An Evaluation of
Private-Sector Digital Forensics Processes and Practices

Applied Research Project Final Report
Presented in Partial Fulfillment of the Requirements
for the Master in Science in Digital Forensics and Cyber Security
John Jay College of Criminal Justice
City University of New York

Cindy Zimmerman

February 2013

An Evaluation of Private-Sector Digital Forensics Processes and Practices

Cindy Zimmerman

This Applied Research Project Final Report has been presented to and accepted by the Office of Graduate Studies of the John Jay College of Criminal Justice of the City University of New York in partial fulfillment of the requirements for the Master in Science in Digital Forensics and Cyber Security.

Dr. Bilal Khan		
Thesis Advisor	Signature	Date
Dr. Spiros Bakiras		
Second Reader	Signature	Date
Dr. Richard Lovely		
Director of D4CS	Signature	Date

Notes

Portions of this thesis will be submitted as a peer-reviewed article to **International Symposium on Security in Computing and Communications (SSCC'13)**, whose submission deadline is April 10, 2013. The conference addresses topics related to digital forensics (see http://icacci-conference.org for complete information).

Table of Contents

1. Motivation

1.1 Dynamism

The "field" of **Digital Forensics** is still in infancy stages, and as such, its contemporary practice continues to evolve in response to changes in both the technological and legal landscape (Shi, 2009, pp. 448-453). One impact of such rapid and continuous changes is that the processes that need to be documented are often evolving faster than the documentation can keep pace. As a consequence, practitioners of digital forensics often find it difficult to justify the expenditure of time and energy necessary to create well documented, universal and standardized investigative processes (Casey, 2004 , pp. xxiv, 10).[1]

Legal dynamism. Laws in the United States have often struggled to keep pace with emerging technology (Caloyannides, 2004, p. 84) since as technology advances, criminal elements find new ways to exploit new inventions and systems, bringing forth an ever-richer variety of types of crime (Leigland & Krings, Fall 2004). Although the enterprise of digital forensics has been around since the 1980's, laws surrounding the field are still evolving, and lawmakers are only just beginning to take systematic action to address the core underlying issues. New laws have not, however, come without controversy, most exemplary of which might be the Stop Online Piracy ACT (SOPA) and Cyber Intelligence Sharing and Protection Act (CISPA). SOPA is aimed at protecting copyrighted intellectual property, and was introduced by U.S. Representative Lamar Smith (Rep Smith, 2011). Opponents of

[1] This paper has been read and approved by Dr. Bilal Khan and Dr. Spiros Bakiras.

SOPA argue that it infringes on First Amendment rights and that SOPA would prevent innovation in the industry (Brito, 2011), and the much-debated bill is still under consideration as of November 2012. CISPA is a proposed law introduced by U.S. Representative Michael Rogers, and was designed to aid the U.S. government in its fight against cyberthreats (Rep. Rogers, 2011). Opponents of CISPA contend that the law will invade citizens' privacy and personal liberties (ACLU, 2011). Despite public opposition to the bill, and public statements by the White House to the effect that President Obama would veto the bill if given the opportunity, the House of Representatives passed CISPA on April 26, 2012 (BBC, 2012). These examples illustrate the emerging trajectory of digital forensics law in the U.S. and its inevitable repeated collision with the Fourth Amendment, which protects citizens rights from government infringement (Brenner, 2009, p. 233) (Jarrett, Bailie, Hagen, & Judish, 2009, pp. 21-22). To complicate matters further, as the boundaries between U.S. citizens and foreign nationals blur in hyper connected cyber space, evolving laws will become harder to enforce and define within the context of international law and transnational regulations.

Technological dynamism. Technological innovation, driven by consumer demands and corporate competition alike, yields a constant stream of new devices in today's marketplace. The current life span of a mobile device is approximately two years, although many customers replace their mobile devices at a more rapid rate, and are driven to do so by service providers who use free device upgrades as a lure for service plan loyalty (Little, 2009, p. 190). In addition, new computing models such as the "Cloud computing" provides ease of data access to customers,

but very few forensics tools are equipped to analyze Cloud storage (Lillard & Garrison, 2010, p. 18). As new devices are introduced, digital forensics practitioners are frequently unable to extract the data from them until new tools have been developed (Zdziarski, 2008). Even once the tools have been developed, not all forensics labs can afford or obtain access, often because of budgetary restrictions or lengthy validation processes (Nelson, Phillips, & Steuart, 2009, pp. 91-92).

1.2 Structural factors

Structural factors—specifically the fact that digital forensics is practiced quite differently in its **public** and **private** sector manifestations—also impede the development of documented, universal, standardized processes. The public sector has, to date, led the way in devising standardized analytic processes, primarily because in this setting digital forensics investigations tend to be regulated by a plethora of laws designed to protect the individual from infringements by the state, and these regulating legal structures are necessarily visible to the public. To wit, when digital forensics operates in public sector settings, it is (at least ostensibly) motivated by community interest and the upholding of citizens' rights as guaranteed by applicable laws (Jarrett, Bailie, Hagen, & Judish, 2009, p. 17). The private sector[2], in contrast, is openly motivated by the maximization of corporate and shareholder profits (e.g. the profits of forensics consulting firms, in-house corporate digital investigative teams, etc) (Bakan, 2005, pp. 117-118). Since the private sector is not

[2] The private sector can be further subdivided into two subsectors, broadly consisting of forensics consulting firms, and in-house corporate digital investigative teams. We refer to these subsectors as **private consulting** and **private in-house**.

driven by communal interest and does not fall quite so close to the interface between the state and the individual (Solove D. J., 2004, p. 64), fewer laws exist to govern and constrain digital forensics processes within the private sector, see for example (Smith v. Maryland, 1979) (United States v. Miller, 1976) (Burdeau v. McDowell, 1921) (US v. Jacobsen, 1984). Thus, although investigations in public and private sectors often require similar technical skill sets, the differences in the motivational assumptions of the two sectors manifests as differences in investigative procedures and practices; these differences then stand to impede the development of common universal and standardized processes.

For an illustrative example of how differences in motivational assumptions lead to difference in procedures, consider the importance given to maintaining chain-of-custody[3] (COC) in public sector versus private sector (specifically in-house corporate digital investigative teams) settings. In the public sector, the COC is essential to the investigative process and is often critical in the outcome of the underlying legal case. Specifically, if it is determined that the COC was not properly maintained for a piece of evidence, this revelation raises the specter of evidence tampering, and could result in a mistrial (Gardner & Anderson, 2010, p. 364). By comparison, in the private sector (in-house), maintaining the COC is not as important because it is assumed that the evidence is company property and the origins have already been documented. Digital forensics operations in the private in-house setting primarily seek to protect the company's data and reputation from

[3] The COC formally documents the sequence of collection, custody, control and analysis of the digital evidence (Casey, Digital Evidence and Computer Crime, Second Edition, 2004).

potential corporate antagonists who may be, but are not limited to, individuals with criminal intent. In practice, the Fourth Amendment creates fewer impositions on the dynamics *within* private sector firms than it does on state-individual dynamics that are so central to public sector digital forensics (United States v. Miller, 1976). Private companies are legally permitted to create policies with wide scope, prohibiting anything from nepotism to theft. Indeed, by to American law, citizens should not have any expectation of privacy when it comes to non-governmental agencies (US v. Jacobsen, 1984) (Solove D. J., 2004, p. 64), and property owned by a company is subject to search by the company despite an employee's informal expectations of privacy.

Similarities in motivational assumptions can, of course lead, to similarities in broad attitudes. For example, practitioners in private in-house and public sector contexts often have similar attitudes, derived from the fact that both are *invested* in trying to prove the veracity (or falsity) of claims against accused antagonists. The difference, of course, being that transgressions in the public sector setting refer to criminal offenses in reference to state and Federal laws, while in the private sector (in-house) the transgressions are in reference to local corporate policy.

In contrast with the private in-house and public sectors, the private consulting subsector operates by offering analytic services that their skilled digital forensics practitioners are capable of providing. Such services are typically estimated and priced out according to the time a digital forensics practitioner is expected to require. In the private consulting subsector, profits (and hence motivations), are driven by the desire to appease the client with analysis

deliverables, while keeping within the negotiated budgetary constraints. Because of this, the motivations of the forensics practitioner in the private consulting subsector are only incidentally related to proving the veracity or falsity of claims against accused antagonists. The most drastic difference that sets the private consulting subsector apart is the manner in which evidence is collected. In private consulting firms the client—who may have budgetary or organizational constraints that limit the extent and nature of evidence collection—dictates data collection.

