VERSION 1.0

JULY 10, 2017

DIGITAL FORENSICS REPORT

EVIDENCE ANALYSIS IN CASE #90033

PRESENTED BY: RYAN NYE

UNIVERSITY OF SAN DIEGO
CSOL590 MODULE 7

1 DIGITAL FORENSICS REPORT

INVESTIGATOR:	Paul Keener
	Badge #3377
	(Professor at University of San Diego)

DIGITAL FORENSICS EXAMINER (Tech):	Ryan Nye
	Digital Forensic Tech #1003373
	(Cyber security student at USD)
	San Diego, CA
	619-461-9461

SUBJECT:	Digital Forensics Examination Report
Accused 1:	Karinthya Sanchez Romero
Offence:	Stalking Online impersonation
Accused 2:	Andres Arturo Villagomez
Offence:	Unlawful disclosure or promotion of intimate visual material
Date of Request:	May 27, 2017
Date of Conclusion:	June 30, 2017
Report Publish Date:	July 10, 2017

Disclaimer: The chosen case scenario is for learning purposes only and any association to an actual case and litigation is purely coincidental. Evidence presented in the case scenario is fictitious and are not intended to reflect actual evidence. Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement, recommendation, or favoring by the U.S., State, or local governments, and the information and statements shall not be used for the purposes of advertising.

2 TABLE OF CONTENTS

2.1 ABSTRACT

The purpose of this report is to provide examination procedures, findings, and recommendations from *fictitious* evidence regarding the cyberbullying events leading to the suicide of Brandy Vela. This information provides for the presentation stage of an investigation. Included in the report are the digital forensic standards, principles, methods, and legal issues that may impact the court's decision.

The creation of the report is unbiased, and intends to assist the court make a judgment of Andres Arturo Villagomez and Karinthya Sanchez Romero. This written report provides detail for the evidence as presented in the Digital Evidence Package Power Point Presentation. The focus of this report is on the digital evidence collected from the two suspects. Therefore, the report omits the evidence collected on Brandy Vela's phone and laptop. References to evidence items collected from Vela or interviews conducted by the investigator may be referenced in this report.

2.2 CASE BACKGROUND

On Tuesday, November 29th, 2016, Brandy Vela committed suicide by a self-inflicted gunshot wound to the chest. The suicide was due to cyber bullies impersonating Vela on Facebook and dating sites (CNN, 2016). The fake profiles posted on the social media sites included her explicit photos and cell phone number (CBS, 2016). Vela received many harassing phone calls and text messages on her cell phone (CBS, 2016). The harassment continued after her death when the tormentors posted harmful images on Vela's Facebook memorial site (Hassan, 2016).

On Thursday, March 16, 2017, two suspects were arrested involved with Brandy Vela's suicide. Police arrested Andres Arturo Villagomez, age 21, and Karinthya Sanchez Romero, age 22, from Galveston, Texas. The police report indicates Villagomez and Romero are currently dating (Keating, 2017).

The search warrants were obtained after investigators analyzed the evidence on Brandy Vela's cell phone and social media account. The seizure of the suspect's devices was performed in a manner consistent with recommendations found in Electronic Crime Scene Investigation: A Guide for First Responders. The investigation was conducted in accordance with processes outlined by the National Institute of Justice (NIJ) and the Technical Working Group for the Examination of Digital Evidence (TWGEDE). The investigation employed the use of FTK Imager and EnCase Mobile Manage to discover and recover deleted files from confiscated laptops and cell phones.

2.2.1 SUSPECT SUMMARY

Priority	Suspect	Connection	Charge	Bail
1	Karinthya Sanchez Romero	Villagomez's girlfriend	-Stalking -Online impersonation	$10,000 each offense
2	Andres Arturo Villagomez	Vela's Ex-boyfriend	Unlawful disclosure or promotion of intimate visual material	$2,500

3 STANDARDS, PRINCIPLES, AND CRITERIA FOLLOWED

The following standards, principles, and criteria outlined below are followed in every investigation. Below we have general principles as outlined by the forensic community, principles and procedures outlined by the NIJ, and criteria recommended by the SWGDE.

3.1 GENERAL PRINCIPLES

The forensic community has outlined the following four main principles to applied during investigation:

- No actions to change original data
- Investigator(s) are competent to access original data
- Audit trail created
- Legal principles are adhered to
  (Keener, 2017)

3.2 NIJ: PRINCIPLES AND PROCEDURES

The investigation followed the recommendations from the National Institute of Justice (NIJ) when examining the digital evidence provided in this report. The NIJ as outlined the following areas of a digital investigation that are listed below are includes investigator's comments in these areas.

3.2.1 POLICY AND PROCEDURE DEVELOPMENT

Comprehensive training program for examiners, sound digital evidence recovery techniques, and a commitment to keep any developed unit operating at maximum efficiency.

Procedures Completed:

- ✓ Procedures for intake forms, point of contact, required documents, acceptance criteria
- ✓ Requirements for the submission of physical evidence
- ✓ Criteria for prioritizing and assigning examinations
- ✓ Guidelines for receiving, processing, documenting, and handling evidence and work products
- ✓ SOPs developed for preserving and processing digital evidence.

3.2.2 ASSESSMENT

Computer forensic examiners should assess digital evidence thoroughly with respect to the scope of the case to determine the course of action to take.

Procedures Completed:

- ✓ Identified legal authority for the forensic examination request
- ✓ Ensured completed request for assistance **SEE Appendix A**
- ✓ Consultation with case investigator completed **SEE Appendix B**
- ✓ Complete documentation of chain of custody **SEE Appendix C & D**

3.2.3 ACQUISITION

Digital evidence, by its very nature, is fragile and can be altered, damaged, or destroyed by improper handling or examination. Examination is best conducted on a copy of the original evidence. The original evidence should be acquired in a manner that protects and preserves the integrity of the evidence. Computer forensic examiners should assess digital evidence thoroughly with respect to the scope of the case to determine the course of action to take.

Details listed in section titled “Search and Seizure” and “Chain of Custody”.

3.2.4 EXAMINATION

The purpose of the examination process is to extract and analyze digital evidence. Extraction refers to the recovery of data from its media. Analysis refers to the interpretation of the recovered data and putting it in a logical and useful format.

Details listed in section titled “Evidence Examination Steps”.

3.2.5 DOCUMENTING AND REPORTING

Actions and observations should be documented throughout the forensic processing of evidence. This will conclude with the preparation of a written report of the findings.

Details listed in sections titled “Evidence Analysis”, “Findings”, and “Recommendations”,

3.3 ADDITIONAL GUIDANCE

Topic	Link
SWGDE Best Practices for Computer Forensics	Weblink
SWGDE Guidelines for Forensic Image Analysis	Weblink
SWGDE Mac OS X Tech Notes	Weblink

4 LEGAL ISSUES

The following issues are important regarding any case concerning digital evidence. Specific rules were chosen the specific cyberbullying case of Brandy Vela. The two main issues for the investigator are *admissibility* and *authenticity*.

4.1.1 ADMISSABILTY OF EVIDENCE

Most difficult part of the case will be the admissibility of content on a cloud. In this case, it's the online harassment on Facebook and dating sites. Below is a summary of the Stored Communication Act sections governing legal access to online content.

Topic	Authority/Rule	Short Description
Facebook Information & Privacy	Stored Communication Act, Title 18 U.S.C. § 2701 - 2712	Facebook follows the Stored Communication Act (Facebook, 2017).
Facebook Non-Content	Title 18 U.S.C. § 2703(c)(2)	Court order provides non-content related data. (Facebook, 2017).
Facebook Limited-Content	Title 18 U.S.C. § 2703(d)	Court order when government entity proves evidence "…relevant and material to an ongoing investigation." Facebook provides: limited content, messages over 180 days. (Facebook, 2017).
Facebook All Content (Emergency)	Title 18 U.S.C. § 2702(b)(6)(c) & 2702(c)(4)	During imminent danger, can make an emergency request for user information if imminent threat of danger exist (Facebook, 2017).
Facebook All Content (Warrant)	Title 18 U.S.C. § 2703(d)	Search warrant provides all content available (Facebook, 2017).
Facebook All Content	Forfeit of 4th Amendment.	Lack of privacy initiated by suspect may provide content. (Kelly, 2012)

4.1.2 AUTHENTICATING EVIDENCE

Authenticating digital evidence may be a challenge as the court may not understand the complexity in various digital communication. Below is a summary of communication methods and cases that properly authenticated the digital evidence. Same or improved procedures to be used in the case of Vela.

