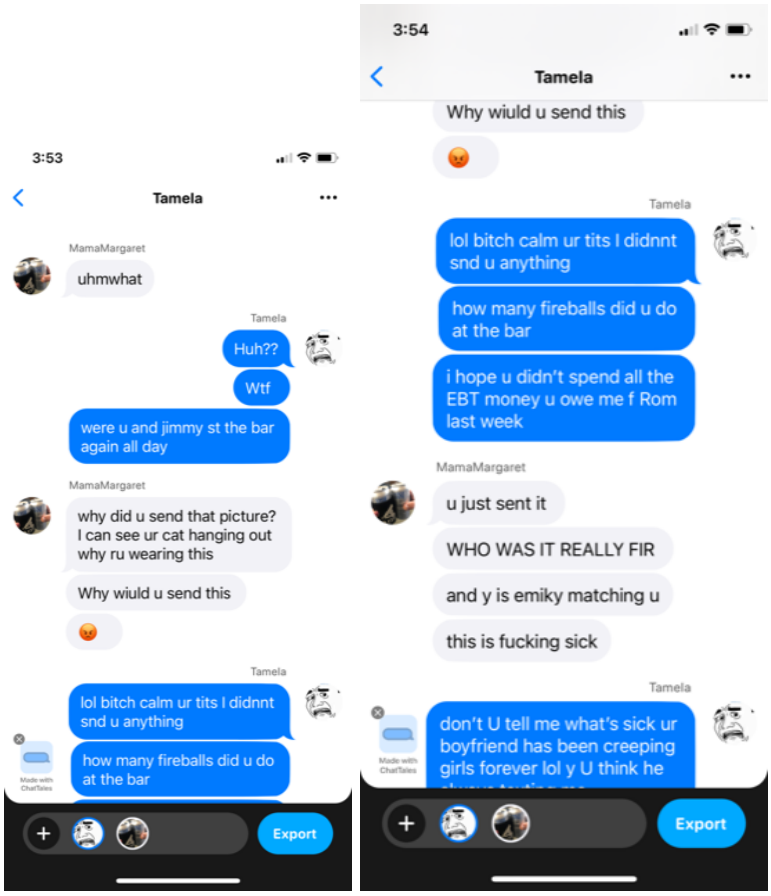
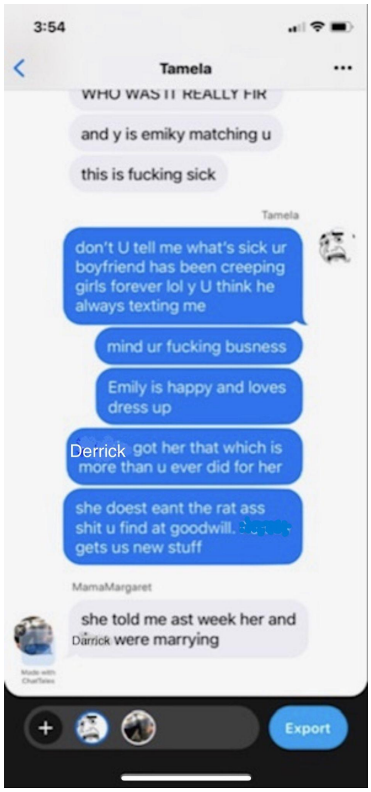
Investigative Packet and Experiential Exercises Instructions

Crime Scene Scenario

The investigation begins (Date-4 weeks) with a CPS report made by Grandmother, Margaret Stone, and her seven year old granddaughter, Emily Stone.

Margaret says that her daughter, Tamela Stone, accidentally sent her a pic of her and Emily wearing matching red lingerie. Margaret deleted the picture but was concerned about this and makes a call to the Child Abuse Reporting Hotline. CPS coordinates with local law enforcement and Emily is interviewed at the local Child Advocacy Center. Det. Doofey Gilmore is assigned the case.





During Emily's forensic interview, she discloses that her mom (Tamela) gives her "prizes" after she and Darrick "marry her." Darrick is Tamela's live in boyfriend. The prizes are different each time but are usually stuffed animals or dolls. One time, Emily got makeup that was lipstick and sparkly eye shadow. Emily describes to her forensic interviewer that when her they are playing "marrying", she and her mom put on matching clothes that "are see-through."

She says that her "see-through marrying suit" has a tear in it because "Darrick ripped it when he pulled it off (of her) fast." Emily tells the forensic interviewer that her mom and Darrick come into her room at nighttime and tell her to put on her "special outfit" so they can "marry" her.

Emily gives details about Tamela and Darrick "licking on her (Emily's) private". Darrick also "rubs his pee-pee" on Emily's private. Emily said Darrick's pee-pee feels "rough" on her skin and when asked to explain, she stated "his rubbing on her feels like it has bones in it but not bones". Emily states that she wants Darrick to stop "marrying her" because he "rubs too hard and it makes my (Emily) private bleed." Once she bled on her underwear and so she hid the underwear. She hid them because it happened once before and Tamela got mad at Emily when she saw the bloody underwear. That night, Emily heard Tamela and Darrick fighting about the blood. The next day, Emily was supposed to go to the doctor but she heard her mother on the phone with the doctor saying Emily was sick and they would come another time. Emily told the interview she didn't feel sick but thought the blood meant she was so she's been worried since then that something was wrong with her.

