Chapter 11

USING A GOAL-DRIVEN APPROACH IN THE INVESTIGATION OF A QUESTIONED CONTRACT

Clive Blackwell, Shareeful Islam and Benjamin Aziz

Abstract This paper presents a systematic process for describing digital forensic investigations. It focuses on forensic goals and anti-forensic obstacles and their operationalization in terms of human and software actions. The paper also demonstrates how the process can be used to capture the various forensic and anti-forensic aspects of a real-world case involving document forgery.

Keywords: Forensic investigation, goal-driven process, questioned documents

1. Introduction

There is an acute need to extend the typical digital forensic investigation process to handle complex cases involving large quantities of data from multiple computers and devices. The investigation process must cope with the many difficulties inherent in evidence collection and analysis from intentional and deliberate causes that may result in evidence being incorrect, incomplete, inconsistent or unreliable.

Many of the existing digital forensic investigation processes emphasize collecting evidence or directly starting with the incident. The processes generally involve steps such as collecting, preserving, examining, analyzing and presenting digital evidence [14–16, 19]. In addition, many investigations are bottom-up, focusing on the collection and analysis of data using an exhaustive search of the media based on keywords and regular expressions. However, it is often infeasible to examine all the supplied media. Also, as Casey and Rose [5] emphasize, it may be ineffective – vital evidence is often missed because there are no matches for low-level patterns.

G. Peterson and S. Shenoi (Eds.): Advances in Digital Forensics IX, IFIP AICT 410, pp. 153–167, 2013.

A systematic reasoning process for analyzing digital forensic investigation requirements is currently unavailable. Additionally, a forensic investigation should address problems posed by anti-forensics, especially when time, cost and resources are critical constraints in the investigation. To address these needs, this paper presents a goal-driven methodology to specify the requirements of a digital forensic investigation. The proposed systematic process initiates with the identification of the main goals of the investigation and the analysis of the obstacles that could hinder the goals. The process integrates the anti-forensics dimension within the digital forensic investigation process at the level of requirements that overcome the deliberate obstacles. In this way, the methodology supports existing forensic processes by offering a systematic investigation strategy to manage evidence so that it helps attain the investigative goals and overcome the technical and legal impediments in a planned manner.

Many formal methodologies have been proposed for requirements engineering and analysis, including i*/Tropos [7] and KAOS [20]. Our approach follows KAOS in line with existing work [1]. According to Leigland and Krings [13], adopting a formal and systematic approach has several benefits: (i) procedural benefits by reducing the amount of data and aiding their management; (ii) technical benefits by allowing digital forensic investigations to adapt to technological changes; (iii) social benefits by capturing the capabilities of the perpetrators within the social and technical dimensions; and (iv) legal benefits by allowing the expression of the legal requirements of forensic investigations.

The systematic process is demonstrated on a recent case involving alleged document forgery and questionable claims made by Paul Ceglia against Mark Zuckerberg of Facebook [18]. The analysis helps outline the main obstacles to the various claims and evidence in the case. Also, it proposes how the requirements underlying the claims and evidence are operationalized by means of investigator activities along with forensic system and software operations.

2. Related Work

Several researchers have discussed the forensic investigation process and techniques relating to anti-forensics. This section presents a brief overview of the approaches relevant to this work.

Kahvedzic and Kechadi [11] have presented a digital investigation ontology as an abstraction of concepts and their relationships for the representation, reuse and analysis of digital investigation knowledge. The ontology is based on four dimensions: crime case, evidence location, in-

formation and forensic resource. The approach has been used to model knowledge about the Windows registry.

Reith, *et al.* [16] have proposed an abstract digital forensics model comprising components such as the identification, preparation, analysis, presentation and return of evidence. The model supports future digital technologies and understanding by non-specialists.

Hunton [10] has used utility theory for cyber crime execution and analysis. The work shows that law enforcement officers could leverage cyber crime execution and analysis models when investigating crimes to support the analysis of the evidence regardless of the level of complexity of the crime.

