The Forensic Validity of Visual Analytics

Robert F. Erbacher
Department of Computer Science, UMC 4205
Utah State University, Logan, UT 84322
Robert.Erbacher@usu.edu

Abstract

The wider use of visualization and visual analytics in wide ranging fields has led to the need for visual analytics capabilities to be legally admissible, especially when applied to digital forensics. This brings the need to consider legal implications when performing visual analytics, an issue not traditionally examined in visualization and visual analytics techniques and research. While digital data is generally admissible under the Federal Rules of Evidence [10][21], a comprehensive validation of the digital evidence is considered prudent. A comprehensive validation requires validation of the digital data under rules for authentication, hearsay, best evidence rule, and privilege.

Additional issues with digital data arise when exploring digital data related to admissibility and the validity of what information was examined, to what extent, and whether the analysis process was sufficiently covered by a search warrant. For instance, a search warrant generally covers very narrow requirements as to what law enforcement is allowed to examine and acquire during an investigation. When searching a hard drive for child pornography, how admissible is evidence of an unrelated crime, i.e. drug dealing. This is further complicated by the concept of "in plain view". When performing an analysis of a hard drive what would be considered "in plain view" when analyzing a hard drive.

The purpose of this paper is to discuss the issues of digital forensics and the related issues as they apply to visual analytics and identify how visual analytics techniques fit into the digital forensics analysis process, how visual analytics techniques can improve the legal admissibility of digital data, and identify what research is needed to further improve this process. The goal of this paper is to open up consideration of legal ramifications among the visualization community; the author is not a lawyer and the discussions are not meant to be inclusive of all differences in laws between states and countries.

Keywords: Visual Analytics, Digital Forensics, Legal Issues, Interactive Feedback Loop

1. Introduction

Visual analytics [14] is increasingly being applied to the analysis of wide-ranging data sources, such as biological data, financial data, medical data, physics data, digital forensics, etc. With most analysis tasks, the results of the analysis are sufficient; they are also the desirable results. With digital forensics, however, this is not sufficient. With digital forensics, the issue that arises is the need to validate not only the results but also the analysis process itself.

Digital forensics involves the analysis of digital data in order to locate information relevant to some form of investigation. The results of forensic analysis are often presented to a jury, either civil or criminal. This need for legal admissibility places additional demands on the visual analytics techniques. Given visual analytic's effectiveness at locating hidden information [12][13] the issues with legal admissibility become even more critical.

To achieve the full benefit of forensic analysis, then, the consideration of legal consequences must be tightly integrated with the process of designing and evaluating developed forensic techniques and the networks themselves. This derives from the work by Erbacher et al. [1][2][11] in which a proposed digital forensic process was presented, as well as work by Popovsky et al [8][9], proposing network forensic readiness and device calibration. In essence, development of forensic techniques are already designed, evaluated, and refined through an iterative process. Combining [1] and [8] we propose that evaluation of legal admissibility be incorporated at each stage of this process and examined to incorporate needed capabilities in order to ensure legal admissibility and validity. This proposed process is much akin to the process of designing visualization techniques in which user evaluation must be considered at each stage in the development of the visualization techniques in order to ensure they are effective, meet the needs of the users, and are perceptually viable.

Visualization and Data Analysis 2008, edited by Katy Börner, Matti T. Gröhn,
Jinah Park, Jonathan C. Roberts, Proc. of SPIE-IS&T Electronic Imaging, SPIE Vol. 6809
68090H, © 2008 SPIE-IS&T · 0277-786X/08/$18

2. Background

The legal admissibility of visual analytics techniques is dependent on the requirements of digital forensic capability as well as the existing legal background that identifies requirements for digital data to be legally admissible.

2.1 Digital Forensics

The goal of the analysis with digital forensics is to

- **Locate hidden information**. This may revolve around identifying how a computer was used to assist in a known crime. It is similarly used to identify how a computer was used inappropriately. The idea here is that a computer was found during the investigation of a crime and any related information on the computer must be identified.

