2017

Evidentiary Report

VELA CASE DIGITAL EVIDENCE REVIEW

CHAD NELLEY

NELLEY CONSULTING | www.nelleyconsulting.com | www.chadnelley.com

Abstract

This report is intended as a fictional case review of fictional evidence items related to the Brandy Vela Suicide case. It is intended as a research submittal project to show and prove strong knowledge of the evidence gathering, review, submittal and objective opinion submission to a court of law from the perspective of an expert witness. In this representation and report I will attempt to demonstrate sufficient knowledge of the Digital Evidence capture, review and demonstration procedures to the court and articulate the methods used and fictional discoveries made through known and researched best practices. This evidentiary report will attempt to capture and present the computer forensics examination process for the court following the 6 stage best practices model. Those stages include: Readiness, Evaluation, Collection, Analysis, Presentation and Review. This paper specifically is a representation of the 5th stage in the overall process.

Case Background - On Tuesday, 29 November 2016, Brandy Vela of Texas City, Texas committed suicide due to cyberbullying. This evidentiary report will take a look at fictional evidence constructed by the author to express and demonstrate thorough understanding of the process, tools and legal considerations as stated above.

Digital Forensics Examiner Info:

Digital Forensics Examiner:	Chad Nelley
	Detective # 1004692
	Private Practice Digital Forensics Expert - USD MS CSOL
	San Diego, CA
	(555) 555-1212
Subject:	Digital Forensics Examination Report
Offence:	Cyber Bullying resulting in Suicide by Victim
Accused:	Undetermined
Date of Request:	1-Dec-16
Date of Conclusion:	23-Dec-16

Disclaimer: *Prior to beginning this formal report – for those reviewing this material, I think it is important to first disclaim that much of this report output is fictional. While the Case of Brady Vela is very real, for purposes of this assignment a number of assumptions and fabricated information will be introduced to validate my knowledge of the Digital Forensics process for purposes of obtaining a grade in the USD CSOL 590 Digital Forensics Masters Level course work. Anything beyond this point in the report should be considered fictional.*

Table of Contents

Case Background Overview & Physical Evidence Collected

On the evening of Tuesday, 29 November 2016, Brandy Vela of Texas City, Texas was found non-responsive in her home, the victim of a self-inflicted gunshot wound to the head. Witnesses at the scene that were interviewed as part of the investigative process gave investigators initial information that would suggest that the victim in this case, Brandy Vela, may have been a victim of online bullying.

Upon receiving this information, the onsite lead investigator promptly began collecting, bagging and tagging all of the physical evidence that may have contained digital evidence elements and incorporated questions about the state and use of these items immediately following the events of the evening to establish an appropriate timeline and to establish the integrity state of the evidentiary items in question.

It was determined that of all of the physical items collected, none had been tampered with or used immediately following the events of the evening and that the physical evidence should be identified and secured as quickly as possible for remote review. The lead investigator on scene at this time also conducted a field onsite triage to capture any and all potential digital evidence from the physical evidence items, in the event that something should go awry in transportation of the items. The items were then secured in shielded containers and transported directly to the primary evidence locker located at Texas City Police Headquarters.

At this point, I was retained by the court to perform a 3rd party assessment of the physical items to determine if, in fact, there were felonious online bullying events and digital evidence that might support such a claim. The request came to my office on the morning of Thursday, December 1, 2016 at approximately 10:15am via email request from the Texas City District Court in reference to case docket # 45678910BV. Included with the request were instructions on which facility was housing the evidence and specific procedures for performing the assessment onsite at said facility in the Shielded Evidence review room. Subsequently, there were also very specific instructions provided on check-in and check-out of the evidentiary materials to ensure evidence integrity all the way through the review process.

Questions Asked Relevant to the Case

1. Were the items collected and received into evidence confirmed to be those of the victim?
2. Has anyone other than yourself and the police staff initial onsite investigator had access to the items or their contents from the time they were collected until the time at which you reviewed them in the Secure/Shielded Evidence Review Room?
3. Were any of these items, deemed to be someone else's property upon review of the contents/access logs?
4. From the activity logs on these devices leading up to the Nov 29, 2016 incident, is there evidence of online activity of a two way or multiple participant exchange?
5. If so, what information/data was the investigator able to obtain in the course of the review?
6. And if so, was there adequate identifiable information from which the court could obtain further search and seizure warrants against other individuals?
7. What are the unbiased and objective recommendations of the Digital Forensics investigator in this case?

