SAMPLE CASE STUDY STUDENT REPORT – UH Maui College

Discussed with students in the Administration of Justice Program

Case Study on the Digital Forensics Capabilities for Small, rural police departments

Problem - Law enforcement agencies in rural areas in the US have limited skills and technologies to support digital forensics investigations. As a result, the problem is that crimes that involve the collection and analysis of digital evidence get delayed or processed incorrectly.

RQ1: What do rural law enforcement agencies, with limited digital forensics capabilities, do now to collect and analyze digital evidence?

RQ2: What is the potential for rural law enforcement agencies to create a starter digital forensics kit, that will enable the speedier collection and processing of digital evidence? What are the components of this kit that would be reasonable and cost-effective for rural law enforcement agencies?

Digital Forensics in Law Enforcement

STUDENT NAME

BUS 393v

University of Hawaii Maui College

Overview

One of the most analytical aspect of present investigations regarding law enforcement is digital forensics. Digital forensics is the science that precisely works with crime that involves electronics. Digital forensics deals with how data is analyzed, studied, stored and gathered. This involves salvaging investigation or analysis data that electronic devices contain in their storage. This type of science is very efficient when it comes to exploring digital data and digging up facts in the digital format like no other category of the current investigation tools.

Furthermore, when people discover that their enterprise has been breached or has been a victim of cybercrime, their initial thoughts go to solving the immediate problem. But for true cyber professionals that is only the beginning. It is important for digital police officers to undergo a thorough process of identifying, preserving, analyzing and presenting digital evidence. Since the 1970's the field of digital forensics has evolved to keep up with the wide spread of adoption of technology and the means in which of these technologies are used for criminal activity.

The use of computers for financial crimes in the 1980's has helped shaped digital forensic methods in what they are today. With the introduction of modern computing a new landscape for criminal activity has emerged. The need to gather new forms of evidence turned digital forensics into a vital tool used by law enforcement in the pursuit and conviction of crimes both computer based such as human exploitation, cyber stalking and cyber terrorism. But also, computer facilitated such as illegal data breaches that result in theft of information.

In addition, digital police officers are also referred as digital forensics detectives. Forensic endeavors or digital forensics professionals can be found working in private institutions or law enforcement agencies. These specialists are vital when it comes to crime investigations.

Background

To support this new discipline specialized tools have also emerged to assist investigators in the capture, analysis and preservation of evidence that might arise during the course of investigating that criminal activity. Any part of an enterprise system can be vulnerable to criminal activity, data theft or unauthorized penetration. Forensic analysts must make sure to analyze storage media, hardware and operating systems, networks, and applications to locate the point of compromise. The mission criticality of the compromised application, system or network determines the level of investigation.

When conducting a forensic investigation, it is important to follow the digital forensics scientific process. This process covers the entire evidence gathering procedure from data collection, to examination and analysis, and to reporting. In the data collection phase investigators obtain search authority, document the chain of custody and hash and duplicate all evidence. In the examination and analysis phase, investigators validate their tools, perform analysis and reproduce those methods and outcomes for reassurance. The reporting phase is critical as it is when conclusions are made, and expert evidence or testimony is presented since investigators are usually required to present evidence as part of expert testimony.

Using this scientific process increases the likelihood that any evidence found will fully be admissible in a court of law. In any organization, there happen to be humanized mistakes and if they are the victim of a breach, they can automatically bring law enforcement digital forensics professionals or an external forensics specialist.

Computer systems, networks and mobile devices can all be utilized in or fall victim to a cyber attack. Each device type has different intrusion methods and requirements for evidence handling. This has led to the formation of three distinct branches of digital forensics. For

instance, computer forensics may rely on the need to create a disc image to preserve evidence or virtual drives may be used to emulate an entire machine. Network forensics focuses on the monitoring and analyzing of computer network traffic. Mobile devices present their own unique challenges due in part to memory volatility as low power DRAM used in smart phones can lose data when powered off. This is why proper handling procedures and adherence the documented chain of custody must be followed to protect and preserve such evidence.

Regardless of where an attack occurs the enterprise cyber security program should have policies that address all forensics considerations such as contacting law enforcement, monitoring and conducting regular reviews of forensic policies, guidelines and procedures. This should take into account the need to preserve and maintain evidence, as well as other requirements such as accreditation for instance, in situations where card holder data is involved as well as the decision to involve outside specialists. When one discovers that their enterprise has been breached, digital forensics can ensure that best practices are observed throughout the evidence gathering process.

