Evaluation of the Semi-automated Crime-Specific Digital Triage Process Model

Gary Cantrell, David Dampier

Chapter 6

EVALUATION OF THE SEMI-AUTOMATED CRIME-SPECIFIC DIGITAL TRIAGE PROCESS MODEL

Gary Cantrell and David Dampier

Abstract The digital forensic process as traditionally laid out is very time intensive – it begins with the collection, duplication and authentication of every piece of digital media prior to examination. Digital triage, a process that takes place prior to this standard methodology, can be used to speed up the process and provide valuable intelligence without subjecting digital evidence to a full examination. This quick intelligence can be used in the field for search and seizure guidance, in the office to determine if media is worth sending out for an examination, or in the laboratory to prioritize cases for analysis. For digital triage to become accepted by the forensic community, it must be modeled, tested and peer reviewed, but there have been very few attempts to model digital triage. This work describes the evaluation of the Semi-Automated Crime-Specific Digital Triage Process Model, and presents the results of five experimental trials.

Keywords: Digital triage, process model, evaluation

1. Introduction

Digital forensics involves the post-event processing 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 was incidental [16]. The artifacts correspond to 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 must be gathered using proven, forensically-sound methodologies. At this time, these methodologies are typically standard operating

procedures that have been created independently by the organizations involved in forensic investigations.

Digital triage is a pre-digital-forensic process performed on a live or dead system. For a live system, digital triage is typically performed to extract information that would be lost when the system is powered down. This information could be stored in volatile memory or on an internal drive in an encrypted format. For a dead system, digital triage is typically performed to gather quick information for intelligence purposes. The intelligence can have many uses, including, but not limited to, determining if an examination is warranted, providing plea bargaining assistance, focusing examination efforts and guiding search and seizure efforts.

Digital triage is a pre-digital-forensic process because it is carried out prior to the accepted digital forensic practice of imaging and authenticating each piece of media before examining it. Digital triage thus examines the original evidence whereas an accepted digital forensic methodology examines an image (forensic copy) of the original evidence.

Several models have been proposed to formalize the discipline of digital forensics and to transform *ad hoc* processes into tested and proven methodologies [2–4, 6, 7]. Although some of these models mention the need for a pre-examination process such as digital triage, none of them include digital triage as a detailed phase. Moreover, very few standalone models have been proposed for digital triage [5, 18]. Thus, digital triage is mostly an unmodeled component in existing process models.

This paper discusses the evaluation of the Semi-Automated Crime-Specific Digital Triage Process Model [5]. The model was created to decrease the time taken to perform a digital triage assessment by at least 50% compared with an *ad hoc* process, but without reducing the accuracy. The model and its implementation are described in detail, and the results of five experimental trials are presented.

2. Process Model

The Semi-Automated Crime-Specific Digital Triage Process Model is designed to be used by novices. It incorporates ongoing concerns regarding pre-digital-forensic processes and can be specialized for different classes of crimes. The most significant contribution of the model is its automated phases (shaded rectangles in Figure 1). Planning and readiness is an on-going phase that occurs pre-event while preservation is an umbrella activity that is performed during all the phases. The remaining phases are presented in a linear fashion. The dotted line in the left-hand side of Figure 1 represents information flow from the computer

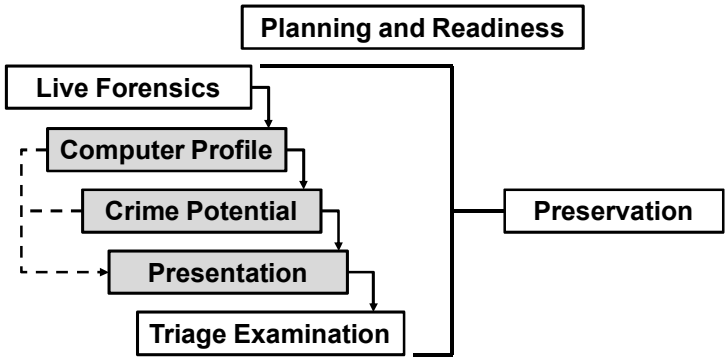

Figure 1. Semi-Automated Crime-Specific Digital Triage Process Model.

profile and crime potential phase to the presentation phase, where the raw information is transformed into usable information for the digital triage examiner.

