

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Middle District of Florida

United States of America
v.
THOMAS LESTER HAZOURI, JR.

Case No.
3:20-mj- 1293-JRK

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of March 26, 2020 in the county of Duval in the Middle District of Florida, the defendant(s) violated:

Code Section
18 U.S.C. § 2252(a)(2)

Offense Description
Knowing distribution of child pornography

This criminal complaint is based on these facts:

See attached.

Continued on the attached sheet.

Abigail Beccaccio
Complainant's signature

Abigail Beccaccio, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 9-4-2020

James R. Klindt
Judge's signature

City and state: Jacksonville, Florida

James R. Klindt, U.S. Magistrate Judge
Printed name and title

**AFFIDAVIT**

I, Abbigail Beccaccio, being duly sworn, state as follows:

**INTRODUCTION**

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been so employed since May 2012. I am currently assigned to the Jacksonville, Florida Division of the FBI where I conduct a variety of investigations in the area of violent crimes. Prior to this assignment, I was employed as Forensics and Technology Unit Supervisor with the Orlando Police Department for approximately 8 years. I have a Bachelor's degree in Molecular Biology & Microbiology. I have received law enforcement training from the FBI Academy at Quantico, Virginia. A substantial portion of my duties are dedicated to investigating cases involving crimes against children under the auspices of the FBI's "Innocent Images" National Initiative. Since becoming a Special Agent, I have worked with experienced Special Agents who also investigate child exploitation offenses. In the performance of my duties, I have investigated and assisted in the investigation of matters involving the solicitation of, possession, collection, production, receipt, and/or transportation of images of child pornography and the solicitation and extortion of children to produce sexually explicit images of themselves. I have been involved in searches of residences pertaining to the solicitation of, possession, collection, production, and/or transportation of child pornography through either

JRK

the execution of search warrants or through the subject providing written consent to permit a search to be conducted.

2. I have investigated and assisted in the investigation of criminal matters involving the sexual exploitation of children that constituted violations of 18 U.S.C. §§ 2251, 2252, 2252A, 2422, and 2423, as well as Florida state statutes that criminalize the sexual activity with minors and other methods of child sexual exploitation. In connection with such investigations, I have served as case agent, have been the affiant for several search warrants and conducted interviews of defendants and witnesses, and have served as an undercover agent in online child exploitation cases. I am a member of a local child pornography task force comprised of the FBI, U.S. Immigration and Customs Enforcement, the Florida Department of Law Enforcement, the Jacksonville Sheriff's Office, the St. Johns County Sheriff's Office, and the Clay County Sheriff's Office, among other agencies. These agencies routinely share information involving the characteristics of child sex offenders as well as investigative techniques and leads. As a federal agent, I am authorized to investigate and assist in the prosecution of violations of laws of the United States, and to execute search warrants and arrest warrants issued by federal and state courts.

3. The statements contained in this affidavit are based on my personal knowledge, as well as on information provided to me by experienced Special Agents

*gju*

and other law enforcement officers and personnel. This affidavit is being submitted for the limited purpose of establishing probable cause for the filing of a criminal complaint, and I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that THOMAS LESTER HAZOURI, JR. has committed a violation of 18 U.S.C. § 2252(a), that is, knowing distribution of child pornography.

4. I make this affidavit in support of a criminal complaint against THOMAS LESTER HAZOURI, JR., that is, on or about March 26, 2020, in the Middle District of Florida, THOMAS LESTER HAZOURI, JR. did knowingly distribute visual depictions, that is, using any means and facility of interstate commerce, that is, by cellular telephone via the internet, when the production of the visual depictions involved the use of a minor engaging in sexually explicit conduct, and the visual depictions were of such conduct, in violation of 18 U.S.C. § 2252(a)(2).

5. On or about August 20, 2020, I spoke with Jacksonville Sheriff's Office (JSO) Detective (Det.) A. L. Means, and she provided information about an ongoing investigation of THOMAS LESTER HAZOURI, JR. for violations of Florida statutes involving child sexual exploitation. I know that Det. Means is a sworn JSO Deputy Sheriff assigned to the JSO Internet Crimes Against Children (ICAC) Unit,

and is a member of the North Florida ICAC and therein conducts investigations involving internet crimes against children. The investigation resulted in the issuance of a Florida state residential search warrant and the application and supporting affidavit, all of which I have reviewed and which are attached as Composite Exhibit A and incorporated by reference herein, for THOMAS LESTER HAZOURI, JR.'s residence located at 524 15th Avenue South, Jacksonville Beach, Florida, on August 5, 2020. This search warrant was executed the following day. I was advised that THOMAS LESTER HAZOURI, JR. was arrested August 19, 2020, following the completion of forensic examination of his electronic devices and his online accounts by members of the Jacksonville Sheriff's Office in Jacksonville, Florida.

6. Det. Means has provided me with documentation and evidence generated during this investigation, including the residential search warrant, several JSO reports detailing this investigation, reports detailing the examination of certain digital devices, and certain audio-recorded statements made on August 6, 2020 by HAZOURI and an adult female who was discovered at his residence on that day. I have reviewed all of these items, and have had numerous conversations about this investigation with Det. Means, both in person and by telephone. I have also viewed several image and video files depicting the sexual abuse of children that were recovered from the Kik account for "mybfsgaynotme," the CyberTip report discussed

JRK

herein, and the devices seized on August 6, 2020 as discussed herein. During the course of this investigation and through the sources of information listed above, I learned, in substance and among other things, the following:

a. On May 1, 2020, CyberTip report (CT) #68235908 was received by JSO from the National Center for Missing and Exploited Children (NCMEC). I have reviewed the information contained in this CyberTip report. Based on my training and experience, I know that NCMEC receives CyberTips from individuals and business entities regarding the possible sexual exploitation and abuse of children. Later on May 1, 2020, Det. A.M. Corbett<sup>1</sup> reviewed CT #68235908, originating from MediaLab/Kik (Kik) for investigation. Based on my training and experience, I know that Kik, or Kik Messenger, is a free instant messaging mobile application that can be used to transmit and receive messages, photos, videos and other content over the internet after a user registers a user name. Kik allows a user to maintain anonymity and protect a user's identity. Kik officials suspected multiple images depicting child sexual abuse material (CSAM) had been uploaded by a Kik user from

---

<sup>1</sup> I know that Det. Corbett is a sworn JSO Deputy Sheriff assigned to the JSO Internet Crimes Against Children (ICAC) Unit, and is a member of the North Florida ICAC and therein conducts investigations involving internet crimes against children. I also know that a portion of Det. Corbett's duties and responsibilities include reviewing and triaging CyberTipline reports from NCMEC before they are assigned to a particular ICAC Detective.

JRK

Internet Protocol (IP) address 23.113.246.250 on March 26, 2020, between the times of 19:47:15 UTC<sup>2</sup> and 20:58:22 UTC. Kik provided certain subscriber information about this user account, including two email addresses for the user account, “tommyhazouri@gmail.com” and “Illestknickas@gmail.com.” Kik also provided the username for this account, “mybfsgaynotme,” and the Electronic Service Provider (ESP) User ID as “mybfsgaynotme\_y6h.” On May 7, 2020, Det. Corbett caused a preservation request, which I have reviewed, to be served to Kik requesting that this Kik account (“mybfsgaynotme”) associated with email addresses “Illestknickas@gmail.com” and “tommyhazouri@gmail.com” be preserved for 90 calendar days.

b. Det. Corbett applied for and received a Florida state search warrant issued on June 2, 2020, which I have reviewed, that authorized viewing, seizing, preserving, and copying for evidentiary purposes of all files provided to JSO by NCMEC in CT #68235908. I have reviewed this search warrant as well as the application and supporting affidavit.

---

<sup>2</sup> Based on my training and experience, I know that UTC is an acronym for “Universal Time Coordinated,” formerly known as “Greenwich Mean Time. UTC time is a standard time set at longitude 0° and is either four or five hours ahead of Eastern Time, depending on the time of year.

c. Det. Corbett confirmed that IP address 23.113.246.250 that was provided by NCMEC was owned by internet service provider AT&T U-Verse. On May 8, 2020, Det. Corbett caused a Florida state subpoena to be served to AT&T U-Verse for the disclosure of subscriber information for the user of IP address 23.113.246.250 on March 26, 2020, between the times of 19:47:15 UTC and 20:58:22 UTC and related to CT #68235908. On or about May 11, 2020, AT&T responded indicating that, on the relevant date and times, this IP address was assigned and resolved to a subscriber identified as TOMMY HAZOURI and with a physical service address of 524 15th Avenue South, Jacksonville Beach, Florida 32250. Moreover, it is noted that the email address “tommyhazouri@gmail.com” associated with the Kik account “mybfsgaynotme” used to upload the child pornography files to Kik users on March 26, 2020 was also listed as part of HAZOURI’s AT&T account subscriber information.

d. On July 2, 2020, Det. Means was assigned CT #68235908 for further investigation and reviewed all files provided by Kik in the CyberTip, identified as five videos. Two of these video files were confirmed by Det. Means to meet the definition of child pornography under Florida law.<sup>3</sup> Det. Means also

---

<sup>3</sup> I have reviewed these videos, and I have probable cause to believe that they constitute child pornography pursuant to 18 U.S.C. § 2256. They are described in greater detail below.



learned through open source internet research that THOMAS HAZOURI was currently employed by Duval County Public Schools (DCPS) as a second grade teacher assigned to Mayport Elementary School in Jacksonville, Florida.

e. On July 7, 2020, Det. Means applied for and received two Florida state ESP search warrants for Google, LLC and Kik for account information and content for accounts associated with "Illestknickas@gmail.com," "tommyhazouri@gmail.com," "mybfsgaynotme," and "mybfsgaynotme\_y6h." I have reviewed these search warrants as well as the applications and supporting affidavits.

f. On July 8, 2020 and July 30, 2020, respectively, Google and Kik provided responsive documents to Det. Means as requested by these two Florida state ESP search warrants. All responsive documents from these search warrants and the information contained in CT #68235908 were then provided to JSO Forensic Examiner Det. S. A. Torres. I have also reviewed these documents and this information.

