UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
JACKSONVILLE DIVISION

UNITED STATES OF AMERICA

vs.

SAMUEL ARTHUR THOMPSON

CRIMINAL COMPLAINT

Case No. 3:19-mj- 1364-JBT

I, the undersigned complainant, being duly sworn, state the following is true and correct to the best of my knowledge and belief. On or about January 26, 2018, in the Middle District of Florida, the defendant,

> did knowingly receive child pornography, that is, a visual depiction of a minor engaging in sexually explicit conduct, using a means and facility of interstate and foreign commerce, that is, by computer via the internet, and the defendant had a prior conviction for Second Degree Sodomy, Victim Younger than 16 and Older than 12, on or about April 22, 1998, in violation of Alabama Criminal Code § 12A-6-64,

all in violation of Title 18, United States Code, Section 2252(a)(2) and (b)(1). I further state that I am a Special Agent of the Federal Bureau of Investigation, and that this Complaint is based on the following facts:

SEE ATTACHED AFFIDAVIT

Continued on the attached sheet and made a part hereof: ☒ Yes ☐ No

Signature of Complainant
Daniel Moxley

Sworn to before me and subscribed in my presence,

on October 7, 2019 at Jacksonville, Florida

JOEL B. TOOMEY
United States Magistrate Judge
Name & Title of Judicial Officer

Signature of Judicial Officer

AFFIDAVIT

I, Daniel Moxley, 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 July 2017. I am currently assigned to the Jacksonville, Florida Division of the FBI, where I conduct investigations in the area of child pornography. Prior to this assignment, I was employed as an Intelligence Analyst and Management and Program Analyst for the FBI for approximately 7 years. I have Bachelor's Degrees in Economics and Political Science. 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 advertisement and solicitation for, possession, collection, production, receipt, and/or transportation of images of child pornography. I have been involved in searches of residences pertaining to the possession, collection, production, and/or transportation of child pornography through the execution of search warrants.

2. I have investigated and assisted in the investigation of criminal matters involving the sexual exploitation of children, including violations of 18 U.S.C. §§ 2251 and 2252. 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 other law enforcement 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 for the requested complaint.

REQUESTED COMPLAINT

4. I make this affidavit in support of a criminal complaint against SAMUEL ARTHUR THOMPSON, for violating 18 U.S.C. § 2252(a)(2), which prohibits knowing receipt of child pornography.

5. As further described herein, on or about January 26, 2018, in the Middle District of Florida and elsewhere, THOMPSON did knowingly receive visual depictions using a means and facility of interstate and foreign commerce, that is, by computer via the internet. The production of the visual depictions involved

the use of minors engaging in sexually explicit conduct and the visual depictions were of such conduct. At least one of the visual depictions involved a prepubescent minor, including that specifically identified in the computer file titled "vAVBHarL," in violation of 18 U.S.C. § 2252(a)(2).

PROBABLE CAUSE

5. On or about August 2, 2019, I spoke to FBI Special Agent Frank Norris regarding the investigation into THOMPSON and learned the following:

a. In December 2018, SA Norris opened an investigation citing THOMPSON as the subject in a computer intrusion investigation. During the investigation, SA Norris developed probable cause to believe that THOMPSON had intentionally accessed a protected computer or computer network without authorization.

b. On July 11, 2019, SA Norris applied for and obtained a federal warrant to search the premises of THOMPSON's residence, known as 113 Marsh Island Circle, Saint Augustine, Florida 32095, for evidence related to the intentional access of a protected computer or computer network without authorization. *See* Case No. 3:19-mj-1251-MCR (the "Computer Intrusion Warrant"). The Computer Intrusion Warrant authorized the

search and seizure of "computers and electronic storage media," with the term "computer" defined to include "all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware." A copy of the application and accompanying affidavit and attachments for the Computer Intrusion Warrant is attached as Composite Exhibit 1. The facts and information contained therein are incorporated by reference.

c. The Computer Intrusion Warrant was executed on July 17, 2019, by Special Agents and Task Force Officers (TFOs) of the FBI. The FBI seized several electronic devices from inside the residence and THOMPSON's cellular phone from his person. The electronic devices and the cellular phone were placed into the Evidence Control Room of the Jacksonville office of the FBI, located at 6061 Gate Parkway North, Jacksonville, Florida, for later review for the purpose of identifying evidence of the computer intrusion.