The planning and readiness phase is an ongoing phase involving the preparation and education of staff, and the continual upgrading of equipment. Including this phase in a digital triage process is important because it ensures the continual testing of triage tools and efforts on the part of the triage examiner to keep abreast of the tools.

Live forensics involves the acquisition and analysis of volatile memory or the analysis of static data on a live machine. It is included as an optional phase based on need and expertise. Digital evidence should be gathered in the order of volatility to prevent the loss of data of evidentiary value [1, 11]. Thus, this step must come before anything else in any digital forensic or pre-digital forensic process. However, it is often skipped in investigations where the volatile memory is ignored.

Computer profiling is the first phase of an automated process in a digital triage process model. In the Field Triage Process Model [18], the intent is to learn about the users of a system by targeting the user profiles on a computer. The Five Minute Forensic Technique [12] incorporates a similar analysis, but the information is used to categorize the users as occasional users, Internet/chat users, office worker users, experienced users and hacker users. On the other hand, the Semi-Automated Crime-Specific Digital Triage Process Model suggests profiling a computer as a whole and dividing the data by volume and by user directory.

The computer profiling phase is the same for every piece of media examined. In contrast, the crime potential phase contains only the components that are dependent on a specific crime class. The phase attempts to guide the triage examiner by raising the red flags that should be con-

sidered for a specific crime class. Information is also gathered during the computer profiling phase using word searches and known file searches. Although this is listed as a separate phase, it could run concurrently with the computer profiling phase to save time.

During the presentation phase, information from the computer profile and crime potential phases are incorporated in a report that can lead the digital triage examiner to artifacts of interest or help the examiner determine how the evidence should be prioritized. The results are interpreted and applied according to need.

During the triage examination phase, the evidence is viewed in a forensically-safe manner according to the guidance provided by the presentation phase. This phase is optional based on need. If the presentation phase has produced enough information, there may be no need for further examination. The triage examination phase corresponds to the *ad hoc* method that is typically used by law enforcement.

Interested readers are referred to Cantrell, *et al.* [5] for additional details about the Semi-Automated Crime-Specific Digital Triage Process Model and its various phases.

3. Model Implementation

In an effort to facilitate model evaluation, we developed a series of scripts for the automated phases of the model: computer profiling, crime potential and presentation. The final product, which comprises open source and custom tools written in Perl, is called the Fast Modular Profiling Utility (FMPU). FMPU quickly gathers useful information to create a profile of a computer. As FMPU creates this profile, the information is monitored for keywords to assist in the determination of the crime potential. FMPU then presents the information to the user as a main report and a red flag alert report, both of them in an HTML report format.

It was decided to employ a modular design for the digital triage tool. The modular design allows for easy expansion and simple customization, and facilitates the incorporation of commands and tools.

Seven steps are involved in the execution of the tool:

- **Step 1:** Main Module accepts the report name and location as input.
- **Step 2:** Main Module writes the HTML header.
- **Step 3:** Main Module passes control to Module 1.
- **Step 4:** Module 1 extracts information.

- **Step 5:** Module 1 formats information as text, HTML table or separate HTML pages.
- **Step 6:** Module 1 appends text, HTML table or HTML links to the appropriate report.
- **Step 7:** Main Module creates the HTML footer to close the report.

Steps 3 through 6 are executed for each data item extracted. A series of scripts incorporating open source and original code were created to implement the desired functionality. Small amounts of information are added directly to the report. Larger sub-reports are written as separate files and linked to the main report or alert report.

FMPU gathers the following information to create a computer profile:

- **File System Information:**
  - Physical/logical disk layout
  - Sector allocation
  - File system types and locations
- **File Classification:**
  - File type report for each user directory
  - File type report per volume
- **Application Information:**
  - Usernames in the system
  - Web browser history
  - Windows registry data

The file system information that is gathered includes the physical disks attached to the computer being examined, the logical volumes available for mounting, the sector layout of the system, and the file system label of each volume. Viewing the physical and logical layouts of the system enables the digital triage examiner to quickly determine the amount of data on the system and the organization of each disk.