- **Identify what happened to a digital system**. This particularly relates to intrusions and misuses. The goal would be to identify how an intrusion occurred, i.e., what weakness allowed it to be successful. This would be used to identify the extent of damage and aid in recovery to determine how to correct the weakness and identify what other systems might be impacted.

- **Identify network communication patterns**. Analyzing and comprehending network activity is critical for detecting and eliminating attacks before they are successful. It is also imperative for the identification of already compromised systems and misuses. For instance, the goal would be to identify botnet peer-to-peer activity or inappropriate data downloads and sharing.

Each of these areas contains volumes of data that make textual analysis unfeasible. Thus, they are prime targets for the application of visual analytics to aid in the analysis of the data. Each of these areas could result in the discovered results being presented to a civil or criminal court of law. For instance, the analysis of a computer break-in could lead to criminal prosecution of the offender. In order for the data that identified the offender and their actions to be admissible, rules of legal admissibility must be followed.

2.2 Goals of Visual Analytics for Digital Forensics

After an attack or an intrusion is identified, the analyst is left with little recourse accept to manually and tediously examine available system log files, network traffic data, and recorded system statistics, in order to determine what did in fact occur in sufficient detail as to resolve the incident. In essence, the goal of network forensics is the examination of data collectable from networks of computer systems in order to examine some form of criminal activity. Using the aforementioned data sources, analyst must be able to identify and examine any form of compromise of a network, whether it is an intrusion from an outside source, an inside job, unauthorized modification of websites, etc. The goal at this stage is for the analyst to answer typical forensic questions.

- What happened?

- How did it happen?

- Why did it happen?

- When did it occur?

More importantly, these questions must be related to the networked infrastructure:

- Who broke into the system/network? More specifically, from where did the attack initiate? The validity of any identification is limited due to IP Spoofing and the use of intermediate compromised hosts. However, it can aid identification of compromised systems being used to launch attacks and aid correlation with other attacks and further identification of compromised systems.

- What did they compromise/damage? We must identify what the focus of the attack was such that we can determine what actions need to be taken in order to recover the systems within the local network from the attack, identify any data that may be compromised, identify local legal liability, and identify any appropriate legal recourse that must be initiated.

- What did they gain access to? Was it sensitive?

- How did the intruder break in? This is critical since if we cannot identify how an attack was deployed we will not be able to defend against it in the future.

- What systems need to be repaired?

- How can future such attacks be protected against?

- Identification of when the attack occurred. The duration of time during which the system was compromised can have an enormous impact on any of the above considerations.

In essence, the analyst must determine what the attacker or intruder did in as much detail as possible such that they can be prevented in the future and the appropriate civil and criminal procedures followed (if needed), based on the associated damage and risk assessments [6]. Should a system be missed by the analyst then a compromised system, and thus vulnerabilities, will continue to exist within the organization. Such compromised systems can be used for future attacks, to sniff the network for data, or be used as future dissemination vehicles for viruses, worms, or denial of service attacks. Consider, for example, the threat of a compromised system at a bank, e-commerce site, or credit card company. The information available is highly sensitive. Should the exact mechanism the attacker used not be identified then the organization will be subjected to a future, perhaps more organized attack. Should the details of the compromised data not be identified then the extent of damage to the companies' Intellectual Property will not be completely determined and the extent of the needed criminal or civil action will not match the damage to the company's bottom line. For example, it is critical that it be identified should credit card information be stolen such that customers can be warned and the credit card numbers deactivated.

With the above explanation of the criticality of the analysis process following an intrusion, analysts are still left with principally reading log files for the relevant data. Simple searches [5], pattern matching [24], and statistical analysis [3] can help but by no means reduce the tediousness of the effort. With the volume of such attacks on the rise, capabilities for improving the task are sorely needed.

2.3 Legal Admissibility

Legal admissibility is fundamentally based on the federal rules of evidence [21][22] as it is applied to digital evidence [23]. This ultimately requires validation of several requirements for admissibility, namely: Authentication, Hearsay, The best evidence rule, and Privilege. The issue of privilege essentially identified that the data and subsequently, the visualization, is *not* subject to restrictions as evidence due to privilege. Restrictions due to privilege are most commonly equated with attorney-client privilege.