Topic	Case
Text Messages	Dickens v. State
Emails	United States v. Siddique
Instant Messages	In re F.P., 2005
Encrypted Apps	State v. Levie

4.1.3 POTENTIAL DEFENSE

The First, Fourth and Fifth Amendment to cyberbullying issues. Below is the summary of the amendments and potential defenses.

Amendment	Amendment Detail	Defense
1st	"Congress shall make no law . . . abridging the freedom of speech."	Defendant can say anything offline or online (with exceptions) as granted by the US Constitution (withoutatraceinvestigations.com, n.d.).
4th	Prohibits "unreasonable" searches and seizures and "reasonable expectation of privacy"	Search and evidence were against US law. How "legitimate" is defined depends heavily on the context of the situation (Withoutatraceinvestigations.com, n.d.).
5th	"no person . . . shall be compelled in any criminal case to be a witness against himself."	Limiting incriminating evidence due to defendant's 5th amendment right (Terzian, 2014).

*Additional defenses include the admissibility and authentication of evidence discussed in the previous section.

5 SEARCH AND SEIZURE

The search warrants for were obtained after investigators analyzed the evidence on Brandy Vela's cell phone and social media account. The search warrant allowed for the confiscation of all digital media.

Both residences were secured before and during the search of the following devices. The models and serial numbers of the phones and laptops were recorded. All devices were connected to WifI and enabled for their home connections. Interviews with the suspects and family members showed they were the sole owners and operators of their devices. No immediate family, relatives, or friends were known to be using their devices on a consistent basis.

Law enforcement did not locate any removable media or offsite storage areas and computing locations. The general condition of the area where the devices were confiscated were free of liquid and substances that would corrupt or destroy data on those devices. No specialists were necessary to obtain, open, or unlock evidence within the household.

5.1 PROCESSING LOCATION

Evidence was processed at the accredited Regional Computer Forensics Laboratory (RCFL) at Houston, Texas. The lab is a dedicated digital forensic laboratory and accredited by the American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB). The laboratory provides examination by certified staff who undergo FBI's CART certification process. The services are performed

by an independent, impartial, and objective staff. Approximately 35 DAYS allotted to forensic lab to locate and analyze evidence and report on findings.

Due to the quality of the laboratory, the court can be assured that:

- ✓ Evidence will be well documented
- ✓ Appropriate packaging, transport, and storage of evidence
- ✓ Storage locations are free from electromagnetic interference and damaging substances
- ✓ Continually assess the quality and condition of the devices

6 CHAIN OF CUSTODY

The forensic community outlines the following areas for maintain the chain of custody:

- ✓ Name & contact information of custodians
- ✓ Detailed identification of evidence (model/serial)
- ✓ When, why, whom evidence was acquired or moved
- ✓ Where evidence is stored
- ✓ When/if returned

*All items listed before have been completed on the Chain of Custody Forms.
SEE Appendix C&D

6.1.1 STORAGE

Items are placed in a heavy-duty mechanical evidence locker room. Fingerprint security system into the room allows that both deposit and retrieval can only be performed by pre-authorized individuals whose prints have already been entered into the system. Lockers are divided into readily identifiable compartments, which are opened and closed with the user-friendly button locks. A heavy-duty steel structure, with welding at the ends to reinforce the strength of the doors. The doors themselves incorporate robust load-bearing hinges and rubber stops to ensure smooth closure. The digital lockers are also enhanced with detection sensors and LED panels that display valuable information at a glance.

(Montel, n.d.)

(Image from Montel, n.d.)

7 EVIDENCE EXAMINATION STEPS

7.1 PREPARATION

Working directories were prepared on separate media where evidentiary files and data will be placed during the extraction process. Sufficient time allocated to the examiner to perform forensic procedures.

Exhibit	Owner Initials	Item	OS	Serial	Tool
A	K.S.R	Dell Latitude D-630 Laptop	Windows 7	7PSG632	AccessData FTK Imager
B	K.S.R	Apple iOS7 Phone	OS7	DMPH74H9D DFHW	EnCase Mobile Investigator
C	A.A.V.	Lenovo ThinkPad SL510 Laptop	Windows 7	78-12AB9	AccessData FTK Imager
D	A.A.V.	Samsung Galaxy S5 Phone	Android 6.0.1	RFBF30W63J0	EnCase Mobile Investigator

7.2 EXTRACTION

Logical extraction was performed on the devices. The data viewable included active files, deleted files, file slack, and unallocated file space. Main steps for extraction listed below. The actions listed may be done automatically by the forensic tool:

Step	Extract Item	Description	Case Specific
1	File system	To reveal characteristics of directory structure, file attributes, file names, date and time stamps, file size.	Extraction of 4 different operating file systems were completed.
2	Pertinent information	Locating pertinent information to the case using file names, extensions, file header, file content, and location on the drive.	Locating images associated with the harassment and impersonation of Vela. Using time stamps to correlate file creation and Facebook post.
3	Unallocated space	To recover deleted files	Recovering images and messages associated with the harassment and impersonation of Vela.

Physical Extraction: Identifies and recovers data across the physical drive without regard to file system.
Logical Extraction: Identifies and recovers files and data based on the installed operating system(s) , file system(s), and/or application(s).
(National Institute of Justice, 2004, p. 15).

7.3 ANALYSIS OF EXTRACTED DATA

The examination of devices proved successful by extracting evidence relevant to the case. The four primary methods are listed below. Analysis may include a review of the request for service, legal authority for the search of physical evidence, investigative leads and/or analytical leads (National Institute of Justice, 2004, p.15).

7.3.1 TIMEFRAME ANALYSIS

Before the analysis was started, the examination confirmed the BIOS date and time reported was correct and consistent. Then, timeframe analysis was used to show key dates when:

1) Romero's motivation for harassment
2) Romero's plots to organize harassment
3) Image creation and last accessed dates of images used in profiles against the social media posted dates
4) The duration of Romero's stalking activity

7.3.2 DATA HIDING ANALYSIS

No attempts to hide data were found on the four devices. The following items were NOT found: password protected documents, encrypted documents, and compressed files, attempts of steganography, or creation of a host protected area. Encrypted applications were found on Romero's laptop and discussed in the next section.

7.3.3 APPLICATION AND FILE ANALYSIS

The following application and file analysis techniques were applied to this case.
For details SEE Sections titled "Evidence Item Processing" and "Evidence Analysis".

1) Reviewing file names for relevance and patterns according to stalker's behavior (Ex. common slurs).
2) Examining file content for similar content and metadata connected to online stalking or impersonating activity. (Ex. Account names and passwords of the fake profiles)
3) Reviewing file names for relevance and patterns.
4) Identifying the number and type of operating system.
5) Correlating the files to the installed applications -encryption programs, dating sites.
6) Considering relationships between files. For example, correlating Internet history to cache files and e-mail files to e-mail attachments related to impersonation and stalking.
7) Identifying unknown file types to determine their value to the investigation.
8) Examining the users' default storage location for applications.
9) File structure of the drive to determine if files have been stored in their default or an alternate location.
10) Examining user-configuration settings.
(NIJ, 2004)

7.3.4 OWNERSHIP AND POSSESSION ANALYSIS

The following ownership analysis of evidence items were done in conjunction with interviews conducted by the lead investigator. Both evidence on the devices and interview show the suspects were the sole owner and user of the devices. As far as access, this includes one exception to Romero's laptop. According to the interview with Villagomez, Romero accessed his laptop unauthorized on January 2nd, 2016 while he was at work.