d. On July 29, 2019, FBI TFO Roger Prendergast began analyzing an Apple iPhone 7 with serial number F725RGL2HG and phone number (904)-813-6066 (hereinafter, "THOMPSON's iPhone"), which was located on THOMPSON's person at the time the Computer Intrusion Warrant was executed, for evidence of the computer intrusion. TFO Prendergast informed SA Norris that, during his review of THOMPSON's iPhone, TFO Prendergast discovered one image that he suspected of being child pornography. SA Norris reviewed the image, which he described as "the front view of a nude prepubescent male, based on the child's lack of pubic hair and the child-like facial features and child-sized arms and legs. In the image, the child is gripping his own erect penis and the child's genitals appear to be the focal point of the image." SA Norris and TFO Prendergast consulted with SA Jonathan McDonald regarding this image. SA MacDonald has been assigned to the FBI Jacksonville Violent Crimes Against Children Task Force for over ten years. In that capacity, SA MacDonald investigates crimes against children, including child pornography offenses, under the auspices of the FBI's "Innocent Images" National Initiative.

During the course of his duties, SA MacDonald has executed search warrants and investigated cases involving the advertisement and solicitation for, possession, collection, receipt, and production of child pornography. SA McDonald reviewed the image of suspected child pornography described above and advised SA Norris that, based on his training and experience, the image discovered by TFO Prendergast during his review of THOMPSON's iPhone and described above constitutes child pornography pursuant to Title 18, United States Code, Section 2256, because the image depicts a minor child engaged in sexually explicit conduct, that is, the graphic lascivious exhibition of his genitals and masturbation. At that point, SA Norris, TFO Prendergast and other Special Agents ceased reviewing the contents of THOMPSON's iPhone and advised Assistant United States Attorney Laura Cofer Taylor of the child pornography image that had been found on THOMPSON's iPhone. AUSA Taylor instructed SA Norris to tell FBI Special Agents to cease the search and forensic examination of THOMPSON's iPhone and that a search warrant authorizing the further search of THOMPSON's iPhone for evidence, fruits, and instrumentalities

of the possession of child pornography would be sought later from this Court. Thus, all examination of THOMPSON's iPhone ceased.

e. On August 2, 2019, SA Norris obtained a warrant to search THOMPSON's iPhone for evidence related to the receipt, possession, and access with intent to view child pornography. *See* Case No. 3:19-mj-1284-JBT (the "iPhone Child Pornography Search Warrant"). The iPhone Child Pornography Search Warrant was executed on August 2, 2019, by SA Norris and other special agents of the FBI. The iPhone Child Pornography Search Warrant authorized the search and seizure of the aforementioned iPhone, which was seized from THOMPSON's person on July 17, 2019, during the execution of the Computer Intrusion Warrant at THOMPSON's residence. A copy of the application and accompanying affidavit and attachments for the iPhone Child Pornography Search Warrant is attached as Composite Exhibit 2. I have reviewed the facts and information contained therein and incorporate them by reference.

f. After a forensic image of THOMPSON's iPhone was created by FBI Computer Analysis Response Team (CART) Forensic

Examiner SA Robert McCallum, the device was secured in the secured evidence storage compartment in the FBI CART office.

g. According to a publicly available website maintained by the Florida Department of Law Enforcement ("FDLE"), THOMPSON is a registered sex offender residing at 113 Marsh Island Circle, Saint Augustine, Florida 32095-9644. According to FDLE, THOMPSON was convicted on April 22, 1998, of Sexual Abuse 2nd and Sodomy 2nd in Mobile, Alabama. SA Norris also reviewed court documents relating to this conviction, and learned that the Sexual Abuse 2nd count was based upon THOMPSON fondling the penis of a child older than 12 and younger than 16, and the Sodomy 2nd count was based upon THOMPSON performing oral sex on a child older than 12 and younger than 16.

6. On August 2, 2019, I reviewed and verified a copy of the iPhone Child Pornography Search Warrant obtained by SA Norris.

7. On August 5, 2019, I opened an FBI child pornography investigation into THOMPSON.

8. From August 5, 2019, to August 22, 2019, I reviewed the contents of THOMPSON's iPhone and identified at least 30 images of nude prepubescent male

children, some of which constituted a lascivious exhibition of their genitalia. I also observed at least five videos of age-difficult males engaged in sexually explicit conduct. Of the images that constituted a lascivious exhibition of the genitalia, I observed the following image:

FILE NAME: "vAVBHarL"

MD5 HASH: 7c3a5553cfe0d2133000810ce9c5cfdd

RECEIPT DATE: January 26, 2018

DESCRIPTION: A color image of a prepubescent male child, based on his child-sized limbs and facial features and lack of pubic hair, is lying on a bed with cartoon characters on the bedding, wearing only a red shirt and socks. The child is not wearing pants or underwear. The child has his legs bent and spread open, fully exposing his genitals, making it the focal point of the image. The child is using his hand to touch his genitals. The child is propping himself up on a yellow and red pillow, tilting his head, while staring into the camera.