It is important to consider that digital data has many types and states on how it is stored and the ways of storage that organizations should implement. Since it is crucial for every organization to properly manage their digital information and taking the right cautionary steps at all times in order to be safer than just a regular computer user that is storing valuable information on their device.

Furthermore, without digital forensics, evidence can go unnoticed or become compromised and systems may remain vulnerable to additional attacks. As cyber criminals get more sophisticated and data breaches become more damaging to enterprises, digital forensics and the digital forensics scientific process will be able to provide a means to bring cyber criminals to justice in the worlds increasingly complex and fast-moving technological landscape.

Problem Statement

Law enforcement agencies in rural areas in the US have limited skills and technologies to support digital forensics investigations. As a result, the problem is that crimes that involve the collection and analysis of digital evidence get delayed or processed incorrectly.

RQ1: What do rural law enforcement agencies, with limited digital forensics capabilities, do now to collect and analyze digital evidence?

RQ2: What is the potential for rural law enforcement agencies to create a starter digital forensics kit, that will enable the speedier collection and processing of digital evidence? What are the components of this kit that would be reasonable and cost-effective for rural law enforcement agencies?

Time is one of the biggest factors when it comes to investigation including violent crime, and the initial and most efficient source of evidence is a criminal's digital footprint. This could be on any device such as laptop, desktop, tablet or smartphone. Every investigator wants to make informed decisions faster. The need for speed without compromising forensic principals is essential.

Most crimes have a digital footprint, common electronic devices can store digital evidence and regardless of the environment there are some basic forensic response strategies that can be used. The rural law enforcement agencies with limited digital forensic capabilities do their investigations by "bagging, tagging and sending" devices to a laboratory for analysis, but this has two significant impacts. Firstly, the number of devices seized for analysis continues to grow and coupled with an ever-increasing storage capacity results in huge backlogs. Secondly there is no discrimination between items likely to contain evidence and items with no relevance to the investigation. This results in increasing number is unnecessary forensic examinations

impacting significantly on laboratory resources, costs and the innocent users of such systems. The forensic laboratories of the rural law enforcement agencies find it impossible to cope with the strategy of seizing everything. In fact, many rural agencies outsource their workload in an effort to keep up, leading to incredibly high costs and extended time scales.

Furthermore, when it comes to onsite imaging, to avoid seizing everything it is very common for forensic investigators to be onsite and to use specialized equipment to perform forensic imaging, the first step in the preservation of digital evidence. For instance, imaging a 500-gigabyte disk takes at least three hours and multiple drives of increasing capacities take even longer. This strategy reduces laboratory efficiency as the experts trying to work through lab backlogs are often the one required to be onsite, spending hours waiting for the imaging to be complete.

Another option called digital triage might help, triage CD's and thumb drives enable the review of some suspect devices such PC Laptops, PC Netbooks, PC Tower, Thumb drive, Memory card but cannot cope with devices like cellphones, iPads, MacBook's, External HDD or GPS devices. Most of these solutions are configured using a Windows computer which is also used to review the reports. However, this can lead to Windows computer being contaminated with the results from previous evidence and the possibility of the triage device becoming infected by viruses. While triage CD's and thumb drives can speed up the forensic response they cannot handle all the devices likely to be encountered or the deployment controls required to enforce a good forensic practice.

What these rural law enforcement agencies need is a real digital forensics starter kit. This Basic starter kit will include, a forensic laptop, tool sets, digital camera, case folder, blank forms, evidence collection supplies, cables for fast data transfer, blank hard drives and hardware write

blockers. This starter kit will contain secure and reusable collectors which store the evidence and allowing unlimited simultaneous deployment in order to save time. This forensic laptop will have a windows 10 operating system as it is relatively faster than other operating systems. This will also include a touchscreen interface which will make the law enforcement investigators job easier and more efficient.

Moreover, removable media such as thumb drives, memory cards or loose hard disks can be examined easily and rapidly using the built in right protected interfaces. On site data collection by using a digital forensic starter kit can be easily used by non-specialized staff or agents. This means the digital forensic kit that will be used will ensure best forensic practices which means immediate results with maximum forensic control. Not to mention this kit will be able to handle multiple phones, tablets and GPS devices at once.

