Global Information Assurance Certification Paper

Evidence Collection From Social Media Sites

GIAC (GLEG) Gold Certification

Author: Keil Hubert, keil.hubert@gmail.com
Advisor: Barbara Filkins

Accepted: December 1, 2014

Abstract

Collecting and presenting digital evidence to support an administrative investigation can make or break the case against the accused. Many companies have policies and procedures for collecting evidence on computers that they have legal authority over; few have procedures for collecting evidence from external sources over which the company has no lawful authority. This paper recommends practical techniques for how best to collect, store, and present digital evidence that was discovered on a social media site or service that lies outside the authority of the company, so that legal affairs and human resources will accept it for use in administrative action against a misbehaving employee. This paper is based on an actual contract fraud case that the author investigated, where social media evidence helped to cement the case's critical timeline and effectively refuted the accused's alibis. All information presented is true, however no actual names, places, or identifying data is incorporated.

1. Introduction

Original content written and posted by an individual to a social media site may identify or substantiate an employee's misconduct, whether their own or misconduct by a fellow employee. Capturing evidence from social media sites can significantly support the evidence gathered from other sources (e.g., text messages, e-mails, etc.) in the construction of an event timeline. Proper capture, handling, and presentation of evidence from social media sites will help the investigator explain what happened to upper management, to legal, and to law enforcement agencies.

2. Context

2.1. Information security as it pertains to investigations

A recurring theme in Information Security training is to focus, conceptually, on the confidentially, integrity, and availability (CIA) factors of information protection (Gibson, 2011). This is regularly taught to students in terms of protecting their own or their company's information from internal or external threats ranging from malicious hackers to natural disasters. The United States Air Force explained it like this in their official regulation titled "Network and Computer Security":

"**1.3. Objectives.** The objectives of COMPUSEC [Computer Security] are to protect and maintain the confidentiality, integrity, availability, authentication, and nonrepudiation of information system resources and information processed throughout the system's life cycle." (AFI 33-202 Volume 1, Incorporating Change 5, 2007)

When pursuing an internal misconduct investigation, an investigator has to keep in mind the same CIA triad as it pertains to evidence; this will often encompass critical information that is hosted on networks and servers outside the company's network boundaries. Commercial services like social networking sites often contain compelling facts about suspects' behavior that are critical to showing who did what, when, and even where. The investigator has to not only collect this evidence – she also has to protect it from loss and corruption (the integrity and availability aspects of Information Security).

2.2. Internal inquiry versus law enforcement

No matter how sophisticated your in-house digital evidence collection and analysis capability might be, law enforcement officials typically have access to one critical capability that no corporation, university, or private citizen can match: the warrant (Fakhoury. 2011). A police investigator's ability to secure a warrant provides him or her with the authority to compel cooperation from outside parties in gathering evidence. A representative from a private company can submit a request for posted content and/or post metadata to a social media company (e.g., Facebook); the social media company is neither obligated to nor legally expected to honor the request. If the suspect's social networking behavior was consistent with the site's Terms & Conditions, release of information to a requester that is not normally available to the general public may expose the site owner to legal liability. If the suspect has posted content that suggests that he or she has committed a crime, the site may have a legal obligation to report that content to law enforcement – and to deny it to non-LE requesters (Monaghan, 2011, 529-530).

For this case, the suspect appeared to have defrauded the company where she worked as a contractor by mischaracterizing her need for paid time off. After reviewing the evidence that fraud had been committed, the harmed company's legal department believed that local law enforcement would decline to get involved.

2.3. External resource versus internal employee

The actions of an employee (whether in the corporate or non-for-profit realms) may be subject to monitoring in support of misconduct investigations. By creating a strong Acceptable Use Policy (AUP) (SANS 2014), a user's activity on computer information systems (e.g., e-mails sent and received, web browsing, etc.) may be captured by company system administrators and entered as evidence for administrative action by the company. An external resource (e.g., a contractor) *may* be subject to the Terms & Conditions of the company's AUP for actions taken while using the company's computers, phones, and networks. Depending on how restrictive the company's AUP is written, acceptable use may not apply to actions taken from a personally-owned device (e.g., a smart phone) that connects to a public network.

Once a misconduct investigation is complete, an actual employee may be subject to reprimand, loss of pay, loss of systems access, or termination depending on the company's discipline policies. A company rarely has the same ability to discipline an external resource; contractors and other outsiders are not employees of the company where they serve. A request by the contracting agency (the company) to the contract holder to discipline a contracted resource may be ignored; unless such actions are spelled out in the contract, the contractor may feel no obligation to cooperate with or respond to the client company's request to reign in a misbehaving contract worker.