g. Det. Means also provided me with a JSO Digital Device Examination Report dated July 16, 2020 that was completed by JSO Det. Torres. I know that Det. Torres has been trained as a forensic examiner and has expertise in the forensic review and analysis of computers, electronic devices, and online

accounts such as Kik and Google. This July 16, 2020 report detailed the examination of the contents of the Google accounts for email addresses “Illestknickas@gmail.com” and “tommyhazouri@gmail.com.” These materials were received from Google pursuant to the Google search warrant referenced above. I have reviewed this report and learned, among other things, the following information:

(i) There were 70 files located in the Google account for “tommyhazouri@gmail.com” that depicted either child erotica or age-difficult pornography. No files depicting child sexual exploitation (CSE) were located in the Google account for “Illestknickas@gmail.com.” The Google account for “tommyhazouri@gmail.com” contained personal files associated with THOMAS LESTER HAZOURI, JR. (date of birth in 1980) such as the following: pictures and videos depicting THOMAS LESTER HAZOURI, JR., many of which appeared to be self-produced by HAZOURI; the resumé for “Thomas L. Hazouri” composed in multiple formats sent as attachments in multiple emails; a picture of a Florida driver’s license issued to “Thomas Lester Hazouri;”<sup>4</sup> a picture of a court document

---

<sup>4</sup> I have viewed this image and I recognize the adult male depicted in the image as THOMAS LESTER HAZOURI from my review of his photograph from the Florida Driver and Vehicle Identification Database (DAVID). Further, Det. Means advised me that she confirmed that the adult male pictured is THOMAS LESTER HAZOURI based on her personal contact with him at his residence in

ju

listing “Thomas Lester Hazouri” as the defendant; and pictures of correspondence sent to Thomas Lester Hazouri.

(ii) Additionally, there were non-exploitative pictures of children located in this Google account for “tommyhazouri@gmail.com,” many of whom were pictured in a school-type setting. Some of these photos contained embedded metadata (latitude and longitude coordinates) that geolocated and resolved to Mayport Elementary School in Jacksonville where HAZOURI was employed. The video files reported to NCMEC and contained in CT #68235908 were not located in the contents of this Google account (“tommyhazouri@gmail.com”). However, two emails were located in this Google account material that each referenced the use of the Kik user name “mybfsgaynotme.” One email was sent by Kik on February 25, 2020 to the email address “tommyhazouri@gmail.com” and the second email was sent by Kik on April 5, 2020 to the email address “Illestknickas@gmail.com.” Both emails appeared to welcome the user to Kik, reading in part, “Welcome to Kik!” This Google account (“tommyhazouri@gmail.com”) also contained a picture of a handwritten letter that appeared to be written in child-like printing and was addressed to “Tommy.” The letter indicated that it was from two individuals, “T” and “N.” The writer asks

---

Jacksonville Beach on August 6, 2020.

“Tommy” if he likes “coconut’s” and has several hearts drawn on it. The only other user-identifying information found within the Google account associated with “Illestknickas@gmail.com” was the email related to the Kik user account that linked the two email addresses together.

h. Det. Means also provided me with a JSO Digital Device Examination Report dated August 3, 2020 that was completed by Det. Torres. This report detailed the examination of the contents of the Kik account for the screen/user name “mybfsgaynotme.” These materials were received from Kik pursuant to the Kik search warrant referenced above. I have reviewed this report and learned, among other things, the following information:

(i) There were 19 images and 45 videos in the Kik account each of which depicts at least one minor engaged in sexually explicit conduct, and therefore, I have probable cause to believe that these depictions constitute child pornography pursuant to 18 U.S.C. § 2256. The files contained in CT #68235908 were not found in the production of materials by Kik pursuant to the search warrant. I know that Kik only retains media data on its servers for 30 days unless a preservation request is submitted. No request for preservation was made prior to the expiration of 30 days from the date of uploading (March 26, 2020) because JSO did not receive this CyberTip until May 1, 2020.

(ii) There were also two images of a young female child contained in the Kik response that appeared to have been taken in a classroom setting. Although the child is wearing different clothing in each of the two pictures, both pictures depict her lying down on her stomach on a colorful rug that appears to be in an school classroom. The child is pictured facing away from the camera, leaning on her elbows, with her legs slightly apart. Although other children are partially shown in these photos, this particular child appears to be the primary subject of both photos, which focus on her clothed bottom and the area between her legs. In one photo, the child is wearing black and the rug appears to have a cartoon rabbit, a green outer border, a light blue inner border with the letters “nflie” visible near what appears to be cartoon dragonflies and butterflies, and a darker pattern in the middle of the rug. In the other photo, the child is wearing white shorts and the rug appears to have a cartoon goldfish surrounded by a similar darker blue as in the first photo. Although the child’s feet partially obscure her clothed buttocks in this photo, the photo is taken at such an angle that the viewer can see up the child’s shorts.

(iii) According to Det. Means, the rug depicted in these two photos appears similar to a third photo, depicting a rug in a classroom, that was recovered from the Google account of “tommyhazouri@gmail.com” pursuant to the

Google search warrant discussed above. This images depicts a classroom full of children sitting on a rug and shows the children's faces. This image shows what appears to be the same cartoon rabbit at the front of the rug as in the first photo described above and further depicts various cartoon animals across the rug. Moreover, this rug displays what appears to be a cartoon goldfish, the same color patterns, and the same type lettering as the first two photos. This third photo, found in the Google "tommyhazouri@gmail.com" account, has embedded metadata containing the latitude and longitude coordinates for Mayport Elementary School in Jacksonville, Florida.

(iv) The materials contained the Kik account for the screen/user name "mybfsgaynotme" also included a short video that briefly displayed the partial, upper face of a male that appeared to be HAZOURI based on comparison with HAZOURI's Florida driver's license photo. There was also a photo of a white male masturbating, showing his wrist, his hand, and his penis, as well as a rug on the floor. The male was wearing a beaded bracelet and displayed a tattoo on his wrist. This photo also depicted a Lenovo laptop computer that was on table in the background.

i. According to Det. Means, a search of property records revealed that “Thomas L. Hazouri, Jr.” is the owner of the residence located at 524 15th Avenue, Jacksonville Beach, Duval County, Florida.

j. On August 5, 2020, a Florida state residential search warrant was issued for HAZOURI’s residence located at 524 15th Avenue South, Jacksonville Beach, Florida, 32250. On August 6, 2020, Det. Means and other JSO personnel executed this search at this residence. HAZOURI, together with an adult female and a four year old child, were at the residence. Outside of the residence, HAZOURI agreed to speak with Det. Means. He was provided a copy of the search warrant and learned that the investigation involved child pornography. He stated, among other things, “I don’t mess with computers at all in that way.” Despite being told that he was not being detained and was free to leave, HAZOURI continued to make unsolicited statements, including that this situation was “so embarrassing” and “I don’t mess with kids like that.”

k. During the execution of the search warrant at HAZOURI’s residence on August 6, 2020, JSO personnel located HAZOURI’s Apple iPhone XR cellular phone with internal SIM card (seized from a dresser in HAZOURI’s bedroom), an Apple MacBook Pro (seized from a closet in HAZOURI’s bedroom), and several other items of evidence, including a Lenovo laptop computer that was

*JRK*

determined to be the property of DCPS.<sup>5</sup> All items were subsequently submitted to the JSO property room, then later checked out and taken to the JSO Internet Crimes Unit for examination as authorized by the search warrant issued for HAZOURI's residence (Composite Exhibit A).

1. Det. Means provided me with a JSO Digital Device Examination Report dated August 13, 2020 that was completed by Det. Torres. This report detailed the examination of the items seized from HAZOURI's residence on August 6, 2020 pursuant to the residence search warrant (Composite Exhibit A). I have reviewed this report, as well as a JSO supplemental report printed on August 25, 2020, and learned, among other things, the following information:

(i) HAZOURI's Apple iPhone XR ("iPhone XR") contained 123 images and three videos depicting child sexual abuse (CSA), that is, depictions of at least one minor engaged in sexually explicit conduct. Seven of the images involved an infant or a toddler-age child. The majority of the CSA image files were thumbnail images associated with MEGA, an application that provides encrypted cloud storage and enables users to upload, download, view, and share files from their devices.

Based on my training and experience, I know that a thumbnail image may remain on

---

<sup>5</sup> A separate state search warrant was obtained August 11, 2020, by Det. Means for this device following a conversation with DCPS Director M.P. Edwards. These results of this search are pending.



a device even after its original file has been deleted. The MEGA application (“app”) was installed on the iPhone XR. There was forensic evidence that the iPhone XR had been used to access websites using child notable keywords in their titles and web addresses. There were search terms that were indicative of child exploitation, including “3d loli vid” and “lolicon<sup>6</sup> floor masturbation vids.” Three of CSA videos on the iPhone XR visually appeared to be the same content as three of the reported videos in CT #68235908 from Kik. The email address “tommyhazouri@gmail.com” reported in CT #68235908 was the email address used for the Gmail, Tinder, and Uber accounts on the iPhone XR. The iPhone XR also had an Apple ID of “hazourit1@duvalschools.org.” There was a picture of a table found on the device that appeared to match the table and flooring shown in the picture of the masturbating male in the material returned from the search warrant for the Kik account for the screen/user name “mybfsgaynotme.”

(ii) The Apple MacBook Pro (“MacBook”) contained 119 binary unique pictures depicting either child erotica or age-difficult pornography. One of the age-difficult files discovered on the MacBook also existed on HAZOURI’s iPhone XR and in the materials from the Kik search warrant return.

---

<sup>6</sup> Based on my training and experience, I know that the terms “loli” and “lolicon” are commonly used online by individuals who have a sexual attraction to young girls.

*JK*

The MacBook was named “tommy hazouri’s MacBook Pro” and only had one user-defined account, which was password-protected. The email address “tommyhazouri@gmail.com” was the Gmail account used for the MacBook.

