SAND2015-0745C

Facilitation of Forensic Analysis Using a Narrative Template

Shelby Hopkins, Andrew Wilson, Austin Silva & Chris Forsythe

Sandia National Laboratories

ABSTRACT

Criminal forensic analysis involves examining a collection of clues to construct a plausible account of the events associated with a crime. In this paper, a study is presented that assessed whether software tools designed to encourage construction of narrative accounts would facilitate cyber forensic analysis. Compared to a baseline condition (i.e., spreadsheet with note-taking capabilities) and a visualization condition, subjects performed best when provided tools that emphasized established components of narratives. Specifically, features that encouraged subjects to identify suspected entities, and their activities and motivations proved beneficial. It is proposed that software tools developed to facilitate cyber forensic analysis and training of cyber security professionals incorporate techniques that facilitate a narrative account of events.

KEYWORDS

Cyber Security, Forensic Analysis, Narrative Comprehension, Human Performance

INTRODUCTION

Criminal forensic analysis involves examining a collection of clues to construct a plausible account of the events associated with a crime. Typically, investigators are provided a relatively sparse set of clues and their task is to apply inferential reasoning to formulate alternative interpretations and deductive reasoning to arrive at a conclusion regarding the most likely account. From a cognitive perspective, several processes are involved. The investigator must interpret clues and recognize associations between clues based on general and specific domain knowledge combined with relevant past experience. Clues must be combined to form a narrative that includes basic narrative components such as the entities, their respective motives, the time and place of events, and intentions and causation (Zwaan & Radvansky, 1998). Narratives must undergo critical evaluation and are appraised with respect to the investigator's confidence in alternative interpretations. Forensic analysis can be a mentally demanding activity. With competent professionals, the prevalence of cognitive biases has been documented, with these biases present despite rigorous standards of practice (Kassin, et al., 2013; NAS, 2009).

Given the increasing prevalence and reliance on information networks, there is a growing demand for professionals capable of conducting cyber forensic analysis. However, a gap exists in the supply of qualified professionals and the demand for their services. Furthermore, with the most seasoned cyber security analysts, forensic analysis can be a difficult activity. Consequently, there is need for training and technologies that accelerate the rate at which individuals attain proficiency while enhancing performance for cyber forensic analysis. The current research was undertaken to gain a greater understanding of the cognitive processes that underlie criminal forensic analysis, and particularly, the use of narrative in the analysis cyber crimes. It was asserted that narrative construction is vital to effective forensic analysis, and hypothesized that technology interventions that facilitate and promote the development of narratives will lead to superior performance.

METHODS

Subjects

Subjects consisted of 52 employees of Sandia National Laboratories who responded to a company-wide announcement soliciting volunteers to participate in a research study concerning criminal forensic analysis. Seven subjects were eliminated due to the data files associated with their narrative analysis being unreadable. An additional six subjects were eliminated due to their scores on an OSPAN measure of working memory being well below average (1.5 standard deviations below the mean). The narrative analysis task was extremely difficult casting doubt on the abilities of the least capable subjects to perform at a meaningful level.

Materials

A scenario was composed based on publicized reports of cyber crimes. The scenario involved a fictitious pharmaceutical manufacturer and subjects were given the pretense that they had been asked to investigate a series of suspicious events at this company. The scenario involved three separate crimes committed by three distinct entities operating independently of one another and with different motives and objectives. The first scenario involved a Hacktivist group intent on proving the pharmaceutical company was involved in controversial activities (i.e., biological weapons research). In the second scenario, a criminal organization committed bank fraud with funds stolen from accounts used by the company. The third scenario consisted of intellectual property theft by an employee of the company (i.e., Insider).

For each crime, a collection of clues were identified that realistically, would be available to a corporate security officer conducting a forensic analysis. There were a total of 16 legitimate clues with the Hacktivist thread being the more complex having 8 clues, and the Criminal and Insider threads being somewhat simpler with 4 clues each. There were eight additional clues that served as “red herrings” and had nothing to do with the three crimes. Laminated cards presented a one sentence description of the clues and the associated date the clue was noted. Two cyber forensic analysts reviewed each

scenario and verified that the storyline and clues were plausible and representative of the types of crimes a cyber forensic analyst might actually encounter.