Device	Owner Initials	Evidence
Dell Latitude D-630 Laptop	K.S.R	Suspect and family admission, Single user (admin account)
Apple iOS7 Phone	K.S.R	Suspect and family admission, Single account on data plan, password protected
Lenovo ThinkPad SL510 Laptop	A.A.V.	Suspect and family admission, Single user (admin account)
Samsung Galaxy S5 Phone	A.A.V.	Suspect and family admission, Single account on data plan, password protected

8 EVIDENCE ITEM PROCESSING

Below are the item details and examination information. Included is a timeline in the "Examination" field.

8.1.1 DELL LAPTOP OF KARINTHYA S. ROMERO

Objective:	**To determine whether Romero stalked and impersonated Brandy Vela on her laptop.**
Device Type:	Dell Latitude D-630 Laptop
Serial#:	7PSG632
Operating System:	Windows 7
Offense:	Stalking Online impersonation
Case Agent:	Investigator Paul Keener
Evidence#:	001
Chain of Custody:	**SEE Example Chain of Custody on Appendix C**
Examination Location:	Digital Forensics Lab of Houston, Texas
Tool Used:	AccessData FTK Imager 3.4.3
Assessment:	✓ Legal Authority Established ✓ Chain of Custody Documented ✓ Request for Service Documented ✓ Equipment for Analysis Available in Lab
Acquisition:	The configuration of the laptop was documented and the data was duplicated multiple times in a manner that preserved original data. Additionally, the CMOS information was documented. **SEE Example Computer Evidence Worksheet Appendix E**
Examination:	**05/27/17 15:00** FTK Forensic Imager used to obtain logical extraction of drive. **05/27/17 15:06** Images relating to harassment or impersonation of Vela was searched through typical directories (Images, Photos, Downloads) then searched in user created directories. **05/27/17 15:10** Located explicit photo of Vela used in fake profiles **05/27/17 15:11** Located "gun in book" and "stick figure holding gun" image used to harass in fake memorial site. **05/27/17 15:18** Identified the account name and password list for fake profiles in word file. **05/27/17 15:30** Unallocated space (deleted files) returned no recoverable images.
Documentation and Reporting:	**SEE Image in section titled "Evidence Analysis" under "Images – Romero laptop"** **SEE Word Document file in section "Evidence Analysis" under "Word Doc (Accounts)- Romero Laptop** Material items were reported in the "Findings" section of this document.
Examiner/Detective Comments:	Word document holding account information was retrieved in the documents folder of the C drive. Noted is the possibility of other victims. Document located named "Tiffany accounts" on Documents folder. Accounts/password list document found allowed the court to provide another search warrant for Facebook and collect further evidence.

8.1.2 APPLE IOS7 PHONE OF KARINTHYA S. ROMERO

Objective:	**To determine whether Romero stalked and impersonated Brandy Vela on her cell phone.**
Device Type:	Apple iOS7
Serial#:	DMPH74H9DFHW
Operating System:	iOS7
Offense:	Stalking Online impersonation
Case Agent:	Investigator Paul Keener
Evidence#:	002
Chain of Custody:	**SEE Example Chain of Custody on Appendix C**
Examination Location:	Digital Forensics Lab of Houston, Texas
Tool Used:	EnCase Mobile Investigator
Assessment:	✓ Legal Authority Established ✓ Chain of Custody Documented ✓ Request for Service Documented ✓ Equipment for Analysis Available in Lab
Acquisition:	The configuration of the phone was documented and the data was duplicated multiple times in a manner that preserved original data.
Examination:	**05/27/17 16:00** Reviewed interview notes with Villagomez provided password to Romero's phone. **05/27/17 16:03** Used Encase to retrieved all data from phone to place on lab drive. **05/27/17 16:05** Pertinent text messages relevant to the case was reproduced on an iOS lab phone. Vela's phone number found listed as "Fat Cow" in address book/contact list. **05/27/17 16:15** Created timeline of events **See Appendix F for message log timeline.**
Documentation and Reporting:	**SEE Image in section titled "Evidence Analysis" under "Facebook and iOS7 Text Messages – Romero"** Material items were reported in the "Findings" section of this document.
Examiner/Detective Comments:	Villagomez provided Romero's cell phone password allowing investigators to access and extract mobile information.

8.1.3 LENOVO SL510 LAPTOP OF ANDRES A. VILLAGOMEZ

Objective:	**To determine whether Villagomez possessed explicit photos of Brandy Vela on his laptop and purposely distributed photo for harassment.**
Device Type:	Lenovo ThinkPad SL510 Laptop
Serial#:	78-12AB9
Operating System:	Microsoft Windows 7 Professional
Offense:	Unlawful disclosure or promotion of intimate visual material
Case Agent:	Investigator Paul Keener
Evidence#:	003
Chain of Custody:	**SEE Example Chain of Custody on Appendix D**
Examination Location:	Digital Forensics Lab of Houston, Texas
Tool Used:	AccessData FTK Imager 3.4.3
Assessment:	✓ Legal Authority Established ✓ Chain of Custody Documented ✓ Request for Service Documented ✓ Equipment for Analysis Available in Lab
Acquisition:	The configuration of the laptop was documented and the data was duplicated multiple times in a manner that preserved original data. Additionally, the CMOS information was documented.
Examination:	**05/28/17 12:41** FTK Forensic Imager used to obtain logical extraction of drive. **05/28/17 13:02** Images relating to harassment or impersonation of Vela was searched through typical directories (Images, Photos, Downloads) then searched in user created directories. **05/28/17 13:45** Unallocated space (deleted files) returned the image of explicit image of Vela -same image used to impersonate on Facebook and dating sites.
Documentation and Reporting:	**SEE Image in section titled "Evidence Analysis" under Deleted Item – Villagomez Laptop** Material item was reported in the "Findings" section of this document.
Examiner/Detective Comments:	Interview with Villagomez indicated Romero may have retrieved naked photos from his laptop without his knowledge. Villagomez was convinced that Romero sent the photos to herself while he was at work and she was in possession of his laptop. He provided the date of January 2nd, 2016, (same date of argument when she discovered the images- **SEE Appendix F Facebook message for 1/02/2016**). Romero was forthcoming with his admission of deleting the photos from his laptop after he found out of Vela's death.

8.1.4 SAMSUNG GALAXY S5 PHONE OF ANDRES A. VILLAGOMEZ

Objective:	**To determine whether Villagomez possessed explicit photos of Brandy Vela and his cell phone and purposely distributed photo for harassment.**
Device Type:	Samsung Galaxy S5 Smart Phone
Serial#:	RFBF30W63J0
Operating System:	Android 6.0.1 Marshmallow
Offense:	Unlawful disclosure or promotion of intimate visual material
Case Agent:	Investigator Paul Keener
Evidence#:	004
Chain of Custody:	**SEE Example Chain of Custody on Appendix D**
Examination Location:	Digital Forensics Lab of Houston, Texas
Tool Used:	EnCase Mobile Investigator
Assessment:	✓ Legal Authority Established ✓ Chain of Custody Documented ✓ Request for Service Documented ✓ Equipment for Analysis Available in Lab
Acquisition:	The configuration of the phone was documented and the data was duplicated multiple times with Encase Mobile Investigator in a manner that preserved original data.
Examination:	**05/28/17 14:45** password provided by Villagomez **05/28/17 14:49** Used Encase to retrieved all data from phone **05/28/17 15:02** The image files on the phone were reviewed. The image files showed images of Villagomez and Vela during the course of their relationship, and did NOT contain any explicit photos. It is important to note that there was no indication that Villagomez was texting or calling Vela on this phone after their relationship ended in late 2015.
Documentation and Reporting:	No material items to report from this device. Any material items are reported in the “Findings” section of this document.
Examiner/Detective Comments:	The interview of the suspect was forthcoming with password on the phone for access. Villagomez admitted that he took explicit photos of Vela with her phone and sent them to his Gmail account. These photos were recovered in the unallocated section of his laptop. See examiner comments for Evidence item 003.