Search and Seizure and transport of the evidence – See Above Details

Exhibits Submitted for Analysis:

1. **Mobile (Smart Phone) Device: Apple iPhone 6 - Physical Evidence Exhibit 9**
2. **Laptop Computer: Dell Inspiron 5200 - Physical Evidence Exhibit 10**
3. **Desktop Printer: HP Photosmart – Physical Evidence Exhibit 11**
4. **Wireless Router: Motorola XV2200 – Physical Evidence Exhibit 12**
5. **Cable Modem: American Scientific – Physical Evidence Exhibit 13**
6. **Mobile (Tablet) Device: Apple iPad 3 – Physical Evidence Exhibit 14**
7. **Thumb drive: Kingston ESET Deslock Encrypted 4GB – Physical Evidence Exhibit 15**
8. **LG 37" Smart TV – Physical Evidence Exhibit 16**

Evidence to Search For

Based on the information gathered through onsite interviews at the scene of the event and the investigator's knowledge and background specific to this type of case it was determined that we would be looking for digital evidence in the area of; (A) acquiring the browsing data from the laptop, smart phone and tablet devices browsers; (B) the call logs and call and text history of the mobile phone device and tablet device; (C) the data files (both deleted and non-deleted) in recent history (last 365 days) on each device as well as the seized thumb drive, and (D) the social media accounts, accesses and histories that can be obtained from each of the devices in question.

Potential Offences

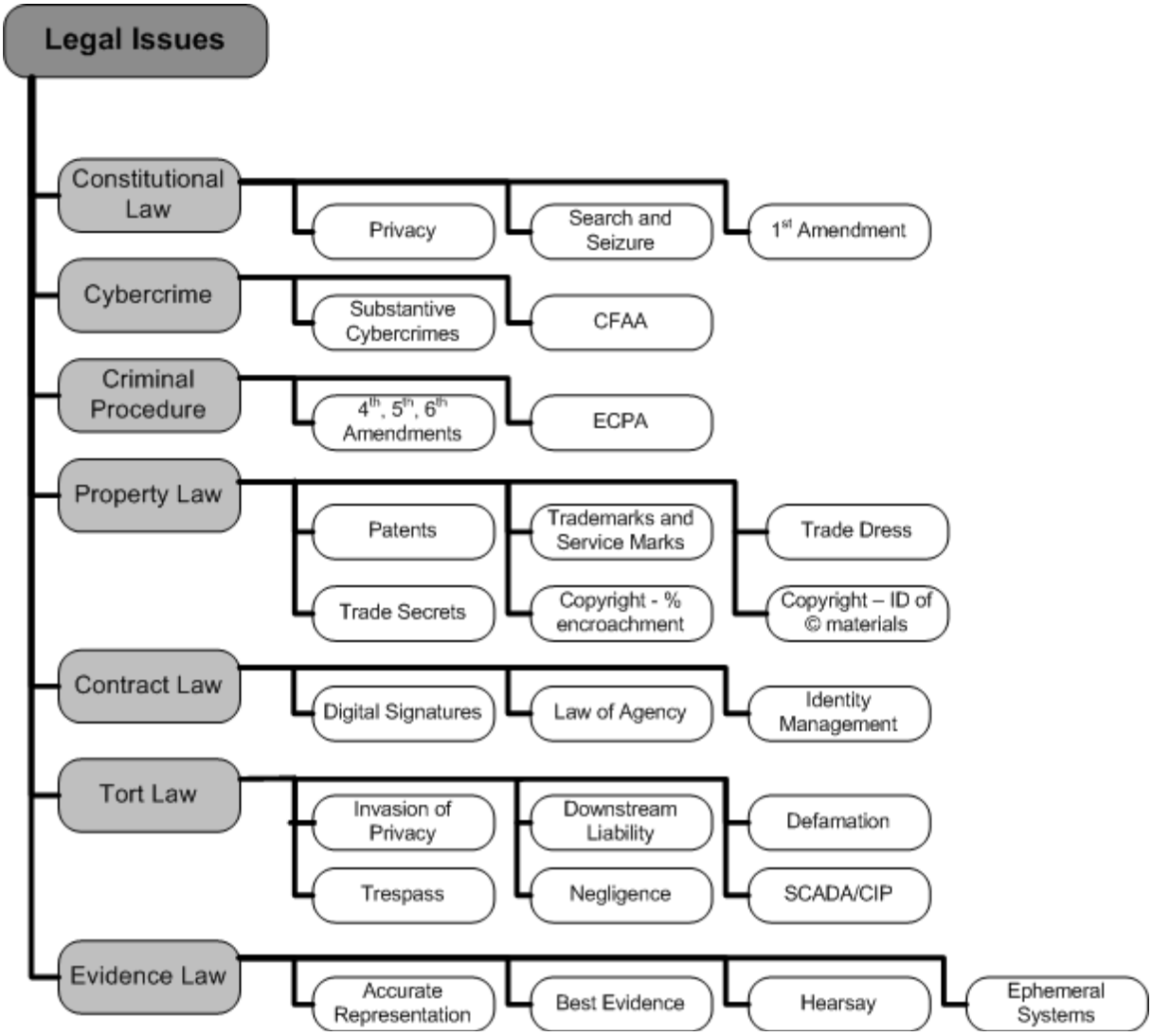
While we have no viable 'suspects' at the onset of this investigation, the potential offences we are seeking to potentially uncover through this process are defined as follows:

- Hate Crimes
- Cyber & Physical Bullying
- Human Trafficking
- Child Pornography & Exploitation
- Extortion
- Threats of Violence
- RICO Violations

Do note that while we do not believe our victim in this case was guilty of any of the above, we do have reason to believe that certain individuals she may have been interacting with online may well have direct ties to the criminal activities listed above. When and if we identify these offences as carried out by others in their interactions with our victim that may have led to or contributed to the outcome in this case, we will make specific recommendation to the courts for follow-up action.

Historical Case Review – Cyber Bullying (Precedence & Legal Factors)

In the diagram referenced below and obtained from a white paper submitted at the proceedings of the 44th Hawaii Conference on System Sciences titled: "Legal Aspects of Digital Forensics" authors Kara Nance and Daniel J. Ryan lay out the Legal factors landscape (1).



(Reference: https://www.computer.org/csdl/proceedings/hicss/2011/4282/00/10-04-03.pdf)

It is from this diagram that we can see what legal implications we will need to be wary of as we move through the Evidence collection and examination process and these are the elements that the Digital Forensics examiner took under consideration as this report was being prepared.

Further, it was critical in the research and preparation phase to look at precedent setting cases in the area of "Cyber Bullying" to ascertain what the courts may and may not accept as evidentiary value and to understand the underpinnings of the decisions that came from these prior cases and how they might impact this case.

Review Case #1: Rebecca Sedwick

This is a juvenile case involving a tri-fecta of tweens and teens that occurred in Florida in 2015. The victim, Rebecca Sedwick was stalked and bullied via her Facebook account by two girls in particular – names to be withheld here. Charges of felony aggravated stalking were brought against the two

perpetrators. In this case, the Digital Forensics investigator assigned was able to review the interactions of the Victim and the suspects via their Facebook accounts and logs and was able to cultivate enough evidence to warrant arrest and bring charges. This case helps us establish that criminal charges can be brought against bullying perpetrators. (ABC News) In my methods and findings section, I will outline the evidence in the Vela case that supports similar charges be brought against our perpetrators when we identify them.