Carrier and Spafford [4] consider a computer or other digital device involved in a crime as a digital crime scene. They employ a process model for forensic investigations that comprises five phases: readiness, deployment, physical/digital crime scene investigation and presentation. Huber, *et al.* [9] have presented techniques for gathering and analyzing digital evidence from online social networking sites.

Harris [8] has discussed techniques for destroying, hiding and eliminating evidence resources as part of anti-forensic activities. Dahbur and Mohammad [6] identify time, cost, forensic software vulnerabilities, victim privacy and the nature of the digital evidence as the main challenges posed by anti-forensic activities.

Several of the works mentioned above focus on systematic forensic investigation processes with an emphasis on collecting and analyzing evidence. However, the systematic process presented in this paper stands out because it combines forensic and anti-forensic considerations in a single investigative framework.

3. Proposed Process

Figure 1 shows the proposed systematic process. The process begins with understanding the investigation processes starting with the incident context analysis and ending with the appropriate actions for analyzing the evidence.

The systematic process considers anti-forensic issues during the forensic investigation process so that possible obstructions can be identified, analyzed and overcome. The process consists of four activities that define the major areas of concern. Each activity incorporates steps concerning the creation of artifacts such as goals, obstacles, evidence and forensic actions relating to the incident. The artifacts are incrementally combined to produce the incident report containing textual and graphical representations. The process defines the roles that take responsibility for

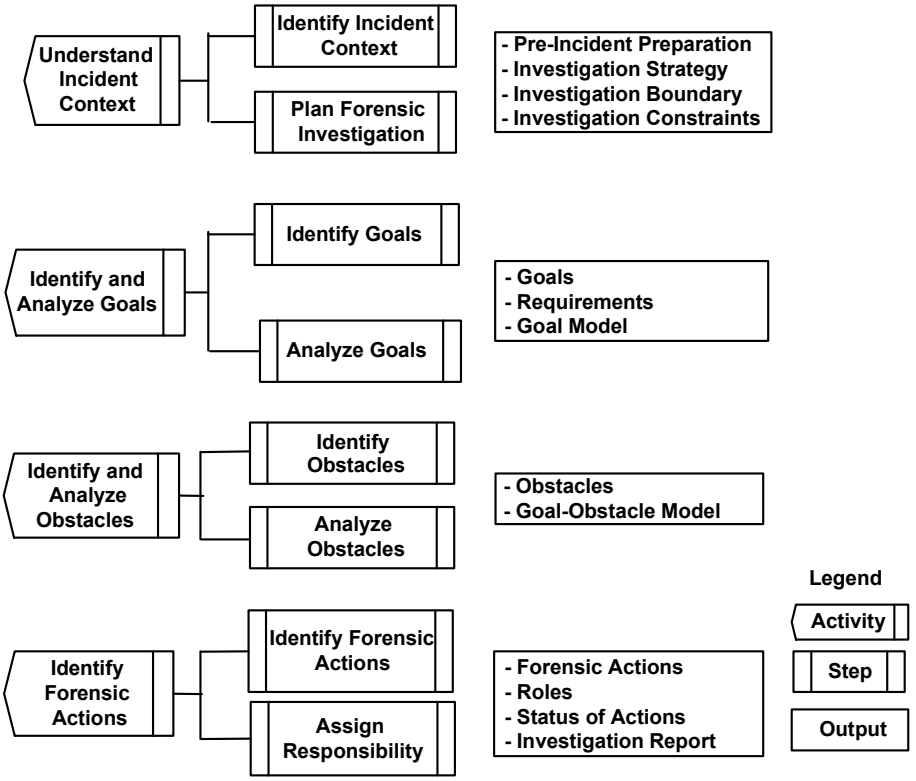

Figure 1. Systematic process for digital forensic investigations.

specific artifacts and perform actions that produce or modify artifacts. The activities are performed sequentially and, if necessary, a number of iterations of individual activities may be performed until they are completed.

