Chapter 22

CONCEPT MAPPING FOR DIGITAL FORENSIC INVESTIGATIONS

April Tanner and David Dampier

Abstract Research in digital forensics has yet to focus on modeling case domain information involved in investigations. This paper shows how concept mapping can be used to create an excellent alternative to the popular checklist approach used in digital forensic investigations. Concept mapping offers several benefits, including creating replicable, reusable techniques, simplifying and guiding the investigative process, capturing and reusing specialized forensic knowledge, and supporting training and knowledge management activities. The paper also discusses how concept mapping can be used to integrate case-specific details throughout the investigative process.

Keywords: Concept mapping, investigative process, knowledge management

1. Introduction

Digital forensic procedures are executed to ensure the integrity of evidence collected at computer crime scenes. Traditionally, the procedures involve the preservation, identification, extraction, documentation and interpretation of computer data [9]. However, due to advancements in technology, digital forensic investigations have moved beyond computers and networks to also encompass portable electronic device, media, software and database forensics [3, 12].

A variety of models have been proposed to improve the digital forensic process; some of the more important ones are investigative models, hypothesis models and domain models. Investigative models focus on the activities that should occur during an investigation [1, 7, 12, 13]. Hypothesis models focus on hypotheses that help answer questions or analyze cases [6]. Domain models concentrate on the information used to examine and analyze cases [3, 4, 14].

G. Peterson and S. Shenoi (Eds.): Advances in Digital Forensics V, IFIP AICT 306, pp. 291–300, 2009.

A common model for the digital forensic investigative process is not yet available. However, a good candidate is the DFRWS investigative process model [12], which was created by a panel of research experts. The DFRWS model defines six phases in a digital forensic investigation: identification, preservation, collection, examination, analysis and presentation. This paper demonstrates how concept mapping can be used to provide an excellent alternative to the checklist approach used in many investigations. In addition, it shows how case-specific details can be integrated with concept maps produced for the six phases of the investigative process.

2. Related Work

Venter [17] has proposed a process flow framework to assist first responders during the identification and collection phases of digital forensic investigations. The framework provides a flowchart-based approach for seizing evidence and a centralized mechanism for recording information collected at a crime scene.

Bogen [3] has created a case domain model that provides a framework for analyzing case details by filtering forensically-relevant information. Bogen's model is based on established ontology and domain modeling methods; artificial intelligence and software engineering concepts are used to express the model. The model provides mechanisms for focusing on case specific information, reusing knowledge, planning for examinations and documenting findings.

Kramer [8] has utilized concept maps to capture the tacit knowledge of design process experts. His focus is on collecting, understanding and reusing the knowledge of multiple domain experts in design processes that drive initial design decisions. His approach illustrates the effectiveness of concept maps in eliciting and representing expert knowledge.

Concept maps are a graphical model for organizing and representing knowledge by expressing the hierarchical relationships between concepts. Concept maps were first used to track and understand the scientific knowledge gained by children [11]. Since then, researchers and practitioners from various fields have used them as evaluation tools and decision aids, to plan curricula, to capture and archive expert knowledge and to map domain information [8, 11].

Figure 1 presents a sample concept map, which itself conveys the key features of concept maps. Concepts are represented as enclosed boxes; the lines show how concepts are related to each other. A concept map is similar to a hierarchically, structured checklist in that it provides an organized, structured way to address key points. Unlike checklists,

