file types. Also, the hashing of all files to determine if they are a known file will take considerable time as well. Known file searches can be sped up by just searching for known file names. This would not be as successful as hashing every file, but would provide considerable speed up. In both of these situations, the tradeoff will be between looking at the file names or file contents.

The inclusion of additional processing will also be a metric to consider. Additional processes mean additional automated intelligence, but it also means increased processing time. For the actual model testing, a more generalized approach can be taken without additional processing options sticking to the simple standard template described in Table 1.

There can be two types of scans that could be performed on a drive during digital triage a surface scanning looking only at present files in allocated space and a deep scan searching through unallocated and allocated space. Both of these ideas were originally considered. However, based on initial testing the idea of doing a deep scan has already been discarded. This type of analysis would be too time intensive to be of use in digital triage to be useful.

All of these speed versus completeness trade-offs are greatly dependent on situation. For example, if a triage examiner is in the field then speed is probably a very high priority. All searches can be reduced to file name searches, and all known file searches could be limited to searching for the names of the files instead of the hash values. If the triage examiner is back in the laboratory and using digital triage to sort cases, then speed might be less of an issue and the examiner can perform the searches using the file contents as well as the file names. The ability to adjust these parameters will be important to the design of this model. It will also be necessary to include the speed differences of the different options to show why it is necessary to adjust them.

6. Conclusion and Future Work

Future work includes the actual instantiation of the model including the coding of the automated portion of the model. There is also a survey planned to help better specify the base components of information that should be gathered during the automated stages of the proposed model. Several speed versus completeness trade-offs were

discussed in the previous section. Some initial research has already been done to compare allocated versus unallocated scans while searching for data artifacts. It was quickly discovered that an unallocated space scan would be too lengthy to be useful in most digital triage situation. Other trade-offs will be explored as the tools are developed.

The computer profiling stage is probably the area of this model that will be the most difficult to develop. Research is underway to develop the template concept further. Examiners already create templates from personal experience for different categories of investigation. It might be the case that the template should be left open for examiners to input their own ideas until a more comprehensive digital forensics corpus can be developed.

Even though it is in the initial stages of development and testing the creators of this process model believe it has a lot of promise, in the field, in the office, and in the laboratory. Currently a prototype is being developed using already existing forensic boot CDs, and soon testing will begin on the computer profiling stage with input from survey results. The survey results and the results of the computer profiling tests will be released as they are documented.

References

Baryamureeba, V., & Tushabe, F. (2004). *The enhanced digital investigation process model*. Paper presented at Digital forensics research workshop, Baltimore, MD. Retrieved from http://www.dfrws.org/

Beebe, N., & Clark, J. (2004). A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigations*, 2(2), 147-167. http://dx.doi.org/10.1016/j.diin.2005.04.002

Bell, G. B., & Boddington, R. (2010). Solid state drives: The beginning of the end for current practice in digital forensic recovery?. *Journal of Digital Forensics, Security and Law*, 5(3), 1-20.

Bogen, A., & Dampier, D. (2005). Unifying computer forensics modeling approaches: a software engineering perspective. *Systematic Approaches to Digital Forensic Engineering First International Workshop on* (pp. 27-39). http://dx.doi.org/10.1109/SADFE.2005.27

Carrier, B., & Spafford, E. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence*, 2(2), 1-20.

Carrier, B., & Spafford, E. (2004). An Event-Based Digital Forensic Investigation Framework. Paper presented at Digital forensics research workshop, Baltimore, MD. Retrieved from http://www.dfrws.org/

Casey, E. & Stellatos, G. J. (2008). The impact of full disk encryption on digital forensics. *SIGOPS Oper. Syst. Rev*, 42, 93-98. http://dx.doi.org/10.1145/1368506.1368519

Choudhury, A., Rogers, M., Gilliam, B., & Watson, K. (2008, May). *A novel skin tone detection algorithm for contraband image analysis*. Third International Workshop on Systematic approaches to digital forensic engineering, 3-9. http://dx.doi.org/10.1109/SADFE.2008.12

Ciardhuain, S. (2004). An Extended Model of Cybercrime Investigation. *International Journal of Digital Evidence*, 3(1), 1-22.

Farmer, D., & Venema, W. (2005). *Forensic discovery*. Upper Saddle New Jersey: Addison-Wesley Longman.