2.3.1. Authentication

The idea with authentication is to show to a jury that the evidence presented is in fact valid and factual. It must be shown that the data could not have been compromised, faked, or include unrepresentative data. It must be considered that the opposing counsel will attempt to discredit the data and show methods that would invalidate the data, even in small ways. The admitter of the data must pre-eminently show the validity of the data and discredit any potential theories by the opposing counsel as to how the data may not be valid. A comprehensive validation of authentication may include, but would not be limited to showing [19]:

- "the reliability of the computer equipment"

- "the manner in which the basic data was initially entered"

- “the measures taken to insure the accuracy of the data as entered”
- “the method of storing the data and the precautions taken to prevent its loss”
- “the reliability of the computer programs used to process the data”
- “the measures taken to verify the accuracy of the program”

With visual analytics, additional steps may include:

- the algorithms used to transform the data into the visual form
- validation that visual artifacts are not compromising the integrity of the visualization
- validation that identifiable visual artifacts *are* representative of the underlying data
- explanation as to why visualization is more effective than looking at the raw data
- validation that a visual display is comparable to a computer printout of the data

2.3.2. Hearsay

Digital data is generally not considered hearsay if it is “the by-product of a machine operation which uses for its input ‘statements’ entered into the machine” and “was generated solely by the electrical and mechanical operations of the computer and telephone equipment.” [18] This clearly includes visualization at a fundamental level. However, the visualization is then interpreted by an analyst, which could be considered hearsay. This reverts to the need to validate the accuracy of the resultant visualization and its relationship to the raw data. Often in such scenarios, the quality of the expert witness will determine the admissibility of the evidence.

2.3.3. The Best Evidence Rule

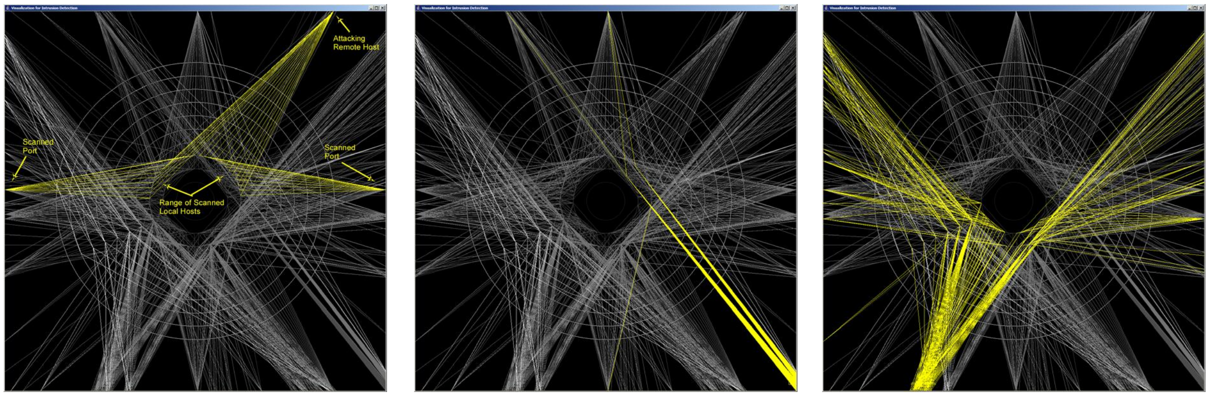
Fundamentally, the best evidence rule states that evidence is only admissible if it is “the best that the nature of the case will allow” [20]. More specifically, The Federal Rules of Evidence states that “if data are stored in a computer…, any printout or other output readable by sight, shown to reflect the data accurately, is an ‘original”. The primary component here is the concept that most computer data is not generally human interpretable in its base form, i.e. raw binary data. Thus, the best evidence rule essentially allows an additional step to allow for the transformation of the data into a readable form; this also includes the printing of the data. The challenge here is showing that a visualization technique reflects the data accurately. When confronted by opposing counsel will such explanations hold up in a juries mind?