9. The image described above, titled "vAVBHarL," resided in file path, "iPhone/Applications/group.mega.ios/Library/Cache/thumbnailsV3/vAVBHarL." This file path indicated the image resided within the MEGA application on THOMPSON's iPhone. According to open sources, MEGA is a cloud storage and

file hosting service offered by Mega, Ltd., based in New Zealand and offers a downloadable application for iPhone cellular phones.

10. On August 6, 2019, FBI Staff Operations Specialist Megan Hammerling served Mega, Ltd. with an administrative subpoena requesting subscriber information for any MEGA accounts registered by THOMPSON's known e-mail addresses. MEGA responded with negative results on the same day.

11. On August 7, 2019, I provided two additional e-mail addresses to Mega, Ltd., including tvdirector911@gmail.com. The email address tvdirector911@gmail.com was previously identified as an email address belonging to THOMPSON through various means, including that tvdirector911@gmail.com is the email associated with the iCloud account for THOMPSON's iPhone. As described in Paragraph 13 of the Affidavit for the attached iPhone Child Pornography Search Warrant, this email address was also associated with THOMPSON through grand jury subpoena results provided by Dropbox.com.

12. On August 7, 2019, Mega, Ltd. provided results, which revealed an active MEGA account was registered to tvdirector911@gmail.com. Additionally, results revealed THOMPSON logged into his MEGA account from the MEGA application on an iPhone on January 26, 2018. According to open source information and conversations with Mega, Ltd., a user can log into their MEGA account from any electronic device connected to the Internet to upload and store

files. The files are then encrypted and stored on MEGA servers until the user logs into his/her MEGA account. Upon logging into his/her MEGA account from any Internet-connected device, the files are transferred to that device.

CONCLUSION

Based upon the foregoing facts, I have probable cause to believe on or about January 26, 2018, in the Middle District of Florida and elsewhere, SAMUEL ARTHUR THOMPSON, did knowingly receive one (1) or more visual depictions using a means and facility of interstate and foreign commerce, that is, by computer via the internet. The production of the visual depictions involved the use of minors engaging in sexually explicit conduct and the visual depictions were of such conduct. At least one of the visual depictions involved a prepubescent minor,

including that specifically identified in the computer file titled "vAVBHarL," in violation of 18 U.S.C. § 2252(a)(2).

DANIEL MOXLEY, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me this
7 day of October, 2019, at Jacksonville, Florida.

JOEL B. TOOMEY
United States Magistrate Judge

COMPOSITE EXHIBIT 1

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Middle District of Florida

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
the premises known as 113 Marsh Island Circle, Saint Augustine, Florida 32095

Case No. 3:19-mj- 1251-MCR

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
the premises known as 113 Marsh Island Circle, Saint Augustine, Florida 32095, more particularly described in Attachment A,

located in the Middle District of Florida, there is now concealed *(identify the person or describe the property to be seized)*:
see Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1030	Intentionally accessing a protected computer or computer network without authorization

The application is based on these facts:

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SA Frank Norris, Federal Bureau of Investigation
Printed name and title

Sworn to before me and signed in my presence.

Date: 7/11/19

Judge's signature

City and state: Jacksonville, Florida

Magistrate Judge Monte C. Richardson
Printed name and title

AFFIDAVIT

I, Frank Norris, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been so employed since March 2018. I am an investigative or law enforcement officer of the United States within the meaning of Rule 41(a)(2)(C) of the Federal Rules of Criminal Procedure. I am currently assigned to the Cyber Task Force of the Jacksonville, Florida, Division of the FBI, where I conduct a variety of investigations in the area of cyber-crimes. Prior to this assignment, I was employed as a Staff Operation Specialist (SOS) for the FBI for approximately 2 years. As an SOS I worked investigations pertaining to violent crimes, white collar crimes, counter intelligence, domestic terrorism, cyber-crimes, cyber-crimes related to national security. Prior to working for the FBI, I received a Bachelor's degree in Criminal Justice and in Political Science and also received a Master's Degree in Information Systems. 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 financial and non-financial motivated computer intrusions and Internet-enabled fraud. Since becoming a Special Agent, I have worked with experienced Special Agents who also investigate financial and non-financial motivated computer intrusions and Internet-enabled fraud. In the performance of my duties, I have investigated and assisted in the investigation of matters involving the unauthorized access of a computer network, fraud facilitated

through the use of the Internet, nation state computer intrusions, and computer intrusions for the purposes of financial gain. I have participated in the execution of numerous search warrants, including search warrants in cyber investigations.