(iii) According to Det. Torres, there were no child notable files located on a Samsung Notebook 9 seized from HAZOURI’s residence. However, the email address “tommyhazouri@gmail.com” was accessed by this device, and multiple emails sent to this email address addressed the recipient as “Tommy” or “Thomas.”

m. On August 19, 2020, Det. Means and other JSO personnel arrested THOMAS LESTER HAZOURI, JR. on state charges related to his possession of child pornography.

7. My review of the JSO supplemental report printed on August 25, 2020 and the August 13, 2020 Digital Device Examination Report revealed the following additional information:

a. On August 6, 2020, while Det. Torres was inside HAZOURI’s residence during the execution of the search warrant, she observed a rug on top of flooring that matched the rug and floor in the Kik account photo that depicted a male masturbating referred to above. Det. Torres also observed a tattoo on HAZOURI’s wrist that matched the tattooed body markings on the male’s arm in

that same photo. HAZOURI was also wearing a beaded bracelet that was similar to the beaded bracelet worn by the male in the same photo. This same Kik account photo depicted a laptop on a table that appeared to match the Lenovo computer owned by DCPS that was seized at HAZOURI's residence.

b. Later on August 6, 2020, after completing her duties of documenting the layout at HAZOURI's residence and photographing the scene and evidentiary items, Det. Torres, Det. Means and other JSO personnel responded to Mayport Elementary School. They were escorted to HAZOURI's classroom, and Det. Torres photographed the area, observing the distinctive rug described above and depicted in the two photos recovered from the Kik account for the screen/user name "mybfsgaynotme" that depicted a clothed child lying on the rug.

8. On August 27, 2020, I reviewed the responsive documents from the Kik search warrant and learned the following: Kik reported username "mybfsgaynotme," unconfirmed email address "Illestknickas@gmail.com," user location as "US" with a time zone of America/NY, IP address 23.113.246.250, and "iPhone" listed as device type. From a review of the files distributed by the user of the "mybfsgaynotme" account, I learned while in a public group chat room, the user of ESP User ID as "mybfsgaynotme\_y6h" distributed at least four videos using the Kik application on March 26, 2020. I have reviewed these videos and I have probable cause to believe

that each of these four videos constitute child pornography. Two of the videos are described as follows:

Distributed on March 26, 2020 at 19:57 UTC to 46 other Kik users

File Name: 98c97450-82f5-4f36-af74-f5f3c56a86f4

Description: This is a color video 1:59 (minutes:seconds) in length depicting a prepubescent female child. The child is standing in a bedroom, facing the camera, and is initially wearing clothing. The child removes her clothing and immediately turns around to expose her buttocks. She then takes her finger and moves it in and out of her anal opening. She eventually turns around and begins to move her hand back and forth over her vagina. Next, she takes the camera and positions it to where the focal point is on her vagina. The child then inserts her finger into her vagina until the video abruptly stops. The child has some initial stages of breast development however there is no visible hair on or around her pubic area. Based on my training and experience, having viewed thousands of images and videos depicting child pornography and together with the information set forth herein, I have probable cause to believe that the image depicts a prepubescent minor engaged in sexually explicit conduct, that is, the lascivious exhibition of the genitals, and therefore

constitutes child pornography pursuant to Title 18, United States Code, Section 2256.

Distributed on March 26, 2020 at 19:58 UTC to 46 other Kik users.

File Name: 8503eb97-b944-44af-a8b7-5d6566a42d14

Description: This is a color video with audio, 1:59 (minutes:seconds) in length depicting a prepubescent male child and a white adult female. Only the top portion of the adult female is visible and she is wearing a shirt and kneeling in front of the child. Only the bottom half of the child's face is visible during the video. The child is completely nude and is facing the adult. The child has an overall lack of musculature and no visible hair in his pubic region. The adult brings her finger to her lips, while smiling, motioning for the child to be quiet. She then alternates between providing oral stimulation to the child's penis and stroking his penis with her fingers. The adult looks directly at the camera during the video, and at one point, licks the length of the child's penis. In the background, another child can be heard saying, "Mama." She eventually responds, speaking in an unknown language. The child bends forward slightly and covers his mouth with one of his hands. The adult nudges him back up, and points her finger at him, and says something in an unknown language as she continues to sexually batter the child. Based on my training

and experience, having viewed thousands of images and videos depicting child pornography and together with the information set forth herein, I have probable cause to believe that this image depicts a minor engaged in sexually explicit conduct, that is, oral to genital sexual intercourse, and therefore constitutes child pornography pursuant to Title 18, United States Code, Section 2256.

9. On August 27, 2020, I viewed several of the image and video files recovered from the iPhone XR belonging to HAZOURI and seized from HAZOURI's residence on August 6, 2020, and that were referenced by Det. Torres in her August 13, 2020 Digital Device Examination Report. One of these videos is described as follows:

FILE NAME: 22160d10aa174c627b6027a62e5fe999c1b7e137.mp4

DESCRIPTION: This is a color video with audio, 0:15


(minutes:seconds) in length, depicting a female child. This child is only wearing a spaghetti-strap tank top and the backside of her body is facing towards the camera. This child uses both of her hands to grab her buttocks, spread them apart, and bends over slightly as she looks towards the camera. This motion exposes a rear view of the child's anal opening and vagina. The child then turns around so that the front of her body is facing the camera. She uses both of her hands to spread her outer labia apart

to expose her clitoris. No pubic hair is observed on or around her pubic area. She then lifts her shirt to expose her bare breasts which display early signs of development. Based on my training and experience, having viewed thousands of images and videos depicting child pornography and together with the information set forth herein, I have probable cause to believe that this image depicts a minor engaged in sexually explicit conduct, that is, lascivious exhibition of the genitalia and pubic area, and therefore constitutes child pornography pursuant to Title 18, United States Code, Section 2256.

10. Based upon the foregoing facts, I have probable cause to believe that on or about March 26, 2020, in the Middle District of Florida and elsewhere, THOMAS LESTER HAZOURI, JR. did knowingly distribute visual depictions, that is, using any means and facility of interstate commerce, that is, by cellular telephone via the internet, when the production of the visual depictions involved the use of a minor

A handwritten signature in black ink, appearing to be the initials 'Jm', is located in the bottom right corner of the page.

engaging in sexually explicit conduct, and the visual depictions were of such conduct, in violation of 18 U.S.C. § 2252(a)(2).

  
ABBIGAIL BECCACCIO, Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me this 4<sup>th</sup> day of September, 2020, at Jacksonville, Florida.

  
JAMES R. KLINDT  
United States Magistrate Judge





**SEARCH WARRANT**

S.A. CASE NO.:

CCR NO.:

2020-306442

IN THE NAME OF THE STATE OF FLORIDA  
TO: ALL AND SINGULAR THE SHERIFF OR DEPUTY  
SHERIFFS OF DUVAL COUNTY, FLORIDA

WHEREAS, complaint on oath and in writing supported by affidavit of credible witness which is incorporated by reference herein, to wit: Detective Andrea L. Means of the Jacksonville Sheriff's Office, has been made to me the undersigned Circuit Court Judge in and for Duval County Florida, and

WHEREAS said facts made known to me and considered by me have caused me to certify and find that there is probable cause to believe that certain laws have been and are being violated, and that evidence of the violation of certain laws in the form of computer equipment and data, or printed or written documents and other related items described herein, are being kept in or about certain premises and the curtilage thereof and/or vehicles upon the curtilage belonging to or used by the resident(s) of said premises, in Duval County, Florida, being known and described as follows:

524 15th Avenue South, Jacksonville Beach, Florida (Duval County)

Description of Premises: From the intersection of Beach Boulevard and 3rd Street / Highway A1A, proceed south to the intersection of 3rd Street South / Highway A1A and 15th Avenue South. Turn west (right hand turn) onto 15th Avenue South. Cross the intersections of South 4th Street and 5th Street South. The structure at 524 15th Avenue South, Jacksonville Beach, Florida (hereinafter the "Premises") is located on the south side of 15th Avenue South and is the fifth residence from the intersection of 15th Avenue South and 5th Street South. The structure is identified as a one story, single family residence. The exterior of the house appears to be made of vertical sheet which is light green (tending towards aqua or teal) in color with white trim. The front door faces to the north and is white in color. From the perspective of standing in before the front door, there is a long, elongated sidelight window located immediately to the left of the front door. There appears to be a screen door immediately in front of the front door and it has a white trim. The residence has a small front porch that is enclosed by a small, white picket fence. There are colored numbers "524" on a multicolored address plate affixed to the home located to the right of the garage. The garage door faces to the north and it is white in color. The driveway extends northward from the garage door to 15th Avenue South. A mailbox is located to the left of the driveway and it is blue in color. There are white colored numbers "524" on the mailbox door. There are white colored rocks located at the base of the mailbox post. A wooden fence, approximately six feet in height, encloses the home's backyard.

The above-described Premises are being used in violation of the following Felony laws: §847.0135(2), Florida Statutes, prohibiting possession of child pornography under the: "Computer Pornography and Child Exploitation Prevention Act", and §827.071, Florida Statutes, prohibiting the sexual performance of a child and the creation, possession or promotion of an image of such conduct. This request for a search warrant is authorized pursuant to §933.18(6), Florida Statutes.

WHEREAS, the Court having found probable cause that a computer or other digital device capable of accessing the internet by means of service provided at or through the above described residence was knowingly used as an instrumentality of a crime and contains evidence relevant to proving a violation of the following Felony laws, to wit: §847.0135(2), Florida Statutes, prohibiting possession of child pornography under the: "Computer Pornography and Child Exploitation Prevention Act", and §827.071, Florida Statutes, prohibiting the sexual performance of a child and the creation, possession or promotion of an image of such conduct, and where the Premises is being occupied by Thomas Lester Hazouri, Jr., and others known and unknown, this search warrant is authorized pursuant to §933.18(6), Florida Statutes.