FMPU gathers file statistics from the system based on file type. This enables the digital triage examiner to quickly create a theory regarding the use of the system. For example, a media machine is likely to have a large variety of video and sound files. A corporate machine would be more likely to have documents and spreadsheets. Unfortunately, it is difficult to conjecture what "normal users" would have on their machines.

Therefore, the classification is left to the experience of the digital triage examiner and the specific template that is employed.

Application information is information that is collected about the user by an application, including the operating system, potentially without user consent. When building a computer profile, FMPU gathers usernames, web browser history and Windows registry information. Usernames are collected by pulling the user directories as listed on the system. This can provide an indication of the number of users on the system along with their identities. However, the digital triage examiner must recognize that there is no easy way to tell exactly who is using or has used a given account. Also, user directories may be placed in non-standard locations, which complicates the task. However, advanced FMPU users could edit the configuration file to specify the user directory locations that can be determined through the examination of system files.

In order to speed up future web browsing, most browsers maintain records of the sites visited by users. This history is preserved unless a user specifically changes the default setting. The first version of FMPU performed web history analysis only for Internet Explorer. This was done because Internet Explorer is arguably the most popular web browser. Internet Explorer stores its web history in `index.dat` files; the structure of these files is well-researched and documented [14, 15, 17].

The goal of FMPU is not to present all possible data. Rather, FMPU is designed to selectively collect items that are of the most interest to the digital examiner and to present the information in a useful manner. For example, in addition to listing URLs, it counts the number of times each domain was visited. The final listing is then sorted by the number of visits and sent as output. The raw output used to create this list is also included in the report in case the triage examiner needs more detail about specific links.

The Windows registry is a database of settings that provides important information to a digital forensic examiner [9, 10]. The format of these settings is not user friendly, and the settings are typically edited by software utilities rather than directly by users. FMPU uses the open-source RegRipper tool [8] to access registry data that it includes in the final report. The information extracted by RegRipper can be adjusted by the digital triage examiner using FMPU. In particular, FMPU collects login information, web history, instant messenger information, connected USB devices and shutdown information.

The final report is provided in the form of easy-to-navigate HTML pages. HTML is a common format for digital forensic reports. The final report is separated into two reports, a main report with all the data and an alert report containing data identified during the crime potential

phase. Users have the option to populate an input list of red flag words prior to running FMPU to facilitate activities during the crime profiling phase. This list is used to identify data that is of special interest. File system information is not changed during this phase; however, the files are classified. During the classification process, filenames that contain any keywords or known filenames are identified and flagged for inclusion in the alert report. Application information is also filtered. As the application information is gathered, it is monitored for keywords and known filenames, and anything identified is also included in the alert report.

4. Evaluation Results

This section describes the experimental procedure and the results of the evaluation of the Semi-Automated Digital Triage Process Model.

The subjects involved in the evaluation were divided into two groups, a validation group and a testing group. The validation group comprised qualified examiners while the testing group consisted of college students who were taking digital forensics courses. The validation group conducted qualitative testing of FMPU on real evidence. On the other hand, the testing group performed quantitative analyses to determine if using FMPU yielded a 50% decrease in processing time without any loss of accuracy compared with an *ad hoc* procedure. Only the validation group was allowed to work with real evidence due to restrictions on accessing real case data. Artificial data sets were created for use by the testing group.

4.1 Validation Results

The validation group consisted of four active digital forensic examiners. These subjects were provided with FMPU and a minimal set of instructions on how to use it. Prior to running the tool on real evidence, they were given a demonstration of FMPU on a test drive and an explanation of the results. The subjects were also asked to list five data elements that would have been useful to know prior to their original examination of the test data. Some of the items listed were large amounts of images, evidence of peer-to-peer sharing and documents with names of interest. After finalizing their lists, the subjects were asked to run the tool and examine the report.