2.4. Operating at the edge of normal authority

Some companies have a defined, official "internal affairs" function; many do not. Depending on the company's organizational structure, there may be a formally defined department or process for conducting an internal investigation into suspected misconduct. The lack of a formal investigative capability does not necessarily relieve the company of its legal obligations to investigate (Montez). In cases where the authority or responsibility to investigate a case may be ambiguous or undefined, management (in whatever form it takes) will likely assume the burden of gathering evidence.

An untrained or inexperienced ad hoc investigator may make mistakes during evidence collection that may negatively impact the company's ability to come to a conclusion, to secure appropriate corrective actions, or to end the alleged misconduct. It is critical that an assigned investigator receive guidance from subject matter experts within the company, including (but not limited to) legal, human resources, contracting, and union officials (if and when applicable). Note that guidance from two or more departments may be contradictory.

3. Synopsis

3.1. Synopsis of fraud case

The case illustrated here centered on a contract fraud allegation. A member of the company executed a pregnancy hoax, using her feigned medical condition to take paid time off from work. Approximately two-thirds of the way through her "pregnancy," the woman separated from the company (i.e., amicably left employment); she returned to the

company a week later as an external contractor. During her time as an employee and as a contractor, multiple co-workers raised compelling doubts with each other about the woman's "pregnancy," but management did not formally investigate the situation.

Unbeknownst to the company, the suspect was hired by a professional services company out of the Washington D.C. beltway area to provide expert services in the same capacity that she had previously held as a corporate employee. The company's parent company cut the contract to augment the staff of its subordinate branches during a hiring freeze – the staff augmentation plan wasn't briefed to affected organizations. The suspect's return to the office in a new legal status complicated how she was perceived and treated by her peers.

The original manager who had daily responsibility for monitoring the suspect's work performance as an employee left the company at/about seven months into the nine-month hoax. The new manager identified several incongruous aspects of the "pregnancy" and initiated an internal departmental investigation into the incident after the feigned "delivery." Company management relied on evidence from social media sites to assemble the case report that company contracting used to compel the contracted agency to take action to correct the misconduct.

3.2. Event Timeline

The suspect was originally hired as a temporary company employee with a fixed end date of 31 December Year 1. Two weeks after leaving, she returned unexpectedly as an external contractor. This change in employment status confused the issue of who was responsible for tracking the suspect's attendance, leave, H&S paperwork, etc. Additionally, the department went through a change of managers at the same time; the outgoing manager did not share any records or observations with her replacement.

The condensed case timeline follows. For the complete timeline, see Annex 1 (section 10) of this paper.

Date	Event
Mid May Year 1	Suspect has a liaison with another employee, claims to have gotten pregnant.
Mid July Year 1	Suspect submits a doctor's note to Health & Safety saying she's pregnant
Late July Year 1	H&S tech completed suspect's Pregnancy Workplace Interview

Late August Year 1	The Workplace Hazards office completes a workplace evaluation
Mid October Year 1	Suspect texted and posted photos of an ultrasound, claims that they're hers
Late October Year 1	New manager takes over the department, begins investigating the situation
Late December Year 1	The suspect misses work, claims to have been hospitalized
End of December Year 1	The suspect's employment contract ends.
Early January Year 2	Suspect tells co-workers that she has been diagnosed with gestational diabetes
Mid January Year 2	Suspect returns to work as a contractor.
Late February Year 2	Subject misses work, claims to have been admitted to hospital for delivery.
Late February Year 2	Suspect is seen consuming food prohibited by her ObGyn's diet restrictions.
Late February Year 2	Co-workers throw a baby shower for the suspect, give her gifts and cash
Early March Year 2	Suspect claims to have been admitted to hospital. Later, claims to have been transferred to the NICU at a different hospital.
Early March Year 2	Suspect texts details of the "birth" to co-worker. Employee calls hospital, hospital says that the suspect was not and had not been a patient there.
Early March Year 2	Suspect sends photo of an infant to a co-worker, claimed it was hers.
Early March Year 2	Suspect posted a photo on Facebook at a party and consuming alcohol, time and date stamped that day.
Early March Year 2	Doctor's office listed on the original pregnancy memo declares it a forgery.
Early March Year 2	Suspect's agency denies that she is on post-partum leave, reveals that suspect is present at the agency's conference out of state.

4. Evidence collection process

4.1. Informal interviews

The opening phase of the investigation required the department manager to ascertain who knew what and when they knew it. This was a note-taking exercise, where each employee described their interactions with the suspect, their observations, and the context of each key event (e.g., the *who, what, where, and when* of each incident that later went into the timeline). All of the hand-written notes for this phase were collected for the supporting evidence file.

4.2. Hardcopy and softcopy documentation

This involved sitting down with each employee individually and documenting all e-mail messages (both company and personal) and other written artifacts that had passed between the suspect and each of the employees. E-mails (both sent and received) that were accessible from within the workplace were opened, printed to PDF copies, and then turned over to the manager as non-alterable electronic files.