NOW THEREFORE, you are hereby ordered and authorized to seize the following items, and to conduct an off site search and analysis, or to delegate the search and analysis to an off-site computer forensic analyst, of the following items (hereinafter the "Property"):

1. Any and all computer(s), computer hardware, computer software, electronic storage media (including any and all disk drives, compact disks, flash drives, cellular telephones, personal digital assistants (PDA), digital cameras and/or memory cards, or any other device capable of electronic storage of data and/or images),

**COMPOSITE EXHIBIT A**

*JRK*

computer-related documentation, computer passwords and data-security devices, videotapes, video recording devices, video recording players, and video display monitors that are or may be used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography or child erotica.

2. Any and all computer software, including programs to run operating systems, applications, such as word processing, graphics, and communications programs peer to peer software, that may be or are used to: visually depict child pornography or child erotica, display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess or receive child pornography or child erotica.

3. Any and all notes, documents, records, or correspondence, in any format and medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in §847.001(4), Florida Statutes, or to the possession, receipt, or distribution of visual depictions of minors engaged in sexual conduct as defined in §847.001(16), Florida Statutes.

4. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in §847.001(4), Florida Statutes, visual depictions of minors engaged in sexual conduct as defined in §847.001(16), Florida Statutes, or child erotica.

5. Any and all diaries or address books containing names or lists of names and addresses of individuals who have been contacted by use of the computer(s) or by other means for the purpose of distributing or receiving child pornography as defined in §847.001(4), Florida Statutes, or visual depictions of minors engaged in sexual conduct as defined in §847.001(16), Florida Statutes.

6. Any and all notes, documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means (including the United States Mail or computer) any child pornography as defined in §847.001(4), Florida Statutes, or any visual depictions of minors engaged in sexual conduct, as defined in §847.001(16), Florida Statutes.

7. Any and all notes, documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in §847.001(4), Florida Statutes, or visual depictions of minors engaged in sexual conduct, as defined in §847.001(16), Florida Statutes.

8. Any and all notes, documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography, that may be or are used to: visually depict child pornography or child erotica, display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess or receive child pornography or child erotica.

9. Any and all notes, documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

10. Any and all records, documents, invoices and materials, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an internet service provider; which may have been used to possess images and/or videos of child pornography.

11. Any and all records, documents, invoices and materials, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage that may be or are used to: visually depict child pornography or child erotica, display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess or receive child pornography or child erotica.

12. Any and all cameras, film, videotapes or other photographic equipment that may be or are used to: visually depict child pornography or child erotica, display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute,

JRK

possess or receive child pornography or child erotica.

13. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means (including the United States Mail or computer) any child pornography as defined in §847.001(4), Florida Statutes, or any visual depiction of minors engaged in sexual conduct, as defined in §847.001(16), Florida Statutes.

14. Any and all documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership of the premises described above, including rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.

15. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexual conduct, as defined in §847.001(16), Florida Statutes, that may be or are used to: visually depict child pornography or child erotica, display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess or receive child pornography or child erotica.

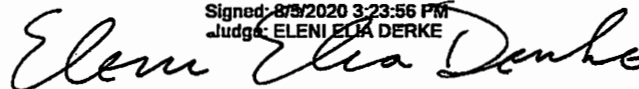
(Paragraphs 1-15 hereinafter, the "Property")

In addition to the seizure of the above mentioned Property, the Court gives permission to seize the computer hardware (and associated peripherals) and software and to conduct an off site analysis of the hardware and software for the evidence described, if, upon arriving at the scene, the law enforcement officers executing the search conclude that it would be impractical to search the computer hardware on site for this evidence. The Court is aware that the recovery of data and digital evidence by a computer forensic analyst takes significant time. For this reason, the "return" inventory will be satisfied by a list of only the tangible items recovered from the premises.

NOW THEREFORE, you, with such lawful assistance as may be necessary, to include forensic computer analyst experts, are hereby commanded, in the daytime or in the nighttime, or on Sunday, as the exigencies of the occasion may demand, to enter and search the aforesaid Premises and curtilage thereof, and any vehicles thereon, or any persons located on the Premises or within the curtilage reasonably believed to be connected with said illegal activity, for the Property described in this warrant, and if the same or any part thereof be found, you are hereby authorized to seize and secure same, giving proper receipt thereof and delivering a completed copy of this warrant to the person in control of the Premises, or in the absence of any such person, leaving a completed copy where the items are found, and making a return of your doings under this warrant within ten (10) days of the date hereof, and you or your designated forensic analyst are further authorized to search the Property for evidence of the crimes described herein, and you are directed to confirm the security of said Property so it may be brought before a Court having jurisdiction of this offense to be used in the prosecution of persons violating this offense and thereafter to be disposed of according to law. In addition, during the execution of said search warrant of the Premises, law enforcement personnel are authorized to press the finger(s) (including thumbs) of any occupant present on the Premises at the time, to a device(s) fingerprint sensor, or present any occupant's iris or face to the device(s) camera in an attempt to unlock the device(s) for the purpose of executing the search authorized by this warrant. These device(s) will include mobile phones, tablets, laptops and/or any electronic device capable of using a biometric authentication system to unlock and access the device.

WITNESS my hand and seal this 5th day of August, 2020.

Control #: 1604946  
Signed: 8/5/2020 3:23:56 PM  
Judge: ELENI ELIA DERKE



Judge of the County Court of the Fourth  
Judicial Circuit in and for Duval County, Florida

Electronically signed per section 933 of Florida Statutes



**INVENTORY AND RECEIPT (SEARCH WARRANT)**

Black Apple iPhone X with teal case  
Silver Mac Book Pro  
Daily Report card blue in color  
Floor Rug  
Lenovo Black Duval County Laptop  
Blue folder with handwritten letters  
White Tend web camera  
Samsung silver laptop with black power cord  
Pentax Blue and silver camera  
Blue Notebook  
CD Optical Disc  
Ziplock bag with school pictures

DATED this 6th day of August, 2020

/s/ ANDREA LYNETTE MEANS

Officer ANDREA LYNETTE MEANS ID# 72545

**RETURN (SEARCH WARRANT)**

STATE OF FLORIDA       )  
COUNTY OF DUVAL       )

Received this Search Warrant the 5th day of August, 2020, and executed and served the Search Warrant in Duval County, Florida, on the 6th day of August, 2020, by searching the Premises and by taking into my custody the property described in the above referenced Inventory and Receipt and by having read and delivered a copy of this Search Warrant and Inventory and Receipt to the undersigned Judge.

I, ANDREA LYNETTE MEANS ID# 72545, the officer by whom the warrant was executed, do swear that the above inventory contains a true and detailed account of all the property taken by me on said warrant.

08/06/2020

Date

/s/ ANDREA LYNETTE MEANS

ANDREA LYNETTE MEANS ID# 72545

Agency: Jacksonville Sheriff's Office

Sworn to and subscribed before me this 8th day of August, 2020, by the aforementioned Affiant  who is personally known to me  who has produced Jacksonville Sheriff's Office identification  or who has produced \_\_\_\_\_ as identification and who did take an oath.

Signature:

/s/ K C ADAMS

Judge or  Police Officer or  Notary

K C ADAMS

Print Name

Electronically administered per sections 92 and 117 of Florida Statutes

RECEIVED this Search Warrant this 8th day of August, 2020.

Control #: 1604946  
Signed: 8/8/2020 2:53:04 PM  
Judge: MEREDITH CHARBULA



Judge of the Circuit Court of the Fourth  
Judicial Circuit in and for Duval County, Florida

Electronically signed per section 933 of Florida Statutes



**AFFIDAVIT FOR SEARCH WARRANT**

STATE OF FLORIDA     )  
COUNTY OF DUVAL    )

BEFORE ME, \_\_\_\_\_, Judge of the Fourth Judicial Circuit, in and for Duval County, Florida, personally came Affiant Andrea L. Means, a Detective with the Jacksonville Sheriff's Office, and being duly sworn, deposes and says that your Affiant has probable cause to believe that certain laws have been and are being violated, and that evidence of the violation of certain laws in the form of computer equipment and data, or printed or written documents and other related items described herein, are being kept in or about certain premises and the curtilage thereof and/or vehicles upon the curtilage belonging to or used by the resident(s) of said premises, in Duval County, Florida, being known and described as follows:

524 15th Avenue South, Jacksonville Beach, Florida (Duval County)

Description of Premises: From the intersection of Beach Boulevard and 3rd Street / Highway A1A, proceed south to the intersection of 3rd Street South / Highway A1A and 15th Avenue South. Turn west (right hand turn) onto 15th Avenue South. Cross the intersections of South 4th Street and 5th Street South. The structure at 524 15th Avenue South, Jacksonville Beach, Florida (hereinafter the "Premises") is located on the south side of 15th Avenue South and is the fifth residence from the intersection of 15th Avenue South and 5th Street South. The structure is identified as a one story, single family residence. The exterior of the house appears to be made of vertical sheet which is light green (tending towards aqua or teal) in color with white trim. The front door faces to the north and is white in color. From the perspective of standing in before the front door, there is a long, elongated sidelight window located immediately to the left of the front door. There appears to be a screen door immediately in front of the front door and it has a white trim. The residence has a small front porch that is enclosed by a small, white picket fence. There are colored numbers "524" on a multicolored address plate affixed to the home located to the right of the garage. The garage door faces to the north and it is white in color. The driveway extends northward from the garage door to 15th Avenue South. A mailbox is located to the left of the driveway and it is blue in color. There are white colored numbers "524" on the mailbox door. There are white colored rocks located at the base of the mailbox post. A wooden fence, approximately six feet in height, encloses the home's backyard.

The above-described Premises are being used in violation of the following Felony laws: §847.0135(2), Florida Statutes, prohibiting possession of child pornography under the: "Computer Pornography and Child Exploitation Prevention Act", and §827.071, Florida Statutes, prohibiting the sexual performance of a child and the creation, possession or promotion of an image of such conduct. This request for a search warrant is authorized pursuant to §933.18(6), Florida Statutes.