Sometimes when the marrying happens, Darrick or Tamela give her a red cup to drink from. Sometimes it tastes like fruit, sometimes it tastes like “how Christmas smells”. She feels sleepy after drinking from the cup and does not remember the marrying.

Emily tells the interviewer Derrick went away for a little while but is back now. When he went away, Tamela talked about friends she wanted Emily to meet. The friends are in mom’s phone and she uses a yellow ghost to talk to them. Emily could see the friends on Tamela’s phone and hear them talk. The friends would ask Emily to do gymnastics moves and spin around. Emily would do that and her mom would record it. Emily never met any of the friends in real life but they were all boys that were older than Emily, about the same age as her mom. The friends called her mom “Miss Maggie” and Emily has heard other people call her mom “Maggie”.

After Emily’s interview, Det. Gilmore collects copies of screenshots Margaret made of the texts between her and Tamela. The detective did not conduct a search of Margaret’s phone or obtain phone records. Det. Gilmore is called out to a homicide investigation at the local high school and forgets about Emily’s case. While the investigation is pending, a Cybertip report is sent to the police department and is assigned to a detective in a different unit.

Cybertip Report

On (Date – 3 weeks) , the National Center for Missing & Exploited Children (NCMEC) received a cybertip from social media platform Discord[1]. Discord flagged two video files that contained child sexual abuse material (F1, F2) and provided that information to NCMEC to begin an investigation. Because of delays in processing, the downloads appear to have been done (Date - 6 months) prior.

F1 is known child sexual abuse material (CSAM) and is referred to as the “Tara series.” This file is recognizable by the distinct Mardi Gras mask the child victim is made to wear. The hash value of this image has been compared to a file with the exact hash value of this file, and verified to be a one minute, five second video of CSAM. This file depicts an approximately eight-year-old nude female victim, being subjected to oral, vaginal, and anal abuse by an adult male. The child victim is wearing a purple and turquoise blue Mardi Gras mask throughout the abuse file.

The following identifying information has been sent to NCMEC by Discord:

Hash Value: 120EA8A25E5D487BF68B57096440019

Email address: Rontam69@gmail.com

Discord UserID: Rontam

IP address: 10.05.0.9.178.163

F2 is unknown child sexual abuse material (CSAM). This video file depicts an approximately seven-year-old female and an adult female wearing similarly styled transparent undergarments. The child victim is listless and appears to at times be nodding off, at other times fully asleep.

The adult female is observed removing the child's underwear and using her fingers to digitally penetrate the child's sex organ. The adult female is being given instructions by an adult male that is holding the recording device.

The following identifying information has been sent to NCMEC by Discord:

Hash Value: 327FA9AB4C5D488PD62V64235220893

Email address: Rontam69@gmail.com

Discord UserID: Rontam

IP address: 10.05.0.9.178.163

Legal Process

The Internet Crimes Against Children Commander of Colorado sent a subpoena to Xfinity Internet Service provider, for IP address 10.05.0.9.178.163. The subpoena return named Darrick Dahmer as the owner of the account using IP address 10.05.0.9.178.163. The address on the account is listed as 502 14th Street, Golden, CO 80401. The email address used on the account is Rontam69@gmail.com. On (Date -1 day), that information was passed on to the local police department and shared with the detective currently assigned to Emily's case.

Additional Information

(Date - 5 months), Darrick Dahmer was arrested for possession of a controlled substance and was held in custody. The intake paperwork shows the address of Darrick's friend Jeremy Sanders. At Darrick's preliminary hearing, he plead guilty to the charge. When the judge asked where he would be living, Darrick stated that he had been staying with Sanders because he was having problems with his girlfriend but they had reconciled while he was in custody and would be returning to live with her at 502 14th Street, Golden, CO 80401. When Emily was interviewed at the CAC, Darrick had been back at the residence for approximately one month.

Through the course of the investigation, it was learned that Tamela Stone has an alias, Maggie Taylor. This information was confirmed through interviews with the Grandmother Margaret Stone and the Emily's godmother Sarah St. Claire.

---

[1] Discord is a Voice over Internet Protocol and instant messaging social platform. Users can communicate with voice calls, video calls, text messaging, media and files in private chats or as part of communities called "servers".

Direct Examination of Digital Forensics Examiner

At trial, Sgt. Jones testified that in the course of the investigation they utilized several open source tools to find social media posts involving the defendant. A Facebook page with the name “Maggie Taylor” was located, with cats in the profile picture. The page listed an email for contact of MmTaylorSweet1@yahoo.com which further investigation showed was related to the defendant. The posts show contact with co-Defendant Derrick Dahmer and Sarah St. Claire who is the godmother of the child victim. The email address was also used to locate a Discord server with the same name.