Each employee was cautioned that they must not delete or modify any records. The manager directed each employee to type, print, and sign a formal memorandum on official company letterhead that detailed their observations of the suspect's behavior.

Additionally, the manager requested (and received) all formal Health & Safety documents, attendance documents, and other company records currently on file from or about the suspect. Files received electronically were converted to PDFs and then printed; files received in hardcopy were scanned into PDFs. This allowed the investigator to compare and contrast printed and electronically saved files to ensure that there had been no changes.

Technique Tip: For hardcopy documentation, have the employee who received the document annotate in pencil in their own handwriting the date (and, if they remember, the time) that they received the artifact in one of the margins. This helps both to build the timeline, and to prove that the document has not been altered.

4.3. Mobile phone text and MMS photo records

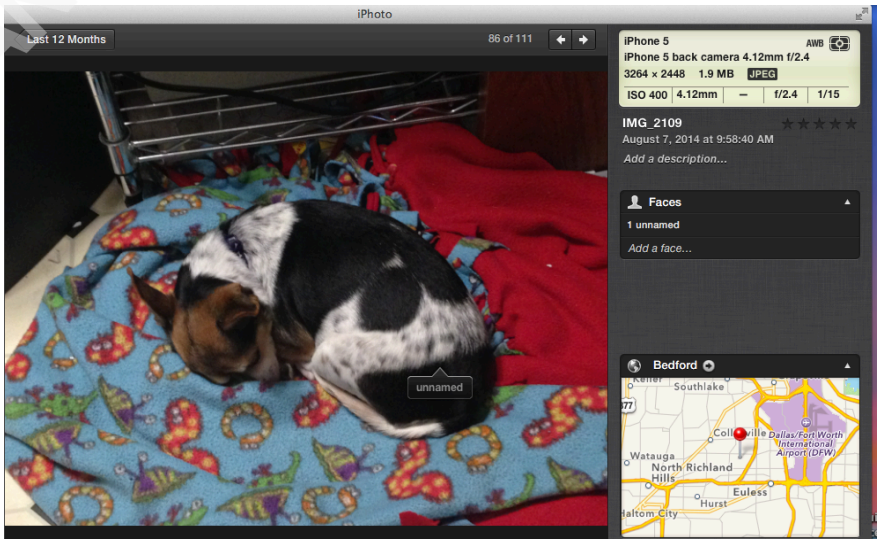
This involved sitting down with each employee individually and examining his or her personal smart phone. While the manager watched, the employee took progressive screen shots of their text conversation chains from the start of the claimed pregnancy episode through the day of the investigation. Screen captures looked like this:

Each employee then forwarded the screen shots to the manager for incorporation into the investigation report. The manager confirmed that each text message in the chain was captured in a screen shot. The manager pasted them in order, from oldest to newest, into a word processing document (four per page fit well enough to be read), and added the screen capture file into the investigation report, along with the name of the employee, the date that the files were provided, and the carrier and number of the mobile phone in case a court needed to subpoena the official records later.

Technique Tip: An iOS device can take a screen capture without needing a third party application. Depress the home button and depress the phone's sleep/wake button. The screen will flash, and the image will be added to the phone's photo library (Apple, 2014). The screen capture on an Android OS phone differs by model (Brewis, 2014); consult your device manufacturer's support page for specific instructions.

Note that the purloined ultrasound photo and newborn photo that demonstrated deliberate fraud in this case were both attached to employees' text messages. For these picture files, the employee forwarded the digital file to the manager who saved the file to a PC for metadata analysis (e.g., the time and date when the photo was taken).

Technique Tip: Apple's iPhoto allows you to view both a photo and its metadata information in the same window, like this screenshot. This includes the brand and model of the camera, and also **when and where** it was taken. Since alibi photos can be down-loaded from the Internet, this metadata helps to prove or disprove a suspect's claims.