The rural law enforcement agencies will benefit by using a starter digital forensic kit during their investigations. This will result in a faster and more efficient way of identifying devices likely to contain evidence which can then be submitted for full analysis. Since there is no time to waste when it comes to real time access to digital evidence at the crime scene can make a hug difference between a case they could end up going cold or a case that could be solved very quickly. This results in the waste of resources and valuable time which can then lead to the investigation being unsolved. It is easy to state that gathering and analyzing takes time especially if officers are using traditional forensic methods where information is gathered and send back to the lab to be analyzed. But the truth is, this is not the best way, officers are looking for a more efficient way where they can easily and not to mention quickly access the devices and get access within minutes. Also, it is important that officers that start a case that they ensure the integrity of the situation and collect accurate evidence every step of the way.

Literature Review

According to an article written by Infosec Institute (Computer Crime Investigation Using Forensic Tools and Technology, 2018, May 21) the number of people with mobile devices or computers are going up at a very high rate. Since evidence is needed in a court of law, a skilled examiner is able to gather crucial data at crime scenes with a digital forensic kit. Law enforcement agencies big and in rural communities are sometimes only dependent on digital forensic investigators in order to extract, preserve, analyze and present that specific data in a court of law.

Just as in the real-world people leave traces of themselves such as fingerprints, clothing fibers, hair or DNA. This happens when people interact with others, places and objects the same thing goes for the activities that happen in the digital realm, where there are pieces of evidence that get left behind. These digital or virtual traces are incredibly valuable when it comes to law enforcement agencies trying to solve an investigation. They may be valuable evidence when it comes to establishing the roots of a document or piece of software for legal purposes while determining the actions of the people involved in a criminal case. This could also be a source for criminals contemplating to rebuild their data or simply identifying credentials on their victims.

Thanks to today's technology, digital forensic investigators have the capability to extract information that has been, encrypted, deleted and/or hidden in any device. This is done by using important digital triage tools, techniques and proprietary software forensic applications, to analyze platforms or devices in order to be able to extract important data and use it to solve that particular crime investigation. Even though digital forensic experts are able to extract data that later becomes analyzed at a lab, it is important to state that time is of the essence during any investigation. For some rural law enforcement agencies, this is a huge problem.

Time is crucial when it comes to any investigation, particularly violent crime. Usually the suspects digital footprint is the most effective and first of evidence. These could be on a laptop, desktop, smartphone or tablet. The rural law enforcement agencies that do not have access to mobile digital forensic kits need to do their investigations the hard way which is known as "traditional forensics". These devices usually get collected at the crime scene which is then transported to a forensics lab for interpretation. Investigators use systematic method to analyze evidence that could be used in a court of law. Though as stated before, usually lab analyzing results in significant time loss.

There are two types of analysis during digital crime investigations, dead analysis and live analysis. Dead analysis means that investigators try retrieve data from unpowered or not working devices. This usually means that they need to be sent back to the lab for examination. The second analysis is live analysis where the devices they seize are still running and they are able to receive data from the device thanks to portable tools like a digital forensics kits that can easily be transported by the examiner to the crime scene to start examination almost instantaneously.

Moreover, it is important to state that there are barriers when it comes to extracting data from mobile phones. Companies like Nokia, Huawei and Apple have unique encryption technologies and protection tools and make extraction of data very tough on investigators while obligates digital forensic examiners to keep up with the most recent developments at a faster rate than ever before. In today's world, the devices that are manufactured are highly advanced and not to mention produced at a very high rate. Extraction of data from these devices offer distinctive challenges even after going through the basic security features that protect these devices. So all and all this also takes time to solve, and if rural law agencies do not use or have access to a simple starter digital forensics kit, their jobs will just become harder and harder.

Findings

After interviewing two digital forensics officers, detailed information has been received from both of them. When it came to how important digital forensics were during their investigations, both of them replied as it is very crucial. All of their investigations rely on digital evidence whether this is internet-based threats or distribution of child pornography etc. They always get cases where they have to extract evidence from mobile phones or computers. Also, there are times when physical evidence is not enough when it comes to crime cases and since we live in a world that is technologically evolving daily most of the cases they work with requires collection of digital evidence in order to solve that specific investigation. For instance, the Charlie Scott murder case that happened in 2014 on Maui was solved with collecting and analyzing digital evidence which came from a mobile phone.