8.2 EVIDENCE HASH

8.2.1 ROMERO EVIDENCE ITEMS

Evidence Item	MD5	SHA1	PATH
Word Document with fake Vela profiles: login and password	fc953eee91202475bcfd0394db3a4459	3636065198ae98a5c34de78ec8301dd7ca4f3e1b	\\.\PHYSICALDRIVE2\BOOTCAMP (3) [43488MB]\NONAME [NTFS]\[root]\Karinthya\Documents\brandy accounts.docx
Vela Explicit Image titled fatcow.jpg	0085a853cb43db23a55874dac9f3c744	1211d3ae044855e2f2662df38ddfbd29e506e5e4	\\.\PHYSICALDRIVE2\BOOTCAMP (3) [43488MB]\NONAME [NTFS]\[root]\Karinthya\Photos\FatCow.jpg
Gun Book Image titled gunbook.jpg	cb3f67aa746b7ddd9a3c875fe79cf665	88c4917c7f23ce0bcc0cf1e7e1bdedd4f86ba95e	\\.\PHYSICALDRIVE2\BOOTCAMP (3) [43488MB]\NONAME [NTFS]\[root]\Karinthya\Photos\gunbook.jpg
Stick figure with gun image titled stickfig.jpg	83194778a6f2f94df165bde3ca3faac2	ce4cba3f5d4cec71aa2bd9ab21565ac772f9e6b5	\\.\PHYSICALDRIVE2\BOOTCAMP (3) [43488MB]\NONAME [NTFS]\[root]\Karinthya\Photos\stickfig.jpeg

8.2.2 VILLAGOMEZ EVIDENCE ITEMS

Evidence Item	MD5	SHA1	PATH
Word Document with fake Vela profiles: login and password	9e27d910d88b4bf6c0ba5a20b257e26d	3f47df5e2a4d3bd4418b164186b0c6b6e9297d11	\\.\PHYSICALDRIVE1\Partition 1 [960MB]\NONAME [FAT32]\[unallocated space]\17025

9 EVIDENCE ANALYSIS

9.1 SUMMARY OF PERTINENT EVIDENCE COLLECTED

#	OWNER	DEVICE/ITEM	MATERIAL EVIDENCE	DESCRIPTION
1	Romero	Dell Laptop	Document of account names and passwords.	Accounts used to harass, collect information, and impersonate vela found as word document on Romero's machine.
2	Romero	Facebook Accounts* (Content request)	Message log displays Romero's intent to harass Vela.	Messages sent to Villagomez indicate a strong motivation to harass Vela over claims that Villagomez is still seeing Vela. Includes impersonation of family members.
3	Villagomez	Lenovo Laptop	Picture of Vela used in fake online profiles.	Picture located in unallocated space (deleted). Item was recovered using FTK tool.
4	Romero	Dell Laptop	Picture of Vela used in fake online profiles.	Picture located in user's "Photo" folder. Item was located using FTK tool.
5	Romero	Dell Laptop	Picture of a gun in book. Same image on memorial Facebook page.	Picture located in user's "Photo" folder. Item was located using FTK tool.
6	Romero	Dell Laptop	Picture of a stick figure holding gun. Same image on memorial Facebook page.	Picture located in user's "Photo" folder. Item was located using FTK tool.
7	Romero	Apple iOS7 Cellphone	Text Messages	Text messages show harassment of Vela and plot to continue harassment with family members.

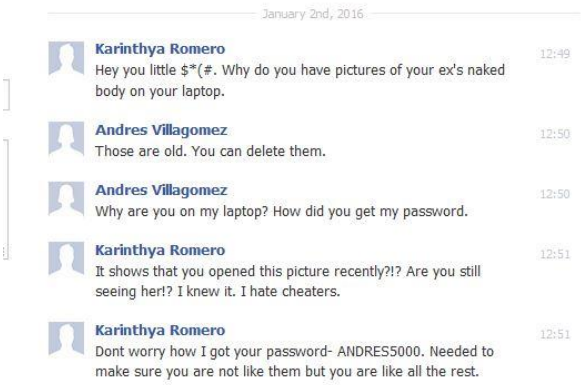
*Account content accessed using document she had on her laptop to keep track of accounts and passwords including fake accounts to impersonate Vela. Existing search warrant allowed the access to these accounts.

9.2 FACEBOOK AND TEXT MESSAGE TIMELINE- ROMERO

Summary of messages sent from laptop and cell phone provided below. **SEE reproduced Facebook and iOS messages on Appendix F**

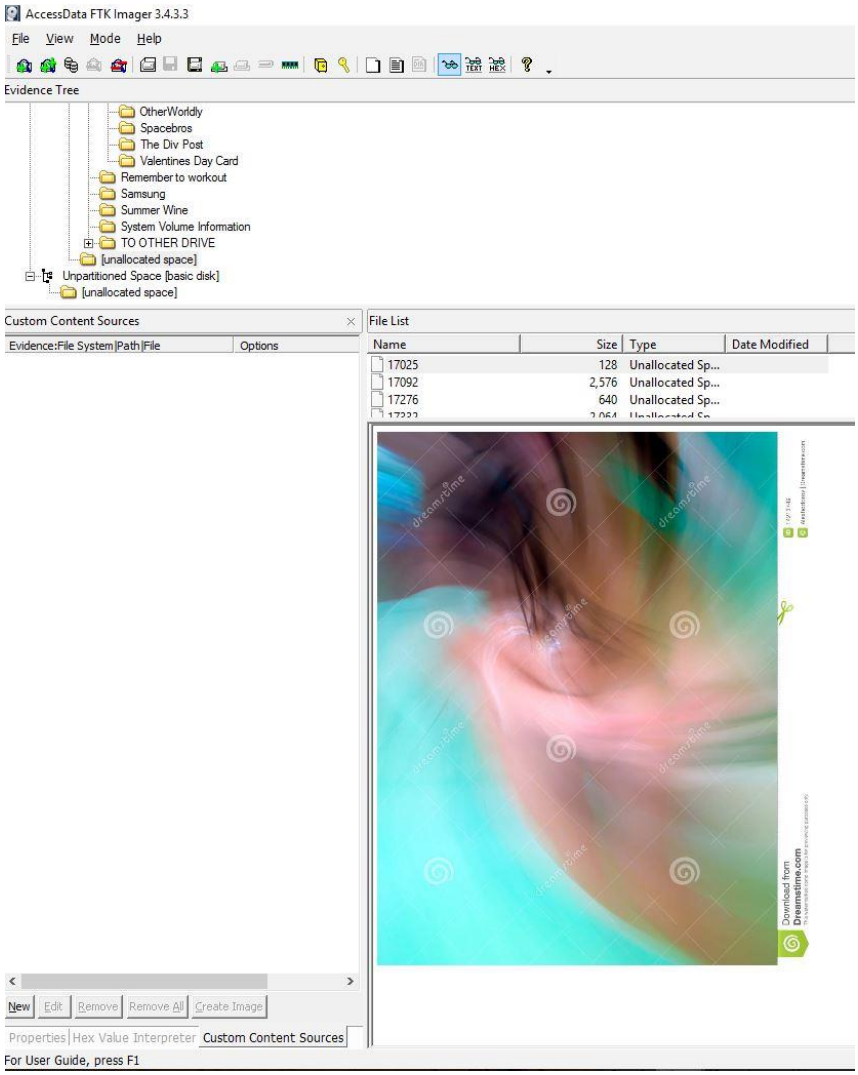
DATE	Media	SENDER	RECEIVER	SUBJECT
01/01/16	iOS7	Romero	Villagomez	Romero retrieves Vela's number using false pretense. Romero threatens Villagomez of consequences of infidelity.
01/02/16	Facebook	Romero	Villagomez	Romero accuses of Villagomez of cheating in the relationship due to nude photo found. Villagomez claims photo is old and is concerned about Romero's unauthorized entry to his laptop.
01/03/16	iOS7	Romero	T. Romero (cousin)	Romero requests help to plot harassment against Vela.
03/20/16	Facebook	Villagomez	Romero	Villagomez asks Romero if she is impersonating Vela. Romero's answer indicate involvement.
03/20/16	iOS7	Romero	Villagomez	Romero accuses Villagomez of being unfaithful due to not answering text messages on his phone. She threatens both Villagomez and Vela.
05/17/16	iOS7	Romero	Villagomez	Romero finds conversation between Vela and Villagomez. Is insulted and declares "revenge" on Vela and claims she "doesn't learn".
08/22/16	Facebook	Romero uses fake profile	Vela	Romero creates fake profile of Vela's family member, Joe Vela, and messages her with "fat cow" slur. Vela doesn't respond.
10/31/16	Facebook	Romero uses fake profile	Vela	Romero uses fake profile to obtain new number.