1.3 Impact on Education

The aforementioned dynamism (legal and technological) and the structural factors within the digital forensics field, together, make it understandably challenging to evaluate the efficacy with which an educational system—such as the Digital Forensics and Cyber Security (D4CS) Masters program at John Jay College—is achieving the objective of "preparing students to be active contributors and leaders in the field of digital forensics". Since its inception, the design of John Jay's curriculum has been influenced largely by the strong relationships between faculty and public sector organizations, including Criminal Justices classes as a requirement to the Master of Science in Digital Forensics and Cyber Security (D4CS)[4] (Lovely, 2012).

The investigation we undertake here will shed light into the until-now dark corners of private digital forensics industry, its needs, processes, and practices. In

[4] Examples of these courses are: FCM 752. "The Law and High Technology Crime", CRJ 727. "Cybercriminology", CRJ 710. "Issues in Criminal Justice", CRJ 708. "Law, Evidence, and Ethics" and CRJ 733. "The Constitution and Criminal Justice".

doing so, this report remedies the dearth of documentation on digital forensics processes within the private sector. For educational establishments, such an inquiry is both strategic and necessary, since the vast majority of the newly created jobs in digital forensics are in the private sector (Wiles, 2007, p. 279). The report we present here provides a valuable first ethnography of private sector digital forensics practices. It provides us a better understanding of the emerging needs in the digital forensics field. In achieving these objectives this report may provide educators with concrete and actionable information by which to strengthen the structure and content of their programs and thus better prepare current and future students to transition into and excel in private sector digital forensics careers.

2. Objectives

The main goal of this applied research project is to assess the commonalities and differences across practice of digital forensics within the private sector.

More specifically, this project seeks to examine the inner workings of several digital forensics labs, with the objective of:

1. Recording how digital forensics analysts perform their daily activities in practice, the *tools* they use, and the *processes* they engage.

Such a description should provide:

2. A picture of the variety of individual *roles* within forensics teams, as well as
3. A view of how the team integrates with the parent organization as a whole.

Since physical access to a lab is restricted due to security reasons, observing a team of digital forensics practitioners in a lab environment is not an option. In lieu of direct observation, we follow the standard ethnographic techniques (Fetterman, 2010, pp. 33-59) of subjecting digital forensics practitioners to a survey consisting of a predetermined set of questions from which we deduce information about actual scenarios that might arise within the lab environment. The individuals sampled will include digital forensics practitioners from both private consulting and private in-house subsectors. A predetermined set of questions is distributed to the subject in written form in advance, as a survey, and the survey responses are later collected through a semi-structured interview.

4. In analyzing the survey/interview responses, we expect there to be significant similarities and differences across respondents; describing these is a key objective.

Moving beyond ethnography and into synthesis, from the responses of study participants, we intend to distill:

5. A set of "core" skills and technological competencies commonly reported to most valuable in the private sector digital forensics.
6. A (fictitious) forensics investigation process that factors out the "core" common work flows reported by study participants.
7. A (fictitious) set of forensics team roles that factor out the "core" common personnel categories reported.

Items 5-7 will then be combined to devise

8. A plan for the operation of a for-profit student-staffed Digital Forensics Services Corporation, complete with a strategy for the training and evaluation of its student staff. Such a plan, if adopted, would provide students in educational institutions, e.g. John Jay's Digital Forensics and Cyber Security (D4CS) Program, with hands-on experience that is designed to align with the contemporary practices of their future employers, while simultaneously providing the Program with operating funds to reinvest in new technologies and training for faculty and students alike.

3. Methodology

There are three common ethnographic methods that could be used to study the similarities and differences among teams of digital forensics practitioners: interviews, participant observation and surveys (Fetterman, 2010, p. 13), each with its own merits and drawbacks.

Participant observation involves immersing oneself in the ecology of interest, whereby one might observe digital forensics practitioners' working environment. This approach enables the observer to gain knowledge of the details of digital forensics practitioners' processes and skills by observing their daily routines. Observation could shed some light into habits that would be common among digital forensics practitioners, and even patterns that the subjects might not be consciously aware of. Participant observation opens up the possibility of making etic/emic distinctions (Headland, Pike, & Harris, 1990) (Jahoda, 1977), which are harder to extract from surveys and interviews. Unfortunately, since most private sector forensics labs require corporate security clearances to even enter, participant observation was deemed to be an impractical strategy for this research.

Surveys are typically used as a quantitative, anonymous and accumulative method (Schensul, Schensul, & LeCompte, 1999, pp. 165-197). Survey questions are constructed with questions that include true/false, ranking answers and/or multiple choice answers so that the answers can be "coded" as a number and easily quantified. The survey then gets distributed to a random sample of people within the demographic population of interest. Because digital forensics practitioners are

scattered among different organizations, the problem of random sampling appears quite daunting. In addition, the number of people that fit into the demographic and are willing to take the survey is quite small, so quantitative analysis would likely yield statistical results with dubious confidence intervals.

Interviewing is an effective method to learn from people how they think and what they believe to be true. There are two different forms of interviews: fully structured and semi-structured. Fully structured are interviews whose question sequence is rigidly pre-determined. Semi-structured interviews begin with a set of pre-determined questions, but also have the malleability to add additional questions based on the interviewees responses. Semi-structured interviews are more flexible and allow for more comprehensive information to be obtained from each interviewee. Interviewees have room to go off in tangents, which give the interviewer better insight into their thought processes. On the flip side, with fully structured interviews comparing participant responses is easier.

Of the above options, we chose to use semi-structured interviews in this research. We deemed this to be the most appropriate method given the expected small size of the demographic population, and the impractical task of observing subjects in a "live" laboratory environment. In addition, because we found individuals to be reluctant to spend much time out of their busy schedules, a predetermined set of initial interview questions was devised as a written survey and distributed to each subject in advance; survey responses were then collected through a semi-structured in-person or telephone interview. To study the similarities and differences across private sector digital forensics practitioners, a

convenience sample of three (N=3) individuals was drawn from a variety of different private sector organizations in which recent alumni of John Jay College's D4CS program are employed. While this aspect of the selection process likely introduces a bias to the sample, we found it to be not overwhelmingly objectionable given that a significant part of our objective (see #5 through #7) was to feed back the results of the survey analysis as recommendations for the D4CS program. As such, we expected that by selecting survey respondents from amongst D4CS alumni, we would be more likely to get answers to survey questions in a form which was directly interpretable within the context of the existing processes of the D4CS program.

The survey that was circulated in advance to subjects consisted of 26 multi-part questions, crafted to cover the experiences of digital forensics practitioners in both private consulting and private in-house subsectors. These questions were worded in unbiased, open-ended language, to ensure that the responses solicited would reflect the interviewee's true and unencumbered thought process.

Below is the 26 question survey instrument which was distributed to each subject (in written form) in advance; the survey responses were collected through a semi-structured in-person or telephone interview.

1. *What are the titles among your colleagues and a brief description of this person's duties?*

   (For example: Forensics Analyst - Conduct computer forensics investigations and electronic discovery requests for legal and corporate clients, using proprietary methodologies and cutting edge forensics tools).

2. *Who (by title only) is responsible for:*
   A. *The acquisition of the devices?*
   B. *The image?*
   C. *The forensic analysis?*
   D. *Is the forensic analysis spilt among multiple people?*
   E. *Deciding that the device is given back to the original owner?*
   F. *Do you rotate any of the above jobs? If so what is that process?*
   G. *Please describe the process from the time a device is decided to be acquired till the device has finished its life cycle of the above steps (including who (by title only) responsible for each step)*

3. *What skills/knowledge did you already possess prior to taking this position?*

4. *What tools are most often used?*
   A. *Do you normally use tools created and sold or use custom tools like Enscript?*

   b. *If you use customs tools, where/how did you learn these skills? What advice would you give to someone trying to obtain these skills?*

5. *How often do you utilize hash values? For what purpose?*
6. *What is the procedure to ensure that the original evidence was not tampered with? Creating a checksum/hash before doing a copy? What hashing functions are used?*
7. *What devices do you most often analyze? Which tool do you most often use for this analysis?*
8. *A request for search comes in…*
   a. *Who (by title only)/Where is this request most often coming from? (the detective, the client, the DA?)*
   b. *How much autonomy do you have to explore hunches on your own?*
   c. *Who (by title only) creates the key word searches, grep analysis etc…*
   d. *How many tools do you normally get to use on the device in question?*
   e. *When the report is done, whom (by title only) does it get passed on to?*
9. *Can more than one person work on the image? If so, what is the handover procedure?*
10. *What skills/knowledge have you picked up on the job that you feel are most important?*
11. *How many devices are typically searched in a case?*
12. *To your recollection, what is the largest number of devices collected for a case?*
13. *What is the typical memory/disk space that you are searching on per device?*