3.1 Activity 1: Understand Incident Context

The first activity is to understand the background of the incident. This includes pre-incident preparation, choosing the investigation team, determining the investigation strategy, discovering the complexity and severity of the incident, and establishing the boundary of the forensic process. After the incident context is identified, the forensic team formulates a plan for performing the investigation. This involves choosing a strategy to isolate, secure and preserve the state of the physical and digital evidence. The plan should consider the investigation constraints such as media size, time and budgetary restrictions, and availability of resources such as tools, equipment and expertise.

3.2 Activity 2: Identify and Analyze Goals

After the incident context is defined, the next activity is to identify and model the goals of the forensic investigation. Forensic investigations have primary goals such as conducting a successful investigation and collecting and preserving evidence. The explicit determination of the goals aids in the justification and delineation of the scope of the investigation. The goals may also include suggesting investigative leads and abandoning fruitless leads, as well as proving cases by discovering and overcoming potential weaknesses.

The next step in the activity is to analyze the identified goals so that the higher-level goals are refined into sub-goals. In particular, this step considers how the various phases of the investigation process link the sub-goals with the main goal and support incident analysis. For example, collecting evidence as a goal can be refined to gathering evidence from different systems, devices and the Internet, possibly from unusual locations. In the Ceglia case [18], information was found that pointed to other locations where important evidence might be located, such as undisclosed email accounts and third party systems belonging to Ceglia's lawyers.

The sub-goals may be linked by AND or OR refinement relations to construct the goal model. An AND refinement specifies that all the sub-goals must be satisfied for the parent goal to be satisfied, while an OR refinement specifies that any one of the sub-goals is sufficient to satisfy the parent goal [20].

3.3 Activity 3: Identify and Analyze Obstacles

Obstacles hinder the ability to achieve the goals. Therefore, obstacle identification and analysis focus on what could go wrong during a forensic investigation, specifically with regard to evidence collection, preservation and analysis. It is necessary to identify all the plausible obstacles to determining the facts about an incident. Determining the obstacles in advance facilitates the selection of a course of action to overcome them.

This step assesses the potential damage to the overall investigation caused by obstacles. These include difficulties in finding evidence, exhausting the anticipated time and resources, dealing with the manipulation of essential metadata such as hashes and timestamps, and storing data anonymously on the Internet rather than locally.

Generally, the evidence should be admissible (must be able to be used in court), authentic (original and unchanged), reliable (correct and accurate), complete (all relevant evidence is available) and believable (easy to understand and credible to a jury). An obstacle can affect the

integrity, completeness, reproducibility, timeliness and believability of a forensic activity as well as the outputs of the activity. Obstacle analysis focuses on understanding the types of obstacles posed by anti-forensic actions.

3.4 Activity 4: Identify Forensic Actions

The final activity of the process is to identify the appropriate forensic actions that must be applied based on the critically of the incident. These actions operationalize goal satisfaction to determine a suitable response strategy to resolve the incident. In order to choose the appropriate actions, it is necessary to understand the risks due to the occurrence of the incident and the obstacles posed by anti-forensic activities. Risk has various dimensions such as financial loss, loss of reputation and privacy, and intellectual property theft. Before choosing the actions, it is necessary to consider the legal constraints regarding notifications to regulatory authorities and the quality of the documentation of the investigative goals and requirements.

Consider for example the Ceglia v. Zuckerberg and Facebook case discussed below, which examined the authenticity of a business contract and the supporting evidence such as relevant emails. An obstacle would exist if a copy rather than the original contract were to be provided and the supporting evidence suggests that it could be authentic. Hence, the forensic actions would focus on the use of low-level tools to find anomalies in metadata and timestamps pertaining to the copy.

The selected forensic actions should be implemented to successfully complete the investigation. Also, the effectiveness of the implemented control actions should be monitored.

4. Case Study

The application of the systematic process is demonstrated using a civil case filed in 2010 by Paul Ceglia against Mark Zuckerberg and Facebook.