2. The statements contained in this affidavit are based on my personal knowledge as well as on information provided to me by other law enforcement officers. This affidavit is being submitted for the limited purpose of securing a search warrant, 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 evidence of violations of federal law is present in the residence to be searched.

REQUESTED WARRANT

3. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 113 Marsh Island Circle, Saint Augustine, Florida 32095 (hereinafter the "SUBJECT PREMISES"), as further described in Attachment A, for the things described in Attachment B.

STATUTORY AUTHORITY

4. As detailed herein, Samuel Arthur THOMPSON is the subject of an FBI investigation into the use of one or more computers to commit violations of Title 18, United States Code, Section 1030, which prohibits intentionally accessing a protected computer or computer network without authorization. A "protected computer" is a computer that is used in or affecting interstate or foreign commerce.

a. Title 18, United States Code, Section 1030(a)(2)(C) provides that it is unlawful for an individual to "intentionally access a computer without authorization or exceed authorized access in order to obtain information from any protected computer."

b. Title 18, United States Code, Section 1030(a)(5)(C) provides that it is unlawful for an individual to "intentionally access a protected computer without authorization, and as a result of such conduct, [cause] damage and loss." The term "damage" means any impairment to the integrity or availability of data, a program, a system, or information.

PROBABLE CAUSE

5. On December 10, 2018, I, Special Agent (SA) JulianCarl Slaughter, and Task Force Officer (TFO) Roger Prendergast interviewed Michael Webb, Vice President of Information Technology for the Jacksonville Jaguars (VICTIM COMPANY). Other employees of the VICTIM COMPANY present for the interview were Senior Manager of Technology and Events Jason Dean, Manager of Facilities Security Bobby Lyle, and Network Administrator Michael Potts. The VICTIM COMPANY is a National Football League (NFL) team that hosts a series of NFL games each football season at TIAA Bank Field, which is a stadium located at 1 TIAA Bank Field Drive, Jacksonville, Florida, within the Middle District of Florida.

6. The interview was conducted as a result of FBI Jacksonville's receipt of a complaint from the VICTIM COMPANY that THOMPSON, a former contractor for the VICTIM COMPANY, had been accessing a secure computer network located within the VICTIM COMPANY's facility. As of February 23, 2018, THOMPSON was no longer employed by the VICTIM COMPANY and thus any access by THOMPSON to the VICTIM COMPANY's secure computer network was unauthorized.

7. Through my investigation, I have learned that from April 1, 2017, to February 23, 2018, THOMPSON was a contract employee with the VICTIM COMPANY. THOMPSON was the video production engineer and control room equipment consultant for the VICTIM COMPANY's video board system located at the company's facility. The video boards controlled by the video monitor network, commonly referred to as a "Jumbotron," are designed to ingest video data from a separate network that controls instant replay, slow motion, and video play back. According to Michael Webb, THOMPSON was the architect of the video board system and is one of a very few people who understand how the VICTIM COMPANY's video monitor network and video boards are designed to operate. According to Michael Webb, THOMPSON was a contract employee of the VICTIM COMPANY. Michael Webb explained that THOMPSON had not informed the

VICTIM COMPANY that he was a convicted sex offender when he was hired.[1] The VICTIM COMPANY chose not to renew THOMPSON's contract after learning he had not disclosed his past criminal record.

8. While THOMPSON was a contract employee for the VICTIM COMPANY, THOMPSON had been authorized to use remote access software called TeamViewer to access the devices that control the video board network. TeamViewer is a proprietary computer software for remote control, desktop sharing, online meetings, web conferencing and file transfer between computers. TeamViewer can be used on devices using Microsoft Windows, macOS, Linux, Chrome OS, iOS, Android, Windows RT, Windows Phone 8 and BlackBerry operating systems. Machines running TeamViewer can also be accessed by web browser. By utilizing the TeamViewer software, THOMPSON had remote access to the video board system from any location with any device with internet service and a compatible operating system. THOMPSON's TeamViewer account was not terminated when his contract ended with the VICTIM COMPANY.