Procedure

Subjects were randomly assigned to one of three experimental conditions (Narrative, Association and Impoverished). There were 14 subjects in the Narrative, 12 in the Association and 13 in the Impoverished condition.

Narrative Condition. Subjects were provided 24 laminated cards with magnetic backings on which the clues and associated dates were printed. Subjects were asked to work at a 57''x 46'' magnetic whiteboard. Subjects arranged the clues by affixing them to the whiteboard, and used dry erase markers (black, blue, green and red) to draw links between clues and boundaries encircling groups of clues, as well as make notes and other markings. As shown in Figure 1, features were provided to facilitate and encourage subjects to construct a narrative. Narrative features included 5 Criminal Entity Cards with labeled spaces for subjects to use dry erase markers to denote the identity of the entities, "What trying to do?" and "Why trying to do it?," and a timeline spanning a period encompassing the dates associated with the clues. The upper right corner of the board was labeled "Red Herrings" to encourage subjects to segregate legitimate and red herring clues and subjects were given 12 annotation cards on which to make notes, 8 context cards to identify contexts, and circular magnets to use as tags with 5 different colors (white, blue, green, yellow, and red) and 6 magnets in each color (total of 30 magnets). The board also had a vertical axis labeled, "Criminal Entities," and a horizontal axis for the timeline with months of the year denoted as tick marks. Once subjects had indicated they understood the assignment, they were given a box with the clues arranged in no particular order and allowed 25 minutes to conduct their analysis.

Association Condition. The Association condition provided the same visuospatial elements as the Narrative condition, but without features to facilitate construction of a narrative. The same laminated cards with clues were provided and work was completed at the whiteboard. However, subjects were only provided with dry erase markers and the colored circular magnets. Subjects were instructed that the goal of this task was to identify clues that were related to one another and then, signify any relationships between the groupings of clues using the dry erase markers or colored magnets

Impoverished Condition. The impoverished condition provided neither the features to facilitate construction of a narrative or the visuospatial elements of the Narrative and Association conditions. Subjects were provided a Microsoft Excel spreadsheet that contained the clues in a randomized order. They were also given a Microsoft Word document that they could use to organize the clues and take notes. Subjects were allowed to use all of the features of Microsoft Excel and Word including copy and paste, sorting, and text formatting.