**INTRODUCTION**

Your Affiant is a Detective with the Jacksonville Sheriffs Office. Your Affiant has been a Police Officer with the Jacksonville Sheriff's Office for seven (7) years. Your Affiant is currently a Detective assigned to Internet Crimes Against Children (ICAC) investigations and has been so assigned for one (1) year. Prior to this assignment, your Affiant was assigned as a Detective in the Special Assault Unit of the Jacksonville Sheriff's Office specializing in Sex Crimes and Child Abuse Investigations for approximately one (1) year. Your Affiant's duties include taking an active role in criminal investigations that relate to the online exploitation of children.

Your Affiant is a member of the North Florida Internet Crimes Against Children (ICAC) Task Force. ICAC is a national organization which provides specialized high-technology training and resources to law enforcement agencies that investigate crimes dealing with online sexual-solicitation and sexual-exploitation of children, including the collection and trading of images of child pornography. Your Affiant has an understanding of the Internet and has participated in investigations involving undercover chat sessions, child sexual-solicitation, and the receipt, transportation, distribution and possession of child pornography.

Your Affiant has investigated and/or assisted in investigations of crimes against children including: Child Neglect, Physical Child Abuse, Sexual Child Abuse, Online Enticement of Children, Obscenity Directed at Minors, and Travelling with the Intent to have Sex with Minors.

*JRK*

Your Affiant has investigated and assisted in the investigation of matters involving the possession, collection, production, advertisement, receipt, and/or transportation of images of child pornography.

The statements contained in this affidavit are based on your Affiant's personal knowledge, and this affidavit is being submitted for the limited purpose of securing a search warrant. Your Affiant has not included each and every fact known to him concerning this investigation and has instead set forth only the facts that he believed were necessary to establish probable cause. Your Affiant has developed probable cause to believe, and does believe, that a computer or other digital device capable of accessing the internet by means of service at the above described residence or on the Premises and/or the curtilage thereof, was knowingly used by an unknown person(s) as an instrumentality of a crime in the commission of violations of §847.0135(2) and §827.071, Florida Statutes, related to the unlawful possession or transmission of images, movies, or visual depictions of sexual conduct or sexual performance by a child or children.

#### DEFINITIONS PERTAINING TO CHILD PORNOGRAPHY

1. "Child Pornography," as used herein, includes the definition in §847.001(3), Florida Statutes, which means "any image depicting a minor engaged in sexual conduct."
2. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.
3. "Sexual conduct," as used herein, includes the definition in §847.001(16), Florida Statutes, which "means actual or simulated sexual intercourse, deviate sexual intercourse, sexual bestiality, masturbation, or sadomasochistic abuse; actual lewd exhibition of the genitals; actual physical contact with a person's clothed or unclothed genitals, pubic area, buttocks, or, if such person is a female, breast with the intent to arouse or gratify the sexual desire of either party; or any act or conduct which constitutes sexual battery or simulates that sexual battery is being or will be committed. A mother's breastfeeding of her baby does not under any circumstance constitute "sexual conduct."
4. "Sexual performance," as used herein, means any performance or part thereof which includes sexual conduct by a child of less than 18 years of age (pursuant to §827.071(1)(i), Florida Statutes).
5. "Sexually Oriented Material," as used herein, includes the definition in §847.001(18), Florida Statutes, which "means any book, article, magazine, publication, or written matter of any kind or any drawing, etching, painting, photograph, motion picture film, or sound recording that depicts sexual activity, actual or simulated, involving human beings or human beings and animals, that exhibits uncovered human genitals or the pubic region in a lewd or lascivious manner, or that exhibits human male genitals in a discernibly turgid state, even if completely and opaquely covered."

#### DEFINITIONS PERTAINING TO TECHNICAL TERMS

As part of your Affiant's training, your Affiant has become familiar with the Internet (also commonly known as the World Wide Web), which is a global network of computers and other electronic devices that communicate with each other using various means, including standard telephone lines, high-speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions including satellite. Due to the structure of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via electronic mail ("e-mail"). An individual who wants to use Internet e-mail must first obtain an account with a computer that is linked to the Internet through a university, an employer, or a commercial service such as an "Electronic Service Provider" or "ESP" (see definition of "Electronic Service Provider" below). Once the individual has accessed the Internet, that individual can use Internet mail services, including sending and receiving e-mail. In addition, the individual can visit web sites and make purchases.

1. "Computer," as used herein, includes the definition in §847.001(4), Florida Statutes, which "means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. The term also includes: any online service, Internet service, or local bulletin board; any electronic storage device, including a floppy disk or other magnetic

JRK

storage device; or any compact disc that has read-only memory and the capacity to store audio, video, or written materials."

2. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

3. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

4. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), personal digital assistants (PDAs), multimedia cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

5. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Digitally coded data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "boobytrap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

6. "Electronic Service Providers (ESPs)" as used herein, ESPs, formerly known as ISPs (Internet Service Providers), are commercial organizations that are in business to provide individuals and businesses access to the Internet. ESPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ESPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ESPs typically charge a fee based upon the type of connection and volume of data, called band-width, which the connection supports. Many ESPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a cable modem (telephone line or through a cable system) or wireless connection, the subscriber can establish communication with an ESP and can access the Internet by using his or her account name and personal password. ESPs maintain records pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ESPs servers, and other information, which may be stored both in computer data format and in written or printed record format. ESPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ESPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files. Typically, e-mail that has not been opened by an ESP customer is stored temporarily by an ESP incident to the transmission of that e-mail to the intended recipient, usually within an area known as the home directory. Such temporary, incidental storage is defined by statute as "electronic storage" (18 U.S.C. §2510 (17)). A service provider that is available to the public and provides storage facilities after an electronic communication has been transmitted and opened by the recipient, or provides other long-term storage services to the public for electronic data and files, is defined by statute as providing a "remote computing service" (18 U.S.C. §2711(2)).

7. "Internet Protocol Address (IP Address)", as used herein, every computer or device on the Internet is

JRK

referenced by a unique Internet Protocol (IP) address the same way every telephone has a unique telephone number. An IPv4 address is a series of four numbers separated by a period, and each number is a whole number between 0 and 254. An example of an IPv4 address is 192.168.10.102. IPv6 was created to deal with the exhaustion of the IPv4. IPv6 is the most recent version of the Internet Protocol (IP). An example of an Ipv6 is 3ffe:1900:4545:3:200:f8ff:fe21:67cf, but methods to abbreviate this full notation exist. Each time an individual has accessed the Internet, the computer from which that individual initiated access is assigned an IP address. A central authority provides each ESP a limited block of IP addresses for use by that ESP's customers or subscribers. Most ESPs employ dynamic IP addressing, that is they allocate any unused IP addresses at the time of initiation of an Internet session each time a customer or subscriber has accessed the Internet. A dynamic IP address is reserved by an ESP to be shared among a group of computers over a period of time. The ESP logs the date, time, and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records. Another method of IP addressing is known as a Static IP address. A Static IP address is an IP address that does not change over a period of time.

8. "Log File", as used herein, log files are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example; web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

9. "Metadata", as used herein, data contained in a file that is not usually associated with the content of a file but is often associated with the properties of the application or device that created that file. For example, a digital camera photograph often has hidden data that contains information identifying the camera that manufactured it and the date the image was taken.

10. "Uploading", as used herein, uploading is transmission in the other direction: from one computer to another computer. From an Internet user's point-of-view, uploading is sending a file to a computer that is set up to receive it.

11. "Downloading", as used herein, downloading is the transmission of a file from one computer system to another. From the Internet user's point-of-view, to download a file is to request it from another computer (or from a Web page on another computer) and to receive it.

12. "Domain Name", as used herein, domain names are common, easy to remember names associated with an Internet Protocol address (defined below). For example, a domain name of "www.usdoj.gov" refers to the Internet Protocol address of 149.101.1.32.

13. "Compressed File", as used herein, a file that has been reduced in size through a compression algorithm to save disk space. The act of compressing a file will make it unreadable to most programs until the file is uncompressed.

14. "Hash Value", as used herein, a mathematical algorithm generated against data to produce a numeric value that is representative of that data. A hash value may be run on media to find the precise data from which the value was generated. Hash values cannot be used to find other data.

15. "Image or Copy", as used herein, an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. "Imaging" or "copying" maintains contents, but attributes may change during the reproduction.

16. "Biometric Authentication Device", as used herein, an electronic device that uses automated methods of verifying or recognizing the identity of a living person based on physiological or behavioral characteristics. These characteristics can include fingerprints, facial images, iris and voice recognition. Biometric Authentication on electronic devices is a security feature to lock/unlock capable devices so that they cannot be accessed without the characteristics already saved on the device by the user of that specific device.

## COMPUTERS AND CHILD PORNOGRAPHY

Based upon your Affiant's training and experience, as well as consultation with other experienced law enforcement officers and computer forensic examiners, your Affiant knows that computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. In the past, child pornography was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images, and to distribute these images on any scale required significant resources and significant risks. The

JRK



photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public and/or law enforcement. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls.

The development of computers has radically changed the way that child pornographers obtain, distribute, and store their contraband. Computers basically serve five functions in connection with child pornography: access, production, communication, distribution, and storage. Child pornographers can now convert paper photographs taken with a traditional camera (using ordinary film) into a computer readable format with a device known as a scanner. Moreover, with the advent and widespread use of digital cameras, the images can now be transferred directly from a digital camera onto a computer using a connection known as a USB cable or other device. Digital cameras have the capacity to store images and videos indefinitely, and memory storage cards used in these cameras are capable of holding thousands of images and videos. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media, that is, the hard disk drive used in home computers has grown tremendously within the last several years. These hard disk drives can store hundreds of thousands of images at very high resolution.

The World Wide Web of the Internet affords collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography frequently use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Hotmail, and Google, among others. The online services allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

As is the case with most digital technology, communication by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an email as a file on the computer or saving particular website locations in, for example, "bookmarked" files. Digital information, images and videos can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). Often, a computer will automatically save transcripts or logs of electronic communications between its user and other users that have occurred over the Internet. These logs are commonly referred to as "chat logs."