(Reference: http://abcnews.go.com/US/teen-charged-fatal-cyberbullying-case-rebecca-sedwick-remain/story?id=20580689)

Review Case #2: Tyler Clementi

Tyler Clementi was an 18 year old student at Rutgers University who committed suicide by jumping from the George Washington Bridge after his Dorm room mate and a friend secretly taped him in a sexual encounter with another male student. The roommate, Dharun Ravi and the friend Molly Wei were brought before the court to stand trial on charges of invasion of privacy (sex crimes), bias intimidation (hate crimes), witness tampering and evidence tampering. Molly Wei, ultimately made a deal with prosecutors.

In this case, extensive digital forensics revealed a long history of communication threads between the suspect another of his cronies that portrayed and built upon the theory that would build the cornerstone of the "Hate Crime" designation in the case. Ultimately Ravi, the defendant in this case was indicted on 15 counts including 2 counts of second degree bias intimidation (Hate Crime).

(Reference: http://www.newyorker.com/magazine/2012/02/06/the-story-of-a-suicide)

Review Case #3: Jessica Logan

Jessica Logan was an 18-year-old high school senior who sent nude photos of herself to her boyfriend. After the couple broke up the boyfriend sent the photo that was meant for his eyes only to hundreds of other teenagers. The photo sharing led to name calling and taunts at school. Phrases like "slut, porn queen and whore" were regularly spoken referring to Jessica by schoolmates. The taunting continued via Facebook, MySpace and through text messages. After attending a funeral for a boy who had committed suicide, Jessica came home and hung herself in her room.

This case was chosen as an example given its close parroting of the Vela case that involved an ex lover distributing imagery that would ultimately lead to a barrage of online taunting and bullying.

(Reference: https://cyberbullying.ua.edu/index.php/case-study-jessica-logan/)

It is these 3 cases (along with a litany of others) that we believe set precedence for prosecution of this case. The Digital Forensics expert will draw conclusions from the evidence discovered and cited in this report that mirror facts and evidence from the 3 above referenced cases.

Findings & Methods

Before moving onto findings, let me first present to the court the tools and methods we used to examine the physical evidence captured in hopes to uncover digital evidence that would prove valuable in the pursuit of justice in this case.

Methods of Collection

The first order of business in doing a forensic analysis is to isolate and lay out the processes that were used to collect data. Evidence and data integrity throughout the process of evaluation is key to maintaining credibility in and throughout the process. This boils down to two key areas: Evidence Preservation and Acquisition.

Preservation consists of the following elements:

- Securing & Evaluating the Scene
- Documenting the Scene
- Isolation
- Packaging, Transporting & Storing Evidence
- Onsite Triage & Processing
- Generic Onsite Decision Tree

While Acquisition consists of the following elements:

- Device Identification
- Tool Selection
- Expectations
- Device Memory Acquisition
- Tangential Equipment
- Cloud Based Services & Implications

To further expand on these concepts for the courts in the preservation of evidence (digital or otherwise)

Securing and Evaluating the scene can best be described as isolating all of the potential evidence in a given scene, tagging the evidence accordingly and ensuring its secure lockdown from the moment it becomes formal evidence in a case. In this case, upon arrival at the suicide scene, law enforcement authorities were able to seize and secure the following devices and equipment:

Mobile Phone

Laptop Computer

Desktop Printer

Wireless Router

Cable Modem

iPad Mini

Thumb Drive

Smart TV

Each item was tagged accordingly and secured into evidence. Each of these items were transported securely by Law enforcement authorities to the secure evidence lockers located at Texas City Police Headquarters. Further, in interviews conducted at the scene, it was determined that each item of evidence had not been used or accessed by anyone other than the victim in the hours following the suicide.

Law enforcement officials on scene have provided extensive documentation that outlines and describes the scene and the state of the items collected. For purposes of this presentation to the courts we will focus primarily on the digital items listed above. In terms of packaging, transportation and digital forensics review, all digital devices were collected and transported in shielded containers and all evidence review was conducted in a shielded environment to ensure proper isolation. In the process of collecting the above stated evidence items, law enforcement informed me upon arrival that an onsite Triage procedure was performed and all of the data collected was securely stored for comparison to later, offsite deep dive digital assessment in the crime lab.

And finally, with regard to preservation, an onsite Generic decision tree was developed by the crime scene evidence technician and also entered into the evidence files. This asset can be provided to court upon request.