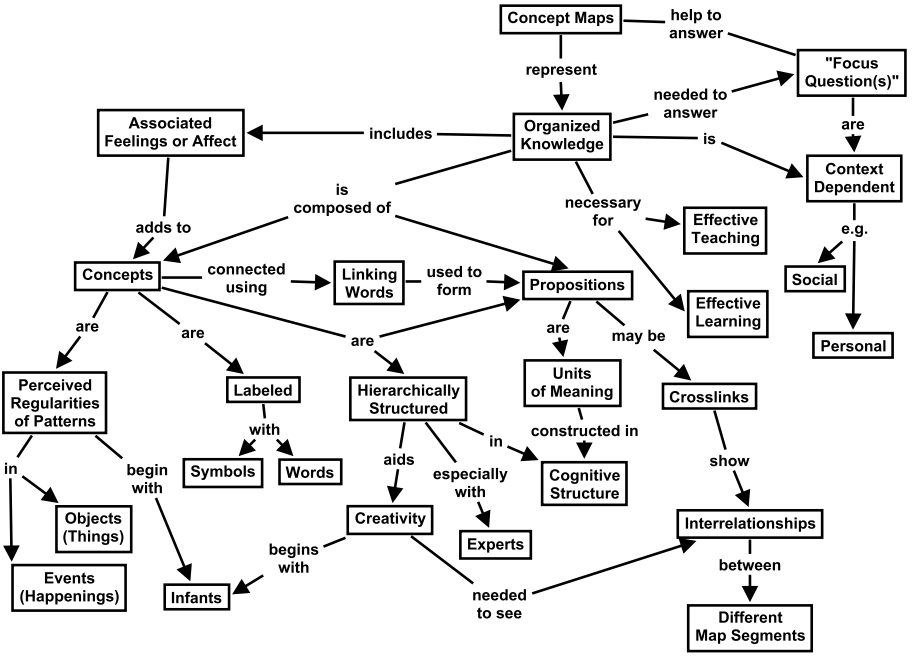

Figure 1. Concept map showing key features of concept maps [11].

however, concept maps show how ideas and concepts are hierarchically linked to each other based on the creator's understanding of the domain. The most inclusive and general concepts are located at the top of the map while more specific concepts are located towards the bottom. Specific event objects, which are not included in boxes, help clarify the meanings of concepts. Prior knowledge of a domain is generally needed to use concept mapping effectively.

Concept maps can be generated manually or using software such as CmapTools. CmapTools, which is used in our work, supports the linking of resources such as photos, images, graphs, videos, charts, tables, texts, web pages, other concept maps and digital media to concepts [11].

Concept maps of the digital forensic investigative process can provide a quick reference of the case domain. Also, they can be used to record case information and to guide novice as well as expert investigators.

3. Modeling the Investigative Process

The digital forensic investigative process has six phases: identification, collection, preservation, examination, analysis and presentation [12]. Checklists and other documents are commonly used to perform specific tasks associated with each phase. However, applying concept

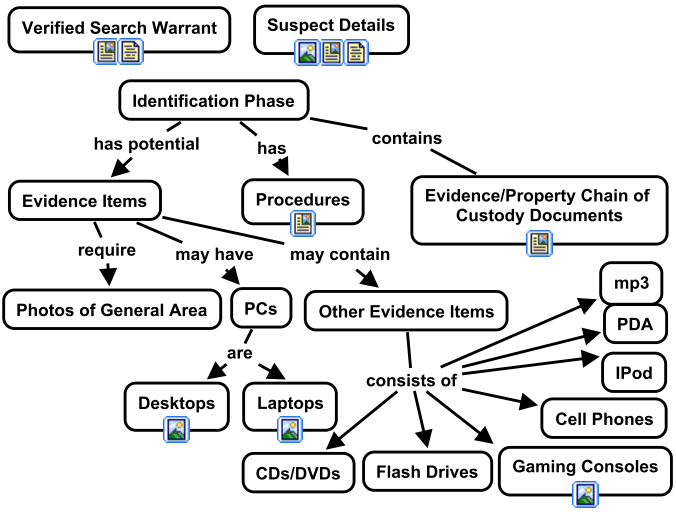

Figure 2. Identification phase concept map.

mapping to model the investigative process can enhance every phase of the process. Figures 2–6, for example, present convenient, graphical views of checklist activities that occur during the key phases of the investigative process. By referring to the concept maps, an investigator can easily determine the actions that should be performed in each phase.

3.1 Identification Phase

The main goal of the identification phase is to determine the items, components and data associated with a crime. The crime scene and evidentiary items should be photographed and documented in detail using proper procedures. According to Kruse and Heiser [9], the computer screen (including open files), the entire computer system and all other potential evidence items should be photographed and documented. Instead of using a checklist for these tasks, Figure 2 provides a graphical view of the steps used to identify digital evidence. The "Chain of Custody Documents" concept shows that specific chain of custody procedures should be followed. The "Evidence Items" concept shows the evidence items that should be identified, and the "Procedures" concept shows the organizational procedures that should be followed.

The concept map can be used by crime scene investigators as a quick reference guide to decide which evidence items should be searched for and as a reminder that the chain of custody should be followed and documented. After all the evidence has been identified and collected, the digital version of the concept map may be augmented to include

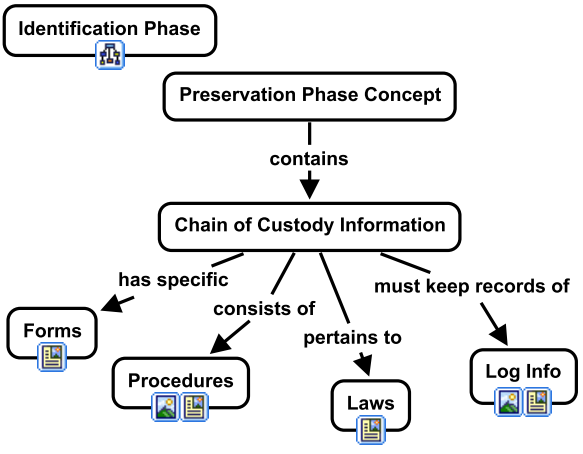

Figure 3. Preservation concept map.