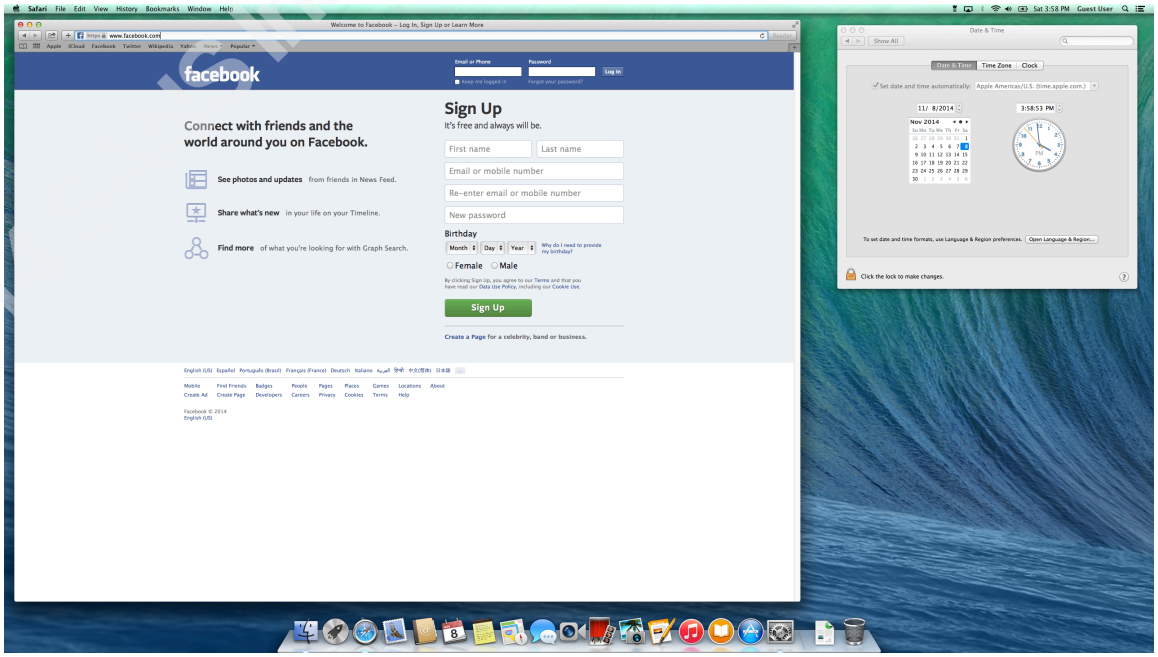
Keil Hubert, keil.hubert@gmail.com

4.4. Social media site records

The subject's willful, deliberate posting of personal information about her "pregnancy" appeared to be the most compelling evidence of willful fraud, since her entries were posted publically, and featured both time and location data for each post. The subject's co-workers had originally interacted with the suspect's social media posts from their personally-owned phones, tablets, and PCs. Fortuitously, the company allowed employees to access facebook.com from work PCs, which guided the capture process.

This involved sitting down with each employee individually at a company PC, having the employee authenticate the network normally with their own user ID and password, open a browser, and then examining their personal Facebook (FB) feed – all while the manager observed and took notes. Each employee then scrolled to relevant entries on their wall and instant messages sent to him or her within FB from the suspect. The employee took whole-screen screenshots (i.e., including the taskbar with the time and date showing) of the FB pages containing relevant content and forwarded each screenshot file through company e-mail to management.

Technique Tip: If your desktop is wide enough to accommodate a full-sized browser window and a second application, show the current settings for the PC's time zone, and Network Time Service settings. This helps support the evidence timeline:



Keil Hubert, keil.hubert@gmail.com

Later on in the investigation, once the suspect learned from a sympathetic co-worker that she was under investigation, she started deleting posts from her own social media account. Co-workers who noticed the attempt repeated the capture process and took additional screen whole-screen captures of the altered pages. They then forwarded the image files to management to compare and contrast the social media site's before and after data.

Technique Tip: Social media sites like Facebook, LinkedIn, and Google+ will frequently truncate the display of comments about a given post. Be sure to expand the comments field, and take multiple screen captures of a given entry (with overlap, as per text message capture) to show all of the comments, the people who wrote then, and when the various additions were posted.

5. Evidence analysis

5.1. Expert assessment

Prior experience in unrelated misconduct investigations motivated the manager to preemptively seek out expert opinions on elements that legal, HR, and/or company executives might express doubt over. He made copies of certain files, redacted any personally-identifiable information, and sought out local subject matter experts.

Technique Tip: Redaction is electronic files can be tricky, since annotations to a digital file can be reversed or removed. Use hardcopies of image when practical.

The manager showed the suspect's digital photos to several senior medical specialists in Health & Safety who confirmed that the child in question did not match the appropriate features of a newborn.

Technique Tip: Print out as large a color copy as you can of a photo or screen capture. Then, have your expert analyst use a felt-tip pen to circle or otherwise identify the elements of the image that they find questionable. Take note of what your experts say, and refer back to the annotated hardcopy. Have your expert initial or sign their markings on the hardcopy, and also initial or sign your transcription of what they told you to ensure that you accurately documented what they tried to say.

The doctor's office listed in the original pregnancy memo examined a faxed copy of said memo and denounced it as a forgery. Upon request, they further explained (in a written statement) which elements in the memo indicated that it was likely a forgery (e.g., using the name of a doctor who had retired years before, etc.).

Technique Tip: When an expert or witness examines a copy of a document, ask them to initial or sign in the margin, and to write in the date that they conducted their examination. Then scan that copy and annotate in your notes how to recognize the exact copy that the expert or witness was referring to.