2.3.4. Summary

The critical factor here is the need to validate the fact that visualization is not hearsay and provide validation that even though it is an abstract representation it is in fact a direct transformation of the raw data. This validation is complicated by the existence of visual and perceptual artifacts within visual displays and the fact that some of these artifacts do *not* represent any relevant underlying data characteristics. With opposing counsel attempting to show that evidence was acquired inappropriately, any limitations in the ability to show a valid and concrete analysis process can lead to the evidence being deemed inadmissible or creating reasonable doubt within members of the jury.

Is it sufficient to show select incriminating features within the visualization and how those visual features relate to the underlying data? The challenge is that with gigabytes or terabytes of data, showing small pieces of data and their relationship to the visualization may not be sufficient. What will be believable by the jury? How many examples must be shown to convince the jury that the visualization is accurate for the entire data set when it is quite unfeasible to examine it in its entirety? This issue is exemplified in figure 1.

Furthermore, the non-trivial nature of many of the transformations will make it difficult for a jury to comprehend exactly how the visual representation is derived from the data. Will a jury *believe* the abstract visualization is a direct


Visualization for Intrusion Detection
Attacking Remote Host
Scanned Port
Scanned Port
Range of Scanned Local Hosts

(a) (b) (c)

Figure 1: Consider explaining a complicated scenario such as that shown in these three figures from network traffic data. Figures (a) and (b) identify network-based attacks, more specifically sophisticated network scans. Figure (c) highlights innocuous activity. While this may be validated by the underlying data, how can juries be made to understand the differences and the validity of the differences under the pressures of opposing counsel?

representation of the raw data; given the extensive transformation, existence of visual artifacts, and complexity of the representations?

An additional issue is related to the accessibility of the data. For instance, did analysts and investigators have the right to look for data that was located on the hard drive? Generally, a search warrant would be rather specific. For instance, after an individual is arrested for child molestation, a search warrant would likely allow for examination of digital media for child pornography or related evidence. What happens if evidence of unrelated criminal activity is found? Since this subsequent evidence is not part of the search warrant, would it be admissible? What would be considered “in plain sight” with respect to digital media; since evidence found in plain sight is generally admissible? Visualization essentially exacerbates these issues and makes it far easier to locate hidden data and evidence. This will lead to challenges as to the admissibility of evidence found through visualization techniques.

3. Integration Visual Analytics into The digital Forensic Process

Forensics is a well-established process through which typical criminal activity is investigated. The process for such typical forensics is well established and accepted by the courts. With digital forensics, we must provide new analysis capabilities to deal with the volume and type of data needing analysis. While forensic analysis is well established, digital forensics is still a very young and developing field. New techniques are constantly being developed and a lot of research has focused on the development of analysis paradigms geared towards improving the effectiveness of the analysis process as well as its legal admissibility. Thus, a process is needed to ensure the acceptability and validity of the underlying data as well as the analysis process and resulting data themselves. Our proposed process for network forensics is exhibited in figure 2. This work builds on and extends other related models developed by the digital forensics research community [7].

Traditional analysis paradigms principally focused on the textual analysis portion of the process, figure 3. With this paradigm, an assumption is made as to the legal admissibility of the data. Additionally, all analysts develop their own paradigm and methodology for analyzing digital data; there is no formalized methodology as there is within other domains. With DNA data, it is expected that labs follow a strict procedure to avoid cross contamination or other compromise of the results. Failure to follow this strict procedure generally leads to the data being dismissed as inadmissible or being rejected by the jury. Since digital data analysis does not have such a strict process, there is the possibility that opposing counsel could attack the validity and accuracy of the analysis process itself. For instance, how can it be shown that data should be considered in plain view when there is no strict analysis process?