14. *In case that the original device (ie. phone or flash drive for example) is damaged, can just the "SIM card" (phone) or memory chip (flash drive) be extracted from the device and be used to look for evidence?*
15. *What is your typical case load per week? Per month? Per year?*
16. *In your opinion, how important is a working knowledge of file systems?*
    a. *Would the master's program benefit from an entire class devoted to file systems? If so why?*
17. *How often does a device come in and you don't have the necessary tools to extract the data?*
18. *How do you handle password-protected or encrypted devices? Is brute-force password guessing allowed to extract the evidence?*
19. *What resources do you use when you hit road blocks? Which websites are most helpful? Your co-workers? Mentors?*
20. *What resources do you use for best practices?*
    a. *Example: Creating guidelines for policy and best procedures?*
21. *What are you feelings about BYOD "bring your own device" vs being given a company phones? e.g. right to investigate a personal phone used for business or a company owned phone.*
22. *What types of investigations having been trending over the past sixth months?*
23. *Are external contractors allowed to work on evidence? If so what's the on-boarding procedure?*
24. *What are your concerns with investigations involving the cloud?*

25. *Are you part of any organizations such as infrared, Electronic Crime Task Force, meetup groups, etc.? If so, do you find these valuable in keeping up with the latest security trends?*
26. *Have you ever testified for a trial? If so, how many times?*

Semi-structured interviewing based off the above 26-question survey enabled us to derive comparisons across interview respondents. Although the responses might be used to provide speculations into possible correlations between particular survey questions, there is insufficient data to withstand rigorous statically analysis. Nevertheless, any such correlations will be noted in the discussion, so that they may be revisited in later research that seeks to expand the size and scope of the survey sample we used.

The end results, upon completing our comparisons across study participants, will provide us with a better understanding of the variety of private sector digital forensics team processes, as well as individual roles, and skills required to function in them. This will shed light into how such teams operate, and the differences and similarities between the teams at different organizations. From such information, we will be able to distill the common "core" processes, roles, and skills that best represent the realities within the world of contemporary private sector digital forensics. These distilled "core" facets will be synthesized, and will then serve as the foundation of our design of a for-profit student-staffed Digital Forensics Services Corporation.

4. Case Studies

In what follows, we present key information collected in the course of the semi-structured interviews of study participants, a convenience sample of three (N=3) D4CS alumni drawn from a variety of different private sector organizations. The organizations will remain anonymous throughout, by referring to them only as A, B, and C. No individuals are named. This section directly addresses objectives #1-#3 described in Section 2 of this report.

4.1. Organization A

Organization A falls under the category of private sector consulting. This team of digital forensics practitioners serves the organization through billable hours to a third party. Most of the investigations tend to follow guidelines dictated through this third party, and team members refer to the 3rd party as "the client". This organization has both a forensics team as well as an eDiscovery team. These two teams are considered separate entities of the organization, although they work collectively on the same projects.

Actors and their Responsibilities for Organization A:

- *Forensics Evidence Technician*:
  - Collects devices from the client.
  - Creates images of the collected devices.
  - Analyzes basic created images, including running automated tasks and necessary admin work. These automated tasks include defining files through given file extensions.

- *Forensics Analyst*:
    - Capable of all responsibilities of a Forensic Evidence Technician.
    - Analyzes deleted files and is responsible for the deleted file reports.
    - Obtains the timestamp of the last time the computer was on.
    - Creates custom scripts as needed on a case-by-case basis.
    - Analyzes dump files and capable of resurrecting data. Ensuring data integrity is a crucial part of this job and must be kept in mind with all of these steps.
    - Decides which tool is the proper tool to use for the image being worked on, this differs from device to device based on the format of the device.
    - Hands over all harvested information to the eDiscovery team. Customizes data for the eDiscovery team.
- *Senior Evidence Examiner*:
    - Capable of performing all responsibilities of a Forensics Analyst.
    - Provides a more in-depth analysis, which is sometimes needed in situations that go beyond the scope of a Forensics Analyst.
    - Functions as a liaison between the analysts and the clients. Provides clients with updates and allows analysts to perform their duties without pressure from the Client.

- *Director*:
    - Capable of performing all responsibilities of a Senior Evidence Examiner (though in practice the Director does very little actual casework).
    - Manages the project. Understands and resolves issues between the analysts and the Client. Attends the first meeting with a new Client to ensure a smooth transition.

Organization A's process always begins with contact from a prospective client. The Director initiates the case by determining if it is feasible in terms of team manpower and client budget. After a case has been established, the Director will choose which team member(s) are to work on the case. The number of team members and level of expertise varies from case to case, based on case needs and competing allocations of personnel to other cases. It is possible that existing work needs to be reassigned to different team members within the project lifetime. It may also be necessary to restructuring existing projects to make profitable contracts feasible with new clients. In this situation, the hand-off procedures across personnel changes do not follow strict Chain of Custody (COC) protocols. Rather, the hand-off procedure is very informal, and usually just involves an oral communication between digital forensics practitioners.

The client dictates most of the investigative processes within the organization. If the client stresses urgency and is willing to pay for priority escalation, the case can have multiple digital forensics practitioners assigned to it. Similarly, if the client knows exactly what they are looking for and where, the client

can customize the search/analysis to their problem area. The most important factor involving the client is the manner in which the data on a device is collected and how the data is imaged. Organization A is unique in the sense that it's one of the few organizations that allow *selective collections*. Selective collection means that when a device is imaged, the whole device is not imaged; only the relevant portion is. Other organizations would not risk imaging only a portion given the option to image the entire device for fear that something might be overlooked. Organization A is able to be this lenient on this, since the end outcome will almost never end up as a court case (Nelson, Phillips, & Steuart, 2009, p. 9). This is because the client hiring Organization A is usually requesting forensic analysis on devices owned by the client, and is seeking answers to questions relating to their internal business operations. Examples of such questions include, but are not limited to misuse of company resources, intellectual property, proprietary information released, fraud and embezzlement. If these business operation-related inquiries were severe enough to end up in court, the client corporation would have filed a police report (instead of hiring Organization A). In fact, the client relies on Organization A's discretion, particularly as the perceptions of stock holders are to be managed.

After collection/imaging, the main responsibility of Organization A's team is reformatting trustworthy data. Reformatting data is transforming data from the image and storing it separately in a new file. Reformatting of data is carried out for two reasons, (i) the data needs to be shown to the client in a more readable form and (ii) the data must go to the eDiscovery team for further investigation. If the data needs to be passed onto the eDiscovery team, some of the data could be reformatted

to ease the computing power needed for conducting searches. A good example of reformatting the data for eDiscovery is separating the emails from the image since the eDiscovery team will need to follow email chains closely. Organization A's team uses a wide range of tools suited for different scenarios. Although Organization A's team uses many off-the-shelf tools, such as EnCase and FTK; the team is encouraged to create custom tools by using Enscript and programming languages like Perl. These tools parse the imaged data for items of interest, verifing the data's integrity and then format the findings for further analysis. At least two tools are used for each extraction, in order to cross-validate results. After a digital forensics examiner completes this analysis, a practitioner of equal or higher experience reviews the work. The analysis report then gets handed over to the eDiscovery team for further investigation.

4.2. Organization B

Organization B falls under the category of private sector consulting. This team of digital forensics practitioners serves the organization through billable hours to a third party, in much the same way as Organization A. Organization B's primary commercial product is off-the-self forensics tools for digital forensics labs in numerous countries. Secondarily, Organization B provides services through its digital forensics team, which may be hired by clients to conduct investigations; the clients for this service tend to be companies without in-house digital forensics teams. The commercial products and services of Organization B thus run complementary to one another.

Actors and their Responsibilities for Organization B:

- *Consultant*:
  - Collects and images the devices.
  - Performs all necessary administrative work revolving around evidence management.
  - Processes the collected images through standard eDiscovery procedures. Extracts the relevant data and reformats the data for eDiscovery to use. Maintains data integrity throughout the process.
- *Senior Consultant*:
  - Capable of performing all responsibilities of a Consultant.
  - Performs basic forensics analysis. Eliminates useless files from the images and flags important files from the image.
  - Interacts with the client and manages client's expectations.
- Manager:
  - Capable of performing all responsibilities of a Senior Consultant.
  - Manages staff and provides clients with staff's statement of works.
  - Engages with the client on a more daily basis than the Senior Consultant.
- *Senior Manager*:
  - Capable of performing all responsibilities of a Manager.

- Conducts the business development of cases.

- *VP*:
  - Builds relationships with clients and other important members of the company**.**
  - Conducts strategic operations:
    - Plans offices openings.
    - Responsible for staff resourcing**.**
  - Engages in revenue management for the division. Budgets cash flows for the division and ensures the division's basic provisions are present.

Organization B's process begins with a client reaching out to a Manager or a Senior Manager. The client will request Organization B to image and perform analysis of a hard drive(s) or some other types of devices. The Manager will then provide a statement-of-work to the client to review and sign off on. The Manager will then examine the availability of the staff on hand and assign a staff manager to perform the collection. In some situations, due to urgency of the matter, the Manager may be best suited to arrive on-site first. The individual performing the collection is responsible for all actions performed during the collection phases including the verification process. Before the Consultant can leave the site, target and backup copies of the evidence must be made. The Consultant must also send documentation and verification information to the Manager prior to leaving the site. This procedure is put in place to ensure the integrity of the data collection while at the client's site.