Forensic. (n.d.). (2011). Merriam-Webster's Dictionary of Law. Retrieved December 29, 2011, from http://dictionary.reference.com/browse/forensic

Garfinkel, S. (2006). Forensic feature extraction and cross-drive analysis. *Digital Investigations*, 3, 71-81. http://dx.doi.org/10.1016/j.diin.2006.06.007

Garfinkel, S., Farrell, P., Roussev, V. & Dinolt, G. (2009). Bringing science to digital forensics with standardized forensic corpora. *Digital Investigation*, 6(1). http://dx.doi.org/10.1016/j.diin.2009.06.016

Gillam, W., & Rogers, M. (2005). File hound: A forensic tool for first responders. Paper presented at Digital forensics research workshop, New Orleans, LA. Retrieved from http://www.dfrws.org/

Grillo, A., Lentini, A., Me, G., & Ottoni, M. (2009). Fast User Classifying to Establish Forensic Analysis Priorities. *IT Security Incident Management & IT Forensics*, 69-77. http://dx.doi.org/10.1109/IMF.2009.16

Hargreaves, C. & Chivers, H. (2008). *Recovery of Encryption Keys from Memory Using a Linear Scan*. Availability, Reliability & Security Third International Conference on, 1369-1376. http://dx.doi.org/10.1109/ARES.2008.109

Ieong, R. (2006). Forza - digital forensics investigation framework that incorporate legal issues. *Digital Investigations*, 3, 29-36. http://dx.doi.org/10.1016/j.diin.2006.06.004

Kruse, W., & Heiser, J. (2002). *Computer forensics: Incident response essentials*. Crawfordsville, IN: Lucent Technologies.

Lanning, K. U. S. Department of Justice Office of Juvenile Justice and Delinquency Prevention, National Center for Missing & Exploited Children. (2010). *Child molesters: A behavioral analysis for professionals investigating the sexual exploitation of children fifth edition*. Retrieved from http://www.missingkids.com/en_US/publications/NC70.pdf

Nance, K., Hay, B., & Bishop, M. (2009). Digital Forensics: Defining a Research Agenda, *System Sciences 42nd Hawaii International Conference on*, 1–6.

National software reference library. (n.d.). (2011). Retrieved December 29, 2011, from http://www.nsrl.nist.gov/

Palmer, G. (2001) A Road Map for Digital Forensic Research, Tech. Report presented at Digital forensics research workshop, Baltimore, MD. Retrieved from http://www.dfrws.org/Utica, NY

Rogers, M., Goldman, J., Mislan, R., Wedge, T. & Debrota, S. (2006). Computer Forensic Field Triage Process Model. *Journal of Digital Forensics, Security & Law*, 1(2).

U. S. Department of Justice, Office of Justice Programs. (2008). *Electronic crime scene investigation: A guide for first responders second edition* (NCJ 219941). Retrieved from https://www.ncjrs.gov/pdffiles1/nij/219941.pdf

Yeschke, C. L. (2003). *The art of investigative interviewing, a human approach to testimonial evidence*. (2 ed.). Butterworth-Heinemann.

Table 1. Standard Crime Template

Keywords	words of particular interest in a crime class or particular case
File Type Alerts	file types that would normally be found on a computer for a specific crime class
Known File Alerts	known files to be of interest in a particular case

Table 2. Child Pornography Template

Child Pornography Template	
Keywords	commonly used words by child pornographer collectors, known victims, known child porn image names
File Type Alerts	JPEG, BMP, MOV, MPEG and other graphic/movie file types
Known File Alerts	known child porn images

Table 3. Murder Investigation Template

Murder Investigation Template	
Keywords	words associated with the case such as persons, places, or things
File Type Alerts	none
Known File Alerts	none

Table 4. Murder Investigation Template

Hacking Incident	
Keywords	commonly used hacker words, common hacking programs
File Type Alerts	scripts and executables
Known File Alerts	common root kits, known hacker tools, non-standard user software

Table 5. Terrorist Activity Sample Template

Terrorist Activity	
Keywords	commonly terrorist groups and contacts
File Type Alerts	AutoCad, ArcInfo
Known File Alerts	known steganography programs

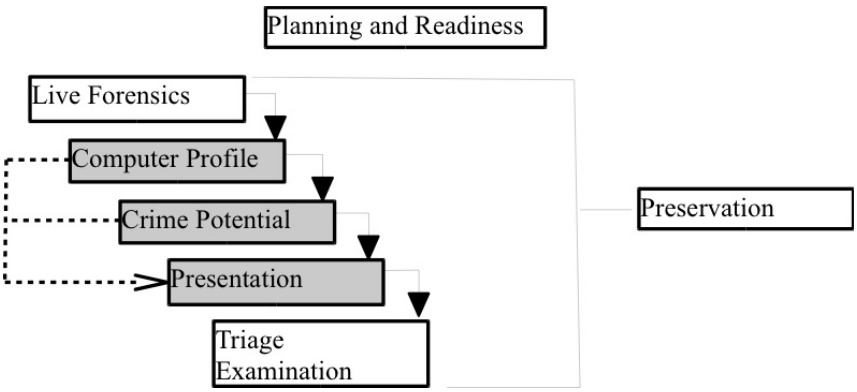

Figure 1. Semi-automated Digital Triage Process Model