As to Acquisition – We identified the 8 items listed in the digital evidence file to be high probability implication devices that would provide good insight to the activities and online behaviors of the victim in this case, whom we have strong reason to believe was bullied extensively by others with whom she communicated with through these devices. Our objective was to review memory and history of activities on the device through a specific subset of tools that we will review shortly. In our selection of tools for use in the subsequent investigation I assessed the following:

According to NIST - The following criteria have been suggested as a fundamental set of requirements for forensic tools, and should be considered when a choice of tools is available:

- **Usability** – the ability to present data in a form that is useful to an investigator
- **Comprehensive** – the ability to present all data to an investigator so that both inculpatory and exculpatory evidence can be identified
- **Accuracy** – the quality of the output of the tool has been verified
- **Deterministic** – the ability for the tool to produce the same output when given the same set of instructions and input data
- **Verifiable** – the ability to ensure accuracy of the output by having access to intermediate translation and presentation results
- **Tested** – the ability to determine if known data present within the mobile device internal memory is not modified and reported accurately by the tool

Finally, we also developed a short list of likely cloud based services and accounts that the victim in this case may have used to communicate and interact with others followed by developing a short list of those particular sites, accounts and interactions and their subsequent implications in this case.

References:

https://www.swgde.org/documents/Current%20Documents/SWGDE%20Focused%20Collection%20and%20Examination%20of%20Digital%20Evidence

https://www.swgde.org/documents/Current%20Documents

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

Analysis Processes

According to NIST - The examination process uncovers digital evidence, including that which may be hidden or obscured. The results are gained through applying established scientifically based methods and should describe the content and state of the data fully, including the source and the potential significance. The potential evidence on these devices may include the following items:

- Subscriber and equipment identifiers
- Date/time, language, and other settings
- Phonebook/Contact information
- Calendar information
- Text messages
- Outgoing, incoming, and missed call logs
- Electronic mail
- Photos
- Audio and video recordings
- Multi-media messages
- Instant messaging
- Web browsing activities
- Electronic documents
- Social media related data
- Application related data
- Location information
- Geolocation data

Two types of computer forensic investigations generally take place. The first type is where an incident has occurred but the identity of the offender is unknown (e.g., a hacking incident). The second is where the suspect and the incident are both known (e.g., a child-porn investigation). Prepared with the background of the incident, the forensic examiner and analyst may proceed toward accomplishing the following objectives:

- Gather information about the individual(s) involved {who}.
- Determine the exact nature of the events that occurred {what}.
- Construct a timeline of events {when}.
- Uncover information that explains the motivation for the offense {why}.
- Discover what tools or exploits were used {how}.

Forensic Examination of Digital Evidence – A Guide for Law Enforcement, produced by the U.S. Department of Justice [DOJ08], offers the following suggestions for the analysis of extracted data:

Ownership and possession – Identify the individuals who created, modified, or accessed a file, and the ownership and possession of questioned data by placing the subject with the device at a particular time and date, locating files of interest in non-default locations, recovering passwords that indicate possession or ownership, and identifying contents of files that are specific to a user.

Application and file analysis – Identify information relevant to the investigation by examining file content, correlating files to installed applications, identifying relationships between files (e.g., e-mail files to e-mail attachments), determining the significance of unknown file types, examining system configuration settings, and examining file metadata (e.g., documents containing authorship identification).

Timeframe analysis – Determine when events occurred on the system to associate usage with an individual by reviewing any logs present and the date/time stamps in the file system, such as the last modified time. Besides call logs, the date/time and content of messages and e-mail can prove useful. Such data can also be corroborated with billing and subscriber records kept by the service provider.

Data hiding analysis – Detect and recover hidden data that may indicate knowledge, ownership, or intent by correlating file headers to file extensions to show intentional obfuscation; gaining access to password-protected, encrypted, and compressed files; gaining access to steganographic information detected in images; and gaining access to reserved areas of data storage outside the normal file system.