When it comes to cyber-attack investigations, rural agencies such as Maui Police Department do not see too much cyber-attacks where they try to attack a network. What they get more is that internet-based extortion type of claims where people get phishing scam emails. Yahoo seems to be getting a lot of attacks like these. Furthermore, it is crucial to collect digital evidence properly and MPD does so by is sending out the initial responding officers that will recover any device that they come into contact with. If it is a patrol investigation they will seize a phone or computer and then submit it into to MPD's evidence room where it will be analyzed until further notice. Not to mention, if the suspect is at the crime scene the officers most of the time are able to get the personal passcode from the suspects in order to receive information from the mobile device.

Furthermore, both officers said that time is very critical when it comes to gathering digital evidence at crime scenes. For instance, when it comes to the recovery of information on a

cellphone, if at the scene they cannot get it, the evidence is basically gone or at least most of the time it ends up being gone. With laptop's they are a little more flexible but with phones, time is very critical. Also, they do not rush their investigations as they might end up missing or gathering digital evidence that could help and solve the case. But the problem they face with this is that it takes too much time sometimes to receive evidence as, it is gathered and sent back to the lab to be examined and they have to wait on the results.

Other information such as how to retrieve data from encrypted hard drives, mobile phones and recovering deleted files were asked the officers. Encrypted phones usually pose a little bit of a problem to MPD. Some phones such as iPhones cannot be accessed without the passcode. So, the officers go to the homes of the crime scene with a search warrant to find if the individual has any information of their passcode written somewhere or they simply ask them until the individual tells it to them. For encrypted hard drives, they also get it with the passcode, which take time to find. Also the way MPD recovers deleted files which is done manually is with a hex viewer. They manually search the hexadecimal code. This comes out to looking for file header information that looks interesting or is related to the crime.

Furthermore, when it comes to using a starter digital forensics kit for their crime cases instead of traditional forensics, both officers replied with very useful in all sorts of aspects when it comes to investigating digital forensic crime cases. Without it their jobs are quite hard and time consuming. For them it will be easier to handle all these cases. The less complicated the procedure is the better it will be for them and MPD. A kit that costs $5,000-$10,000 would not be too much for MPD since it will be saving money in the long run and help MPD receive data faster and in a more efficient way.

Finally, law enforcement as a whole is generally behind the curve when it comes to technology. For instance, apple could one day come out with a new operating system and every agency would be scrambling in order to update all their tools and how they work because apple changes how the file system is storing information etc. Or how Facebook and Google, how the algorithms are storing and sharing data is constantly evolving. Since almost every individual has access to a device such as mobile phones, computers, smart watches etc. These devices keep track of almost everything you do and if one becomes involved in a crime either as a victim or offender, this will help officers track and solve digital evidence related investigations. To have a tool that could help MPD speed up triage would be extremely beneficial.

Analysis

After receiving a good amount of data from the findings report, it is easy to state that rural police departments such as the Maui Police Department are behind the curve when it comes to high tech solutions or devices in order to solve cyber crime cases. For instance, when Maui Police Department was trying to solve the Charlie Scott murder case that happened back in 2014, they did not have access to the newest technologically available digital forensics equipment. This has led the investigation to be delayed. As the officers had to create a map manually and map out what these cellphone records said. It took MPD an entire month going through each line of the phone records.

It was very interesting to hear that MPD does not see much cyber-attack investigations where a criminal tries to attack a network or simply hack into it. Since these attacks are what mostly digital forensics investigators deal with around the country. The investigations that they deal with seemed pretty basic such as phishing scams or extortion claims. So, it is very hard to

tell if the Maui Police Department is well prepared and ready when it comes to the hacking of a big enterprise that is located in a rural place like Maui.

Rural area agencies like MPD usually collect evidence using two paths which was a good thing to hear. As mentioned before, they send out their team to collect all the evidence at the crime scene and take the evidence back to MPD is submitted to their evidence room. Or the second path for instance is usually if an individual gets threatened over a social media website, the officers send a search warrant to the appropriate social media website provider and get information sent directly to the officers, which is a good thing but still does take time.

The officers at MPD both emphasized on how important time was when it came to crime investigations, yet they still are not able to operate their investigations in a faster more efficient way because they do not have access to the right equipment at the moment. Since they are doing their investigations the traditional way, this takes up a lot of valuable time. At the same time, they reported that they do not rush their investigations since they don't want to skip any evidence which also burns up valuable time. The way that MPD is operating their investigations seem to be out dated and needs a proper upgrade.