photos, documents and other information obtained from the crime scene. This evidentiary information can be added to the concept map as icons that contain information specific to the case. For example, the "Verified Search Warrant" concept in Figure 2 is associated with an icon that represents a copy of the search warrant. Likewise, the "Photos of General Area" concept could be associated with digital photographs of the crime scene (e.g., computer screen, cabling and network connections).

Note that a concept does not have to be linked to another concept. For example, the "Suspect Details" concept is included in the concept map to provide the investigator with photographs, identifying information and the criminal history of the suspect.

A concept map augmented with icons and related information is very useful for cases that may take years to go to trial. The map could enable an investigator to quickly review the details of the case and the evidentiary items.

3.2 Preservation Phase

Chain of custody is one of the most important tasks associated with the preservation phase [5, 9]. Thorough documentation of the chain of custody helps ensure the authenticity of evidence and refute claims of evidence tampering. It provides complete details about the possession and location of the evidence during the lifetime of a case; these details decrease the likelihood that the evidence will not be admitted in court.

As shown in Figure 3, the chain of custody establishes who collected the evidence ("Forms" concept), how and where the evidence was collected ("Forms" and "Procedures" concepts), who took possession of

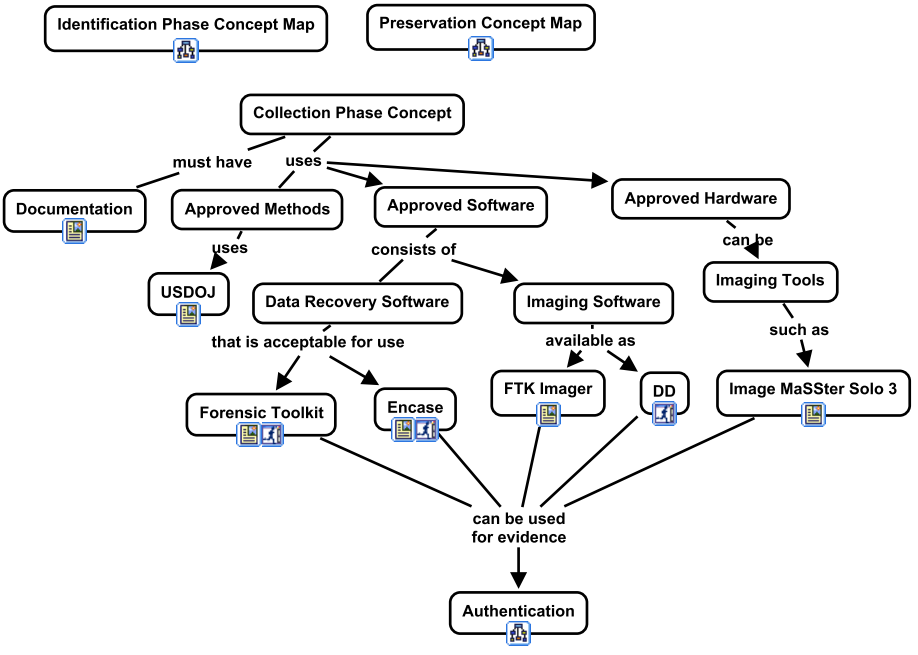

Figure 4. Collection phase concept map.

the evidence ("Log Info" concept), how the evidence was protected and stored ("Forms" concept), and who removed it from storage and the reasons for its removal ("Log Info" concept) [9]. Other tasks associated with the presentation phase include properly shutting down the computer or evidence item, transporting the evidence to a secure location and limiting access to the original evidence, which are found in the "Procedures," "Forms " and "Log Info" concepts, respectively.

3.3 Collection Phase

Evidence collection involves the use of approved recovery techniques and tools, and the detailed documentation of the collection efforts. All the techniques and tools involved in the evidence collection phase are represented as concepts in Figure 4.

The "Documentation" concept in Figure 4 contains a file icon representing the techniques and tools used to collect the evidence. The tools could be launched from their corresponding concept icons. These icons could also contain links to websites and electronic manuals pertaining to the tools. The identification and preservation phase concept maps (Figures 2 and 3) could be accessed directly from the collection phase concept map as well.