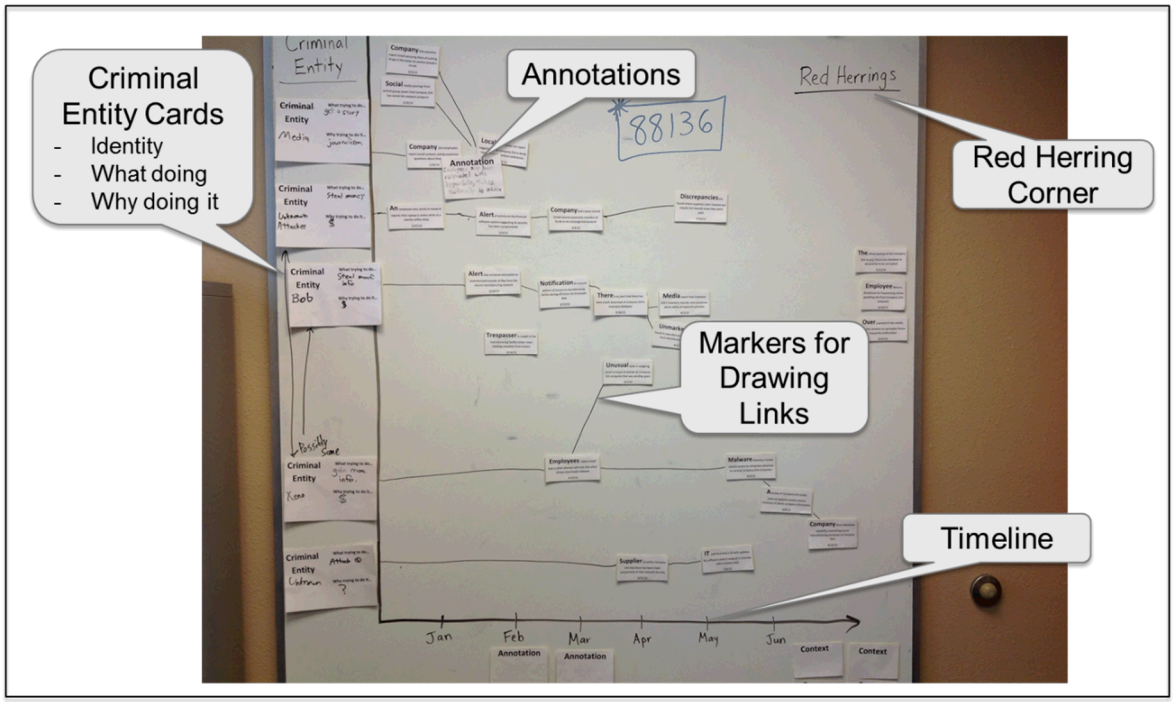

Figure 1 Example of the whiteboard configuration and features provided to subjects in the Narrative condition. Magnetic markers that could be used as tags are not shown here.

Following the forensic analysis, subjects were asked to depict their interpretation of the events using the software tool PlotWeaver. PlotWeaver provides an XML-based graphical interface for events. As shown in Figure 2, in diagraming stories, PlotWeaver allows entities and interactions between entities to be identified as a time-dependent series of events. Subjects were provided a brief tutorial on how to use the key features of PlotWeaver. Once the experimenter had verified that subjects understood these features, subjrcts were given 25 min to create their PlotWeaver interpretation of events. During this time, whiteboard diagrams created by subjects in the Narrative and Association conditions and word documents created by subjects in the Impoverished condition were available and could be referenced at any time.

RESULTS

In scoring the PlotWeaver diagrams, there were many ambiguities due to there being an indirect mapping between the labels created by subjects within PlotWeaver and the actual wording of the clues. To minimize inconsistencies in scoring from one subject to another, most of the plots (80%) were jointly scored by two experimenters. The remaining plots were separately scored by the same two experimenters, with there being a 96% inter-rater reliability.