According to the complaint, Paul Ceglia, an entrepreneur, engaged Mark Zuckerberg to perform some work on his StreetFax Project around the time that Zuckerberg founded Facebook in 2003. Ceglia paid Zuckerberg $1,000 for work on StreetFax and also claimed that he paid $1,000 to fund Zuckerberg's "face book project." He produced a work for hire contract that was apparently signed by himself and Zuckerberg covering the two projects [2]. According to Ceglia, the agreement stated that Ceglia would get 50% of the "face book project" in exchange for funding its initial development. Zuckerberg clearly discussed Facebook with

Ceglia; this fact was supported by multiple email exchanges between the two parties.

The court ordered Mr. Ceglia to produce relevant electronic assets such as an electronic copy of the contract, copies of the purported emails, and the computers and electronic media under Ceglia's control. The court also issued an electronic asset inspection protocol for inspecting the collected evidence, requesting that the investigators check the authenticity and availability of the evidence and provide a report to the court.

The digital forensic analysis was provided in an expert report by Stroz Friedberg [18] for Zuckerberg, which was made public after it was submitted to the court. Several expert reports related to the physical evidence were also provided, especially those by LaPorte [12] and Romano [17].

4.1 Activity 1: Understand Incident Context

This activity focuses on understanding the issues related to the investigation. The main scope of the investigation is to confirm the authenticity of the claims submitted by Ceglia pertaining to the work for hire contract and purported emails, including checking the timestamps and formats of the collected evidence. In addition, the evidence has to be forensically sound to support the electronic asset inspection protocol and it should be possible to identify if any of the evidentiary materials are forgeries.

A crucial first step is to acquire all of Ceglia's computer equipment and other devices that he used in his dealings with Zuckerberg, such as his parents' computer that was found to contain the original contract, and to discover and preserve evidence from his online activities, including his use of multiple email accounts. The complexity of the investigation mainly arises from the quantity of electronic data from different geographical locations and the need to preserve and check all the possible evidence. The digital evidence was contained in three hard drives, 174 floppy disks and 1,087 CDs. The relevant evidence was in the form of image files, email communications, and draft and deleted documents. Appropriate skills and tools exist for the investigation, and we do not consider issues such as investigation team management and time and budget in this case study.

4.2 Activity 2: Identify and Analyze Goals

The goal of the defense in the Ceglia case is to prove that the work for hire contract is a forgery. This would result in the failure of Ceglia's

claim of part ownership of Facebook because it is the only evidence available that could prove Ceglia's version of the events. The main goal, as shown in Figure 2, can be refined into sub-goals related to the production and analysis of all the relevant computer and electronic media, including the purported contract and email correspondence.

A generic goal tree for document forgery developed for similar cases can help determine an initial approach that focuses attention on the likely evidence and its potential locations. The goal tree has three branches to demonstrate the invalidity of the work for hire document, and an additional branch to show that the case fails on technical grounds due to withheld or spoiled evidence.

In theory, it is sufficient to prove forgery in only one way, so the goal is an OR refinement of the four possibilities shown in Figure 2. However, the proof of forgery should be considered in multiple ways to ensure that the case is resilient to unanticipated new evidence and legal challenges.

We decomposed all four branches of the goal tree, but choose to explain only the most convincing branch that makes the fewest assumptions by directly attempting to show that the contract is a forgery. This is adequate because Ceglia's case would fail because the purported contract is the only compelling evidence for his claim.

4.3 Activity 3: Identify and Analyze Obstacles

Several obstacles impede the goal of the investigation to show that the work for hire contract is a forgery. Obstacles to a direct proof of forgery are the lack of original documents; only copies are available to support the contract. Figure 3 shows the goal tree for overcoming the obstacles in this branch. The obstacles slope in the opposite way than do goals, are colored gray and have dotted borders. The figure also shows that further goals overcome many of the obstacles as children of the obstacle nodes, but any obstacle without a child goal node is not surmounted. The evidence is convincing in this case. However, in other cases of alleged document forgery, the obstacles to direct proof may be considerable. This may require other branches that provide weaker substantiation to be investigated instead (Figure 2).