A representative from each team will conduct an approximately 15-minute portion of the State’s digital forensic examiner’s direct examination. The participant will play the role of the prosecutor, asking questions of the digital forensic examiner and seeking to admit exhibit(s) over defense objections. The focus of direct examination exercises is testimony regarding, and admission of, the digital evidence. You may assume that all digital evidence was seized pursuant to a valid search warrant, with the exception of the Facebook posts, which were in plain view and screenshot by Sgt. Jones.

Each team will be given one of the following assignments:

Assignment #1: Elicit testimony regarding the Apple iPhone Validation Report prepared for Tamela Stone’s phone, (pre-marked as state's EXH 1) and seek its admission into evidence.

Assignment #2: Elicit testimony regarding the Apple iPhone Validation Report prepared for Darrick Dahmer’s phone, (pre-marked as state's EXH 2) and seek its admission into evidence.

Assignment #3: Elicit testimony regarding the SD Thumb Drive located in the crime scene and elicit testimony regarding metadata associated with child sexual abuse material (pre-marked as state’s EXH 3) and seek admission of the metadata into evidence. You should assume the date in the exhibit is correct and consistent with the scenario.

Assignment #4: Elicit testimony regarding a CashApp thread (pre-marked as state's EXH 4) created with Defendant Tamela's alias and seek its admission into evidence. The information contained in the exhibit is the result of a search warrant return.

Assignment #5: Elicit testimony regarding social media posts by Maggie (pre-marked as state's EXH 5A, 5B, and 5C) and seek their admission into evidence. The social media posts were collected by way of screenshots by Sgt. Jones.

Assignment #6: Elicit testimony regarding content from the Discord server created with the alias Maggie Taylor (pre-marked as state's EXH 7) and seek its admission into evidence.

Cross-Examination of Digital Forensics Defense Expert

A representative from each team will conduct an approximately 15-minute cross-examination of the digital forensics defense expert. Assume that the defense expert's CV below and each of the forensic artifacts provided for the scenario were previously admitted into evidence. Also, assume that the defense expert testified on direct examination consistently with his report. The report is accessible through the STARK materials link and labeled "Report of Defense Expert."

Digital Forensics Defense Expert Curriculum Vitae

Ray Ibiza
EnSparks Computers, LLC
2001 Blake St
Denver, CO 80205

EMPLOYMENT

Founder and Director of Forensics

EnSparks Computers, LLC February 2017 to Current

· Conducts forensically sound and well documented data extraction methods for digital device and adheres to strict chain of custody practices for search and storage.

· Provides a professional report detailing objective findings and expert testimony related to those findings.

· Expert level knowledge has been accumulated throughout the years through extensive hands-on examinations and continuing education.

Police Officer/Detective

Granville Police Department June, 2007 to February, 2017

· Responded to calls for service with the town of Granville.

· Conducted proactive/preventative patrols.

· Investigated misdemeanor and felony crimes including crimes involving digital evidence.

TRAINING AND EDUCATION

Champlain College, Burlington, VT Master of Science Degree, Spring 2020

Major: Digital Forensic Science

Research: Android Marshmallow 6.0.1 Factory Reset and Remote Wiping Forensic Artifacts

4.0 cumulative GPA

Federal Bureau of Investigation National Academy (FBI NA)
Quantico, VA

October 2016- December 2016

4.0 GPA

Internship – National White-Collar Crime Center (NW3C) Internet Crime Complaint Center (IC3)

1000 Technology Dr., Fairmont, WV 26554

Internet Fraud Analyst (Completed 200 hours of employment)

Analyzed internet crime complaints submitted via the NW3C website, which ranged from auction fraud to child exploitation. Also responsible for examining complaints and organizing them into cases based on similarity and submitting to law enforcement agencies in the appropriate jurisdiction.

Marshall University
2011-2015

Bachelors of Science Degree, Cyber Forensics and Security

4.0 cumulative GPA

Marshall's program included extensive experience using industry-standard tools such as MAGNET Axiom's Process and Examine, Kali Linux, Cellebrite, WireShark, Social Engineering Toolkit (SET), Network Miner, Metasploit, Armitage, NMAP and many others.

PROFESSIONAL TRAINING/CERTIFICATIONS

American College of Forensic Examiners Institute (ACFEI), Certified Forensic Consultant (2015)

National Computer Forensics Institute (NCFI), United States Secret Service Advanced Forensics Training (2016)

International Association of Computer Investigative Specialists (IACIS), IACIS Windows Forensic Examiner Training (2015)

Certified Cyber Crime Examiner, National White Collar Crime Center (NW3C) (2019)

Certified Forensic Video Analyst, Law Enforcement and Emergency Services Video Association (LEVA) (2017)

Cellebrite Certified Mobile Examiner (2016)

Cellebrite Certified Logical Operator (2014)

Cellebrite Certified Physical Analyst (2014)