---

[1] I note that, based on my review of a publicly available website maintained by the Florida Department of Law Enforcement ("FDLE"), THOMPSON is a registered sex offender residing at 113 Marsh Island Circle, Saint Augustine, Florida 32095-9644. According to FDLE, THOMPSON was convicted on April 22, 1998, of Sexual Abuse 2nd and Sodomy 2nd in Mobile, Alabama. I have ordered copies of court records associated with this conviction.

9. On December 10, 2018, Michael Webb provided SA Slaughter with documents of the VICTIM COMPANY's investigation into the incident. From the documents provided I learned the following:

a. December 3, 2018, the VICTIM COMPANY conducted an investigation into a series of video monitor network incidents that were from suspected improper accesses. During three events hosted by the VICTIM COMPANY, the video boards had experienced an outage from their standard operating design, as described below:

i. On September 16, 2018, from 18:06:03 – 18:06:20 Eastern Time, during an event a video board experienced a loss in reference sync which manifested as a large horizontal green lines appearing across one whole video board.

ii. On November 18, 2018, from 14:55:18 to 14:55:21 Eastern Time, during an event a video board experienced a loss in which resulted in green screens for multiple boards.

iii. On December 2, 2018, from 14:38:37 to 14:38:42 Eastern Time, during an event a single video board experienced a change of what seemed to be the zoom of one of the base graphics displayed.

b. At no point before or after the suspected problems being fixed were the operators or engineers for the VICTIM COMPANY able to replicate the issue causing the incidents. In all of the incidents, the outage

resulted in the inability for the video board system operators to display the desired content. This type of attack commonly is called a denial-of-service (DoS) attack. A DoS attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor.

c. An investigation conducted by the VICTIM COMPANY into the December 2, 2018, incident revealed that a command to change a specific parameter was the source of the outage. An unknown or "rogue" device had sent the command. The rogue device was an Abekas Mira workstation (named MIRA9120) that had been decommissioned from service and had been replaced with a new one. Abekas Mira is a server made by Ross Video, which is designed to produce instant video replays for live events.

d. Unbeknownst to the VICTIM COMPANY, the rogue device had been moved to a server rack adjacent to the server rack housing the active Abekas Mira servers in the facility's video board server room (referred to as the "Rack Room"). In its decommissioned state, MIRA9120 had no connections to any video system and only had a power cable and network cable connected to it. The rogue device had the appearance of an active and functioning part of the network because the new/replacement device and the rogue device display the label "SLOMO 03."

e. After the rogue device (MIRA9120) was identified, it was examined by the VICTIM COMPANY and was found to have the TeamViewer software installed and active. The TeamViewer software logs all connections by default but that feature had been disabled by the user who installed the program making any connections used by the TeamViewer software untraceable.

f. TeamViewer software previously had been removed from all of the devices in the network by the VICTIM COMPANY IT staff.

10. On or about December 3, 2018, the VICTIM COMPANY IT staff disconnected the MIRA9120 from the video board network and re-enabled the TeamViewer connection logging in an attempt to discover any new connections made to MIRA9120 during the upcoming event on December 16, 2018. The VICTIM COMPANY IT staff re-enabled the TeamViewer logging in order to catch any unauthorized connections in the act of gaining access to the network.

11. On January 3, 2019, Michael Webb provided SA Slaughter an image copy of the MIRA9120 hard drive and the results of the incident investigation from December 3, 2018. SA Slaughter, FBI Computer Scientist Tim McCrohan, and I conducted a complete review of the image and learned the following:

a. February 23, 2018 (THOMPSON's last day at work for the VICTIM COMPANY.)

i. 9:09 am – According the Internet Browse History file, a user logged on to TeamViewer.us and downloaded TeamViewer onto the Abekas MIRA9120 Station.

ii. 9:14 am – According to the TeamViewer Logfile, the username "Sam7" with TeamViewer User Identification Number 938826091 logged into TeamViewer and connected with username "MIRA9120" TeamViewer User Identification Number 625675632.

iii. 9:24 am – According to the Internet Browse History file, a user logged on to rossvideo.com and downloaded the "Dashboard" software. Dashboard is a free software program that is designed for facility control and monitoring of devices in a network. The product is designed to work with Ross Video devices such as the Abekas Mira devices.

iv. 9:43 am – According the Internet Browse History file, a user with ID 11649557 logged on to Dropbox.com to download the file "CarboniteLoadSave.grid" from the "Jag_SaveForLater" folder. On January 30, 2019, SA Slaughter served a subpoena to Dropbox.com for subscriber information for the account using ID 11649557. The results returned from Dropbox.com showed that Sam THOMPSON is the owner of account 11649557.