The two primary pieces of evidence supplied by Ceglia are the alleged work for hire contract and supporting emails. There is the apparent authenticity of the contract based on its content, and the supporting emails appear to give a consistent account that supports Ceglia's version of the events. An important obstacle to proving forgery is that the original contract and supporting email messages are not available. Therefore, the investigation has to rely on secondary evidence from deleted and

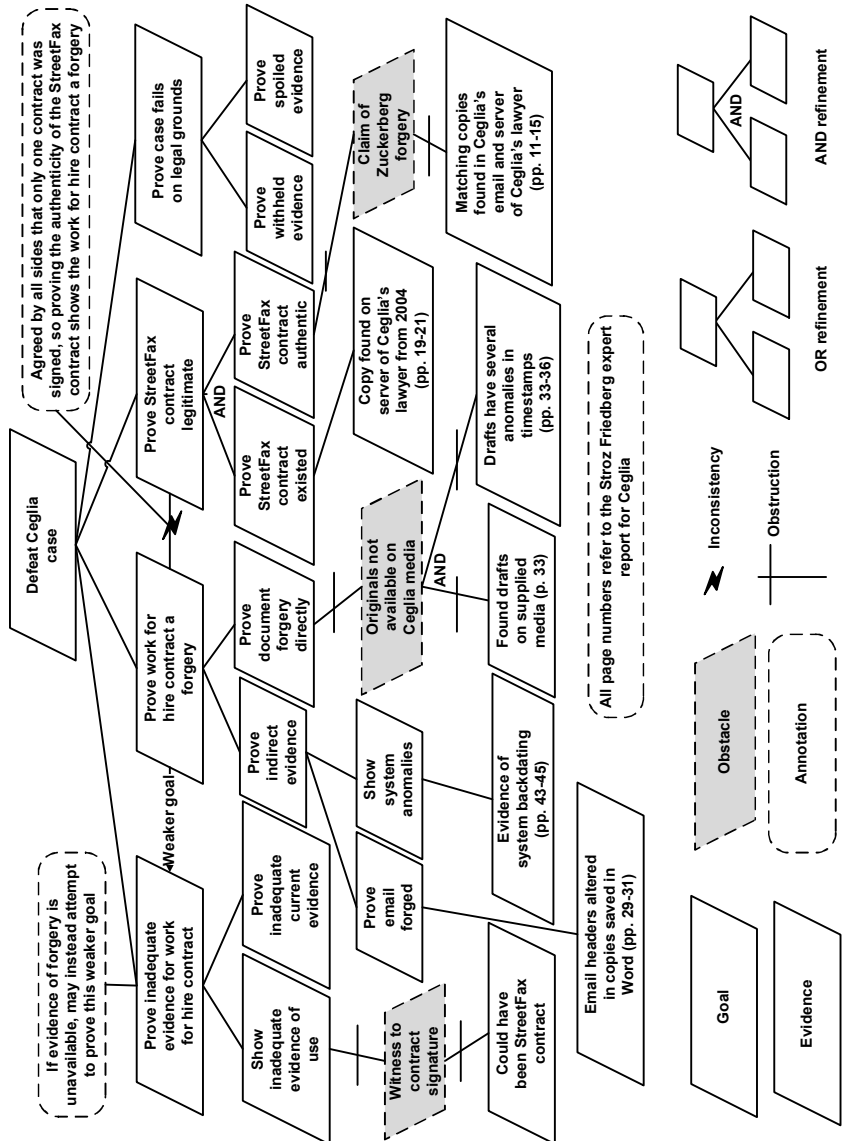

Figure 2. Ceglia case overview.