The goal with our proposed methodology in figure 2 is to begin resolving many of the issues discussed to this point; for instance:

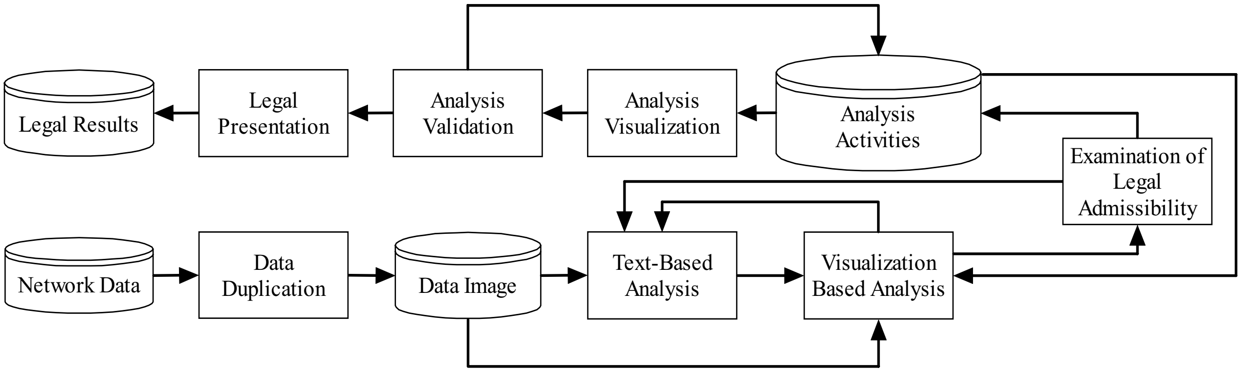


Figure 2: Abstract network forensic process diagram. The interactive feedback loops affecting the visualization component are of key importance. Also of importance is the incorporation of legal needs into the process design. In this way, we ensure that all aspects of the analysis process are recorded for later examination.

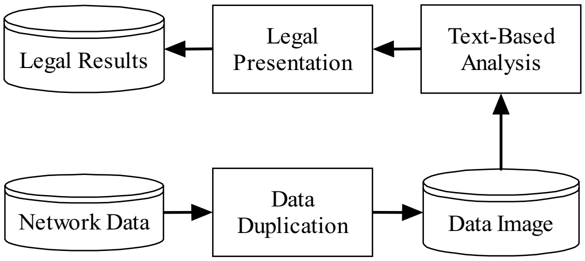


Figure 3: This diagram shows a more traditional analysis process. A more complete description of traditionally proposed processes can be found in [7].

- The methodology stores activities performed by analysts to keep track of what was successful and not successful. This will aid in training new analysts and identification of the legal admissibility of analysis paradigms.

- The methodology integrates visualization into the analyst's more traditional process. The goal is to add to and work with an analyst's more traditional capabilities.

- The methodology considers the legal admissibility of an analysis paradigm throughout the process. This is designed both for validating the analyst as well as the visualization techniques. This is critical since the use of visualization for forensic analysis has not been legally vetted.

The remainder of this section discusses each of the principal components of the methodology and how these components are expected to interact with one another. It is the interaction between the components, especially the feedback loops, which will improve the effectiveness and legal validity of the digital forensic process. The methodology attempts to identify what would be required of a complete set of capabilities to improve the effectiveness of a forensic analyst when dealing with the scale of today's data while improving the legal admissibility of the forensic analysis process when applied to digital evidence.

3.1 Data Validation

Clearly, we will be starting from some form of raw data associated with the identified intrusion or compromise. This original data source must be protected in order to ensure validity and verification. The idea here is to be able to prove that the data has not been modified since it was collected. This can be done by encrypting the data with a dated certificate or making a complete copy of the hard drive and storing the entire hard drive, following complete chain of custody and evidence storage procedures. The key is to not operate on the original data but protect the original data in some way such that it can be shown that any evidence identified exists in this original data source and this original data source is uncompromised.

3.2 Text-Based Analysis

The fundamental capabilities for analyzing network traffic data hinges on the analysis of textual representation of the underlying network traffic data and binary-based pattern matching to a limited extent.