The manager included all of these supporting expert opinion documents as elements of evidence in the formal evidence analysis package.

5.2. Timeline construction

Using all of the assembled messages, documents, photos, texts, social media posts, and logged calls, the manager constructed a comprehensive timeline that linked each piece of evidence to a specific date and time, along with the name of each witness. The timeline itself was a chronological table where each statement was linked to an evidence document that had its own identifying number.

Technique Tip: See Annex 1 of this paper for a redacted example of the event timeline. In the formal report, be sure to list all associated witnesses who can comment on the entry, and also the file names of any associated evidence. This is an example:

Table 1. Misconduct Investigation Timeline

Date	Event	Status	Evidence
[Date and Time]	[Suspect] texted [Witness 1], claiming to have had an [done some thing relevant to the case]	Both suspect and Witness 1 were on company time and on company premises	Company Misconduct Investigation file, "Findings, Analysis and Conclusions" (A11, page 6, Table 2)
[Date]	[Suspect] presented [Witness 2] with a memo from [organization name] stating [something about the case]	Suspect was not on company time, but Witness 2 was	Fraudulent document (A12), Witness 2's formal statement (A16)

The manager then organized the collections of screen captures by collecting all of the image files and then creating individual "container" files (using Microsoft Word) for each witness's text message files and each witness's social media image files. Each container then showed all of the screen capture images in chronological order.

5.3. Request for information

After the manager assembled and validated all of the timeline data and copied all of the evidence into a formal report, he delivered it to the first executive in the management chain for assessment. The executive considered the totality of evidence, challenged elements that might be questionable, and (once satisfied with the report) formally briefed the company's chief legal officer on the probability that a fraud had been perpetrated against the company.

The legal department, in turn, examined the evidence and briefed executive management. Once satisfied that propriety had been satisfied, legal contacted the parent company's contracting office, explained what had transpired, and asked them to intercede with the contracted agency to determine what remedies might be available to contain the fraud. Legal also insisted that the suspect be suspended from on-site work until the issue could be resolved.

6. End result

When presented with the assembled evidence, the contract holder removed the suspect from duty at the company site without admitting any wrongdoing. The contract holder's representative informed the company that they were not obligated under the terms of their contract to reimburse the company for hours of work paid out even though the work hours were not actually performed. Nor, they said, were they obligated to take legal action against their employee for fraud committed against the client. Company legal declined to sue, provided the contractor agreed to immediately terminate the suspect and walk away from the contract.

Company legal declined to pursue either civil charges (for falsification of official documents) or criminal charges (for theft by deception) against the suspect provided she never returned to the company site in any capacity.

7. Lessons learned

7.1. Evidence capture process

The investigation illustrated in this study was conducted using the first half (what would normally be the "law enforcement track") of Eoghan Casey's "case/incident resolution process" timeline (Casey, 2004, 92-93): discovery/accusation, seizure, preservation, examination, analysis, and reporting of findings. The new manager assigned to the department had previously received formal training on conducting cybercrime investigations, and fell back on Casey's methodology for assembling case evidence.

As outlined in section 4, several employees came to the shared understanding within a 72-hour period that a fraud had been committed against the company by the suspect. When the department manager was presented the initial reports, his first order of business was to discover who knew what, when, and via what medium. This involved extensive interviewing in order to identify what messages, texts, posts, and other information might be captured for inclusion in the formal report.

This first phase – interviewing the affected witnesses – turned out to be key to capturing evidence. Once an employee mentioned that they had previously received a digital message (e.g., e-mail, text message) or had seen a social media post, the onus was on the manager to capture that content before the suspect could delete or change it to cover her tracks.

The manager knew from prior experience in the organization that the legal department was hesitant to request law enforcement support, especially when it came to getting warrants to seize and forensically image an employee's personal phone or PC. Rather than attempt to capture complete forensic images of each employee's phone, the manager requested (and received) each employee's permission to share screen shots of text message chains. By observing the process from start to finish, and by ensuring that the start of each sequential screen shot included the last element of the previous shot, the manager could confidently document in a separate memorandum to upper management that each phone's message chain was turned over in its entirety. After that, the time and date stamps associated with each message could be incorporated into the incident timeline with confidence.

Keil Hubert, keil.hubert@gmail.com

The text message capture process influenced the social media data capture process in turn: understanding that social media content is, by its nature, volatile (e.g., the originator can sometimes delete or modify a previously posted element), the manager recognized the need to capture each post in its entirety along with its time/date data *and* the posts that both preceded and followed the desired element.

The organization's previous unofficial process for capturing social media content was to "print" the browser windows to a PDF file that showed all of the page as it existed at the moment of capture. The PDF file would have its own date and time from when it, itself was generated. The problem with this method was that the social media content often didn't display in the PDF file the way it did on the user's screen, potentially confusing the viewer's comprehension of the message.