Using the scenario in which the evidence is being returned back to the owner. The Consultant will make sure the Chain of Custody (COC) for obtaining and returning the original evidence has been signed, and that the COC for the target and backup drives have also been completed and are associated with the original evidence. The evidence will then be taken to one of Organization B's primary facilities were evidence is stored or uploaded for processing and analysis. The evidence must be signed into the evidence room, or shipped to one of Organization B's primary labs. Standard policy and procedures (devised internally by Organization B's staff) are used when transporting, using encrypted drives and shipping one drive at a time. The assigned Consultant will then inform the Manager that the evidence is available for processing and analysis. The Manager in turn will either then keep the Consultant who performed the collection or, depending on the specific skill set needed, assign a different Consultant to perform the analysis.

The Analyst, Manager, and client will work on time lines and communications and reporting. Any information provided to the client will be channeled through the Manager; unless the Manager has made request for the Analyst to provide an update. Once a final report has been submitted, the case is backed up in Organization B's repository. After a fixed period of time the client is informed of the drives in Organization B's facility with option of having the evidence returned or destroyed.

Since Organization B is a forensics tool creator, Organization B mainly uses tools previously created by the company. Sometimes custom tools are developed, but the tool must to be approved by a software committee within Organization B,

prior to their use in analysis.

4.3. Organization C

Organization C falls under the category of private in-house digital forensics. Organization C is in an information sensitive industry. Loss, mishandled, altered or unauthorized access to Organization C's data can adversely affect the welfare of the organization and Organization C's customers. The Computer Incident Response Team (CIRT) in Organization C consists of digital forensics practitioners whose responsibility is to protect the organization's data from theft and misuse. The team serves the organization by investigating potential threats. These threats can originate internally from employees and clients, or externally from 3rd parties seeking to exploit organization C's assets or undermine its operations.

Actors and their Responsibilities for Organization C:

- *CIRT Investigator*:
    - Reviews the natural lifecycle of security plans. This natural lifecycle includes development of the plan, testing the plan and proper implementation of the plan.
    - Explores latest security products and end-user (employees) control techniques. These security products and control techniques are put in place to prevent theft and enforce company policy.
    - Identifies regulatory changes that will affect the information

security policies. Some of these policies include policies enforced by government, for an example Payment Card Industry Data Security Standard (PCI Security Standards Council, LLC, 2006-2012) or Basel III Accord (Bank for International Settlements ("BIS"), 2012).

- Creates standards and procedures documentation. This documentation is essentially a do's and don'ts list for employees to follow when using company's devices.
- Investigates breaches in data security. Recommends appropriate actions to rectify the incident.
- Develops and provides training to the staff on distributed information security administration procedures. This company stores sensitive information in multiple physical places and must take extraordinary steps to ensure the data's integrity when transferring it over the network.
- Produces security effectiveness metrics and reporting to management.

- *CIRT Senior Investigator*:
  - Capable of performing all responsibilities of a CIRT Investigator.
  - Evaluates new and proposed security systems and technologies.
  - Provides technical support to clients, management, security administrators and network operations.
  - Defines, establishes and maintains data security-related

infrastructure. This infrastructure includes data security-related applications and processes.

- Reviews circumstances surrounding data security incidents and designs corrective actions.

- *CIRT Manager*:
  - Manages staff and the department's day-to-day operations.
  - Leads development and enforces policies and procedures.
  - Monitors audits to ensure the company's procedures are in accordance with government regulations and board members' expectations.
  - Assesses business needs against security concerns. Many times employees will perform acts to ease their work load; these acts can create a security breach. An example would be an employee uploading a document to the cloud to work on outside the office. If the document contained sensitive information and ended up in the wrong place or wrong hands, it could create a major security breach.
  - Works closely with server and network operations and application development. Server and network applications must function properly to ensure security procedures and systems work. Server and network operations are the enforcers of the policies, after all any policy can be created but without enforcement the policies will not be followed.

- Monitors and assesses security violations, incidents and responses.

Organization C's process begins with a CIRT Case opened by CIRT Manager or any other CIRT member. These cases most likely originated from an incident identified by a different department within the organization. The departments most apt to initiate cases include eDiscovery, Legal, HR, Corporate Security and Fraud.

After the case has been initiated, the device in question must undergo acquisition. There are several methods used by Organization C to perform an acquisition; imaging on-site, imaging through a live acquisition and imaging at the lab. The most common method is to image the device on-site. The hard drive is imaged onsite by a CIRT member or Field Services using EnCase Portable; the forensic image is delivered to the Forensics Lab with a completed COC. The CIRT team has the ability to acquire images via EnCase Servlet, which is a live acquisition connecting to the end point over the network. This live acquisition method is not generally used since data can be modified in the process and lack of bandwidth creates constraints. Another commonly used acquisition method is for the CIRT team or Field Services (by request of CIRT) to collect the physical machine in order to image the machine back at the lab. After the machine is collected, the COC is completed stating where the device was confiscated and where it was delivered (e.g. the Forensics lab). The source machine is never powered on and must be imaged. The hard drive is then removed from the machine and connected to a Tableau write blocker/Forensics workstation. A forensic image is acquired using EnCase, this

process can be performed by any CIRT member. An MD5 hash value is computed to ensure forensically sound or "pristine" image.

Once the acquisition is complete, a CIRT member performs the investigation. The CIRT team has the authorization to perform any investigation approved within the policy approved by the Chief Security Officer. CIRT members must adhere to the highest ethical standards. These standards are created internally mainly utilizing documentation from National Institute of Standards and Technologies (NIST) best practices (National Institute of Standards and Technologies, 2012), though Organization C's staff and third party vendors have made amendments to the NIST standards in order to conform to their industry specific needs. The investigations vary greatly, however the most common investigations include cyber attacks, DDoS attacks, Java/Javascript malware infections, and unauthorized file sharing or "data loss".

After the investigation is complete, data and the report may be transferred back to the department where the case originated (Legal, HR, Corporate Security, Fraud, Law Enforcement, etc). Once the case is closed, the device may be returned to user after approval from CIRT Manager, or the device may be put on legal hold (by order of the Legal department). If the hard drive is no longer needed, Field Services may recycle the hard drive. Prior to recycling the hard drive, the device must be wiped clean by a CIRT member or Field Services depending on the nature of the evidence extracted from the hard drive. To complete the process, a CIRT member will store the forensic image and digital evidence on the organization's long-term storage system. The same CIRT member will mark the case as closed in

the case management system. Most cases within Organization C both begin and end internally, even when the threat originates at an external source (e.g. when a malware infection has occurred, the report originates from an end user within an internal department, and the investigation is performed to ensure the department's sensitive data has not been stolen or maliciously altered).

5. Survey Analysis

In this section, we describe similarities and variations among the interviewed respondents' answers, thus charting out the practice of digital forensics across private sector Organizations A, B, and C. The discussion is grouped into topics areas, covering attitudes, tools, hash values, information resources, procedures, devices, and keeping current. This section thus directly addresses our objective #4 described in Section 2 of this document.

Attitudes. Though each interviewed individual was unique, all practitioners interviewed reported common traits suited to the profession of digital forensics. These are best summarized in the following declaration made by one of the practitioners being interviewed:

> "A digital forensics practitioner will never begin a case with a preconceived outcome. Instead, a good digital forensics practitioner will listen and obtain as much information about the case as possible prior to going onto the case. Once on the case, a digital forensics practitioner will keep all prior information gathered during pre-case status and try to match to case with the gained information. If the case matches up, then it's a smooth day on the job. More likely than not though, it won't match up."

In the course of the interviews, many incidents were related in which initial expectations of the investigators did not match later revelations. One interviewee was asked to image 20 machines for a case; however when arrived on-site it turned out to be over 200 computers. Another analyst was supposed to be working on a

theft case, but it turned out the person of interest had a huge stash of child pornography on the device. The device and all the findings of the digital forensics practitioner had to then be turned over to the law enforcement authorities.

Tools. When the conversation turned to which forensics tools are used, two tools are always mentioned: EnCase and Cellebrite. FTK came in a close third, though EnCase was almost always used when investigating Windows PCs. Some teams will use both EnCase and FTK on a Windows machine to cross-validate results. Cellebrite is always used for smart phones. After these three forensics tools, the list of second-tier tools used grows long quickly. Each team has its own preferences. Tools mentioned include Nuix, NetAnalysis, Sawmill, HBGary, Paraben, ECA, MPE and SilentRunner. A common problem reported is that it is often very complicated to extract data from new devices. Depending on the organization, which tools are appropriate can be a sensitive subject. One interviewee's organization creates tools as their main commercial product, so using custom or third party tools is almost a serious offense. Other organizations encourage their team members to improve their skills through individual tool creation. One interviewee created a custom parsing tool using their Java/C# skills, which were first learned in their undergraduate studies. Others were encouraged to improve their Enscript skills while employed. Yet another interviewee mentioned using a third party call Index Engine for obtaining forensic images on some difficult devices. The interviewee praised Index Engine (Wiles, Cardwel, & Reyes, 2007, p. 161) but acknowledged that it was very expensive.