The results of the validation testing supported FMPU. Table 1 shows the numbers of items listed and the numbers of items found by the subjects. All the subjects found at least one item that was predicted

Table 1. Validation group results.

Subject	Case Type	Items Listed	Items Found
1	Child Pornography	5	4
2	Child Pornography	4	3
3	Slander	4	1
4	Child Pornography	4	3

after hearing a description of the tool. Also, all the subjects stated that they found several items they had not predicted, but that were beneficial.

Table 2. Validation group responses.

Rating	Agree	Somewhat Agree	Do Not Agree	Not Applicable
Decrease Triage Time	2	2	0	0
Decrease Exam Time	3	1	0	0
Allow Case Prioritization	4	0	0	0

Table 2 presents the general opinions of the tool as provided by the validation subjects. The majority of the subjects believed that the tool would decrease triage time, examination time and allow for case prioritization. No validation subjects disagreed or felt that the tool would not be applicable.

The results also show that FMPU works on real-world evidence. Every subject found items that were anticipated as well as items that had not been listed before running FMPU. Even in the tests with limited results, it was noted that there was also very little found in the original examinations. During the more successful attempts, the subjects noted that, while items identified during the original examination were found, they were found much quicker using FMPU. These results support the use of FMPU on real evidence and facilitated the testing procedures conducted using artificial evidence sets.

4.2 Testing Results

The testing group was divided into experimental and control groups. The assignment of subjects to the experimental and control groups was done randomly. Experimental group subjects used FMPU while control group subjects used an *ad hoc* digital triage procedure.

The tests were quantitative in nature. As mentioned earlier, the testing group subjects were students with basic knowledge of the digital

forensic process, not active examiners. This substitution is acceptable because digital triage is conducted by individuals with varying levels of expertise, and it should be possible for novices to use a digital triage tool.

Subjects in both the experimental and control groups were given lectures on digital triage. The subjects performed short exercises or viewed demonstrations associated with each topic as part of the lectures. The lectures included the following topics:

- Using Linux boot environments (CD and USB).
- Mounting and viewing attached disks in Linux.
- Finding, listing and sorting files in Linux.
- Using the `strings` command to strip and view file content.
- Using the RegRipper utility.
- Using the Linux `file` command.

These concepts are the core of FMPU, and covering these topics ensured that most subjects could perform digital triage at a basic level before beginning the experiments. The subjects were encouraged to take notes and record the individual commands. They were allowed to bring these and any other materials they desired to the testing.

The subjects were further divided into five trials based on their levels of expertise and the testing locations. Each test subject was given the timed task of classifying three drives attached to the test machine by crime category – nothing of interest, murder scenario or child pornography (kitten pictures and phrases were used instead of real pornography). The experimental group performed this task using FMPU while the control group used an *ad hoc* procedure. The classification of these drives by crime category assesses the ability of the digital triage examiner to make decisions about digital evidence. Subjects were also asked for the confidence level regarding their selections – very confident, somewhat confident or complete guess. This allowed for outlier evaluation for subjects who gave up or simply guessed the answers.

Subjects in Trials 1 and 2 comprised law enforcement officers who were attending training courses at the Mississippi State National Forensics Training Center. Trial 1 had four subjects and Trial 2 had eight subjects. The subjects in these two trials had intermediate level expertise – they did not have a great deal of digital forensics training, but they more than made up for it with real-world investigation experience.

The subjects in Trials 3 through 5 were college students who were enrolled in digital forensics courses at Dixie State University in St. George, Utah. The subjects were given the same lectures and demonstrations as those in Trials 1 and 2, but the testing was carried out during scheduled time slots over a seven-day period. The expertise levels of the subjects in Trials 3–5 were determined based on their academic status. Trial 3 subjects were enrolled in 3000 and 4000 level classes and were classified as "advanced." Trial 4 subjects were enrolled in 2000 level courses and were classified as "intermediate." Trial 5 subjects were enrolled in 1000 level courses and were classified as "novice."

Note that, although Trial 1 is included in the testing results, it was not used in computing of the final mean times. It was, however, used in the final computation of accuracy. In addition to helping evaluate the primary goals of the research, Trial 1 was conducted in order to assess the effectiveness of the test data sets, evaluate the use of the tools on three test data sets at once, and refine the presentation materials given to the subjects prior to testing.