To mitigate this, the manager decided to use company PCs authenticated to the production domain. By using known-good end-user devices, the company's IT department would be able to certify that the date and time shown on each whole-screen screen capture was both accurate and set by the Network Time Service, not modified by a user. The full-size screen shots also showed the content as it was designed to be viewed.

The printed documentation proved to be more sensitive than the personally-owned device records. After considerable debate, the manager determined that formal records, like the workplace safety interview, were probably still protected under HIPAA (Gragido, 2011, 41) even though the medical information in them was deemed to be fraudulent. This was a tactical decision; protecting the files as if they contained restricted data wouldn't significantly impede the assembly of the timeline, and the evidence materials had to be secured each night anyways to prevent potential tampering.

Telephone calls made to and from the suspect couldn't be recorded after the fact, but the fact that they happened could be. For employees with smart phones, the individual call records were still logged on their phones along with the day and time the call took place, whether it was an outgoing or incoming call, how long the call lasted and the phone number contacted. In keeping with the practice of capturing the absolute minimum of the employees' personal information, each call record was captured as a screen shot that the employee then forwarded to the manager via e-mail.

Keil Hubert, keil.hubert@gmail.com

7.2. Evidence presentation process

This was the most difficult part of the investigation: communicating to upper management and legal the *who, what, where, when, and how* of the aggregated body of evidence. Each piece of evidence had to be relevant, clear, and incontrovertible on its own merits. To meet this objective, the formal report was built as follows:

The report opened with a cover memorandum from the department manager to the first executive in the management chain, summarizing the case, including when management first became aware that there was a potential problem.

Next came a timeline in table form that laid out the elements of information in chronological order, detailing the date, a description of the event, the names of each witness, the specific elements of evidence related to the event, and the unique attachment number for each element. The table allowed the governing executive, the head of legal, and the chief executive (in turn) to follow the timeline logically and, thereby, understand the extent and evolution of the alleged fraud.

Then came a report summarizing actions taken to-date, including the suspension of the suspect's company network account to ensure preservation of official records.

After the legal office's review, the manager compiled the entire report into a single large PDF that incorporated the cover memo, the timeline, and all evidence into one document that legal could formally deliver to the national contracting office. The final report came to a centimeter-thick stack of printed content with an associated CD-R of digital files.

7.3. Mitigating contested evidence

As predicted, legal challenged several elements in the initial compiled report. For example, how could anyone be confident that the "baby photo" sent by the suspect to multiple coworkers *not* be a newborn? In each case where there might be subjective bias or the potential for misinterpretation, the manager took the individual piece of evidence to a subject matter expert within the company and asked for a written opinion.

In the baby picture example, one of the employees was a credentialed neonatal nurse; that employee declared in writing that in her expert opinion, the child in the photo

could not be less than 12 weeks old, and therefore could not be a photo of a newborn less than 24 hours old (as claimed). In another example, two credentialed nurses declared that the suspect's statement that a doctor would allow a newborn in a NICU to be removed from life support equipment for the sake of taking a photograph would constitute an unacceptable violation of clinical practices.

The manager submitted each expert opinion to legal and incorporated a copy of legal's acknowledgement of receipt into the open case file. He assumed that all correspondence concerning the case would eventually be submitted to a civil or criminal court, and wanted to ensure that all relevant documents were organized, accounted for, and ready for inspection.

The screen shots of text-based conversations and the social media posts turned out to be the critical elements that the case hinged on. Legal opined that the suspect could simply have been wrong about being pregnant when she completed her Health & Safety forms. When it came to posting public statements like "I just gave birth at XX hospital" on Facebook, however, there was no way that the suspect could have been mistaken about where she was or what she was doing at that time. Since the report included evidence that specifically refuted the place where the employee was at the time (thanks to location-stamped social media posts), the suspect's story unraveled rather quickly.

8. Conclusion

It can be difficult and frustrating to try and capture evidence to support suspected misconduct when key evidence has been posted to social media sites and other resources that exist outside the lawful and technological control of the company. The investigator often cannot leverage warrants, subpoenas, and other legal tools to compel the holder of the critical content to turn it over. What the investigator can do, as a minimum acceptable alternative, is to convince each witness in the case to meticulously save unalterable records of their own social media feeds (e.g., screenshots, PDF prints, etc.) that include time and date data, and other content that helps to establish the incident timeline. This is best supplemented with official written statements from each witness recounting what they saw in each of their relevant social media feeds, when they saw it, and how they

responded to it. These supporting documents help to construct the context of the exchange, which can (in turn) help a reviewer to interpret the suspects' and witness's intent in each exchange.