Some programs allow computer users to trade images while simultaneously engaging in electronic communications with each other. This is often referred to as "chatting," or "instant messaging." Based upon your Affiant's training and experience, as well as conversations with other law enforcement officers and computer forensic examiners, your Affiant knows that these electronic "chat logs" often have great evidentiary value in child pornography investigations, as they record communication in transcript form, show the date and time of such communication, and also may show the dates and times when images of child pornography were traded over the Internet. In addition to electronic communication, a computer user's internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained on a computer for long periods of time until overwritten by other data.

#### SEARCH AND SEIZURE OF COMPUTER SYSTEMS

Based upon your Affiant's training and experience, as well as conversations with other experienced law enforcement officers, your Affiant knows that searches and seizures of evidence from computers commonly require Forensic Examiners to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related

JRK

documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

1. Computer storage devices (e.g., hard drives, compact discs ("CDs"), diskettes, tapes, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site.
2. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. The search of a computer system, which includes the use of data search protocols, is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover hidden, erased, compressed, password protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

#### CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

Based on your Affiant's experience, training, and consultation with other experienced law enforcement officers who investigate cases involving the sexual exploitation of children, your Affiant knows that certain common characteristics are often present in individuals who collect child pornography. Your Affiant has observed and/or learned about the reliability of these commonalities and conclusions involving individuals, who collect, produce and trade images of child pornography. Based upon your Affiant's training and experience, and conversations with other experienced law enforcement officers in the area of investigating cases involving sexual exploitation of children, your Affiant knows that the following traits and characteristics are often present in individuals who collect child pornography:

1. Many individuals who traffic in and trade images of child pornography also collect child pornography. Many individuals who collect child pornography have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by sexually explicit depictions of children.
2. Many individuals who collect child pornography collect sexually oriented materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. Many of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography, but which nonetheless fuel their deviant sexual fantasies involving children. Such individuals often do not destroy these materials.
3. Many individuals who collect child pornography often seek out like minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance, and support. This contact also helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet based vehicles used by such individuals to communicate with each other include, but are not limited to, Peer-to-Peer (P2P), email, email groups, bulletin boards, Internet Relay Chat Rooms (IRC), newsgroups, instant messaging, and other similar vehicles.
4. Many individuals who collect child pornography often collect, read, copy or maintain names, addresses (including email addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.
5. Many individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect them from discovery, theft, or damage. These individuals view their sexually explicit materials as prized and valuable materials, even as commodities to be traded with other likeminded individuals over the Internet. As such, they tend to maintain or "hoard" their visual depictions of child pornography for long periods of time in the privacy and security of their homes or other secure locations. Based on your Affiant's training and experience, as well as your Affiant's conversations with other experienced law enforcement officers, your Affiant knows that individuals who possess, receive, and/or distribute child pornography by computer using the Internet often continue to maintain and/or possess

JRK

the items.

The known desire of such individuals to retain child pornography, coupled with the sense of security afforded by using computers, provides probable cause to believe that computer images, especially child pornography and child erotic nudity involving minors, will be retained by the collector indefinitely. These individuals may protect their illicit materials by passwords, encryption, and other security measures, save it on movable media such as CDs, DVDs, flash memory, thumb drives, and removable hard drives, which can be very small in size, including as small as a postage stamp, and easily secreted, or send it to third party image storage sites via the Internet.

#### BACKGROUND OF INVESTIGATION AND FACTS ESTABLISHING PROBABLE CAUSE

On July 2, 2020, your Affiant was assigned a Cyber Tip Report from the National Center for Missing and Exploited Children (Report #68235908). The National Center for Missing and Exploited Children (NCMEC) Cyber Tip Line is an online reporting mechanism for cases of child sexual exploitation including child pornography, online enticement of children for sex acts, molestation of children outside the family, sex tourism of children, child victims of prostitution, and unsolicited obscene material sent to a child. NCMEC staff reviews reports, sometimes doing basic analysis work, and then distributes the Cyber Tip Report to the appropriate investigatory agencies for review. This Cyber Tip Report came from MediaLab/Kik (hereinafter "Kik"). Kik is a free instant messaging and social networking app that uses a smartphone's data plan or Wi-Fi connection to send messages to other Kik users, bypassing SMS (short message service).

The Cyber Tip provided the following information:

##### Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)

Incident Time: 04-07-2020 15:52:47 UTC

Description of Incident Time: Timestamp when user was reported to Kik

##### Chat/Instant Messaging

Chat Service/IM Client: Kik Messenger

Chat Logs: Video/Image file(s) uploaded/shared with another user or group of users.

##### Suspect

Email Address: llestknickas@gmail.com

Email Address: tommyhazouri@gmail.com

Screen/User Name: mybfsgaynotme

ESP User ID: mybfsgaynotme\_y6h

IP Address: 23.113.246.250 (Login)

04-06-2020 10:51:06 UTC

The Cyber Tip Report disclosed that the person being reported uploaded five (5) files on March 26, 2020, between the times of 19:47:15 UTC and 20:57:36 UTC.

Your Affiant personally viewed the images in the Cyber Tip Report, and based on the images observed, four (4) of the images meet the definition of child pornography, pursuant to §847.001(3), Florida Statutes. The following is a description of two (2) of the images viewed by your Affiant:

##### IMAGE 1

FILE NAME: 98c97450-82f5-4f36-af74-f5f3c56a86f4.mp4

MD5: d33a4f17741b4425e33c3b324b65074e

DESCRIPTION: This image is a video depicting an unknown white pubescent female child. Breast bud is observed on the child; however, no hair is observed around her pubic area. The child is standing in a bedroom, facing the camera, and is initially wearing clothing. The child removes her clothing and immediately turns around to expose her buttocks. She then takes her finger and moves it in and out of her

*gmk*

anal opening. She eventually turns around and begins to move her hand back and forth over her vagina. Next, she takes the camera and positions it to where it focuses on her vagina. She then digitally penetrates her vagina until the video abruptly stops. The video is 1 minute 59 seconds in length.

#### IMAGE 2

FILE NAME: 8503eb97-b944-44af-a8b7-5d6566a42d14.mp4

MD5: d8cf93042b9457fddd7e5f2954a3227d

DESCRIPTION: This image is a video depicting an unknown white prepubescent male child and an adult white female. Only the top portion of the adult is visible and she is wearing a shirt and kneeling in front of the child. Only the bottom half of the child's face is visible during the video. The child is completely nude and is facing towards the adult. The adult brings her finger to her lips, while smiling, motioning for the child to be quiet. She then alternates between providing oral stimulation to the child's penis and stroking his penis with her fingers. The adult looks directly at the camera during the video, and at one point, she licks the length of his penis. In the background, another child can be heard saying, "Mama." She eventually responds, speaking in an unknown language. The child bends forward slightly and covers his mouth with one of his hands. The adult nudges him back up, points her finger at him, and says something in an unknown language as she continues sexually battering the child. This video image is 1 minute 59 seconds in length.

A search of the IP address revealed that it is registered to AT&T Internet Services (hereinafter "AT&T") located in Jacksonville, Florida.

On May 7, 2020, Detective A. M. Corbett #63873 caused a preservation request to be served to Kik requesting that the Kik account associated with email addresses llestknickas@gmail.com and tommyhazouri@gmail.com be preserved for 90 calendar days.

On May 8, 2020, Detective A. M. Corbett #63873 caused a Fourth Judicial Circuit Subpoena Duces Tecum to be served to AT&T requesting all available account subscriber information for IP address 23.113.246.250 which the Cyber Tip, containing the child pornography, was accessed. Detective Corbett received a response from AT&T disclosing the following information for the above referenced IP address:

#### Subscriber Information

Contact Name: Tommy Hazouri

CBR: 904-██████████

ALT CBR: 904-██████████

Preferred Email: tommyhazouri@gmail.com

Service/Billing Address: 524 15th Avenue South,  
Jacksonville Beach, FL 32250

Account Status: Active

Established: 01/14/2019

It should be noted that the preferred email address "tommyhazouri@gmail.com" provided by AT&T matches one of the email addresses provided in the Cyber Tip Report.

On July 7, 2020, your Affiant presented Electronic Service Provider (ESP) search warrants for Google and Kik which were subsequently signed by the Honorable Judge Kevin Blazs. Both search warrants were submitted to Google and Kik on the same date.

On July 8, 2020, your Affiant received a response from Google. The Google response and the NCMEC Cyber Tip Report (68235908) were provided to Forensic Examiner Detective S. A. Torres #7833 to be reviewed on July 14, 2020. On July 30, 2020, your Affiant received a response from Kik. The Kik response was provided to Forensic Examiner Detective S. A. Torres #7833 to be reviewed on July 31, 2020.

Key definitions in Detective Torres' reports include the following:

1. Child Sexual Abuse (CSA): visual depictions of a least one minor engaged in sexually explicit conduct (actual or simulated sexual intercourse, bestiality, masturbation, sadistic or masochistic abuse, or the lascivious exhibition of genitalia or pubic area of any persons.
2. Child Sexual Exploitation (CSE): The use of a child or material related to a child for sexual gratification.

JAK

3. BDSM: Bondage and Discipline, Dominance and Submission, Sadochism and Masochism.
4. Category 1: Pictures and/or videos depicting Child Sexual Abuse (CSA) material.
5. Category 2: Pictures and/or videos depicting either child erotica or age-difficult pornography.
6. Category 3: Computer-generated imagery (CGI) or animation of a child-exploitive nature.

On July 16, 2020, Detective Torres advised that her examination of the Google response was completed. Detective Torres advised the following:

"There were 70 Category 2 files in the Google account for tommyhazouri@gmail.com. I did not find any CSE files in the Google account for Illestknickas@gmail.com. The CSE files reported in the NCMEC CTs were not present in the data provided by Google. However, I located emails concerning the use of the Kik screen/user name of mybfgaynotme by both reported Google accounts. The Google account for tommyhazouri@gmail.com contained personal files associated with Thomas Lester Hazouri (date of birth: April 26, 2980). I did not find any user-attributable data in the Google account of Illestknickas@gmail.com, other than the email concerning the use of the reported Kik screen/user that was also connected to tommyhazouri@gmail.com."