Hash Values. Every digital forensics practitioner interviewed had a

proficient working knowledge of hash values and reported using hash functions routinely. The reported uses of hash values were consistent, with three major types of use appearing. The first way in which hash values are used is to assist in the hash validation of forensic images. The hash value allows a digital forensics practitioner to verify that the forensic image was captured successfully. Most forensics imaging tools provide MD5, SHA1 (Aquilina, Malin, & Casey, 2009, pp. 243,400-402), and SHA256 (Sobh, 2008, p. 314) results, therefore as an examiner if you receive forensic images you did not collect personally collect, your first step should be to verify the image integrity by recalculating the hash value. The second procedure in which hash values are used is called hash analysis. Hash analysis is a quick way to do file comparison, and so can be used to locate files of interest within a large datasets in a relatively short time. When performing hash analysis, a digital forensics practitioner will use a collection of hash values called a hash set. Hash sets are used for two main purposes; 1) identify files the digital forensics practitioner may be potentially interested in and 2) eliminating known "clean" files that are harmless or have nothing to do with the case. A good example of using hash sets to identify files of interest is searching an employee's flash for a copy of a specific company file. Most digital forensics practitioners begin analysis by identifying files that are basic software commonly found on most desktops (Windows Registry Dataset) (Nelson, Phillips, & Steuart, 2009, pp. 230-237). NIST has hash sets for both types of files; files of interest and files to eliminate (The National Institute of Standards and Technology, 2012) . If the digital forensics practitioner knows the exact file(s) they are looking for, the digital forensics practitioner can create a hash

set of the hash value(s) of the file(s). An example of looking for a known file(s) is when searching for known viruses or child pornography. If the digital forensics practitioner does not know the exact file(s) he or she is looking for, eliminating benign files, such as executable files of Windows preinstalled software; is effective in narrowing down the search (Nelson, Phillips, & Steuart, 2009, p. 264).

Information resources. A consistent grievance among all interviewed digital forensics practitioners is the lack of documentation in the field. Many subjects claim that their team members are their first source of information when dealing with unfamiliar situations. One organization has monthly and quarterly meetings to go over training needs. Those that are fortunate enough to work with very knowledge teams are in the best situation. Regardless of knowledge of their team members, all digital forensics practitioners seem to assign a premium value to their professional network. Most subjects report joining professional organizations (such as High Technology Crime Investigation Association (HTCIA) (HTCIA Inc, 2010) and NYNJ Electronic Crimes Task Force (United States Secret Service, 2012)) and foster the relationships created within these organizations. These organizations tend to have mailing list, where users post questions. The next source of information is the forensics tool's support forums and forensics tool's tech support. One digital forensics practitioner praised EnCase's support forum as a secondary resource to turn to (after his co-workers). When all else fails Google is often the last resort, though "the problems that occur in the digital forensics field are so obscure and so specific that Google is hardly an option".

Procedures. Each organization had their own standards for processes and

procedures created to fit their own needs. Only one organization used an outside resource to define their daily procedures. This particular organization used NIST (National Institute of Standards and Technologies) best practices (National Institute of Standards and Technologies, 2012) to formalize protocols involving internal staff and third party vendors. Each organization did have standard internal operating procedures for certain job-related functions in order to create consistency between digital forensics practitioners on their own team. The details of reported procedures and team roles/structure were presented in depth in Section 4.

Devices. The digital forensics practitioners interviewed consider computer hard drives to be the device type that is most often analyzed. Analyzed hard drives are often either extracted from desktops or laptops, and are installed with Windows XP or Windows 7 operating systems. Computer hard drive data is most commonly analyzed, understandably since most end users perform their primary work functions on desktops or laptops. The next most commonly analyzed device is a Windows 2003/Windows 2008 servers. All these devices can be analyzed using EnCase and/or FTK. All digital forensics practitioners interviewed reported noticing an increase in the number of analyses performed on tablet and cell phone devices. One digital forensics practitioner noticed a growing trend in needing to collect data from cloud storage. This same practitioner also stated that they had created a customized script to obtain metadata from Google Docs, and that as tablet and cell phone devices continue to flood the market, cloud storage and mobile forensics would be an ever-larger fraction of forensic analyses conducted.

Keeping Current. In the ever growing, ever changing field of digital

forensics; a practitioner must stay current with today's problems and observe the upcoming trends. The digital forensics practitioners interviewed keep current by joining organizations (e.g. Meetups and professional chapters) and reading recommended books in the fields. Digital forensics practitioners recommend following discussion forums, twitter feeds, and blogs of companies and individuals in the forensics field to keep abreast about the field and emerging trends.

6. Discussion

6.1. Skills and Technological Competencies in Digital Forensics

Here we address Objective #5 by reporting the skills and technological competencies that study participants reported were used daily in the profession of digital forensics practitioners. Although each digital forensics practitioner interviewed possessed wide ranging knowledge about digital forensics (both practical and theoretical), they appeared to rely on a small arsenal of forensics tools to carry out their work. Without familiarity with these tools, it would have been "impossible to meet professional deadlines". Although the list here consists of tools that were emphasized by at least one of the study participants, list contents are prioritized from highest to lowest importance, based on the number of subject participants who gave the item emphasis in their narrative.

6.1.1. Tools:

HIGHEST IMPORTANCE

EnCase is a software application that is capable of producing a bit-by-bit image of a device that is forensically sound (Casey, 2011, p. 112). The image's integrity can be verified through hash values (Casey, 2011, p. 482), including MD5 and SHA-1, which are most commonly used today (Casey, 2011, p. 22). After creating an image, EnCase has the ability to analyze it. EnCase can go through slack space and identify files using a myriad of ways, including file name extensions. Although EnCase can perform many analyses, many digital forensics practitioners

prefer to use other tools created for specific purposes since these tools do a better job (Olivier & Shenoi, 2006 , p. 88) (Guidance Software, Inc., 2012).

FTK is the abbreviated name for Forensic Toolkit (AccessData Group, LLC., 2012), and is a software application similar to EnCase but with a smaller user base. FTK also has the ability to produce a bit-by-bit image of a device using hash values to ensure data integrity, as well as analyzing the image slack space and perform basic file identification. EnCase and FTK have such similar capabilities that it is advised to create images and run the analysis on both tools and compare the outputs to validate correctness of results (AccessData Group, LLC., 2012) (Aquilina, Malin, & Casey, 2009, p. 187).

Cellebrite is hardware and software used mainly for forensic data extraction from mobile devices. Cellebrite is capable of performing extractions on numerous devices, including devices running iOS, Android and BlackBerry operating systems. Cellebrite also has the capability to forensic extraction on GPS devices (Cellebrite Mobile Synchronization LTD, 2012) (Hoog, 2011, pp. 229-234) (Hoog & Strzempka, 2011, pp. 220-228) .

MEDIUM IMPORTANCE

EnCase Portable is a USB drive equipped to create forensic images in both live mode (i.e. when the machine is running) and boot mode (when the target machine is off) (Guidance Software, Inc., 2012) (Bunting, 2012).

RegRipper is a Windows registry data extraction tool, developed as an open source forensics software application by Harlan Carvey. RegRipper extracts

Windows registry hives from an EnCase image and produces a readable report (Aquilina, Malin, & Casey, 2009) (Churchill, 2010, p. 196).

Tableau is a hardware write blocker. Write blockers allow read commands to execute but blocks write commands from being executed (Guidance Software, Inc., 2012) (Sammons, 2011, p. 41).

Encase Servlet is part of the EnCase Enterprise suite, and is a server that will communicate with the target machine to perform a remote extraction (Bunting, 2012, pp. 164-167) (Guidance Software, Inc., 2012).

WinHex (Windows) and **HexEditor** (Linux) are hexadecimal editors that allow digital forensics practitioners to analyze and compare files (Aquilina, Malin, & Casey, 2009, p. 190) (X-Ways Software Technology AG, 2012).

HBGary Responder Pro is a software tool that analyzes RAM, pagefiles and VMWare images, as well as reconstruct dismembered executable files within memory dumps (Aquilina, Malin, & Casey, 2009, p. 103) (HBGary, Inc., 2011).

HBGary FGET is a software tool that performs remote data collection in a forensically sound manner from Windows operating systems. HBGary FGET collects raw NTFS volumes and is capable of recreating a file access and modification time line (HBGary, Inc., 2011) (Aquilina, Malin, & Casey, 2009, p. 89) (Higgins, 2010).