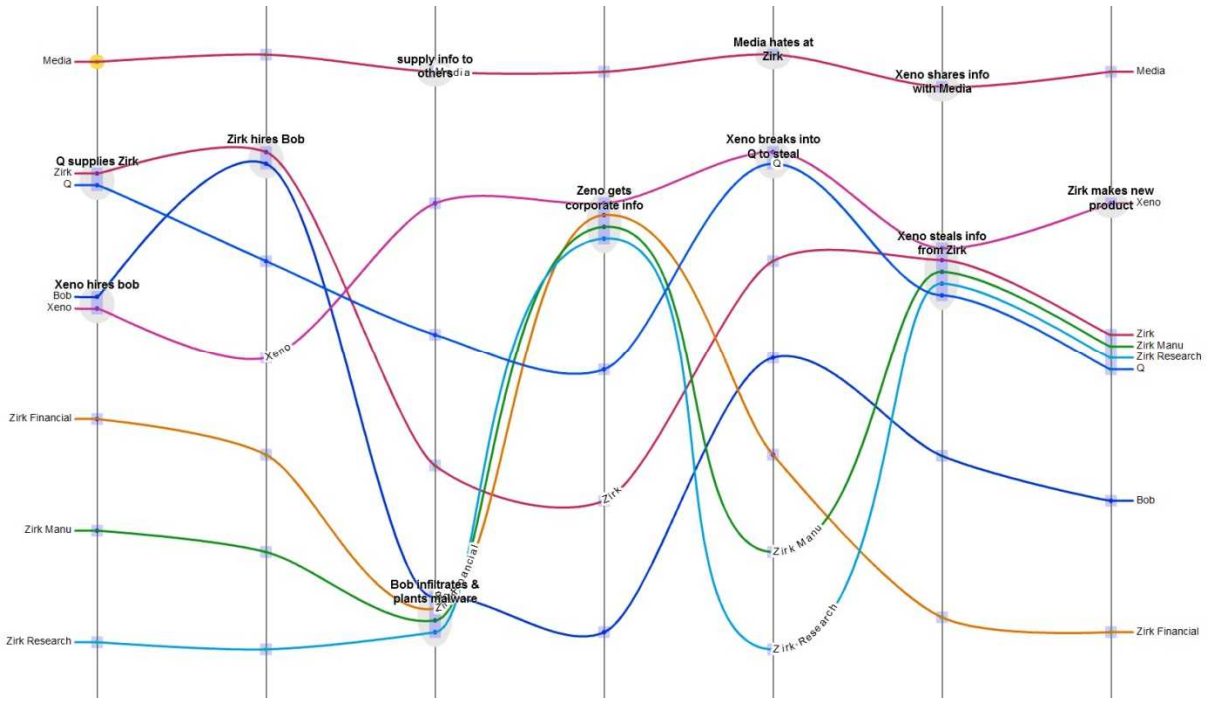

Figure 2. Example of a PlotWeaver diagram illustrating the subject's interpretation of events within the scenario.

Initially, there was a consideration of the clues appearing in the diagrams. It was found that subjects in the Narrative condition used more of the clues in their PlotWeaver diagrams (F=3.49 (df=2); p<0.05). Notably, this difference corresponded to their using more of the legitimate clues (F=3.37 (df=2); p<0.05), with there being little difference in their use of Red Herring clues (F=0.55 (df=2); NS) (See Figure 3).

The second analysis of the PlotWeaver diagrams considered the relationships between clues. If two clues appeared in the same PlotWeaver storyline, it was deemed that the subject believed that there was a relationship, or connection, between the clues. An analysis was undertaken that identified each instance in which subjects expressed a connection between a pair of clues based on them appearing within the same PlotWeaver storyline. It was found that while subjects in the Narrative condition identified more connections between pairs of clues and more connections between pairs of clues consisting of two legitimate clues, these differences were not statistically significant (F=1.72 (df=2); NS and F=1.44 (df=2); NS, respectively). Likewise, differences between experimental conditions for the number of connections between pairs of clues for which one or both clues was a Red Herring was not statistically significant (F=1.63 (df=2); NS).