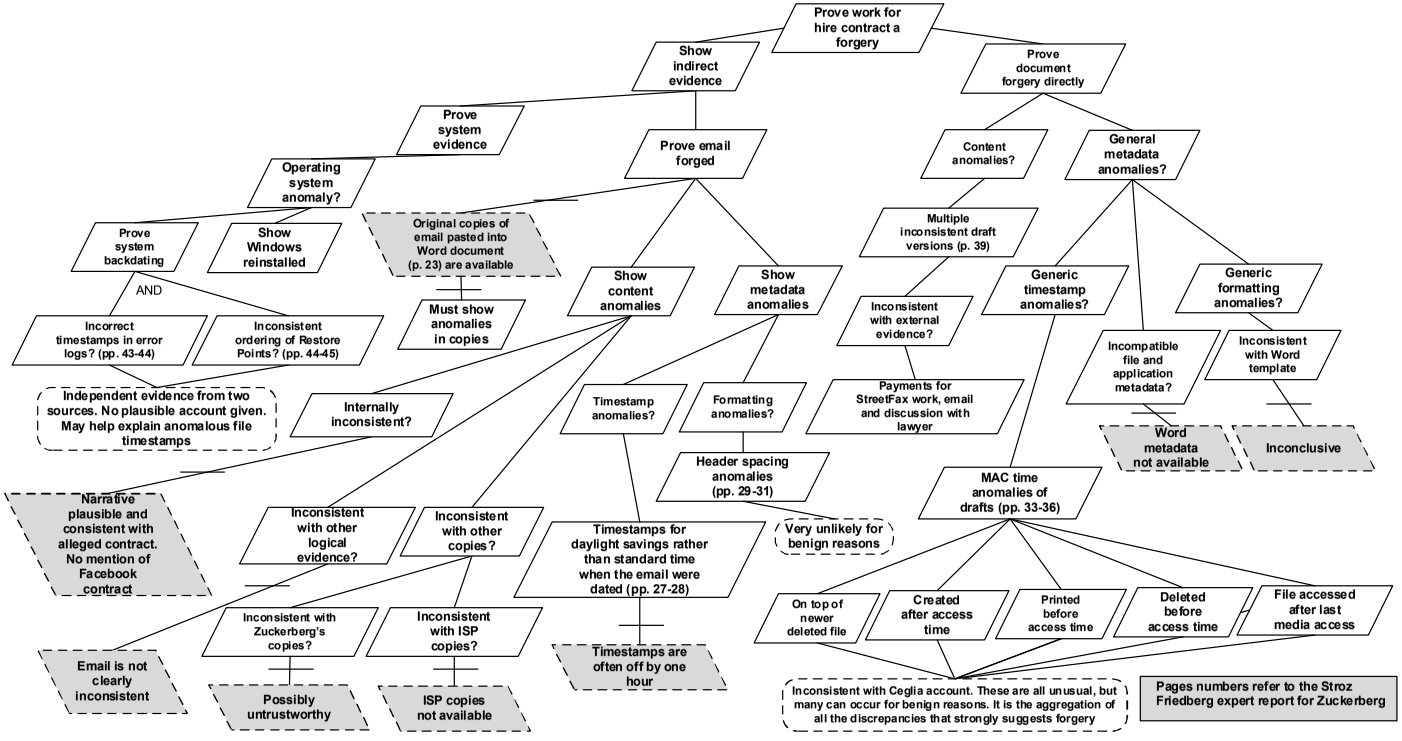

Figure 3. Decomposition of part of the goal tree to prove that the work for hire contract is a forgery.

draft contract files, and email messages that were cut and pasted into a Word document. However, the purported emails have formatting discrepancies in their headers that are inconsistent and indicate that the emails were manually typed and edited after being copied to the Word document. There is evidence of possible spoliation, especially due to multiple re-installations of the Windows operating system and the deletion and overwriting of relevant files. Therefore, the obstacles in this case are mainly unverified and incomplete evidence, with the primary evidence being unavailable because no exact copies of the work for hire document were found on the media.

4.4 Activity 4: Identify and Execute Actions

The forensic actions need to achieve sufficient goals and overcome obstacles to achieve the primary goal of showing that the work for hire contract is a forgery. Most of the nodes are OR branches, so only one path with sufficient evidence from a leaf node to the root is necessary, and there are always alternatives for bypassing insurmountable obstacles. However, as mentioned above, it is safer to prove a case in multiple ways. Therefore, each branch of the primary goal tree in Figure 2 is decomposed to prove the case in four different ways.