Example from 1/02/2016:



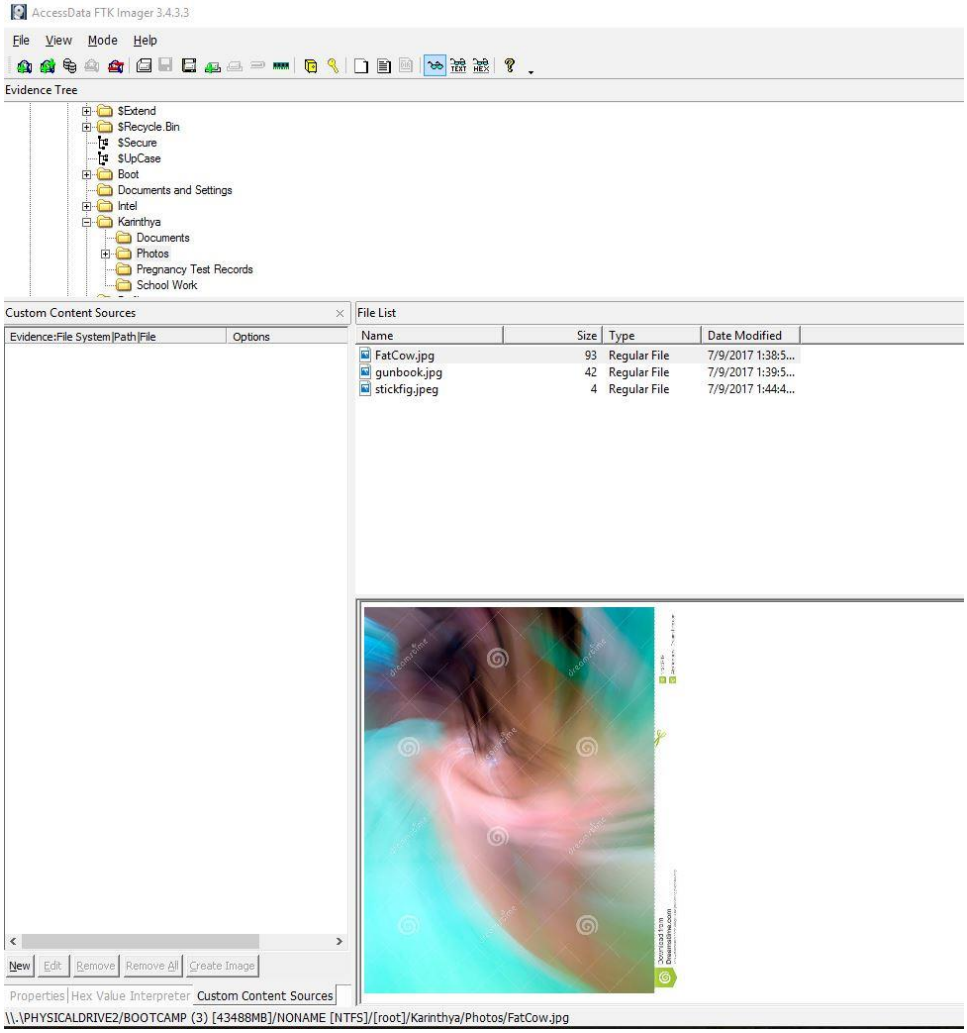
9.3 DELETED ITEM – VILLAGOMEZ LAPTOP

The following photo was recovered from Villagomez's Lenovo Laptop. The explicit photo is a match to the photo posted on fake online profiles.