EnScript is a scripting language used by EnCase. EnScript's language is based on C++ operators and C++ basic syntax extended using a built-in set of classes and functions. Scripts or small pieces of code written in EnScript are called EnScripts, and can be used to automate a number of forensics processing tasks. Digital forensics practitioners can create their own EnScripts, or can take advantage

of the ones provided by Guidance Software (Bunting, 2012, pp. 508-511) (Guidance Software, Inc., 2012).

LOWER IMPORTANCE

Nuix is a software analysis tool that is especially useful at analyzing emails, particularly when the email is stored in an application called Thunderbird (Nuix, 2012).

Paraben P2 Commander is a forensics tool which serves a multitude of purposes, similar to EnCase and FTK. Paraben P2 Commander specializes in email analysis but is capable of performing other types of analysis including file detection and registry analysis (Paraben Corporation 2012, 2012) (Wilding, 2006).

Sawmill is a software router log analyzer. Sawmill will process log files, analyze the log files and then create reports from the analysis (Ec-Council (Ed), 2009, pp. 4-18) (Flowerfire, Inc., 2012).

NetAnalysis is a software tool designed to extract and analyze internet history, and was created by Craig Wilson in 2001 as part the Kent Police Digital Forensics Unit in the U.K. (Digital Detective Group Ltd, 2001-2012) (Mohay, 2003, p. 159).

MPE is the short name for Mobile Phone Examiner, and is a software application designed to image mobile devices. Collected images are fully compatible and designed to be analyzed using FTK software (AccessData Group, LLC., 2012).

SilentRunner is tool that analyzes a company's network, investigating the network looking for anomalies in the system. SilentRunner is similar to an intrusion

detection system and can be used in evaluating vulnerabilities as part of incidence response (AccessData Group, LLC., 2012).

Index Engine is a product that extracts data from an offline tape drive and presents the data in a readable and searchable manner (Index Engines Inc, 2012) (Wiles, Cardwel, & Reyes, 2007, p. 161).

6.1.2. Skills and Other Common Technological Competencies:

Programing language fluency and experience in coding and software development is often cited as highly advantageous to the digital forensics practitioner. Some digital forensics practitioners described the professional benefits they derived from creating a custom using Java, C# and/or Perl. Although these skills are not necessary to perform most of their duties, they give the practitioner a clearer understanding of how the tools they are using achieve their goals (and how they might be being thwarted). Some digital forensics practitioners have created their own customized tools drawing on their knowledge of programming. A practitioner will create a customized tool when the current off the shelf options fail to meet their needs.

Hash values are crucial to the practice of digital forensics. The most commonly used hash value functions are MD5 and SHA1, however as computing power increases SHA256 will gradually replace the phased out MD5 and SHA1 (Aquilina, Malin, & Casey, 2009, pp. 400-402) (Sobh, 2008, p. 314). Study participants emphasized knowing what hash values are and how they are created; the different types of hash values functions used in field and some of the problems surrounding specific hash values functions. Many indicated that they

underestimated the significance of hash values and how hash values are utilized in the field when they first started.

File system familiarity is a universal obsession for the study participants, who considered their lack of understanding of file systems to be a serious liability when they first entered the work force. Several reported hurriedly learning the material on their own: reading about file systems concepts, and building practical skills involving narrowly-focused off-the shelf forensics tools. Having such a conceptual scaffold made them more able to harness the vast capabilities (and minutia) of forensics tools like EnCase and FTK.

Public speaking was seen as important by all of the digital forensics practitioners interviewed, though the nature of public speaking differed from organization to organization. Although none of the subjects have yet testified in court, several anticipated doing so. One subject stated that most people who have testified have started their careers in the public sector, though that doesn't imply that people in the private sector do not testify. Some of the subjects said that their public speaking skills were invaluable in explaining the situation and options to their clients. Some subjects reported using their public speaking skills to lobby superiors concerning potentially advantageous policy changes. In short, public speaking and communication skills were reported to be essential to distinguishing oneself as a digital forensics practitioner.

Research was seen as another important experience by the study subjects. All of the digital forensics practitioners interviewed reported that their research experience helped prepare them for the process of procuring information and

evaluating its usefulness. One study participant mentioned, Toyota's "5 Whys" (Ōno, 1988, pp. 17-18) technique as a recommended perspective on research methodology. Another subject pointed out that the lack of documentation in the digital forensics field requires a person to be proficient researcher if they want to advance and succeed.

6.2. The Digital Forensics Process

Here we address Objective #6 by synthesizing a digital forensics process (i.e. a "workflow") that draws inspiration from (and so remains close to) the structures reported to exist in the N=3 private-sector organizations whose members were surveyed.

Although each organization we investigated had slightly different processes in place, each of the digital forensics practitioners interviewed knew his or her process well. In our interviews, we found that the process adopted within each organization served to prescribe how each case was worked on, and so greatly influenced how the digital forensics practitioner conducted their daily work. If the practitioner was working in an organization where billable hours were valued, the practitioner was conscious of needing to follow orders and respect the constraints of the client who held the purse strings. If the practitioner was working as an in-house analyst within an organization where shareholders were calling the shots, the practitioner was conscious that their job was to shine light on anything that went against company policy. These subtle pressures highlight the fact that students of digital forensics need to be made aware that the real-world practice of the

profession looks quite different in each of the aforementioned settings, and that practitioners in different setting often produce results that reflect the skew of the pressures and priorities at play in the specific context.

With the above caveat in mind, we found that the investigative processes in all three organizations shared 5 common elements:

1. **Initiation**: Contacting with client to specify services requested and objectives (as a series of questions to be answered or information to be obtained), as well as to negotiate the timeline, budget and other constraints.

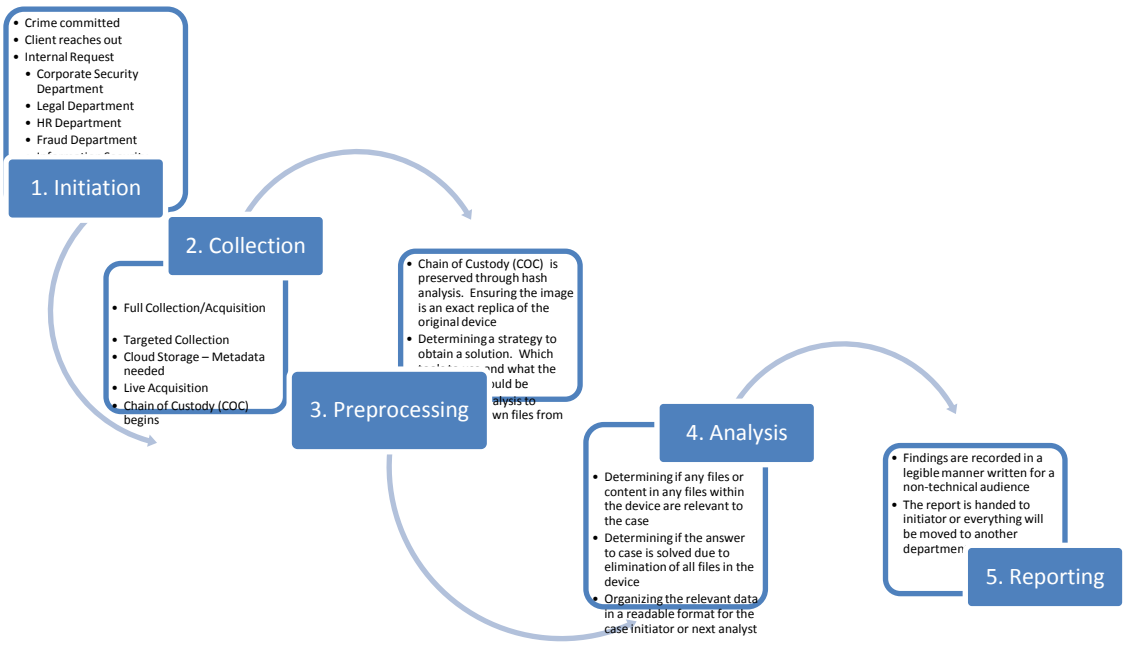
2. **Collection**: Full or targeted collection, initiation of chain of custody.

3. **Preprocessing**: Determination of best strategies given service request and objectives, exclusion of irrelevant data using hash analysis.

4. **Analysis**: Filtering data down to a set of files that appear to be relevant to service objectives. Determination if these files resolve the objectives determined in the Initiation phase (i.e. questions to be answered or information to be obtained).

5. **Reporting**: Communicating the conclusions of step 4 back to the client in a non-technical report.