In the first branch, there is no independent evidence for the work for hire contract, except for the eyewitness who witnessed a contract signature, but the StreetFax contract has better provenance and it is more likely that it was in fact signed. The third branch contains convincing evidence for the authenticity of the StreetFax contract, which shows the work for hire contract to be a forgery, because there was only one contract between the two parties. In his expert report for Ceglia, Broom [3] gave an alternative hypothesis that Zuckerberg or his agents could have forged the StreetFax contract. However, this is convincingly refuted by the discovery of the StreetFax contract independently in Ceglia's email and on a server belonging to Ceglia's lawyer from 2004, six years before the case was filed [18]. The fourth branch checks for evidence spoliation and evidence withholding. The evidence includes the deletion of relevant files such as the StreetFax contract and draft work for hire documents, the deletion of email messages and the deactivation of email accounts in an apparent attempt to avoid discovery. Multiple operating system re-installations that overwrote the data on the hard disk is evidence of spoliation, but this could also have an innocent explanation.

The second branch demonstrates the evidence that the work for hire contract is a forgery (Figure 3). Although the content appears plausible, the metadata provides evidence of forgery. Several actions lead to

convincing evidence, including checking for inconsistency in email messages. The emails give a plausible account and support. Additionally, the physical tests demonstrate beyond reasonable doubt that the work for hire contract was created using a fake page 2 attached to the legitimate page 1 from the StreetFax contract. This was demonstrated in multiple ways by experts, especially LaPorte [12] and Romano [17], who showed that different toners and inks were used on the two pages. We do not discuss this further because it is outside the domain of digital forensics.

The artifacts produced from the previous activities are incrementally combined to produce the forensic investigation report. The report should also include the status of the implemented forensic actions and their effectiveness. Although, the expert report for Zuckerberg by Stroz Friedberg [18] was comprehensive and highlighted all the relevant points, a more systematic exposition of the overall argument would have provided a clearer narrative.

5. Discussion

The Caglia v. Zuckerberg and Facebook case demonstrates that many useful points of a systematic goal tree analysis can be incorporated into forensic investigations. These include:

- Reuse of knowledge about previous similar cases, shown by the common upper branches of the goal tree.
- Formulation and execution of an investigation strategy and advance planning to overcome known obstacles, such as analyzing copies of the contract and email messages rather than the originals.
- Formulation and analysis of alternative hypotheses, such as if the anomalies in the time zones in email headers indicate fraud or have alternative explanations.
- Clarification of the reliance on assumptions. The opposing parties agreed that only one contract was signed by Zuckerberg, an assumption needed to prove that the work for hire contract is a forgery after showing that the StreetFax contract is authentic.
- Explanation of the overall argument in the case by combining all the claims in each branch into a coherent, comprehensive and consistent narrative.

One limitation is the absence of a detailed analysis of timelines and timestamps that is crucial to most investigations. The goal tree de-

composition may suggest possible avenues for investigation by creating requirements to discover anomalous temporal metadata, but they would be broad and possibly difficult for an analyst to perform. We plan to investigate how the goal tree analysis may inform and integrate with a timeline tool.

6. Conclusions

The systematic digital forensic investigation process presented in this paper has four main activities for understanding the context of incidents. The activities include the identification and analysis of the goals, the identification and analysis of obstacles, the identification and execution of the required actions, and the operations that must be applied to satisfy the main investigation goals. The application to the real-world contract forgery case of Ceglia v. Zuckerberg and Facebook demonstrates that the process can effectively capture the various forensic and anti-forensic aspects of an investigation.

Our future research will focus on defining a framework for the extraction of common patterns for describing goal-driven digital forensic investigations along with their obstacles and operationalization. Document forgery as in Ceglia v. Zuckerberg and Facebook would be an excellent domain to investigate. A limitation of the paper is the use of an existing case study, which is overcome by comprehensively modeling the entire case. To address this limitation, we plan to construct a general model that could be applied to document forgery cases. Additionally, we plan to utilize formal languages and formal verification tools to provide more rigor in specifying forensic investigations and to prove claims with a high level of assurance.

References

[1] B. Aziz, Towards requirements-driven digital forensic investigations, *Proceedings of the Second International Conference on Cyber Crime, Security and Digital Forensics*, 2012.