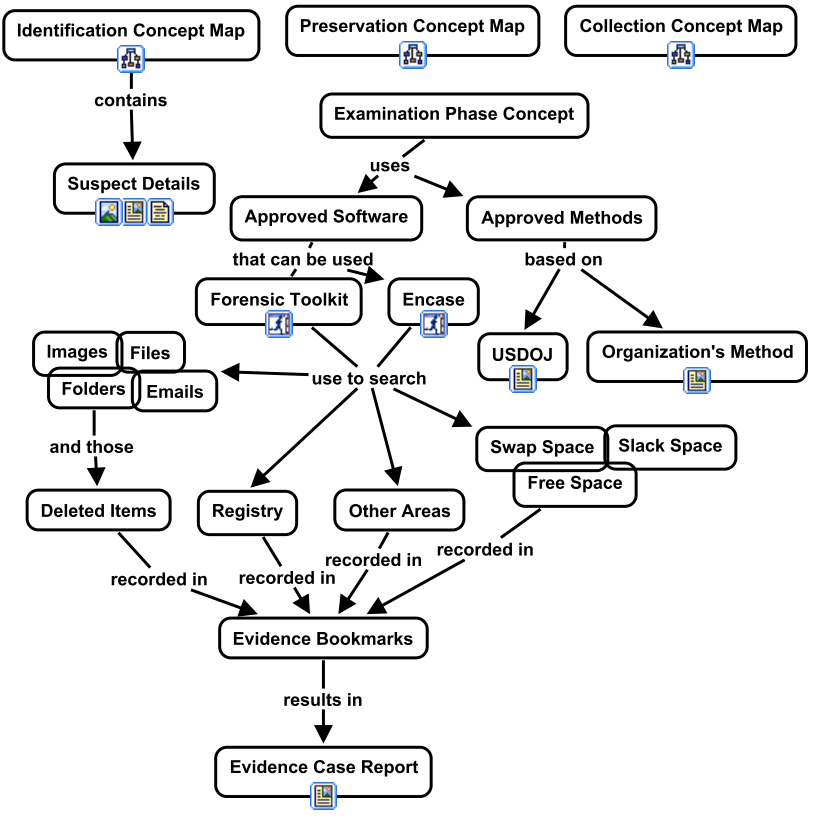

Figure 5. Examination phase concept map.

3.4 Examination Phase

During the examination phase, specialized tools and techniques are used to search for and identify evidence [10]. Evidence may exist in files, emails, images, folders and hidden space on the disk (e.g., slack space, swap space and free space), the registry and other areas as shown in Figure 5. Tools such as the Forensic Toolkit (FTK) and Encase are often used to examine these areas more effectively; these tools also reduce the amount of time spent searching for evidence. Individuals should be trained to operate forensic tools and should use them with utmost care because evidence authenticity is of prime importance.

The "Forensic Toolkit" and "Encase" concepts in Figure 5 have executable icons that could allow the examiner to launch the software and begin examining the evidence. The "Suspect Details" concept is included to accommodate keywords and keyword variations that could assist the examiner in finding more evidence. Bookmarks containing pic-

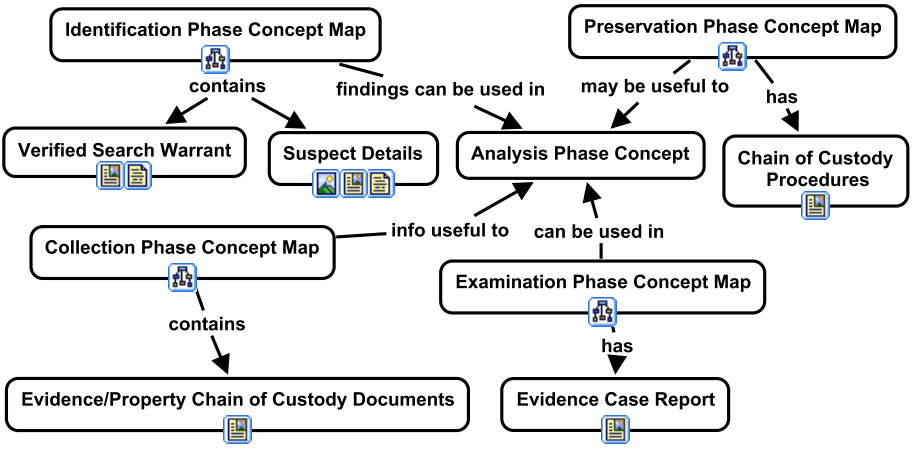

Figure 6. Analysis phase concept map.

tures, video, emails, files and other items may be used to document the evidence. These bookmarks could be included in the final evidence case report, which is accessible via the icon associated with the "Evidence Case Report" concept.