After getting information on how they receive or collect data from encrypted hard drive, mobile phones or recovering deleted files, it was very interesting to see that they were having a difficult time collecting data from encrypted phones. They usually get access with the passcode, but if they cannot find the passcode, they have to send the mobile device back to the lab until it is cracked. This takes valuable time away, as mention before MPD has to send everything back to their lab in order to receive information. This is definitely not a good way to run investigations. Same result goes for the encrypted hard drives, they need to find the passcode without that they

face difficulties. Lastly when they try to recover deleted files they have to do it manually which is not the best practice.

It was interesting to hear that, not only rural areas, but law enforcement in general is not to technologically evolved (excluding the FBI of course). A lot of the police departments seem to lack in faster more efficient equipment, which ends up delaying everything. From the looks of it, all of these officers end up with more work and the loss of time. Finally, after asking them if a starter digital forensics kit would make their jobs easier, both officers were very positive towards this idea. It was good to hear that starter digital forensics kit would be very beneficial for every rural police department as it will simply make their jobs easier.

Recommendations

A digital forensic kit made by Tritech forensics has helped thousands of officers collect digital evidence faster and more efficiently. The Momentum MT500 DF Mobile Triage kit is one of the most innovated and superior kit that is offered to investigators when it comes to collecting and gathering digital evidence at crime scenes. Even though the mobile digital forensic solution is very sophisticated this starter kit in particular will not require a high level of computer expertise in order to be used. With this great benefit, efficient and faster ways of getting information will be easier for investigators.

The Momentum MT500 DF Mobile Triage kit includes a great add on which is the ADF Solutions software or Cellebrite Software which at the moment is the best digital forensic tools for investigators and examiners. This specific digital evidence investigator has been created to meet both field triage and forensic lab requests. Both of these software's provide examiners with advanced search configurations, and separate collection and authentications keys which enables the investigator or examiner to scan multiple devices at the same time and

instantaneously (these could be laptops, mobile phones, tablets etc). It is also user friendly and limits user risk since its ease of use.

The Celebrite software is known as an all in one software solution. It automatically familiarizes itself with variety of environments and user workflows and at the same time is compatible with Windows which most of the individuals that have computers are running on this system. Forensic sound extractions are offered by a closed and self-contained environment. As mentioned before, operations or extraction of data can easily be handled simultaneously, all type of data is supported, and it enables the validations of recovered data by its unique state of the art verification engine. Not to mention the system comes with automatic frequent updates.

The ADF Solutions Software offers a version called the Triage Investigator. This has simply been designed for field triage investigations. Investigators in rural areas can highly benefit from Triage investigator because it is primarily used by examiners with limited digital forensic training and like mentioned before, the examiners can greatly benefit from the basic ease of use and the limited risks. Just like the Cellebrite Software, the ADF solutions software extracts critical data in a matter of minutes it easily accesses platforms such as Linux. Macintosh and Windows, it enables examiner to see the results pop up on the criminal's device, offers advanced image analysis and devices that are on and off are easily scannable.

Moreover, Momentum MT500 DF Mobile Triage kit comes with the choice of and L1 or L2 laptop which runs on an incredibly strong i7 processor. As mentioned before this kit allows the investigator to take their lab to the crime scene. The kit in general includes a pelican 1510 case with built in smooth rolling wheels for easy transportation, laser cut foam with a large that comes with a storage pouch, 1 TB hard drives (2 per kit), cellphone tip and cable set, 32 GB rugged usb 3.0 tubes (2 per kit), there are faraday pouches for laptops, notebooks and mobile

phones, a digital camera, L1 or L2 i7 processor laptop, complete logical and physical extraction software, and lastly a choice of ADF solution software (as mentioned before the “Triage Investigator” would be best for rural law enforcement agencies).

Lastly, another good idea could be (if the rural agencies cannot afford or do not have a budget for a starter digital forensics kit) is take all of the extra tools that they have in a lab since most of the time digital forensic labs have a backup and a backup of a tool, and simply convert a police van into a mobile digital forensics lab which they can easily drive it to the crime scene. As soon as they arrive at the scene they can easily extract evidence using their mobile lab which will save a lot of time and make their jobs a little easier. Though the starter kit would be the best.