For instance, when analyzing network traffic data, the analyst will have identified at least one system that has been compromised. This compromised system provides a focal point for initial analysis and the first step is generally to perform an initial filter to leave only events related to the target system. Later in the analysis process, after more details of the attack and attacking system are well known then the analyst can return to the full set of raw data in order to identify other systems that may have been targeted by this attack.

Given the volume of data intrinsic to network forensics, the filtering of data to narrow analysis focus is crucial. Additional analysis capabilities, however, are also necessary, including:

- **Pattern matching** – In order to identify the attack sequence which led to the compromise it is critical to be able search for patterns of activity. The patterns may be fixed or regular expressions. Typical activities searched for would include sequences of bytes used in known buffer overflow attacks, or sequences of packets that do not match typical connection sequences, etc.

- **Stream identification** – With the number of packets collected, the ability to cluster packets can greatly reduce the amount of effort involved. The most fundamental clustering parameter is based on event streams. Associating packets with event streams allows the analyst to eliminate large numbers of packets rapidly, if the event stream can be identified as being acceptable, i.e., not part of the compromise.

- **Data browsing/examination** – At a final level, analysts will need to examine the raw packet data in a binary, textual, or hybrid format. Ultimately, there is no way to do searches for all types of attacks. This requires that the analyst examine this raw data in order to perform the final steps in identifying what packets were involved in the attack and how the compromise was instigated.

- **Domain knowledge** – Given the level of analysis at all levels required to analyze network data forensically, the analyst must have extensive experience and understanding of network data in order to determine if packets are innocuous or malicious. Additionally, knowledge of the local network will aid in improving of the analysis process, as often identification of whether a packet or packet sequence is innocuous is dependent on local policy.

These capabilities will need to be integrated into the visualization capabilities. The work by Lakkaraju et al. [4] provides a starting point for some of this integration but much more work is needed to provide analysts with all of the capabilities they have become familiar with. Forensic analysts have come to count on these types of capabilities and have grown familiar with how to use them for their typical tasks. Thus, the visualization techniques must work with these types of capabilities and not separate from them. This is where visual analytics can truly make an impact. By integrating the typical text-based metaphors analysts are use to into a visual and interactive paradigm, the analyst will have their familiar capabilities but in a far more efficient interface.

3.3 Visualization Based Analysis

Clearly, much of the analysis process is inhibited by the volume of data and the need to filter or cluster data. The extensive amount of data examination required makes network data analysis a very slow process. Consequently, visualization techniques work with the analyst to improve the process. These visualization techniques must be designed to work with the typical forensic analysis capabilities. Through visualization and graphical user interfaces the typical commands are still available but are made more accessible.

While the visualization techniques will rely extensively on the raw data, they will also rely on the results of the more traditional techniques. This creates an interactive feedback loop in which the textual analysis capabilities provide more meaning and context as the results are incorporated into the visualization. The visualization then aids better comprehension of these results and provides better access to the traditional commands such that the next sequence of commands can be initiated in a more effective fashion. Thus, the goal of the visualization is to make the analysis process more effective and efficient.

3.4 Analysis Legal Admissibility

Given the considerations for legal admissibility (as discussed in section 2), we must analyze the generated results and the process used to generate those results for legal validity. This analysis would consider the relevancy of the results, the methodology applied, as well as the clarity and verifiability of the results. While initially this analysis would have to be applied manually, likely in consultation with lawyers, the long-term goal will be to have much of this analysis done automatically. Specifically, we propose that the results and analysis methodology be stored. The success/failure of prior analysis paradigms can be used to train new analysts and aid in focusing experienced analysts in using approaches identified as being more effective. The important aspect here is that by storing the legal validity of different analysis paradigms, the environment can notify analysts immediately should they be using analysis paradigms that may not be legally successful and ultimately offer advice as to what analysis paradigms to use. Given a failing strategy, the user could restart their analysis using a more appropriate strategy.

3.5 Analysis Results

Typically, the key aspect of an analysis is simply the results of the analysis. With our proposed model, the analysis process itself is of critical importance. The analysis results provide an additional interactive feedback loop to aid future analysis as well as aiding in proving the legal admissibility of the results.