3.5 Analysis Phase

The analysis phase involves reconstructing all the evidentiary findings in order to theorize what occurred [16]. The evidence collected during the examination phase is used to create event timelines, relationships between the evidentiary items and criminal intent.

Concept maps are useful in the analysis phase because they can be used to create event timelines of events from the evidence case report and suspect details. Moreover, concept maps help clarify how the evidentiary items are related to each other. All the evidential findings can be placed in one location and accessed via concept icons. Beebe and Clark [2] state that "data analysis is often the most complex and time-consuming phase in the digital forensic process." Figure 6 provides a good example of how concept maps can provide organization, structure and easy accessibility to the evidence, case details, procedures and chain of custody documentation during the analysis phase.

3.6 Presentation Phase

Every task in the previous five phases plays a role in the presentation of evidence in court. The presentation phase is very important because it is where the legal ramifications of the suspect's actions are determined.

The investigator must be able to show exactly what occurred during the identification, collection, preservation, examination, and analysis phases of the investigation. Often, specialized tools and techniques are used to present the findings in court proceedings [5]. As shown in Figure 6, concept maps provide an attractive alternative for presenting the findings in an organized manner. The investigator would be able to show the court exactly what tasks were performed to obtain the evidence, what evidence was found, and the steps taken to ensure evidence authenticity.

4. Conclusions

Concept mapping can enhance every phase of a digital forensic investigation. The principal benefits are an intuitive graphical view of the investigative process and a simple method for documenting and storing case-specific information such as evidence, case reports, chain of custody documents and procedures. Concept maps also provide a framework for creating a digital forensic repository where case-specific concept maps and specialized techniques can be accessed and shared by the law enforcement community. Other benefits include the ability to uncover misunderstandings in the investigative process, create knowledge management strategies specific to criminal investigations, and provide training and support to novice and expert investigators.

References

[1] V. Baryamureeba and F. Tushabe, The enhanced digital investigation process model, *Proceedings of the Fourth Digital Forensic Research Workshop*, 2004.

[2] N. Beebe and J. Clark, A hierarchical, objectives-based framework for the digital investigation process, *Proceedings of the Fourth Digital Forensic Research Workshop*, 2004.

[3] A. Bogen, Selecting Keyword Search Terms in Computer Forensic Examinations using Domain Analysis and Modeling, Ph.D. Dissertation, Department of Computer Science and Engineering, Mississippi State University, Mississippi State, Mississippi, 2006.

[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] D. Brezinski and T. Killalea, RFC3227: Guideline for Evidence Collection and Archiving, Networking Working Group, Internet Engineering Task Force (www.ietf.org/rfc/rfc3227.txt), 2002.

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

[7] S. Ciardhuain, An extended model of cybercrime investigations, *International Journal of Digital Evidence*, vol. 3(1), 2004.

[8] M. Kramer, Using Concept Maps for Knowledge Acquisition in Satellite Design: Translating "Statement of Requirements on Orbit" to "Design Requirements," Ph.D. Dissertation, Graduate School of Computer and Information Sciences, Nova Southeastern University, Fort Lauderdale-Davie, Florida, 2005.

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

[10] M. Noblett, M. Pollitt and L. Presley, Recovering and examining computer forensic evidence, *Forensic Science Communications*, vol. 2(4), 2000.

[11] J. Novak and A. Canas, The Theory Underlying Concept Maps and How to Construct and Use Them, Technical Report IHMC Cmap Tools 2006-01, Florida Institute for Human and Machine Cognition, Pensacola, Florida, 2006.

[12] G. Palmer, A Road Map for Digital Forensic Research, DFRWS Technical Report, DTR-T001-01 Final, Air Force Research Laboratory, Rome, New York, 2001.

[13] M. Pollitt, An ad hoc review of digital forensic models, *Proceedings of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering*, pp. 43–54, 2007.

[14] G. Ruibin, T. Yun and M. Gaertner, Case-relevance information investigation: Binding computer intelligence to the current computer forensic framework, *International Journal of Digital Evidence*, vol. 4(1), 2005.

[15] United States Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Washington, DC (www.usdoj.gov/criminal/cybercrime/s&smanual2002.pdf), 2002.

[16] J. Vacca, *Computer Forensics: Computer Crime Scene Investigation*, Charles River Media, Boston, Massachusetts, 2005.

[17] J. Venter, Process flow diagrams for training and operations, in *Advances in Digital Forensics II*, M. Olivier and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 331–342, 2006.