There was little variation in the times for the experimental and control group subjects in Trial 1, and there was only a decrease of 19% in the average times in favor of the experimental group. There was, however, an increase in average accuracy from 1.5 out of 3 to 2 out of 3 in favor of the experimental group. This can be attributed to the small size of the Trial 1 population. However, it was questioned if the tool itself could have been a contributing factor.

The test procedure and tool function were closely examined after Trial 1 was completed. The computer used for testing connected all three test sets at the same time to make the testing easier. However, this created considerable wait time before the subjects could begin the examination process.

FMPU was used to examine each volume in turn and to produce the report separated by physical disk, logical volume and user when possible. Each of the three test sets took approximately 4.5 minutes to process, resulting in more than 15 minutes of total processing time. Although 4.5 minutes does not seem like a lot of time, the 15 minutes taken to perform a combined analysis can stretch the patience of test subjects. More importantly, the time taken may be too large to provide an advantage over the *ad hoc* procedure used by the control group.

An analysis of FMPU revealed that 80% of the processing time was involved in file classification. In an effort to determine the use of a volume, FMPU classifies all the files by file type and creates a summary of the information. The first iteration performs this identification based on the file signature, a common digital forensic technique. An

Table 3. Experimental results by expertise.

Group	**Expertise**	**Average Time (Minutes)**	**Standard Deviation**	**Accuracy**
Experimental	Novice	19.00	14.85	100%
Experimental	Intermediate	16.60	7.09	100%
Experimental	Expert	10.89	9.77	93%
Control	Novice	33.33	20.59	44%
Control	Intermediate	32.00	18.09	40%
Control	Expert	37.14	19.55	70%

alternative file identification technique is to use the file extension. This type of identification is less accurate because a user or an application can intentionally rename a file extension in an attempt to obscure data. However, this is acceptable in digital triage because it is about collecting quick intelligence, not performing analysis.

During Trial 1, it was also observed that the file classification results did not seem to be as vital as the more specific application information that was gathered. With this in mind, prior to running Trial 2, the tool was set to perform file classification based on file extension instead of the first-byte signature. This change decreased the total processing time for the three drives from fifteen minutes to just four minutes. Therefore, the remaining trials were conducted using file extension identification instead of first-byte signature identification. The type of classification desired is easily set using the FMPU configuration file.

Trial 1 helped validate the quality of the test sets. Two users were able to identify all the test sets correctly with at least some confidence. Also, even with the delay imposed by file identification, crime classification could be completed within a reasonable amount of time. The accuracy results had a wide spread. Some subjects were completely correct, some were partially correct, and a few were totally wrong. These observations were also supported by the subsequent trials.

The independent variables in the tests are the presence of the FMPU report and level of expertise. The dependent variables are time and accuracy. The most apparent result in Table 3 is the difference in accuracy between the experimental and control groups. Most test subjects in the experimental group had 100% accuracy on average while the control group subjects had less than 50%, with the exception of the expert subjects in the control group (but their accuracy ratings are less than the lowest accuracy ratings in the experimental group).

The evaluation of processing time is more complex. It is not unreasonable to believe that the FMPU report would provide a greater benefit to novices than to intermediate users and a greater benefit to intermediate users than to experts. Thus, the subjects were divided into trials based on their expertise level and testing location. This division was made in an effort to explore this predicted effect. However, the results in Table 3 do not support this prediction. The expert subjects had a mean time decrease of 71% between the experimental and control groups. In the case of novice subjects, the mean time decrease was only 43%.

It is reasonable to assume that a greater level of digital forensics expertise would facilitate quicker and easier use of the tool. The average time for the experimental group subjects supports this assumption. However, this assumption does not appear to hold for the control group subjects.

We suspect that the lack of predictable responses in the control group is due to a higher degree of random chance and varying levels of expertise with the Linux environment used in the tests. The control group subjects with Linux experience were likely more confident in their results, but the likelihood of success and speed were dependent on if and how quickly they found the data that allowed them to make decisions. After all, finding the pertinent files can be a matter of chance with an *ad hoc* approach.