Call & subscriber Examination: Records maintained by the service provider capture information needed to accurately bill a subscriber or, in the case of a prepaid service plan, debit the balance. The records collected are referred to as call detail records (CDRs), which are generated by the switch handling an originating call or SMS message from a mobile device. Besides call detail records, subscriber records maintained by a service provider can provide data useful in an investigation. For example, for GSM systems, the database usually contains the following information about each customer:

- Customer name and address
- Billing name and address (if other than customer)
- User name and address (if other than customer)
- Billing account details
- Telephone number (MSISDN)
- IMSI
- UICC serial number (ICCID)
- PIN/PUK for the UICC
- Services allowed

References:

https://www.swgde.org/documents/Current%20Documents/SWGDE%20Focused%20Collection%20and%20Examination%20of%20Digital%20Evidence

https://www.swgde.org/documents/Current%20Documents

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

Tools Employed

Cain & Abel - Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kind of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords and analyzing routing protocols.

FTK Imager - A purpose-built forensics solution that interoperates with mobile device and e-discovery technology. Powerful and proven, FTK processes and indexes data upfront, eliminating wasted time waiting for searches to execute.

Autopsy Forensic Browser – This product is part of the Sleuth Kit, is open source and is available for Mac, Windows and Linux platforms. This specific tool along with the Sleuth Kit allow an end user to investigate the file systems and data volumes of a target computer system. It touts an easy to use interface and has been adopted by numerous law enforcement entities to conduct investigative work on systems that have been entered into evidence. It touts an extensible platform for easy interoperability with other tools and some of its key features include: Timeline Analysis; Keyword Search; Web Artifact gathering; and Data Carving to name a few. In addition it is fast, cost effective and relatively user friendly.

Encase – Encase is a suite of tools designed to aid in the digital forensics process. It is commercial grade and runs on the Windows platform. Encase touts itself as Easy to use with powerful and customizable processing, integrated investigation workflows and flexible reporting options. The makers of Encase also tout their “Proven in Courts” and “Best in Class”.

Nuix – Nuix is a software platform for the Windows environment that performs extensive indexing, searching, analysis and extraction of information from unstructured data sources. Nuix touts is strength from its core engine as high velocity output, data volume & through-put capabilities and its breadth of coverage in artifacts, file types and storage formats.

X-Ways - X-Ways Forensics is an advanced work environment for computer forensic examiners. It runs under Windows XP/2003/Vista/2008/7/8/8.1/2012/10*, 32 Bit/64 Bit, standard/PE/FE.

References:

http://www.sleuthkit.org/autopsy/index.php

https://www.guidancesoftware.com/encase-forensic?cmpid=nav_r

https://www.nuix.com/

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

http://www.oxid.it/cain.html

http://www.accessdata.com/products-services/forensic-toolkit-ftk

http://www.x-ways.net/forensics/index-m.html

Findings

Through our use of Cain and Abel we were able to perform dictionary attacks and brute force attacks to gain access to Vela's various passwords for the laptop and thumb drive devices and her online cloud accounts and activity. From there I was able to apply a mix of tools as listed above to obtain IP activity on both Vela's internal networks (at home) as well as potential IP and Mac address information for potential suspects. There is an overwhelming amount of activity in particular related to Vela's Facebook and Instagram accounts and a number of deleted chat sessions between a mix of 3 different screen name users that suggest cyber bullying was occurring and could be a contributing factor in Vela's suicide. In fact, just hours before Vela took her life, there is a flurry of deleted chat message exchanges.

Similarly, I used Autopsy Forensic Browser to gain access and insight to all of the data and interactions from Vela's Apple iOS devices. Fortunately for us in our investigation, Vela's password mix across devices was non-existent. Her Windows passwords discovered via our use of C&A when applied to other devices, netted us access to the devices and their contents.

Through my use of Autopsy, I was able to quickly retrieve browser histories and deleted sessions on the Apple devices. Here I found a repository of over 50 Facebook and Instagram interactions that had been deleted by our victim. Here-in you will find various hostile interactions with 3 usernames in particular:

H8tr_tween

Laclustr218

Bigdawg1422

Upon doing further forensics on these digital fingerprints, I was able to ascertain the IP addresses associated with each:

H8tr_tween: 14.228.62.302, 91.265.48.119,

Laclustr218: 168.36.241.219

Bigdawg1422: 162.198.25.63, 175.25.36.219, 185.98.52.36, 165.25.14.367

Based on this information, we can ascertain that both H8tr_tween and Bigdawg1422 are likely using multiple devices to connect and engage our victim in this case. However, all of the (24) sessions from Laclustr218 seem to be from the same device/IP location.