[2] H. Blodget, The guy who says he owns 50% of Facebook just filed a boatload of new evidence – and it's breathtaking, *Business Insider*, April 12, 2011.

[3] N. Broom, Declaration of Neil Broom, Paul D. Ceglia v. Mark Elliot Zuckerberg and Facebook, Inc., United States District Court, Western District of New York, Civil Action 1:10-cv-569-RJA-LGF, Technical Resource Center, Atlanta, Georgia, 2012.

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

[5] E. Casey and C. Rose, Forensic analysis, in *Handbook of Digital Forensics and Investigation*, E. Casey (Ed.), Elsevier Academic Press, Burlington, Massachusetts, pp. 21–62, 2010.

[6] K. Dahbur and B. Mohammad, The anti-forensics challenge, *Proceedings of the International Conference on Intelligent Semantic Web-Services and Applications*, article no. 14, 2011.

[7] A. Fuxman, R. Kazhamiakin, M. Pistore and M. Roveri, Formal Tropos: Language and Semantics, Technical Report, Department of Information and Communication Technology, University of Trento, Trento, Italy (`disi.unitn.it/~ft/papers/ftsem03.pdf`), 2003.

[8] R. Harris, Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem, *Digital Investigation*, vol. 3(S), pp. S44–S49, 2006.

[9] M. Huber, M. Mulazzani, M. Leithner, S. Schrittwieser, G. Wondracek and E. Weippl, Social snapshots: Digital forensics for online social networks, *Proceedings of the Twenty-Seventh Annual Computer Security Applications Conference*, pp. 113–122, 2011.

[10] P. Hunton, The growing phenomenon of crime and the Internet: A cyber crime execution and analysis model, *Computer Law and Security Review*, vol. 25(6), pp. 528–535, 2009.

[11] D. Kahvedzic and T. Kechadi, DIALOG: A framework for modeling, analysis and reuse of digital forensic knowledge, *Digital Investigation*, vol. 6(S), pp. S23–S33, 2009.

[12] G. LaPorte, Paul D. Ceglia v. Mark Elliot Zuckerberg and Facebook, Inc., United States District Court, Western District of New York, Civil Action 1:10-cv-00569-RJA, Document 326, Riley Welch LaPorte and Associates Forensic Laboratories, Lansing, Michigan, 2012.

[13] R. Leigland and A. Krings, A formalization of digital forensics, *International Journal of Digital Evidence*, vol. 3(2), 2004.

[14] S. O'Ciardhuain, An extended model of cyber crime investigations, *International Journal of Digital Evidence*, vol. 3(1), 2004.

[15] G. Palmer, A Road Map for Digital Forensic Research, DFRWS Technical Report DTR-T001-01 Final, Digital Forensic Research Workshop, Utica, New York (`www.dfrws.org/2001/dfrws-rm-final.pdf`), 2001.

[16] M. Reith, C. Carr and G. Gunsch, An examination of digital forensic models, *International Journal of Digital Evidence*, vol. 1(3), 2002.

[17] F. Romano, Report and Recommendation, Paul D. Ceglia v. Mark Elliot Zuckerberg and Facebook, Inc., United States District Court, Western District of New York, Civil Action 1:10-cv-00569-RJA, Document 327, Rochester, New York, 2012.

[18] Stroz Friedberg, Report of Digital Forensic Analysis in: Paul D. Ceglia v. Mark Elliot Zuckerberg, Individually, and Facebook, Inc., United States District Court, Western District of New York, Civil Action 1:10-cv-00569-RJA, New York (`www.wired.com/images_blogs/threatlevel/2012/03/celiginvestigation.pdf`), 2012.

[19] Technical Working Group for Electronic Crime Scene Investigation, Electronic Crime Scene Investigation: A Guide for First Responders, Technical Report, National Institute of Justice, Washington, DC, 2001.

[20] A. van Lamsweerde, *Requirements Engineering: From System Goals to UML Models to Software Specifications*, Wiley, Chichester, United Kingdom, 2009.