This technique is **not** submitted as a law enforcement or intelligence community standard operating procedure, where the chain of evidence must be sacrosanct; in an internal corporate misconduct investigation, the worst possible outcome of an investigation might be an employee termination – an outcome that can be corrected if new evidence comes to light exonerating a suspect. The process of swiftly discovering, capturing, analyzing and presenting evidence collected from multiple communications channels (including but not limited to social media sites) is presented as a quick-and-dirty technique for assembling statements, event locations, event times and dates, and records of witnesses for incorporation into the investigator's timeline and initial report.

9. References

Apple Inc. (2014). Take a screenshot on your iPhone. Retrieved November 08, 2014, from Son of citation machine Web site: http://support.apple.com/en-us/HT200289

Brewis, Marie (2014). How to take a screenshot on Android phones and tablets: including Galaxy S3/S4/S5, Xperia Z2, HTC One and Nexus 5, Retrieved November 08, 2014, from Son of citation machine Web site: http://www.pcadvisor.co.uk/how-to/google-android/3446798/how-take-screenshot-on-android-phones-tablets/

Casey, Eoghan. Handbook of Computer Crime Investigation: Forensic Tools and Technology. London, UK: Elsevier Academic Press

Fakhoury, Hanni (2011). Know Your Rights! Retrieved September 03, 2014, from Son of citation machine Web site: https://www.eff.org/wp/know-your-rights

Gibson, Darril (2011). Understanding The Security Triad (Confidentiality, Integrity, and Availability). Retrieved November 08, 2014, from Son of citation machine Web site: http://www.pearsonitcertification.com/articles/article.aspx?p=1708668

Gragido, Will; & Pirc, John, *Cybercrime and Espionage: An Analysis of Multivector Threats*, Burlington, MA: Syngress Publishing, Inc.

Keil Hubert, keil.hubert@gmail.com

Headquarters, Air Force Communications Agency, *Air Force Instruction 33-202, Volume 1, Network and Computer Security*, incorporating through Change 5. Scott Air Force Base, MO: HQ AFCA/EVPI.

Howard, Rick. *Cyber Fraud: Tactics, Techniques and Procedures*. Boca Raton, FL: Auerbach Publications

Hubert, Keil (2013), Great Expectations, Retrieved September 03, 2014 from Son of citation machine Web site: http://business-technology.co.uk/Year 2/12/keil-hubert-great-expectations/

Hubert, Keil (2013), Inescapable Exposure, Retrieved September 03, 2014 from Son of citation machine Web site: http://biztechreport.co.uk/Year 2/02/inescapable-exposure/

Hubert, Keil (2013), Internet Drownproofing, Retrieved September 03, 2014 from Son of citation machine Web site: http://business-technology.co.uk/Year 2/11/keil-hubert-internet-drownproofing/

Lawson, Tony; & Heaton, Tim, *Crime & Deviance*, Chippingham, England, UK: Palgrave Macmillan.

Mandia, Kevin; Prosise, Chris; & Pere, Matt. *Incident Response & Computer Forensics*. Emeryville, CA: McGraw-Hill/Osborne

Monaghan, Joseph (2011). Social Networking Websites' Liability for User Illegality. Retrieved September 03, 2014, from Son of citation machine Web site: http://law.shu.edu/Students/academics/journals/sports-entertainment/Issues/current/upload/sportslaw_monaghan_social_networking.pdf

Montez, Rory (no publication date). Internal Affairs: When Situations Demand Investigation, Retrieved September 03, 2014 from Son of citation machine Web site: http://www.diversifiedriskmanagement.com/articles/internal-affairs.html

SANS Consensus Policy Resource Community (2014), Acceptable Use Policy. Retrieved September 03, 2014, from Son of citation machine Web site: https://www.sans.org/security-resources/policies/general/pdf/acceptable-use-policy

Keil Hubert, keil.hubert@gmail.com

Varsalone, Jesse; Kubasiak, Ryan; Morrissey, Sean; Barr, Walter; Brown, James; Caceres, Max; Chasman, Mike; and Cornell, James, *Mac OS X, iPod, and iPhone Forensic Analysis DVD Toolkit*, Burlington, MA: Syngress Publishing, Inc.

Annex 1. Event Timeline

This is the correct, chronological order of events for the case discussed. Note that all of the events in this list have been abstracted slightly to obfuscate the people involved in the actual event. Because the suspect was never convicted in a either a civil or criminal court, she shall be referred to only as a suspect, and not by name.

Mid-May Year 1: The suspect had an intimate encounter with a company employee during an off-site training course. She later claimed this weekend as the time and place of conception.

Mid July Year 1: The suspect submitted a forged memo from a local hospital to the company's Health & Safety office that said that she was eight weeks pregnant. The H&S tech did not validate the information, and did not report the pregnancy to management.