In terms of the analysis process, the goal is to keep track of what the analyst has examined, why (through annotation), when this was done, and how. The sum of the identified activities of the analyst provides a picture of the analysis process.

This database of activities provides benefits for future analysis, both by this analyst and by other analysts. For instance, we envision the development of machine learning techniques to guide analysts by identifying typical activities performed during previous analysis sessions that bore out successfully; especially if a previous session can be deemed to be particularly similar to the current session. Additionally, these machine-learning techniques could automatically create macros for typically performed activities, shortening aspects of the analysis process.

In terms of legal validity, the database will provide background as to what types of activities are typically done by analysts. This will show that the current analysis follows convention; a current lacking identified earlier in this paper. Evidence identifying an unrelated crime found while using an “accepted” analysis process would have a higher likelihood of being admissible than evidence found using a unique analysis process. Given the wide variety of analysis scenarios, this paradigm is not perfect, as it will require a very large database in order to validate an analysis sequence. However, it is an effective and necessary first step.

3.6 Analysis Visualization and Validation

As the analysis process data is collected, it will be necessary to analyze this data itself. More importantly, it will be necessary to present this data in court proceedings. This essentially will require the development of further visualization techniques. The goal of these techniques will be for analysis, for instance:

- What analysis techniques or processes appear to be most effective?
- What techniques are missing or not used effectively?
- How effective are individual analysts and their associated techniques?

In essence, these techniques are similar to the visualization-based analysis techniques previously introduced but applied to the collected analysis data and with the change in focus of validating and presenting the data, with less focus on actual analysis capabilities.

The more important portion of these visualization techniques will be to present the results in court proceedings and otherwise validate the analysis process under examination. Thus, the visualization techniques must be designed to present the data, rather than providing the ability to analyze the data. In terms of presentation, the visualizations must show the difference between the analysis under discussion and typical analysis processes. Given that no two data sets will be the same, there will obviously be differences but we must be able to show that these differences are not significant and that the overall process is identical. This will amount to a validation process with respect to the forensic analysis process.

The results of this validation will further feed back into the analysis results database such that analysts using processes or steps deemed invalid can be warned of such and focused on techniques that are more appropriate. Additionally, the machine learning techniques would be able to provide indications as to the likelihood of evidence admissibility given the processes followed by the analyst and the relationship of the identified evidence to the analysis task.

4. Conclusions

The VizSec community has begun publishing a body of work related to intrusion detection through a series of workshops [15][16][17]. The focus of this body of work is on intrusion detection and the body of work does not deal with the unique issues intrinsic to network forensics. For instance, few of the techniques provide the level of detail or the level of interaction necessary and certainly not combined. This body of work can be used as an indicator of what visualization strategies will and will not work. Thus, it can be used to avoid reinventing the wheel and while our tasks and challenges differ, there are characteristics of the visualizations that will remain similar.

The proposed model will ultimately need to be implemented in a complete system for testing and refinement. This model itself is in an early stage and seeing continuing refinement based on feedback from legal experts and other domain experts within the forensic community. This model is not designed to be independent of the work being done by other researchers, as summarized by Pollitt [7]. Rather, this work takes a more applied view of the needs of forensic analysis. The work of other researchers should also be taken into consideration when a complete environment is being developed.

Finally, with the volume of data being made available in today's digital systems the traditional text only analysis is going to be hard pressed to keep pace. Visualization has the unique potential to greatly improve the efficiency of the analysis process and allow analysts to handle much larger volumes of data to deal with the ever-increasing scale of storage devices. Visualization also has the ability to aid location of ever more cleverly hidden data that analysts may not know they need to look for. However, even with all these advantages for forensic analysis, visualization has its own unique challenges with respect to being legally admissible.