Another element of randomness was introduced by the subjects who guessed the results. For example, Subjects 2 and 3 indicated that their responses were complete guesses, but they took 45 minutes to complete the task. On the other hand, Subjects 4, 5 and 6, who also guessed, did so after only thirteen minutes. This randomness does not invalidate the results, it just makes the analysis more complex.

The effect of expertise level on accuracy and mean time was investigated further. We suspected that the expertise level had little or no significant effect on time or accuracy of the group as a whole because the expertise level classification was one dimensional. The experimental group subjects all followed the same process with assistance from FMPU, thereby normalizing their times. However, the control group subjects each approached the task in an *ad hoc* manner, leading to chance playing a greater role in the outcome. This leads us to believe the best evaluation metrics would be for the entire group combined or to limit the comparison to the subjects who correctly classified all three drives, which would serve to reduce the effect of the outliers who guessed and gave up at random times.

A multivariate analysis of variance (MANOVA) test was used to investigate the interaction between the independent variables (expertise and presence of the FMPU report) and the dependent variables (time

Table 4. MANOVA univariate test results.

Independent Variable	Dependent Variable	Degrees of Freedom	F-Value	p-Value
Expertise	Time	2, 44	0.131	0.878
Expertise	Accuracy	2, 44	0.863	0.429
FMPU Report	Time	1, 44	18.40	0.000
FMPU Report	Accuracy	1, 44	18.99	0.000

and accuracy). A MANOVA test compares the means of several groups to determine the statistical significance of the groups. It addresses the interaction significance between the dependent and independent variables. MANOVA is typically used when there is the possibility of noise caused by the interaction of the variables. In this circumstance, noise can be attributed to random chance in the control group and varying digital forensics and/or Linux expertise. MANOVA reports the different interactions of the variables as separate univariate results as part of the primary multivariate analysis [13].

Table 4 presents the MANOVA univariate test results. A p-value of 0.05 was used to determine if the null hypothesis is rejected or fails to be rejected. The null hypothesis in this case is that there is no statistical difference in the mean values of the two sets. As shown in Figure 4, the effect of expertise on time resulted in $F = 0.131$ and $p = 0.878$, so the test fails to reject the null hypothesis that there is no difference between the expertise groups with regard to time. The effect of expertise on accuracy resulted in $F = 0.863$ and $p = 0.429$, so this test also fails to reject the null hypothesis that there is no difference between the expertise groups with regard to accuracy. This shows that expertise has no statistical significance on the test results.

The MANOVA test considering the effect of the presence or absence of the FMPU report on time yielded $F = 18.40$ and $p = 0.000$. The presence or absence of the FMPU report effect on accuracy resulting in values $F = 18.99$ and $p = 0.000$. The Wilks Lambda statistic for the multivariate test itself yielded $F = 0.462$ and $p = 0.000$, which supports the validity of the test results. Thus, the null hypothesis that the means of the experimental and control groups are the same with regard to both time and accuracy is rejected, i.e., the means are significantly different for the experimental and control groups.

Based on the statistical evaluation, the metric that best describes the experimental results is the total experimental group mean compared with the control group mean. For additional analysis, the results of

Table 5. Final test results.

Trial Combination	Group	Mean Time (Minutes)	Standard Deviation	Mean Accuracy
All Correct	Control Group	40.70	19.10	100%
All Correct	Experimental	16.35	8.97	100%
Percent Decrease	60%			
All	Control Group	33.91	18.42	51%
All	Experimental	14.91	7.13	95%
Percent Decrease	53%			

only the groups who got everything correct are of interest as well. With the means between the experimental group and control group confirmed statistically as being different by the MANOVA test, the final results can now be considered. However as mentioned above, the five trial separation by expertise classification was shown to be not significant. Therefore, no *post hoc* analysis was conducted. The final test results are summarized in Table 5.