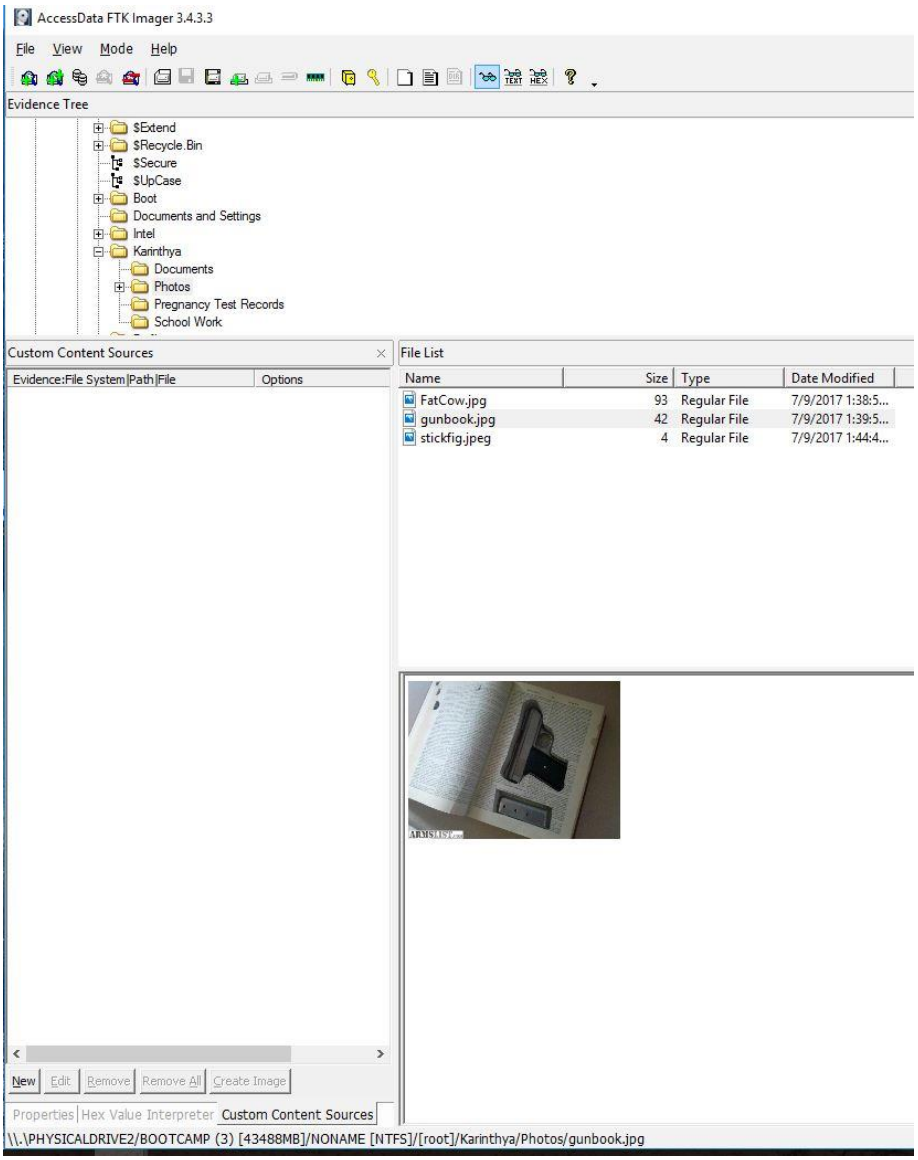


9.4 IMAGES – ROMERO'S LAPTOP

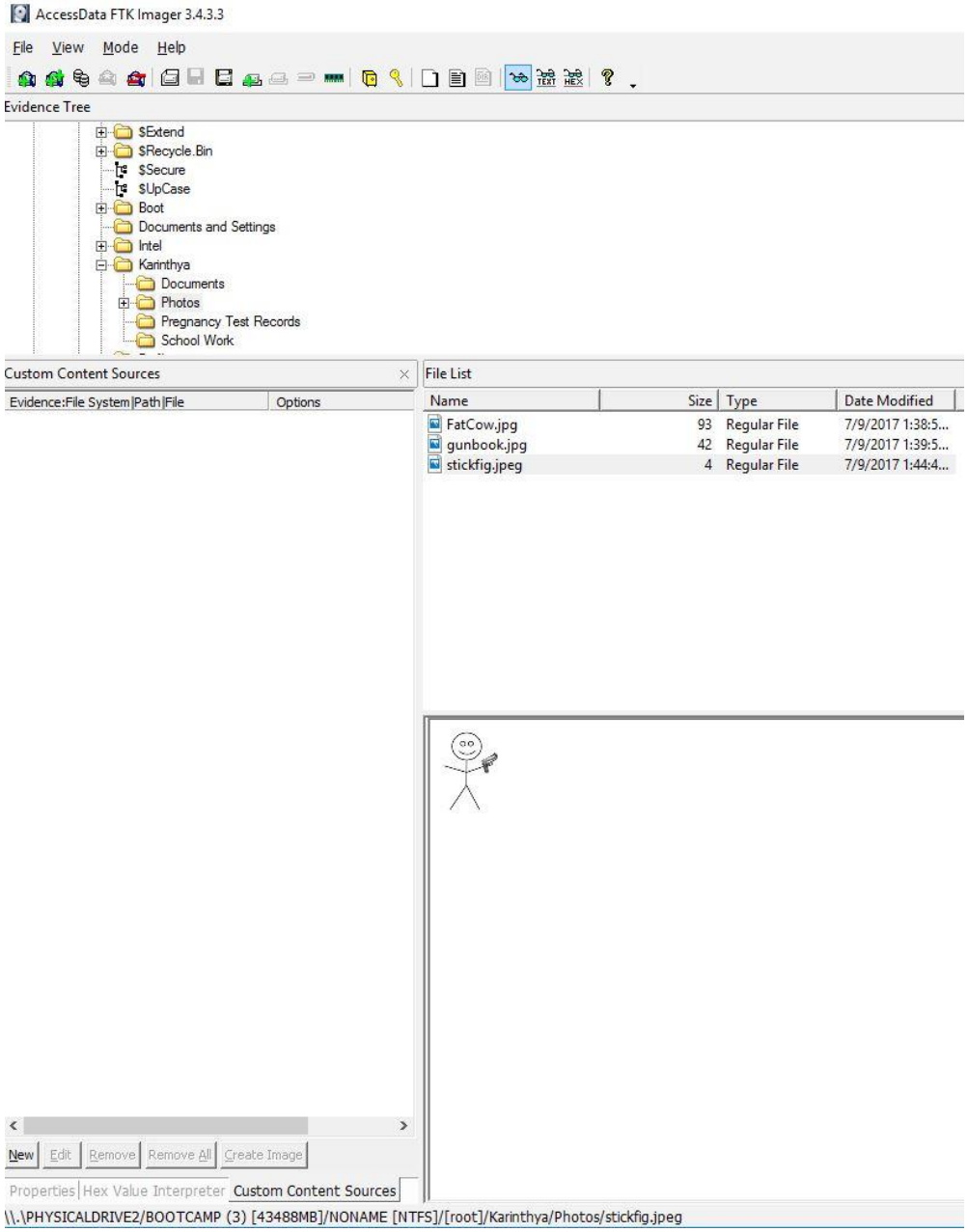
On Romero's Dell Laptop, the same photo was located in her photos folder and named "Fat Cow" on the main drive. Unlike Villagomez's file, this photo was not deleted.



Romero's laptop contained the same two photos posted on Brandy Vela's fake memorial site on Facebook. First photo is the gun on book.

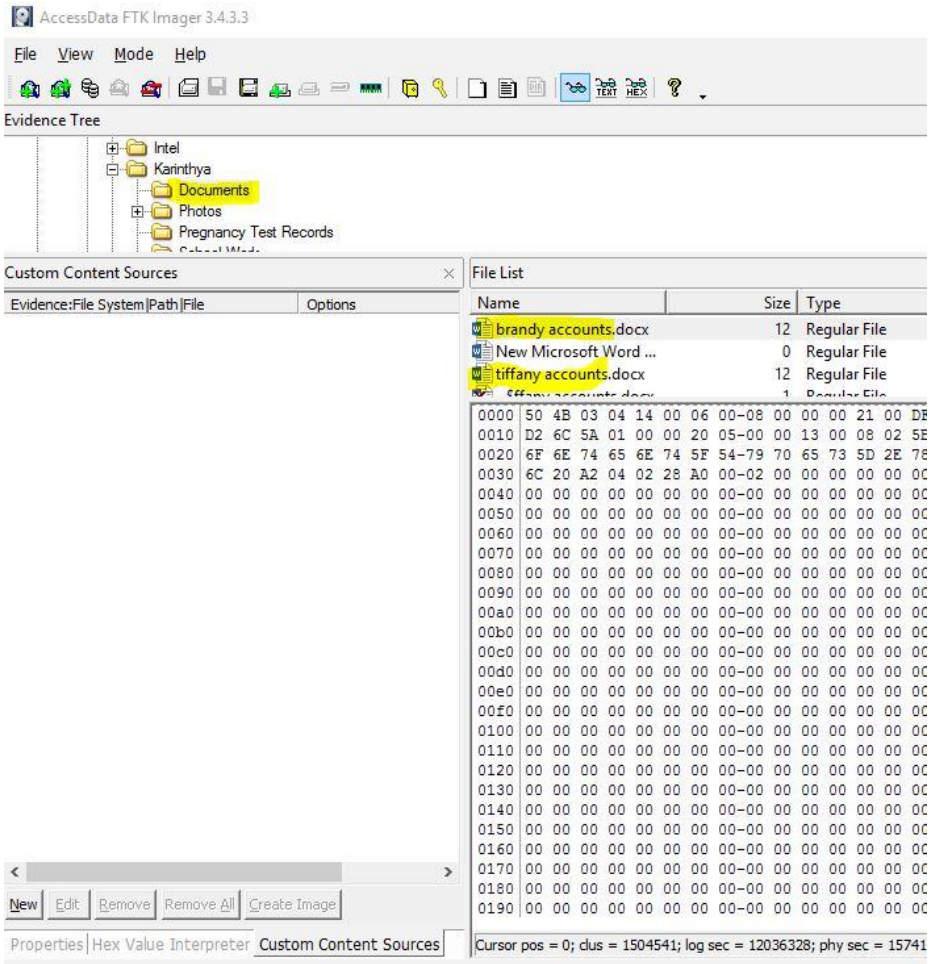


Second image involved in the fake memorial site is the stick figure with the gun in hand.



9.5 WORD DOC (ACCOUNTS) – ROMERO'S LAPTOP

FTK Imager displaying the document holding account and passwords of fake Brandy Vela accounts.



Snapshot of document displaying:

1)website

2) Account(email)

3) password,

4) Profile information

SITE facebook

AACCOUNT brandyv@gmail.com

PASSWORD ihatemyself

Site match.com

AACCOUNT brandyv@gmail.com

PASSWORD ih4temyself

Site tinder

AACCOUNT bravela@gmail.com

PASSWORD ihat3myself23

Hi my name is brandy and [expletives]

10 BEHAVIORAL EVIDENCE ANALYSIS (BEA)

Behavioral evidence analysis (BEA) was completed concurrently with digital evidence analysis. BEA allows the investigator to understand the suspect(s) motivation and help identify patterns in evidence associated with his/her profile. There are four steps to conduct behavioral analysis:

1) Forensic analysis (SEE section 9 above titled "Evidence Analysis ".)
2) Victimology
3) Crime scene characteristics
4) Offender characteristics

10.1 VICTIMOLOGY

Victimology is defined as investigating, establishing, and evaluating victim traits and history: learning everything there is to know about victims, who they were, where and how they spent their time, and how they lived their life. The characteristics of the victim can provide inferences about the offender's fantasy, motive, modus operandi, knowledge, and skill (Turvey, 2008).