5. References

1. Robert F. Erbacher, Kim Christensen, and Amanda Sundberg, "Visual Forensic Techniques and Processes," *Proceedings of the 9th Annual NYS Cyber Security Conference Symposium on Information Assurance*, Albany, NY, June 2006, pp. 72-80.
2. Robert F. Erbacher, Barbara Endicott-Popovsky, and Deborah A. Frincke, "Challenge Paper: Validation of Forensic Techniques for Criminal Prosecution," *Proceedings of the 2nd International Workshop on Systematic Approaches to Digital Forensic Engineering*, Seattle, WA, April 2007, pp. 150-151.
3. Akira Kanaoka and Eiji Okamoto, "Multivariate Statistical Analysis of Network Traffic for Intrusion Detection," *Proceedings of the 14th International Workshop on Database and Expert Systems Applications* (DEXA'03), September 2003, pp. 472-476.
4. Kiran Lakkaraju, Ratna Bearavolu, A. Slagell, W. Yurcik, "Closing-the-loop: discovery and search in security visualizations," *Proceedings of the 6th annual Information Assurance Workshop*, IEEE Computer Society Press, West Point, NY, pp. 42-49, 2005.
5. Gonzalo Navarro, Mathieu Raffinot, *Flexible Pattern Matching in Strings*, Cambridge University Press; 1st Edition, 2002.
6. Thomas R. Peltier, *Information Security Risk Analysis*, Auerbach Pub; 1st Edition, 2001.

7. Mark M. Pollitt, “An Ad Hoc Review of Digital Forensics Models,” *Proceedings of the 2nd International Workshop on Systematic Approaches to Digital Forensic Engineering*, Seattle, WA, April 2007, pp. 43-52.

8. B. Popovsky and D. Frincke, “Network Device Calibration for Establishing Foundation for Expert Testimony,” *Proceedings for 3rd Annual IFIP WG 1.9 International Conference*, to appear 2007.

9. B. Popovsky and D. Frincke. “Embedding Forensic Capabilities into Networks: Addressing Inefficiencies in Digital Forensics Investigations,” *7th Annual IEEE Information Assurance Workshop*, West Point, June 2006.

10. P. Rothstein, M. S. Raeder, D. Crump, *Evidence in a Nutshell*, 4th edition, Thomson/West, 2003.

11. Richard Swart and Robert F. Erbacher, “Legal Developments in eDiscovery: Implications for Security Management*,” Proceedings of the 6th Security Conference*, Las Vegas, NV, April 2007.

12. Sheldon Teerlink and Robert F. Erbacher, “Improving the Computer Forensic Analysis Process through Visualization,” *Communications of the ACM*, Vol. 49, No. 2, 2006, pp. 71-75.

13. Sheldon Teerlink and Robert F. Erbacher, “Foundations of Visual Forensic Analysis,” *Proceedings of the IEEE Information Assurance Workshop*, West Point, NY June 2006, pp. 192-199.

14. James J. Thomas and Kristin A. Cook, *Illuminating the Path: The Research and Development Agenda for Visual Analytics*, National Visualization and Analytics Ctr., 2005.

15. *Proceedings of the 2005 IEEE Workshops on Visualization for Computer Security*, Editors: Kwan-Liu Ma, Stephen North, Bill Yurcik, IEEE Press, 2005.

16. *Proceedings of the 2006 ACM Workshops on Visualization for Computer Security*, Editors: William Yurcik, Stefan Axelsson, Kiran Lakkaraju, Soon Tee Teoh, ACM Press, 2006.

17. *Proceedings of the 2007 IEEE Workshops on Visualization for Computer Security*, Editors: John Goodall, Kwan-Liu Ma, Gregory Conti, IEEE Press, 2007.

18. *State v. Armstead*, 432 So.2d 837, 839 (La. 1983).

19. *American Law Reports* 4th, 8, 2b.

20. *Omychund v Barker* (1745) 1 Atk, 21, 49; 26 ER 15, 33

21. http://www.law.cornell.edu/rules/fre/index.html

22. http://en.wikipedia.org/wiki/Federal_Rules_of_Evidence

23. http://en.wikipedia.org/wiki/Digital_evidence

24. http://www.snort.org