In reference to the email addresses found during Detective Torres' examination of the Google response, it should be noted that Kik sent emails to both email addresses with the following subject: "Welcome to Kik! Confirm your details inside..." The email address tommyhazouri@gmail.com received the welcome email on February 25, 2020, and the email address Illestknickas@gmail.com received the welcome email address on April 5, 2020 (after the March 26 uploads in the original Cyber Tip). Both emails advised that the username associated with the email address was "mybfgaynotme." Both email addresses and the username were provided in the NCMEC Cyber Tip Report.

Regarding the Google attribution, Detective Torres advised the following:

"The Google account for tommyhazouri@gmail.com contained the following:

1. pictures and videos of Thomas Hazouri, many of which appeared to be self-taken;
2. the resume for Thomas L. Hazouri in multiple formats sent as attachments in multiple emails from tommyhazouri@gmail.com;
3. a picture of a Florida Driver License issued to Thomas Lester Hazouri;
4. a picture of a court document listing Thomas Lester Hazouri as the Defendant; and
5. pictures of correspondence sent to Thomas Hazouri;

Additionally, there were non-exploitive pictures of children, many of whom were captured in an educational setting. Some of these pictures contained latitude and longitude coordinates that resolved to Mayport Elementary, where Thomas Hazouri was employed as a teacher at the time of my investigation."

Detective Torres also advised that there was a picture of a letter in the Google account that appeared to be written by a child that was questionable in nature. The letter was addressed to "Tommy" and was from "T" and "N," appearing to be the names of two (2) female children. In the letter, the author asks "Tommy" if he likes "coconuts." The author writes, "Well I will show you how I can draw a coconut's (sic). And if you don't like my coconut's cicel (sic) no. If you like my coconut cicel (sic) yes."

On August 3, 2020, Detective Torres advised that her examination was completed regarding the Kik response. Detective Torres advised the following:

"Over 60 CSA files were identified in the data from the Kik account. I found two pictures depicting a female child . . . These two pictures appeared to have been taken in a classroom at Mayport Elementary, where Thomas Hazouri was employed at the time of my investigation."

"I found a video that partially exposed the head of the person capturing the video. The male was bald and similar in appearance to Thomas Hazouri. Other than this video of a partially exposed head and the picture of the girl that was connected to Mayport Elementary, I did not find any definitive evidence linking the Kik account to Hazouri. There were files that may contain leads to the identity of the Kik user. I provided them to Det. Means for her review."

JHK

Regarding the Kik attribution, Detective Torres further advised the following:

"There were two pictures depicting a female child lying prone on a rug in the Kik account that matched the rug in a picture of a classroom found in Thomas Hazouri's Google account. The related picture from the Google account had latitude and longitude coordinates that resolved to Mayport Elementary, where Thomas Hazouri was employed as a teacher at the time of my investigation."

The Kik account contained 64 - Category 1 images, 494 - Category 2 images, and 4 - Category 3 images. The CSE files reported in the NCMEC Cyber Tip Report were not found in the data provided by Kik. Unless a preservation request is submitted to Kik to preserve all account data, including pictures and videos, Kik will only retain media data on its servers for 30 days. The NCMEC Cyber Tip Report advised that the files in the tip were uploaded on to the Kik account on March 26, 2020. According to the Cyber Tip Report, the timestamp when the user was reported to Kik was April 7, 2020. The Jacksonville Sheriff's Office ICAC Unit was assigned the Cyber Tip Report on May 1, 2020 and the preservation request was submitted on May 7, 2020. Because Kik only retains its media content for 30 days unless a preservation request is submitted to preserve the account data, the files found in the Cyber Tip Report would not have been included in the Kik production. A preservation request would have needed to be submitted by April 25, 2020, for the original Cyber Tip report files to be included in the Kik production.

The following summaries provide a description regarding the content of at least 11 of the child pornography files Detective Torres found during her forensic examination of the Kik return:

ITEM 1

FILE NAME: 21c67ddd-f419-4fd3-bfc1-b73a50298601

HASH VALUE: 531CAE64AFF148F62EC5FF256F19B9B0

DESCRIPTION: This image is a video depicting a pubescent female and a prepubescent male child of unknown ethnicities. Initially, both are standing. The male child appears to insert his penis between the female's buttocks. The female then turns around, gets onto her knees, places the child's penis in her mouth, and begins to move her head back and forth before stopping abruptly. The video is 43 seconds in length.

ITEM 2

FILE NAME: e3f779d5-08bb-4b11-a052-8b4ccab3c382

HASH VALUE: 4F8BF424661DDD32967D8C9237A3C9E3

DESCRIPTION: This image is video depicting a white, pubescent male child and adult white female. Initially, the adult is kneeling in front of the child as she uses her fingers to fondle the child's exposed penis. Next, the adult stops, lifts her shirt, and the child leans forward, grabs both of her exposed breasts with his hands and squeezes them. After the child stops, he stands up straight as the adult leans forward, inserts his exposed penis into her mouth and begins to move her head back and forth. The video ends with the female using her fingers to fondle the child's penis, again. The video is 1 minute 10 seconds in length.

ITEM 3

FILE NAME: 91641b8b-0647-491d-8d41-d689f26cfb71

HASH VALUE: D6880501EA56C0570F6D8BBD08C26BA5

DESCRIPTION: This image is a picture depicting a white, prepubescent female child and an adult white male. The adult's exposed penis, thighs, and pubic area are the only parts of his body that are visible. The child is leaning forward towards the male and looking at the camera as she grins. The adult's exposed penis is erect and pressed against the side of the child's mouth and nose. A white substance appears to be dripping from the child's mouth and flows along the shaft of the adult's penis. A white substance is also observed at the tip of the adult's penis.

ITEM 4

FILE NAME: 7bce674d-dc24-4b90-b8c0-99ee9d813b11

HASH VALUE: 39F42E2868F42755ED54B669D3022F8B

DESCRIPTION: This image is a picture depicting a white, prepubescent female child. The child is completely nude. She has her legs spread apart, with one of her legs hoisted up in the air, exposing her vaginal opening, outer labia, clitoris, and anal opening.

*JMK*

## ITEM 5

FILE NAME: 93d8b070-1e11-4341-9fb3-c350b4fa9c0c

HASH VALUE: DC684343F294C3E08131891C30C4A492

DESCRIPTION: This image is a picture depicting a white, prepubescent male child and a white adult female. The child is completely nude as the adult is leaning forward with the child's penis inserted into her mouth.

## ITEM 6

FILE NAME: b431d78f-2af4-4c78-b91e-257093727e37

HASH VALUE: E976C2DBB3724774B1660352EBB1CEBD

DESCRIPTION: This image is a picture depicting a white, prepubescent female child. The child is bent over and looking backwards at the camera as she uses her hands to spread her buttocks apart to expose her vaginal and anal openings.

## ITEM 7

FILE NAME: 9f189bf8-0e3d-4618-9e7f-967ceff350bc

HASH VALUE: 1A973168771BA0DA35688A310BD5DE4B

DESCRIPTION: This image is a picture depicting a white, prepubescent female child. The child is completely naked. One of her hands is covering her breasts as the other hand is placed over her vaginal area. One of her fingers is bent giving the appearance of it being inserted into her vagina.

## ITEM 8

FILE NAME: c91fd9fd-522d-41ce-afdc-57a9e006400b

HASH VALUE: 63C1D4D238BF7EB5DEC7B7820356D029

DESCRIPTION: This image is a picture depicting a very young, white, prepubescent female child. The child is completely naked and lying on a beach. She is leaning backwards and is propped up on her elbows. Her legs are spread apart exposing her buttocks and vagina.

## ITEM 9

FILE NAME: cc0f1f7b-af0e-4fa2-a2f9-98af8a347fbf

HASH VALUE: 47AB521E597D68FEFBAAC1BBA67374D1

DESCRIPTION: This image is a picture depicting a very young, white, prepubescent female child. The child is completely naked and lying on her back as she stares at the camera. Her legs are spread apart exposing her anal opening, vaginal opening, outer labia, inner labia, and clitoris.

## ITEM 10

FILE NAME: 3fae7e71-32ca-446d-b84b-a7353b8020f6

HASH VALUE: 2E847CD6CD7D1AB726626E27DD4CABE4

DESCRIPTION: This image is a picture depicting a very young, white, prepubescent female child, an adult white male, and an adult white female. The child is positioned between the adult male and the adult female. The adult male is standing, and his face is not visible. The adult female is leaning forward and kissing the child on the mouth. A white substance is smeared over the child's face and her neck. As the adult female kisses the child, she is reaching around the child's head and grasping the male's exposed penis. A white substance is also visible on the adult female's hand.

## ITEM 11

FILE NAME: 59a9bb21-2525-44e6-b26d-fdad1772e42e

HASH VALUE: 879F01B8BA3327A346066EB10DB5A3E4

DESCRIPTION: This image is a video depicting a white, prepubescent female. During the video, the child removes pieces of her clothing to expose her bare breasts, buttocks, and vagina. She is observed grasping her buttocks and spreading them apart to show her vaginal opening. The child repositions the camera to capture a close-up view of her using her fingers to fondle her vagina. The video is 1 minute 1 second in length.

In the file descriptions contained in this affidavit, your Affiant frequently uses the terms "prepubescent" and "pubescent". Your Affiant has had no formal medical training in the use of those terms but in applying the terms, your Affiant relies on experience as an investigator in child pornography investigations and common experience. Your Affiant uses the term "pubescent" to mean a child who has begun to develop and display mature body shape and genital organs and/or secondary sexual characteristics such as, but not

JRK

limited to, the development of breasts in females and the appearance of pubic hair and underarm hair, typically seen in children between 11-16 years of age. The term "pubescent" indicates that the person depicted is a child but evidences some physical and sexual maturation consistent generally with a young teenager or teenager. Your Affiant uses the term "prepubescent" to describe a child who does not exhibit any, or only very limited, physical-sexual development such as those indicators mentioned above, such that the child appears to be well under the age of 18 years and likely under the age of 13 years in the case of both males or females. The terms "infant" and "toddler" or "very young child" should be given their common meanings and are used to communicate that the child depicted is clearly prepubescent and does not appear to be even nearing pubescence.