10.1.1 EVIDENCE ANALYSIS

The analysis shows Vela spent considerable time on Facebook and talking on the cell phone. Romero discovered this fact when she logged into her boyfriend's account (Villagomez) and found that he had lengthy chats with her.

10.1.2 EXPOSURE ASSESSMENT

Due to the accessibility and availability of the internet, the harm associated with digital stalking and impersonation can take place any time of the day. By providing personal contact information of Vela, Romero had essentially provided open source harassment by individuals outside her own control.

10.2 CRIME SCENE CHARACTERISTICS

Sites on the internet were chosen to expose Vela as much as possible. The three sites chosen by Romero were Facebook, Match.com and Tinder. Romero showed she opened up more accounts after the website shut down the profiles. The account document holding the login/passwords to fake brandy files indicate other victims subject to impersonation and stalking.

10.3 OFFENDER CHARACTERISTICS

The harasser(s) that were anonymous during the stalking campaign called Vela a "fat cow" on Vela's Facebook page and over the phone. During the analysis of her cell phone, we found Vela's number listed with the same slur. Additionally, an image file, and message logs showed her referencing Vela as a "Fat Cow". The iOS7 and Facebook messages obtained show a very jealous, insecure, and vengeful individual. These characteristics are common in stalking activity, manipulation, rage and/or physical abuse.

11 FINDINGS

Finding 1 Word document containing Facebook and dating site accounts/passwords to impersonate Vela (and another woman) found on Romero's laptop. Show evidence of previous impersonation and stalking attempts.

Finding 2 2 images found related to harassment on the Facebook memorial site of Brandy Vela: a gun inside a book and a stick figure holding a gun. Both images found on Romero's Dell Laptop.

Finding 3 Romero's communications showed animosity to Vela after discovering nude photos of Vela on Villagomez's laptop. Facebook chat logs between Villagomez and Romero showed:

a) Romero accusing Villagomez of continuing a relationship with Vela.
b) Romero's intent to harass Vela over suspected relationship.

Finding 4 Vela's phone number found on Romero's cell phone. Contact listed as "Fat Cow"- name consistent with harassing messages sent to Vela's profile.

Finding 5 I0s7 messaging logs between Romero and relatives show discussions regarding revenge against Vela.

Finding 6 Romero Facebook content show impersonations of Vela's family members to harass and gain information to continue stalking attempts.

Finding 7 No evidence of Villagomez to intentionally distribute explicit images of Vela.

12 RECOMMENDATIONS

The jury should consider Romero as the originator in the harassment of Brandy Vela due to the high volume of evidence collected on her laptop, phone, and social media accounts. The evidence collected show Romero can be classified as a composed cyberstalker. A composed cyber stalker causes constant annoyance and irritation to the targeted victim. They have no desire to establish a relationship with their victim, and are motivated to cause them distress (Mutwa, 2016).

The evidence demonstrated three elements of stalking which is a pattern of conduct, implicit or explicit threats, and reasonable fear. In this case, the reasonable fear aspect is the victim's fear of seeing no end to the persistent stalking effort. The electronic communications and media collected on her devices undeniably support this claim as well as the possibility there was a collective effort lead by Romero.

Additionally, the court should consider whether Villagomez was unaware of Romero's access to his laptop to obtain images of Vela and send them to herself. From the evidence gathered, it is possible Villagomez was unaware of Romero's intrusion to his files and her cyber stalking activity of Brandy Vela.
The evidence obtained show no intent to distribute explicit images.

13 APPENDIX

13.1 APPENDIX A: COMPLETED REQUEST FOR ASSISTANCE EXAMPLE

REQUEST FOR SERVICE

CASE INFORMATION:

		RCFL Case #: 90033
Submitting Person/ID#: Paul Keener	Date: 3/16/2017	Agency Case #: 90033
Submitting Agency: USD	Service: **Field** (**Lab**) **Tech**	Case Title: Valn
Agency Property Tag #: XYZ 1	Suspect's Name: Karinthya S. Romero	
Case Agent: Paul Keener	Phone #: 619-555-0000	
DDA/AUSA Assigned: Watis Thistlefield	Phone #:	
Date Seized: 3/16/2017	Case/Crime Type: Stalking/Impersonation	
Location Seized: 123 St. Galveston, Tx	Pending Court Dates: 11/10/2017	
Site #: 42	Date Analysis Needed: 6/30/2017	
Suspect In Custody: (**Yes**/**No**)	Expected Evidence Return Date: 7/05/2017	
Narcotics Related: **Yes**/(**No**)	Number of Computers Anticipated: 1 (TOTAL 2 from 2 suspects)	

Type of Seizure: (Circle) **Search Warrant** **Probation** **Parole** **Consent** **Admin** **Fed. Grand Jury** **Other:**

Has this evidence been previously viewed and/or accessed by anyone? (Explain) NO. Submitted to lab

Are you aware of any privileged information contained within evidence? (Explain) NO.

Do you want Standard Case Related Search Strings run against evidence? (**Yes**/**No**)

(Circle Requested Searches) **Child Porn** **Narcotics** **Financial Crimes** **Internet Crimes** **Extortion** **Other:** Terms associated with stalking activity

SERVICE REQUESTED: ***(Requests for Field Service must be received at least 2 business days prior to the search.)***

Full examination of evidence pertinent to stalking/impersonation charges

INSTRUCTIONS:

a. Please prepare one form for each search site (address).
b. Please provide ***ALL*** requested information and note any unusual circumstances in the Service Request area.
c. Please attach an Evidence Custody Form listing each individual container or package of submitted evidence.

RCFL USE ONLY **Date Case**	**Received By:** RYAN NYE
Case Priority: Lvl 1	**Priority Established By:** RN

13.2 APPENDIX B: DIGITAL INVESTIGATOR CONSULTATION LETTER EXAMPLE

DATE: 05/27/2017
TO: PAUL KEENER
FROM: RYAN NYE (#1003373)

SUBJECT: Consultation of Digital Evidence for Case #90033

The purpose of the document is to inform you (case investigator) what may or may not be discovered. Additionally, we will explore preliminary topics in digital analysis relevant to this case.

From the request placed by your team, I see no other forensic processes required for the evidence. This includes all items listed: hard drives, cell phone, and social media information requests. I recommend the possibility of pursuing a preservation order to the suspects Internet service provider (ISP) to identify the IP address and application used to access the internet.

The potential evidence being sought remain to be images, messages, emails, social media artifacts, and other information related to the cyberbullying of Brandy Vela. Password may need to be retrieved through interview/interrogation, existing documents, or by using applications designed to crack the password of the device.

From our understanding, the suspects have a low to medium level of understanding of computers. Therefore, there is reasonable doubt no concealment or destruction programs were deployed on the devices and no additional specialized personnel will be needed.

The evidence priority requested by your team is noted. Evidence analysis will begin with Karinthya Romero's devices, the lead suspect for stalking and impersonation of the victim. Second, we will inspect the devices of Andres Villagomez, suspected of unlawful disclosure or promotion of intimate visual material.

If we discover other criminal activity unrelated to charges in case #90033, we will be looking for further guidance from your team.

Sincerely,

Ryan Nye

Ryan Nye
Digital Forensic Investigator

13.3 APPENDIX C: CHAIN OF CUSTODY EXAMPLE- ROMERO'S DEVICES

Chain of Custody Document

Sequence Number: 312123

Receiving Organization: Regional Computer Forensic Lab

Location: RFCL Lab

Name of Person From Whom Received: Paul Keener

Address: 1333 NW Freeway, Suite 1100, Houston, Tx

Location from Where Obtained: 13 Guitty St., Galveston, TX

Reason: Crime Incident.