A visual rendering of the 5-phase process is given below:



6.3. The Digital Forensics Roles

Here we address Objective #7 by distilling out a set of roles within digital forensics teams, and assigning functions to each role (in terms of the process synthesized in Section 6.2). The roles we identified are:

A. **Technician**. Responsible for conducting process phases 2 and 3, using *at least* following subset of tools and skills identified in Section 6.1:

- Collection and Preprocessing
    - Disk images: Encase, FTK, Encase Portable, Tableau write blocker
    - Mobile platforms: Cellebrite, MPE
    - Network: Sawmill, NetAnalysis, SilentRunner
    - Live acquisition: HBGary

- Email: Nuix, Paraben
- Knowledge of hash value functions such as MD5, SHA1, SHA256

B. **Analyst**. Upon acquiring a specified amount of experience and demonstrated competency as Technician, a team member may advance to the role of Analyst. In this role he or she is engaged in phase 4 of the process, using the following subset of tools and skills identified in Section 6.1:

- Disk images: Encase, FTK, Encase Portable, Tableau write blocker
- Mobile platforms: Cellebrite, MPE
- Network: Sawmill, NetAnalysis, SilentRunner
- Live acquisition: HBGary
- Email: Nuix, Paraben
- Knowledge of hash value functions such as MD5, SHA1, SHA256
- Custom EnScripts, C++ programs.

C. **Consultant**. Upon acquiring a specified amount of experience and demonstrated competency as Analyst, a team member may advance to the role of Consultant. In this role he or she is engaged in phases 1 and 5 of the process, and so additionally leveraging communication skills in client interactions so as to clearly convey technical information to nontechnical people.

D. **Director**. Upon acquiring a specified amount of experience and demonstrated competency as a Consultant, a team member may advance to the role of Director. In this role he or she is engaged in developing and extending the scope of services offered and potential clients (i.e. broadening the scope of phases 1 and 5).

6.4. The Design of a Digital Forensics Services Corporation

The question arises on how to reify the processes and roles synthesized in Sections 6.2 and 6.3 to form a viable, self-sustaining, student operated Digital Forensics Services Corporation at a college—a business within the school. Here we present one idea for achieving this, through the vehicle of a data recovery service business. First we address the question of basic business viability; then, subsequently, we describe how digital forensics operations can be embedded inside of a data recovery business.

Business Analysis. John Jay College enrolls approximately 14,000 undergraduate students each semester. If 0.5% of them (1 in 200) experience loss of electronic data in the course of a semester (e.g. loss of data due to a hard disk crash, loss of contacts on a broken cell phone, a non-functioning USB drive), then this would imply that roughly 70 individuals are in need of digital forensics services each semester. If college-wide advertising (e.g. electronic signage, orientation services, the school bulletin, etc.) reaches 50% of these potential clients, these informed clients provide a steady stream of approximately 88 cases per year (counting Summer enrollment as half that of regular semesters). At present, commercial data recovery services charge an upfront fee to check if media is recoverable (typically $50); if so, then full data recovery becomes an option (typically costing may cost $800, or more for large drives). This is standard pricing for established data recovery companies, e.g. Scott Moulton (myharddrivedied.com). Let us assume that 75% of the drives that are brought in are determined to be

recoverable (the remaining have physical damage which requires clean room facilities beyond what is available at the college); then this means that 66 cases each year are expected to be recoverable, while 22 are not. If the John Jay Digital Forensics Lab charges a similar $50 fee to check, and a very competitive $200 (as opposed to $800) for recovery services, the anticipated revenue stream from such an operation would be $17,600 per annum. Such funds could be recycled into the digital forensics lab's resources, which ultimately serve as a resource for students in the Master's program.

Embedding Digital Forensics inside Data Recovery. On the one hand, we have chosen *personal data recovery* as our proposed business service offering because (i) The college students and employees provides a steady customer stream for data recovery; (ii) Personal data recovery also does not suffer from the same level of pressure as digital forensics does by being in a high-stakes legal setting, and (iii) Personal data recovery is less susceptible to branding and reputation concerns. On the other hand, the purpose of this lab is to provide students with practical experience in *digital forensics* investigation before they enter professional private sector employment. On the surface, the concerns and experiences of digital forensics seem quite different from the concerns and experiences of personal data recovery. How can the two be bridged?

What we propose to do is the following. When a client approaches the lab for personal data recovery services, the on-staff consultant (see roles in Section 6.3) will ask the client to describe all the "information of interest" which was present on the drive, when these files were created and modified, and hints about the

information that the files contained. These questions will be asked "to help the analysts recover as much of your data as possible". The consultant will then interpret this description as though it is a request for digital forensics analysis seeking specifically to determine if those files exist on the drive, when they were created/modified, and if their content is as described. The consultant will draft a "Request for digital Forensics Analysis" (RFA) document based on their initial discussion with the client, and the 5-stage process (see Section 6.2) will be conducted with this RFA serving as the authoritative guideline. At the end of the 5-stage process, at the end-of-case meeting, the client will be presented the imaged recovered drive (to the extent that it was possible), together with the report that was generated to address the request for analysis.

7. Conclusions

In the course of this research, various trends are apparent. Digital forensics is a wide and rapidly growing field in the private sector. Private sector labs appear to use a core set of identifiable tools, and forensics teams are organized around a functionally similar set of roles that serve to streamline the forensics process. The ability to communicate ideas between peers and research new solutions are both critically important, since there is little documentation to refer to (and little hope for it given the rapid changes in the field). Currently, most of the devices that are investigated within the private sector are hard drives from servers. Most of the study subjects indicated that the future trend is mobile devices such as cell phones and tablets. Though most practitioners are aware of the governing laws, particularly Chain of Custody and company policies on client confidentiality, beyond these well-known guidelines, study participants did not put too much weight on the potential impact of emerging laws, since they felt that the field would have plenty of time to adapt given the pace of the legislative process.

Those aspiring to be future digital forensics practitioners have many options for education, training and experience. Despite the lack of official standards in this rapidly changing field, striking commonalities exist across private sector digital forensic labs, in terms of tools, skills, roles and processes. These commonalities can be used to synthesize a viable, self-sustaining, student operated Digital Forensics Services Corporation within a college like John Jay, which could in turn help prepare students to transition into private sector employment in digital forensics.

8. Glossary

Acquisition - See Imaging

Backup Drives – are hard drives containing the copy of forensic image/collection.

COC – aka Chain of Custody is the chronological documentation of the lifecycle of the evidence collected. Proof of certainty that the evidence collected has not been tampered with. Each person having custody/being in possession of the evidence verified the integrity of the evidence has remained the same since inception of the acquirement.

Collection - See target collection

Consultant – a person who give professional advice and/or services.

Evidence – presentation of an item that hold a proof of fact relating to an incident.

eDiscovery – as oppose to forensics is an ongoing investigation. eDiscovery goes through a series of analysis over long periods of time, sometimes years.

Forensics – short for Digital Forensics or Computer Forensics encompasses but not limited to the procedure of imaging a device, analyzing the image and formatting the data.

Hash Value – an unique number of a constant length produced by a unidirectional function using arbitrary length input. Each input should always produce the same output and theoretically no two different inputs should ever produce the same output.

Imaging - the process where the entire device's contents are duplicated to a file and a hash value is calculated to verify the data's integrity. Both software tool and hardware tool can be used to create an image.

Private Consulting Forensics – a group of consultants who perform digital forensics activities for private firms for a fee on the private firm's own devices.

Private In-House Forensics – forensics activities performed on company's devices by their own employees.

Public Sector Forensics – forensics activities performed on personal devices after the device was confiscated due to an illegal infraction.

Target Collection – the process where the parts of a device's contents are duplicated to a file and a hash value is calculated to verify the data's integrity. Both software tool and hardware tool can be used to create an image.

Target Drives – are hard drives containing the forensics image/collection.

Windows Registry Dataset – a database used by Windows operating systems to store configurations needed for end-users, applications and hardware devices.

Write blocker – are devices, software or hardware, which is used during imaging to prevent damage to the device being imaged. Write blockers allow read commands to execute but prevents or blocks write commands from being executed.

9. Bibliography

AccessData Group, LLC. (2012). *FTK AccessData Digital Forensics Software*. Retrieved October 2, 2012, from AccessData: http://www.accessdata.com/products/digital-forensics/ftk

ACLU. (2011, December 1). *ACLU Opposition to H.R. 3523, the Cyber Intelligence Sharing and Protection Act of 2011*. Retrieved October 18, 2012, from ACLU American Civil Liberties Union: http://www.aclu.org/technology-and-liberty/aclu-opposition-hr-3523-cyber-intelligence-sharing-and-protection-act-2011

Aquilina, J. M., Malin, C. H., & Casey, E. (2009). *Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides.* Elsevier.

Bakan, J. (2005). *The Corporation: The Pathological Pursuit of Profit and Power.* Simon and Schuster.