Late July Year 1: The suspect completed her annual health assessment and did not indicate on the form that she was pregnant. The H&S tech failed to note the discrepancy, but completed a standard Pregnancy Workplace Interview with the suspect.

Early August Year 1: The suspect confided to a co-worker that she was pregnant, and that a specific co-worker was the child's father. She went on to discuss her plans for the delivery, her family's plans to attend the birth, and other information that convinced the co-worker that the pregnancy was legitimate.

Late August Year 1: The Workplace Hazards office completed a workplace evaluation on the suspect.

Early September Year 1: The suspect informed a co-worker that her obstetrician was performing monthly test on her for sexually transmitted diseases. This peculiar statement triggered inter-office discussions about the "pregnancy."

Keil Hubert, keil.hubert@gmail.com

Late September Year 1: A member of the staff formally reported to management that the suspect's pregnancy might have been the result of a coercive sexual assault.

Late September Year 1: The suspect texted a co-worker, claiming to have had an ultrasound and that her baby's sex was female.

Mid October Year 1: The suspect brought photos of another mother's ultrasound to the office and claimed that they were here own.

Late October Year 1: A new manager took over the department, received the report about the sexual assault allegations, and called on local law enforcement to initiate a formal investigation. The L-E investigator corroborated the sexual encounter between the two employees, but judged it to be consensual. No charges were filed.

Late November Year 1: The manager collected e-mails, calendar entries, and statements from employees about workdays that the contractor had missed for "pregnancy-related" medical events.

Late December Year 1: The suspect texted a co-worker claiming to have been hospitalized for kidney stones, and said that her unborn child was unaffected.

End of December Year 1: The suspect's employment contract ended.

Early January Year 2: The suspect told several co-workers that she had been diagnosed with gestational diabetes as a direct result of her pregnancy.

Mid January Year 2: The suspect returned to the office, claiming to have been hired as a contractor. No one in the company was aware of such a contract, and the suspect had no paperwork to substantiate her claim. It took two weeks to identify the agency in D.C. that had cut the national contract, and to validate that they had employed the suspect.

Mid January Year 2: The suspect confided in a co-worker that she planned to use the courts to garnish her child's father's wages for child support.

Late February Year 2: The suspect told her co-workers that her doctor planned to induce delivery the following Friday.

Keil Hubert, keil.hubert@gmail.com

Late February Year 2: The suspect did not show up to work. When queried by a co-worker, the suspect said (via text message) that she had been admitted to a local hospital for delivery.

Late February Year 2: A co-worker texted the suspect to see how the deliver was going. The suspect claimed that it was just "pressure," and would be back to work the next day. This inspired doubt.

Late February Year 2: Co-workers took the suspect out for lunch, and chided her for eating foods that were specifically forbidden to her under her (claimed) diagnosis of gestational diabetes. The suspect didn't seem to care about the effect of diet on her "child." This inspired doubt.

Late February Year 2: Several co-workers threw a baby shower for the suspect at the office, and gave the suspect gifts and cash. The suspect told the workers at the shower that she was scheduled for a 1 p.m. delivery that Friday.

Early March Year 2: The suspect claimed to co-workers to have been admitted to a specific local hospital. Later that same day, she claimed to have been transferred to the Neonatal Intensive Care Unit at a completely different hospital. This inspired doubt.

Early March Year 2: The suspect texted data about her "newborn" to a co-worker who called the delivery hospital to arrange for a delivery of flowers. The hospital said that the suspect was not and had not been a patient there. This inspired doubt.

Early March Year 2: The suspect sent a photograph of someone else's three-month old infant to a co-worker and claimed that it was "her newborn." When the co-worker asked if the child had been released from the NICU, the suspect said "no," and claimed that the doctor had removed all of the medical equipment (e.g., oxygen tubing, etc.) from the baby specifically to facilitate the photo. This inspired considerable doubt.

Early March Year 2: Two days after the "delivery," the suspect posted a photo on Facebook of herself attending a party and clearly consuming alcohol. The photo was time and date stamped that day. Co-workers raised the issue to management, asking how a brand-new mother could be partying so soon after giving birth.

Keil Hubert, keil.hubert@gmail.com

Early March Year 2: The next day, several co-workers met the suspect at a local restaurant. The suspect claimed that she had been allowed to leave her newborn at the hospital. One co-worker then called the hospital to confirm; the hospital said that neither the suspect nor her child was nor had been a patient there.

Early March Year 2: Based on frantic reports from the suspect's co-workers, management initiated an investigation into the facts of the pregnancy and delivery. On request, the doctor's office listed on the original pregnancy memo from July Year 1 examined it and declared it a forgery. The manager called the agency that employed the suspect and asked if the suspect was listed as being on post-partum leave. The contract manager claimed to know nothing about a pregnancy, and revealed that the suspect was attending a company conference in Washington D.C. that day.