5. Conclusions

An important goal during the development of the Semi-Automated Crime-Specific Digital Triage Process Model and the Fast Modular Profiling Utility (FMPU) was to decrease the digital triage assessment time by at least 50% without any loss of accuracy compared with an *ad hoc* approach. The experimental results indicate that this goal has been met. Comparison of the mean time of all the subjects and the mean time of the subjects who obtained correct results reveals a decrease in the mean time of at least 50%. Meanwhile, no loss of accuracy was observed when the subjects used FMPU.

The level of expertise of the users was deemed to be not significant. Digital forensics expertise appears to have a slight effect, but Linux expertise may have more of an effect. The statistical analysis reveals that the presence or absence of FMPU has a statistically significant effect on time and accuracy. This leads to the conclusion that the Semi-Automated Digital Triage Process Model implemented with FMPU is useful in digital triage regardless of the expertise level of the user.

Our future research will focus on a more thorough evaluation of the digital triage model, including designing experiments that would examine additional variables, and increasing the numbers of subjects and subject groups in the qualitative and quantitative evaluations. We will also

focus on alternate implementations of the model and utility, additional user classifications and further crime template development.

References

[1] F. Adelstein, Live forensics: Diagnosing your system without killing it first, *Communications of the ACM*, vol. 49(2), pp. 63–66, 2005.

[2] V. Baryamureeba and F. Tushabe, The enhanced digital investigation process model, *Asian Journal of Information Technology*, vol. 5(7), pp. 790–794, 2006.

[3] N. Beebe and J. Clark, A hierarchical, objectives-based framework for the digital investigation process, *Digital Investigation*, vol. 2(2), pp. 147–167, 2005.

[4] A. Bogen and D. Dampier, Unifying computer forensics modeling approaches: A software engineering perspective, *Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering*, pp. 27–39, 2005.

[5] G. Cantrell, D. Dampier, Y. Dandass, N. Niu and A. Bogen, Research toward a partially-automated and crime-specific digital triage process model, *Computer and Information Science*, vol. 5(2), pp. 29–38, 2012.

[6] B. Carrier and E. Spafford, Getting physical with the digital investigation process, *International Journal of Digital Evidence*, vol. 2(2), 2003.

[7] B. Carrier and E. Spafford, An event-based digital forensic investigation framework, *Proceedings of the Digital Forensics Research Workshop*, 2004.

[8] H. Carvey, RegRipper (`regripper.wordpress.com`).

[9] H. Carvey, The Windows registry as a forensic resource, *Digital Investigation*, vol. 2(3), pp. 201–205, 2005.

[10] B. Dolan-Gavitt, Forensic analysis of the Windows registry in memory, *Digital Investigation*, vol. 5S, pp. S26–S32, 2008.

[11] D. Farmer and W. Venema, *Forensic Discovery*, Addison-Wesley, Upper Saddle River, New Jersey, 2004.

[12] A. Grillo, A. Lentini, G. Me and M. Ottoni, Fast user classifying to establish forensic analysis priorities, *Proceedings of the Fifth International Conference on IT Security Incident Management and IT Forensics*, pp. 69–77, 2009.

[13] T. Hill and P. Lewicki, *Statistics: Methods and Applications*, StatSoft, Tulsa, Oklahoma, 2006.

[14] K. Jones and R. Blani, Web Browser Forensics, Part 1, Symantec, Mountain View, California (www.symantec.com/connect/articles/web-browser-forensics-part-1), 2010.

[15] K. Jones and R. Blani, Web Browser Forensics, Part 2, Symantec, Mountain View, California (www.symantec.com/connect/articles/web-browser-forensics-part-2), 2010.

[16] W. Kruse and J. Heiser, *Computer Forensics: Incident Response Essentials*, Addison-Wesley, Boston, Massachusetts, 2001.

[17] J. Oh, S. Lee, and S. Lee, Advanced evidence collection and analysis of web browser activity, *Digital Investigation*, vol. 8S, pp. S62–S70, 2011.

[18] M. Rogers, J. Goldman, R. Mislan, T. Wedge and S. Debrota, Computer forensics field triage process model, *Journal of Digital Forensics, Security and Law*, vol. 1(2), pp. 27–40, 2006.