The IP address provided in the Cyber Tip Report was determined to belong to the AT&T Internet Service Provider and lists "Tommy Hazour" as the account subscriber. Additionally, the AT&T account provides 524 15th Avenue South as the residential address and it also lists tommyhazouri@gmail.com as the email address associated to the account. The email address tommyhazouri@gmail.com was also provided in the Cyber Tip Report as being linked to the Kik account.

An investigative search has revealed that Thomas Lester Hazouri, Jr. has a white Toyota pick-up registered to him bearing Florida Tag [REDACTED]. On multiple dates, this vehicle has been observed parked in the driveway of 524 15th Avenue South. A search of the City of Jacksonville's property records reveals that "Thomas L. Hazouri, Jr." is the owner of the residence located at 524 15th Avenue South.

In addition to the CSA files found in the Kik production, the two pictures referred to in Det. Torres' report appeared to depict the same young girl. Although she is wearing different clothing in each picture, both pictures depict her lying down on her stomach on a colorful rug that appears to be in a classroom. The girl is facing away from the camera, leaning on her elbows, with her legs slightly apart. The pictures only show a small portion of other children; thus, this specific girl appears to be the primary subject of the two Kik photos, specifically focusing on her entire backside and the crevice between her legs.

In the first photograph, the child is wearing black and the rug appears to have a cartoon rabbit, a green outer border, a light blue inner border with the letters "nflie" visible near what appear to be cartoon dragonflies and butterflies, and a darker blue pattern in the middle of the rug. In the second image, the child is wearing white shorts and the rug appears to have a cartoon goldfish surrounded by a similar darker blue as in the first image. Although the child's feet partially obscure her clothed buttocks in this photo, the photo is taken at such an angle that the viewer can see up the child's shorts.

It should be noted that the rug depicted in the two Kik production pictures appears similar to a third picture, including a rug, taken in a classroom from one of the photographs included in the Google production of tommyhazouri@gmail.com. This third image includes a classroom full of children sitting on a rug and is taken of their faces. This image shows what appears to be the same cartoon rabbit at the front of the rug that the female child wearing black is laying on from the first image and further depicts various cartoon animals across the rug. There appears to be a portion of the cartoon goldfish towards the back of the rug that a male student is obscuring. Additionally, the rug has a green outer border, a light blue inner border with the letters "rtles" visible near a cartoon turtle, and a darker blue pattern in the middle of the rug. It should be noted that the font, letter size, and coloring of "nflie" and "rtles" appears similar. The Google photograph from tommyhazouri@gmail.com contained latitude and longitude coordinates that also resolved to Mayport Elementary. An investigative search reveals that Thomas Lester Hazouri, Jr. is employed as a Second Grade Teacher at Mayport Elementary School.

The Kik return also had a short video that briefly displayed the partial, upper face of a male that appeared to be Thomas Lester Hazouri, Jr. based on pictures of Thomas Lester Hazouri, Jr., including his driver license photograph where he is identified as "Thomas Lester Hazouri."

## CONCLUSION

The above information leads your Affiant to believe that a computer or other digital media capable of securing Internet access at the above described Premises, residence, curtilage or related vehicles thereon, was knowingly used by a known person/s as an instrumentality of a crime or as a means by which a Felony was committed, (§933.18(6), Florida Statutes). The following Felony laws were violated through the use of

JRK



said computer: §847.0135(2), Florida Statutes, prohibiting possession of child pornography under the: "Computer Pornography and Child Exploitation Prevention Act," and §827.071, Florida Statutes, prohibiting the sexual performance of a child and the creation, possession or promotion of an image of such conduct.

Your Affiant hereby requests the Courts permission to seize the following items, and to conduct a search and analysis, or to delegate the search and analysis to a computer forensic analyst, on-scene or off-site at another secure location, of the following items (hereinafter the "Property"):

1. Any and all computer(s), computer hardware, computer software, electronic storage media (including any and all disk drives, compact disks, flash drives, cellular telephones, personal digital assistants (PDA), digital cameras and/or memory cards, or any other device capable of electronic storage of data and/or images), computer-related documentation, computer passwords and data-security devices, videotapes, video recording devices, video recording players, and video display monitors that are or may be used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography or child erotica.
2. Any and all computer software, including programs to run operating systems, applications, such as word processing, graphics, and communications programs peer to peer software, that may be or are used to: visually depict child pornography or child erotica, display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess or receive child pornography or child erotica.
3. Any and all notes, documents, records, or correspondence, in any format and medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in §847.001(4), Florida Statutes, or to the possession, receipt, or distribution of visual depictions of minors engaged in sexual conduct as defined in §847.001(16), Florida Statutes.
4. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in §847.001(4), Florida Statutes, visual depictions of minors engaged in sexual conduct as defined in §847.001(16), Florida Statutes, or child erotica.
5. Any and all diaries or address books containing names or lists of names and addresses of individuals who have been contacted by use of the computer(s) or by other means for the purpose of distributing or receiving child pornography as defined in §847.001(4), Florida Statutes, or visual depictions of minors engaged in sexual conduct as defined in §847.001(16), Florida Statutes.
6. Any and all notes, documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means (including the United States Mail or computer) any child pornography as defined in §847.001(4), Florida Statutes, or any visual depictions of minors engaged in sexual conduct, as defined in §847.001(16), Florida Statutes.
7. Any and all notes, documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in §847.001(4), Florida Statutes, or visual depictions of minors engaged in sexual conduct, as defined in §847.001(16), Florida Statutes.
8. Any and all notes, documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography, that may be or are used to: visually depict child pornography or child erotica, display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess or receive child pornography or child erotica.
9. Any and all notes, documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.
10. Any and all records, documents, invoices and materials, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an internet service provider; which may have been used to possess images and/or videos of child pornography.

JKK

11. Any and all records, documents, invoices and materials, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage that may be or are used to: visually depict child pornography or child erotica, display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess or receive child pornography or child erotica.

12. Any and all cameras, film, videotapes or other photographic equipment that may be or are used to: visually depict child pornography or child erotica, display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess or receive child pornography or child erotica.

13. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means (including the United States Mail or computer) any child pornography as defined in §847.001(4), Florida Statutes, or any visual depiction of minors engaged in sexual conduct, as defined in §847.001(16), Florida Statutes.

14. Any and all documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership of the premises described above, including rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.

15. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexual conduct, as defined in §847.001(16), Florida Statutes, that may be or are used to: visually depict child pornography or child erotica, display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess or receive child pornography or child erotica.

(Paragraphs 1-15 hereinafter referred to as the "Property")

Your Affiant believes that the above items are being kept at 524 15th Avenue South, Jacksonville Beach, Florida and are being used in violation of the laws of the State of Florida, and constitute evidence of, or evidence relevant to proving, a violation of the laws of the State of Florida, to wit: §847.0135(2), Florida Statutes, prohibiting possession of child pornography under the: "Computer Pornography and Child Exploitation Prevention Act", and §827.071, Florida Statutes, prohibiting the sexual performance of a child and the creation, possession or promotion of an image of such conduct.

Your Affiant is aware that the recovery of data by a computer forensic analyst takes significant time, and much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

WHEREFORE, your Affiant makes this affidavit and requests the issuance of a Search Warrant in due form of law commanding the Sheriff of the Jacksonville Sheriff's Office, or any of his duly constituted officers, with any proper and necessary assistance, including the assistance of a trained computer forensic analyst, to search the above described Premises and the curtilage thereof and/or the vehicle(s) on the curtilage thereof, or persons located within the Premises and the curtilage reasonably believed to be connected with said illegal activity, for the said Property heretofore described, and to search and analyze said Property described above or delegate, either on premises or off-site, such analysis and to seize and safely keep same, either in the daytime or in the nighttime, or on Sunday, as the exigencies of the occasion may demand, in order that the evidence may be procured to be used in the prosecution of such person or persons who have unlawfully used, possessed, or are using or possessing the same in violation of the laws of the State of Florida. Your Affiant also requests that this Court authorize law enforcement officers to press the finger(s) (including thumbs) of any occupant present on the Premises at the time of the service of said search warrant, to a device(s) fingerprint sensor, or present any occupant's iris or face to the device(s) camera during the search

JRK

of the Premises in an attempt to unlock the device(s) for the purpose of executing the search authorized by this warrant. These device(s) may include mobile phones, tablets, laptops and/or any electronic device capable of using a biometric authentication system to unlock and access the device.

08/05/2020

/s/ ANDREA LYNETTE MEANS

Date

Affiant: ANDREA LYNETTE MEANS ID# 72545

Agency: Jacksonville Sheriff's Office

Sworn to and subscribed before me this 5th day of August, 2020, by the aforementioned Affiant [X] who is personally known to me [ ] who has produced Jacksonville Sheriff's Office identification [ ] or who has produced \_\_\_\_\_ as identification and who did take an oath.

Signature:

/s/ K C ADAMS

[ ] Judge or [X] Police Officer or [ ] Notary

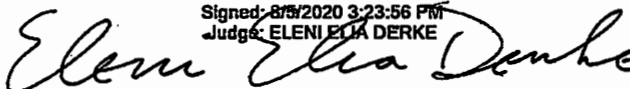
K C ADAMS

Print Name

Electronically administered per sections 92 and 117 of Florida Statutes

THE FOREGOING APPLICATION AND AFFIDAVIT for a Search Warrant having been presented the Application and Affidavit, made under oath and after considering the facts alleged, and being satisfied there is probable cause to believe the grounds set forth in the Application and Affidavit do exist and that the Laws of the State of Florida are being violated as alleged, I find that a Search Warrant is authorized and thus, is issued.

Control #: 1604946  
Signed: 8/5/2020 3:23:56 PM  
Judge: ELENI ELIA DERKE



Judge of the County Court of the Fourth  
Judicial Circuit in and for Duval County, Florida

Electronically signed per section 933 of Florida Statutes

gmk