Bank for International Settlements ("BIS"). (2012, October). *International regulatory framework for banks (Basel III)*. Retrieved October 8, 2012, from Bank for International Settlements: http://www.bis.org/bcbs/basel3.htm

BBC. (2012, April 26). *Cyber-security bill Cispa passes US Hous*. Retrieved October 15, 2012, from BBC: http://www.bbc.co.uk/news/world-us-canada-17864539

Brenner, S. W. (2009). *Cyberthreats: The Emerging Fault Lines of the Nation State.* Oxford University Press.

Brito, J. (2011, November 7). Congress's Piracy Blacklist Plan: A Cure Worse than the Disease? *Time* .

Bunting, S. (2012). *EnCase Computer Forensics -- The Official EnCE: EnCase Certified Examiner Study Guide.* John Wiley & Sons.

Burdeau v. McDowell, 256 U.S. 465 (1921) (Supreme Court of United States June 1, 1921).

Caloyannides, M. A. (2004). *Privacy Protection And Computer Forensics.* Artech House.

Casey, E. (2004). *Digital Evidence and Computer Crime, Second Edition.* San Diego, California: Academic Press.

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet.* Academic Press.

Cellebrite Mobile Synchronization LTD. (2012). *THE WORLD OF UFED...* Retrieved September 30, 2012, from Cellebrite delivering mobile expertise: http://www.cellebrite.com/mobile-forensics-products/forensics-products.html

Churchill, M. (2010, June 14). *Turning Regripper into Windowsripper*. Retrieved from SANS™ Institute Computer Forensics and Incident Response: http://computer-forensics.sans.org/blog/2010/06/14/turning-regripper-windowsripper/

Digital Detective Group Ltd. (2001-2012). *Internet History Extraction & Analysis: NetAnalysis*. Retrieved October 20, 2012, from Digital Detective: Forensic Software Products: http://www.digital-detective.co.uk/products.asp

Ec-Council (Ed). (2009). *Computer Forensics: Investigating Network Intrusions and Cybercrime.* Cengage Learning.

Fetterman, D. M. (2010). *Ethnography: Step-by-Step.* London UK: SAGE Publications.

Flowerfire, Inc. (2012). *Sawmill*. Retrieved October 12, 2012, from Sawmill: http://www.sawmill.net/products.html

Gardner, T. J., & Anderson, T. M. (2010). *Criminal Evidence: Principles and Cases.* Belmont, CA: Wadsworth Publishing; 6 edition.

Guidance Software, Inc. (2012). *EnCase Enterprise v7*. Retrieved October 15, 2012, from Guidance Software: http://www.guidancesoftware.com/encase-enterprise.htm

Guidance Software, Inc. (2012). *Guidance Software*. Retrieved September 30, 2012, from http://www.guidancesoftware.com/: http://www.guidancesoftware.com/

HBGary, Inc. (2011). *HB Gary Products and Services*. Retrieved October 20, 2012, from HB Gary: http://www.hbgary.com/products

Headland, T., Pike, K., & Harris, M. (. (1990). *Emics and Etics: The Insider/Outsider Debate.* Sage Publications, Inc.

Higgins, K. J. (2010 , September 8). Forensics Out Of Reach For Most Small To Midsize Organizations. *Dark Reading* .

Hoog, A. (2011). *Android Forensics: Investigation, Analysis and Mobile Security for Google Android.* Elsevier.

Hoog, A., & Strzempka, K. (2011). *iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices.* Elsevier.

HTCIA Inc. (2010). *High Technology Crime Investigation Association (HTCIA)*. Retrieved November 10, 2012, from High Technology Crime Investigation Association (HTCIA): http://www.htcia.org/

Index Engines Inc. (2012). *Backup Tapes Index, Search and Extract Data from Offline Tape without Restore*. Retrieved October 10, 2012, from Index Engines Power Over Information: http://www.indexengines.com/tape_engine.htm

Jahoda, G. (1977). *"In Pursuit of the Emic-Etic Distinction: Can We Ever Capture It?".* Basic Problems in Cross-Cultural Psychology (Y.J. Poortinga, ed.).

Jarrett, H., Bailie, M. W., Hagen, E., & Judish, N. (2009). Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. *Computer Crime and Intellectual Property Section Criminal Division* . Office of Legal Education Executive Office for United States Attorneys. Retrieved from http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf

Leigland, R., & Krings, A. W. (Fall 2004). A Formalization of Digital Forensics. *International Journal of Digital Evidence , 3* (2).

Lillard, T., & Garrison, C. P. (2010). *Digital Forensics for Network, Internet, and Cloud Computing: A Forensic Evidence Guide for Moving Targets and Data.* Syngress.

Little, A. (2009). *Power Trip: From Oil Wells to Solar Cells---Our Ride to the Renewable Future.* HarperCollins.

Lovely, R. W. (2012). *Comparison of Existing and Anticipated Programs of Study*. Retrieved November 25, 2012, from Digital Forensics and Cybersecurity - D4CS: http://web.jjay.cuny.edu/~fcm/pdfs/Comparison of Existing and Anticipated Programs of Study.pdf

Mohay, G. M. (2003). *Computer and Intrusion Forensics.* Artech House.

National Institute of Standards and Technologies. (2012, September 18). *Computer Security Division Computer Security Resource Center*. Retrieved from http://csrc.nist.gov/publications/PubsSPs.html

Nelson, B., Phillips, A., & Steuart, C. (2009). *Guide to Computer Forensics and Investigations.* Cengage Learning.

Nuix. (2012). *Nuix*. Retrieved October 16, 2012, from http://www.nuix.com/Products

Olivier, M. S., & Shenoi, S. (. (2006). *Advances in Digital Forensics II.* Springer.

Ōno, T. (1988). *Toyota production system: beyond large-scale production.* Productivity Press.

Paraben Corporation 2012. (2012). *P2 Commander v2 Computer Forensic Analysis Software*. Retrieved October 25, 2012, from Paraben Corporation: http://www.paraben-forensics.com/p2-commander.html

PCI Security Standards Council, LLC. (2006-2012). *PCI SSC Data Security Standards Overview*. Retrieved October 9, 2012, from Security Standards Council: https://www.pcisecuritystandards.org/security_standards/index.php

Rep Smith, L. (2011). Stop Online Piracy Act. *H.R.3261* . Committee Consideration and Mark-up Session Held.

Rep. Rogers, M. (2011). Cyber Intelligence Sharing and Protection Act of 2011 (Introduced in House - IH). *H.R. 3523* .

Sammons, J. (2011). *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics.* Elsevier.

Schensul, S., Schensul, J. J., & LeCompte, M. (1999). *Essential Ethnographic Methods: Observations, Interviews, and Questionnaires.* Rowman Altamira.

Shi, Y. Q. (2009). *First Digit Law and Its Application to Digital Forensics.* Busan, Korea: Springer Berlin Heidelberg.

Smith v. Maryland, 442 U.S. 735 (1979) (Supreme Court of United States June 20, 1979).

Sobh, T. (2008). *Advances in Computer and Information Sciences and Engineering.* Springer.

Solove, D. J. (2010). Fourth Amendment Pregmatism. *Boston College Law Review Vol. 51* , 1511-1538.

Solove, D. J. (2004). *The Digital Person: Technology And Privacy In The Information Age.* NYU Press.

Solove, D. J. (2008). *Understanding Privacy.* Cambridge, MA: President and Fellows of Harvard College.

The National Institute of Standards and Technology. (2012, September). *Downloads*. Retrieved from The National Institute of Standards and Technology Information Technology Laboratory: http://www.nsrl.nist.gov/Downloads.htm

United States Secret Service. (2012). *New York/New Jersey Electronic Crimes Task Force*. Retrieved November 12, 2012, from United States Secret Service: http://www.secretservice.gov/ectf_newyork.shtml

United States v. Miller, 425 U.S. 435 (1976) (Supreme Court of United States April 21, 1976).

US v. Jacobsen, 466 US 109 (1984) (Supreme Court of United States April 2, 1984).

Wilding, E. L. (2006). *Information Risk and Security: How to Protect Your Corporate Assets.* Gower Publishing, Ltd.

Wiles, J. (2007). *TechnoSecurity's Guide to E-Discovery and Digital Forensics: A Comprehensive Handbook.* Elsevier.

Wiles, J., Cardwel, K., & Reyes, R. (2007). *The Best Damn Cybercrime and Digital Forensics Book Period: Your Guide to Digital Information Seizure, Incident Response, and Computer Forensics.* Syngress.

X-Ways Software Technology AG. (2012). *WinHex: Computer Forensics & Data Recovery Software, Hex Editor & Disk Editor*. Retrieved October 20, 2012, from X-Ways Software Technology AG: http://www.x-ways.net/winhex/index-m.html

Zdziarski, J. (2008). *iPhone Forensics: Recovering Evidence, Personal Data, and Corporate Assets.* O'Reilly Media, Inc.