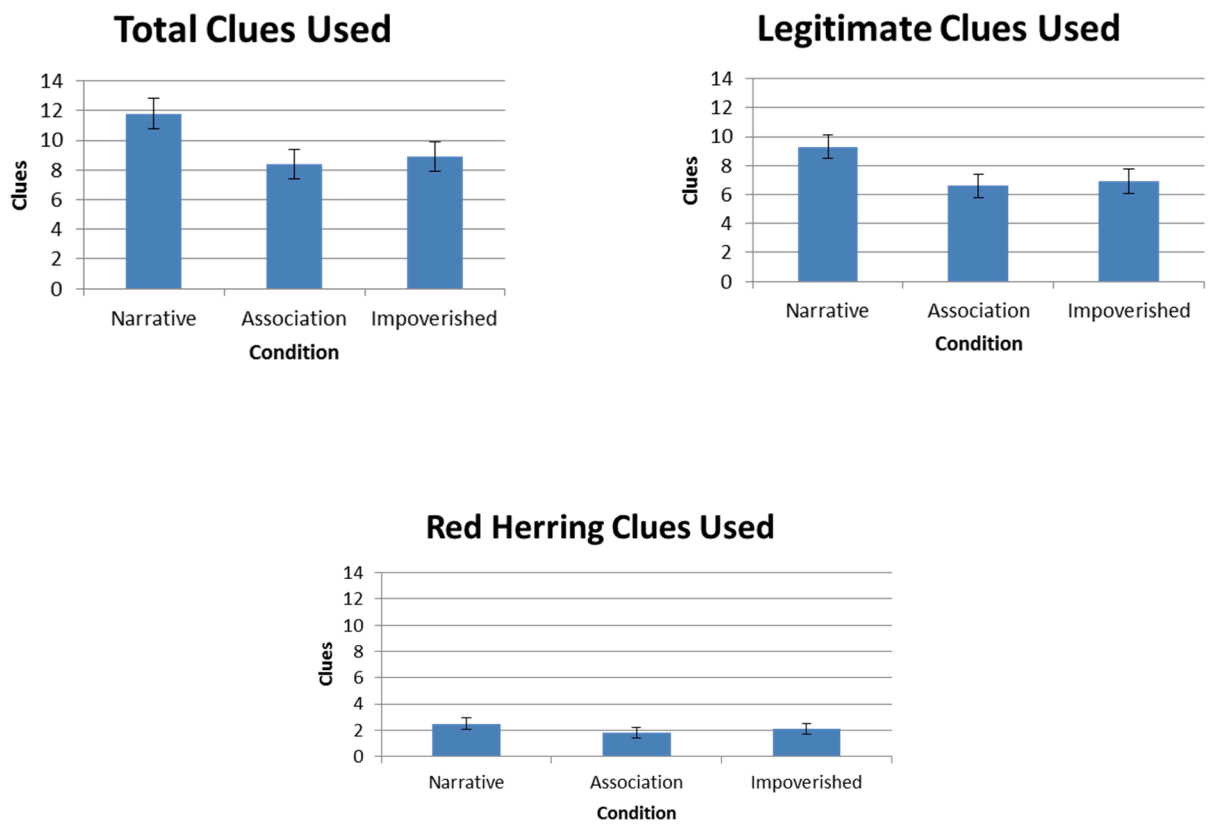

Figure 3. Subjects in the Narrative condition used more of the clues overall with this being a product of their using more of the legitimate clues, with all three groups incorporating approximately the same number of Red Herring clues.

Finally, in comparing the connections identified between clues, there was consideration of the three crimes . These connections would have involved instances in which a connection was identified between a pair of legitimate clues that were both elements of the same crime. There were 28 possible connections for the Hacktivist, and 6 each for the Criminal and Insider. While the subjects in the Narrative condition identified more connections for each crime, there was a statistically significant difference for the Criminal (F=5.68 (df=2); p<0.01), but not for the Hacktivist or Insider (F=0.31 (df=2); NS and F=0.97 (df=2); NS, respectively).

CONCLUSION

Findings suggests that features facilitating and encouraging construction of a narrative account enable subjects to more effectively interpret events within the context of cyber forensic analysis. These results have direct bearing on the software tools provided to cyber security professionals, as well as cyber security education and training. There is currently an extremely lucrative market for software tools to

support cyber security forensic analysis. While these software tools provide essential capabilities, generally, they do not offer utilities to translate the results of data analysis (e.g., packet capture analysis) into a meaningful narrative. Consequently, as has been previously reported, cyber security professionals frequently turn to additional artifacts (e.g., Excel spreadsheets, digital notepads) to facilitate their analysis (Singh et al., 2011), with performance predicted on the basis of the extent to which individuals utilize these supporting artifacts (Silva et al., 2014). While discussed here in the context of cyber security forensic analysis, it may be inferred that the same conclusions apply to other domains that involve the reconstruction of series of events (e.g., law enforcement and medical forensic analysis, accident and root cause analysis, etc.)

ACKNOWLEDGEMENTS

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. (SAND2014-2123 C)

REFERENCES

Conway, A. R., Cowan, N., Bunting, M. F., Therriault, D. J., & Minkoff, S. R. (2002). A latent variable analysis of working memory capacity, short-term memory capacity, processing speed, and general fluid intelligence. Intelligence, 30(2), 163-183.

Kassin, S. M., Dror, I. E., & Kukucka, J. (2013). The forensic confirmation bias: Problems, perspectives, and proposed solutions. Journal of Applied Research in Memory and Cognition, 2(1), 42-52.

National Research Council. (2009). Strengthening forensic science in the United States: a path forward.

Silva, A., McClain, J., Reed, T., Anderson, B., Nauer, K., Abbott, R. & Forsythe, C. (2014). Factors impacting performance in competitive cyber exercises. Proceedings of the Interservice/Interagency Training, Simulation and Education Conference, Orlando FL.

Singh, A., Bradel, L., Endert, A., Kincaid, R., Andrews, C., & North, C. (2011). Supporting the cyber analytic process using visual history on large displays. In Proceedings of the 8th International Symposium on Visualization for Cyber Security (p. 3).

Unsworth, N., Heitz, R. P., Schrock, J. C., & Engle, R. W. (2005). An automated version of the operation span task. Behavior research methods, 37(3), 498-505.

Zwaan, R. A., & Radvansky, G. A. (1998). Situation models in language comprehension and memory. Psychological bulletin, 123(2), 162.