Date/Time Obtained: 5/27/2017

Item Number	Quantity	Description
001 Ex A	1	Dell Latitude D-630 Laptop, Serial# 7PS6632 - Good Condition
002 Ex B	1	Apple iOS7 phone, Serial# DMPH74H9DFHW - Good Condition

Item Number	Date	Released By:	Received By:	Reason for Change:
1) 001 2) 002	5/27/17 14:00	Signature P.K. Name & Title Paul Keener, Inv.	Signature T.M. Name & Title Tom Hanks, Cust.	Drop off at Lab to forensic storage area
1) 001 2) 002	5/27/17 14:05	Signature T.M Name & Title Tom Hanks, Cust.	Signature [illegible] Name & Title Ryan Nye Inv.	obtained by digital investigator for analysis
1) 001 2) 002	6/30/17 13:01	Signature [illegible] Name & Title Ryan Nye	Signature P.K. Name & Title Paul Keener	Returned to Lead Investigator
		Signature Name & Title	Signature Name & Title	

The American Society of Digital Forensics & eDiscovery

Download additional copies at www.asdfed.com

Network with other professional by visiting www.asdfed.com/ join.

13.4 APPENDIX D: CHAIN OF CUSTODY EXAMPLE- VILLAGOMEZ'S DEVICES

Chain of Custody Document

Sequence Number: 312124

Receiving Organization: Regional Computer Forensics Lab

Location: RCFL, Houston

Name of Person From Whom Received: Paul Keener

Address: 1333 NW Freeway Suite 400, Houston, TX

Location from Where Obtained: 27 Image St., Galveston, Tx

Reason: Crime, illegal dist. of image

Date/Time Obtained: 5/27/2017

Item Number	Quantity	Description
003 Ex C	1	Lenovo ThinkPad SL510 Laptop S# 76-12AB9 - Good Condition
004 Ex D	1	Samsung Galaxy S5 S# RFBF30W63XD - Good Condition

Item Number	Date	Released By:	Received By:	Reason for Change:
003 004	5/27/17 14:00	Signature P.K. Name & Title Paul Keener, Investigator	Signature T.M. Name & Title Tom Hanks, Evidence Handler	Drop-off at lab storage Pending Analysis
003 004	5/27/17 14:05	Signature T.M. Name & Title Tom Hanks, Evidence Handler	Signature [illegible] Name & Title Ryan Nye, Digital Forensics	Analysis of Evidence
003 004	6/30/17 13:01	Signature [illegible] Name & Title Ryan Nye, Digital Forensics	Signature P.K. Name & Title Paul Keener	Return to lead investigator
		Signature Name & Title	Signature [illegible] Name & Title	

The American Society of Digital Forensics & eDiscovery

Network with other professional by visiting www.asdfed.com/ join.

Download additional copies at www.asdfed.com

13.5 APPENDIX E: COMPUTER EVIDENCE WORKSHEET EXAMPLE- ROMERO'S LAPTOP

Computer Evidence Worksheet

Case Number: #90033 Exhibit Number: 001

Laboratory Number: 900-1-AZ1 Control Number: AZ1

Computer Information

Manufacturer: DELL Model: D-630 LAPTOP

Serial Number: 7P5663Z

Examiner Markings: Red sticker '13' on lower right corner

Computer Type: Desktop ☐ Laptop ☒ Other: ____

Computer Condition: Good ☒ Damaged ☐ (See Remarks)

Number of Hard Drives: 1 3.5" Floppy Drive ☐ 5.25" Floppy Drive ☐

Modem ☐ Network Card ☒ Tape Drive ☐ Tape Drive Type: ____

100 MB Zip ☐ 250 MB Zip ☐ CD Reader ☐ CD Read/Write ☒

DVD ☒ Other: USB Dock

CMOS Information Not Available ☒

Password Logon: Yes ☐ No ☒ Password = ____

Current Time: 15:00/3:00 AM ☐ PM ☒ Current Date: 5/27/2017

CMOS Time: 15:00/3:00 AM ☐ PM ☒ CMOS Date: 5/2/2017

CMOS Hard Drive #1 Settings Auto ☐

Capacity: 80 Gig Cylinders: N/A Heads: N/A Sectors: N/A

Mode: LBA ☐ Normal ☒ Auto ☐ Legacy CHS ☐

CMOS Hard Drive #2 Settings Auto ☐

Capacity: ____ Cylinders: ____ Heads: ____ Sectors: ____

Mode: LBA ☐ Normal ☐ Auto ☐ Legacy CHS ☐

Computer Evidence Worksheet Page 1 of 2

Sub Exhibits Split From This Computer

Sub Number	Type	Where Found

N/A

Remarks

Laptop in good condition
Excessive oil, hairspray?, on keyboard

15:00 5/27 Extracted drive to lab device
15:03 5/27 Multiple copies made

15:06 5/27 Images related to case found
15:10 1) fatcow.jpg
15:11 2) gunboat.jpg
15:11 3) sticking.jpg
Documents

15:18 5/27 Word file located involving
— account names (passwords)
of fake profiles

Computer Evidence Worksheet Page 2 of 2

14 REFERENCES

CBS. (2017, March 16). *Texas Couple Charged in Alleged Cyberbullying that Led to Teen's Suicide*. CBSNews,.com. Retrieved from http://www.cbsnews.com/news/texas-couple-charged-in-alleged-cyberbullying-that-led-to-teens-suicide/

CNN. [CNN News]. (2016, December 4). *Bullied Teen Kills Herself in Front of Family on CNN* [Video File]. CNN News. Retrieved from https://www.youtube.com/watch?v=IGLwEKxMjT8

Facebook. (2017). *Information for Law Enforcement Authorities.* Facebook.com. Retrieved from https://www.facebook.com/safety/groups/law/guidelines/

Hassan, C. (2016, December 14). *Teen who shot herself in front of her parents is still being bullied*. CNN.com. Retrieved from http://www.cnn.com/2016/12/14/health/teen-suicide-cyberbullying-continues-trnd/index.html

Keener, P. (2017). *The Final Project.* University of San Diego. Retrieved from https://ole.sandiego.edu/webapps/blackboard/content/listContent.jsp?course_id=_49642_1&content_id=_975024_1

Kelly, H. (2012, August 30). *Police embrace social media as crime-fighting tool.* CNN.com. Retrieved from http://www.cnn.com/2012/08/30/tech/social-media/fighting-crime-social-media/index.html

Montel.com (n.d.). *Digital and Mechanical Evidence Lockers: Protect Your Evidence and Control Access to It with Montel's High-Security, Heavy-Duty Storage Solutions*. Montel.com. Retrieved from http://www.montel.com/en/products/evidence-storage-lockers

Mutawa, N.A., Byrce, J., Franqueira, V., Marrington, A. (2016, January 12). *Forensic Investigation of Cyberstalking Cases Using Behavioral Evidence Analysis.* ScienceDirect.com. Retrieved from http://www.sciencedirect.com/science/article/pii/S1742287616300068#bib34

National Institute of Justice. (2001, July). *Electronic Crime Scene Investigation: A Guide for First Responders*. U.S. Department of Justice. Retrieved from https://ole.sandiego.edu/bbcswebdav/pid-975029-dt-content-rid-4005588_1/courses/CSOL-590-MASTER/M7/Crime_Scene.pdf

National Institute of Justice. (2004, April). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement.* U.S. Department of Justice. Retrieved from

https://ole.sandiego.edu/bbcswebdav/pid-975029-dt-content-rid-4005592_1/courses/CSOL-590-MASTER/M7/Forensic_Exam.pdf

Patzakis, J. (2014). *Overcoming Potential Legal Challenges to the Authentication of Social Media Evidence. X1.com.* Retrieved from http://www.x1.com/download/X1Discovery_whitepaper_Social_Media.pdf

Terzian, D. (2014). *The Fifth Amendment, Encryption, and the Forgotten State Interest*. UCLALaw Review.org. Retrieved from https://www.uclalawreview.org/pdf/discourse/61-19.pdf

Turvey, B.E. (2008). *Criminal Profiling: An Introduction to Behavioral Evidence Analysis.* Burlington, MA: Elsivier, Inc.

Withoutatraceinvestigations.com. (n.d.).*US Schools and the US Constitution - A Cyberbullying Legal Guide.* Wired Safety and Parry Aftab. Retrieved from http://www.withoutatraceinvestigations.com/wp-content/uploads/2012/02/US_Schools_and_Constitution_Legal_Guide.pdf