References

Achieve rapid investigation results with a field digital forensics solution. (2018, March 26). Retrieved from http://www.policeone.com/police-products/investigation/articles/472755006-Achieve-rapid-investigation-results-with-a-field-digital-forensics-solution/

Computer Crime Investigation Using Forensic Tools and Technology. (2018, May 21). Retrieved from https://resources.infosecinstitute.com/computer-crime-investigation-using-forensic-tools-and-technology/#gref

5 digital forensics tools. (2014, May 09). Retrieved from http://www.policeone.com/police-products/Forensics/articles/7170976-5-digital-forensics-tools/

NIST's free software helps agencies test computer forensics tools. (2017, November 27). Retrieved from http://www.policeone.com/police-products/investigation/computer-digital-forensics/articles/461928006-NISTs-free-software-helps-agencies-test-computer-forensics-tools/

ElcomSoft. (n.d.). Digital Forensic Tools For Government and Law Enforcement. Retrieved from http://www.elcomsoft.com/police_and_law_enforcement_solutions.html

The Best Open Source Digital Forensic Tools. (n.d.). Retrieved from https://h11dfs.com/the-best-open-source-digital-forensic-tools/

Momentum MT500 Digital Forensics Mobile Triage Kits/Mobile Triage Kits/Tritech Digital Forensics Online Catalog. (n.d.). Retrieved from https://www.tritechdf.com/mt500-digital-forensics-mobile-triage-kit.html

WHAT IS DIGITAL FORENSICS AND WHY IS IT IMPORTANT? (2018, June 18). Retrieved from http://www.firstlegal.com/what-is-digital-forensics-and-why-is-it-important/

Lally, C. (n.d.). How 1 St. Louis group uses digital forensics to solve crimes. Retrieved from http://news.stlpublicradio.org/post/how-1-st-louis-group-uses-digital-forensics-solve-crimes#stream/0

Walker, J., Stock, A. V., Neray, P., Spaulding, S., Flavell, S., & Patel, Y. (2017, December 11). Digital Forensic And Investigation Capabilities. Retrieved from http://www.informationsecuritybuzz.com/articles/digital-forensic-investigation-capabilities/

Digital Forensics and Crime. (n.d.). Retrieved from http://researchbriefings.files.parliament.uk/documents/POST-PN-0520/POST-PN-0520.pdf

Sloan, J. J. (2018, September 18). There's no code of ethics to govern digital forensics – and we need one. Retrieved from https://theconversation.com/theres-no-code-of-ethics-to-govern-digital-forensics-and-we-need-one-45755

Burger, B. (2018, May 12). Columbus police to create digital forensics unit to analyze cellphone evidence. Retrieved from https://www.dispatch.com/news/20180511/columbus-police-to-create-digital-forensics-unit-to-analyze-cellphone-evidence

Digital Forensics for Law Enforcement. (n.d.). Retrieved from http://www.milwforensics.com/PrivateInvestigatorReviews-computerInvestigationsforPolice

Why UK police are learning cyber forensics. (n.d.). Retrieved from http://www.computerweekly.com/news/450429957/Why-UK-police-are-learning-cyber-forensics

Cracking Cases with Digital Forensics. (n.d.). Retrieved from http://www.rasmussen.edu/degrees/justice-studies/blog/cracking-cases-with-digital-forensics/

Analyze and share digital evidence faster with a tool developed by and for police. (2018, March 12). Retrieved from http://www.policeone.com/police-products/investigation/computer-digital-forensics/articles/471944006-Analyze-and-share-digital-evidence-faster-with-a-tool-developed-by-and-for-police/

Digital Forensics and Enforcement of the Law. (n.d.). Retrieved from https://internetinitiative.ieee.org/newsletter/march-2018/digital-forensics-and-enforcement-of-the-law

Digital Evidence and Forensics. (n.d.). Retrieved from http://www.nij.gov/topics/forensics/evidence/digital/Pages/welcome.aspx

Computer Forensics in the Digital Age. (n.d.). Retrieved from http://www.policemag.com/channel/technology/articles/2012/02/uncovering-truths-in-the-digital-age.aspx

Mayo, K. (n.d.). Computer Forensics. Retrieved from http://www.evidencemagazine.com/index.php?option=com_content&task=view&id=116&Itemid=49

Live Response vs. Traditional Forensics. (n.d.). Retrieved from http://www.symantec.com/connect/blogs/live-response-vs-traditional-forensics-0