All of these evidentiary findings have been submitted to the court for review separate to this report as Evidence packages and exhibits.

Lastly, based on all of my knowledge, I employed Encase against all of the devices to double check and validate my investigative work and to bring commercial level credibility to the investigative process.

Analysis & Results

Ultimately, our analysis of all of the physical evidence spawned a significant amount of digital evidence that has been submitted to the court as additional evidence to support further action in this case. I believe the evidence will show that a case can be built against the 3 listed SN perpetrators that would

include the following charges: Invasion of Privacy, Hate Crime, Extortion, Online threats of violence, Human Trafficking (Sexual Exploitation) and Child Pornography.

In all we found over 1,000 interactions, digital files, text exchanges and interactions that can be used to build an effective case against the perpetrators (and potentially others) in this scenario. All items have been submitted to the court outside of this report, with specific detail to be used as evidence in the event a prosecutable suspect or suspects are identified, arrested and brought before the court.

Based on all of the information gathered and retained from my investigation and review of the digital evidence, I would find for the court that there is a significant correlation between Vela's online interactions with several individuals that would suggest she may have been the victim of online bullying and that further subpoenas and court orders may be required to bring closure and justice to the Vela family.

My prevailing recommendation to the court at this time would be to issue search warrants and further subpoenas to individuals identified with the submitted list of IP addresses. Additionally, I would recommend to issue court orders to Facebook and Instagram as well as for ISP carriers identified in the chain of liability for all information and transactional history for all usernames and accounts listed in the court submitted evidence package.

Conclusions

In conclusion, I hope this Evidentiary Report has demonstrated my knowledge and understanding of the Digital Forensics process. Through this report you can see the actions a Digital Forensics expert would need to be prepared to defend and present in a court of law, with an objective viewpoint and perspective. Further, all of the tangential elements that come into play like: Evidence handling, Chain of Custody, Tools of the trade, Legal implications and considerations along with Methods and Operational Procedures that need be employed in the process of conducting a Digital Forensics review and analysis.

I'll remind everyone reading this that all evidence and references to the Vela case portrayed here are, in fact, fictional. Nothing in this paper should be represented or interpreted as fact or reality of any sort.

REFERENCES

Nance | Ryan, 2011, *Legal Aspects of Digital Forensics* https://www.computer.org/csdl/proceedings/hicss/2011/4282/00/10-04-03.pdf

Newcomb, 2013, *Teen Charged in Fatal Cyberbullying Case of Rebecca Sedwick to Remain in Jail* http://abcnews.go.com/US/teen-charged-fatal-cyberbullying-case-rebecca-sedwick-remain/story?id=20580689

Parker, 2012, *The Story of a Suicide,* http://www.newyorker.com/magazine/2012/02/06/the-story-of-a-suicide

Kranz, Unknown, *Case Study: Jessica Logan,* https://cyberbullying.ua.edu/index.php/case-study-jessica-logan/

Unknown, 2014, *SWGDE Focused Collection and Examination of Digital Evidence,* https://www.swgde.org/documents/Current%20Documents/SWGDE%20Focused%20Collection%20and%20Examination%20of%20Digital%20Evidence

Unknown, 2014, *SWGDE Focused Collection and Examination of Digital Evidence,* https://www.swgde.org/documents/Current%20Documents

Ayers | Brothers| Jansen, 2014, *Guidelines on Mobile Device Forensics* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

http://www.sleuthkit.org/autopsy/index.php

https://www.guidancesoftware.com/encase-forensic?cmpid=nav_r

https://www.nuix.com/

http://www.oxid.it/cain.html

http://www.accessdata.com/products-services/forensic-toolkit-ftk

http://www.x-ways.net/forensics/index-m.html