b. December 16, 2018 (VICTIM COMPANY had a scheduled event):

i. The first scheduled event the VICTIM COMPANY held with the MIRA9120 set to log connections made with the TeamViewer software.

ii. 2:04 pm – According to the TeamViewer log file, user "DESKTOP-0ASEJS8 (1118559964)" logged into TeamViewer and connected with "MIRA9120 (625675632)". On February 1, 2019, I served a subpoena to TeamViewer for subscriber information for account 1118559964. According to the TeamViewer subpoena results received on February 26, 2019, account 118559964 logged into account 625675632 (the Abekas MIRA9120 Station) a total of 5 times, the last session using IP address *67.190.234.123* from a machine using a Windows 10 operating system.

12. On January 9, 2019, I served a grand jury subpoena to TeamViewer and on January 24, 2019, TeamViewer returned the information requested. Based on my review of the return, I learned that the 938826091 ("Sam7") account had 14 sessions with the 625675632 ("MIRA9120") account. The last access to the 938826091 account started on November 18, 2018, by IP address *67.190.234.123* using an iPhone.

13. On January 29, 2019, SA Slaughter served a grand jury subpoena to Dropbox.com and on February 1, 2019, Dropbox.com returned the information requested. Based on my review of the return, I learned that Dropbox.com account

11649557 was accessed using the IP address *67.190.234.123* on January 29, 2019, by the host "DESKTOP-0NP&MUJ" and January 30, 2019, by an iPhone using AT&T. The DropBox.com account 11649557 is registered to Sam THOMPSON who used the email address tvdirector911@gmail.com. This account was accessed to download the "CarboniteLoadSave.grid" file from the "Jag_SaveForLater" to the Abekas MIRA9120 Station during the unauthorized access on February 23, 2018.

14. On March 4, 2019, I served a grand jury subpoena to Comcast Cable, and on March 11, 2019, Comcast Cable returned the information requested. Based on my review of the return, I learned that on December 16, 2018, the IP address *67.190.234.123* was assigned to Jean Louise Pucket at 113 Marsh Island Circle, St. Augustine, Florida, within the Middle District of Florida.

15. Through my investigation I discovered that a rogue network device (MIRA9120), unknown to the IT staff of the VICTIM COMPANY, was used to conduct attacks on the Victim Company's video board network during scheduled events. I learned that the MIRA9120 device was accessed a by TeamViewer account that used the IP address *67.190.234.123* on THOMPSON's last day of work for the VICTIM COMPANY. I learned that on that same day files from THOMPSON's Dropbox account were accessed and downloaded via internet browser on the MIRA9120. That same MIRA9120 device was the source of several attacks carried out on the VICTIM COMPANY's network during scheduled events. On December 16, 2018, during a scheduled event the MIRA9120 device was accessed by a TeamViewer account that used the IP address *67.190.234.123*. I learned that the

67.190.234.123 IP address is a Comcast Cable IP that is assigned to the residence of THOMPSON.

16. On May 9, 2019, TFO Roger Prendergast observed a grey Mercedes SUV with the license plate ADAMS 2 parked next to a Black Chevrolet Tahoe at 113 Marsh Island Circle, St. Augustine, Florida. According to DAVID records pulled on May 9, 2019, Samuel THOMPSON and Jean Louise Pucket reside at 113 Marsh Island Circle, St. Augustine, Florida. Jean Louise Pucket has a Mercedes SUV with the license plate ADAMS 2 registered to her at 113 Marsh Island Circle, St. Augustine, Florida. The DAVID records also show that THOMPSON has a black Chevrolet SUV registered to the address 113 Marsh Island Circle, St. Augustine, Florida.

TECHNICAL TERMS

17. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP

addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

d. "Computer," as used herein, is defined pursuant to 18 U.S.C. §1030(e)(1), as "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."

e. "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).

f. "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.

g. 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).

h. "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, or hide protected data to make it

inaccessible or unusable, as well as reverse the progress to restore it.

i. Wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device. Many wireless telephones are minicomputers or "smart phones" with immense storage capacity.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

18. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media (including, for example, a smartphone or tablet computer). Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

19. *Probable cause.* I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe that records of evidentiary value will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data

remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

20. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media

that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or

consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a

storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain unauthorized access to a victim computer over the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

21. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media.

Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be

present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

22. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

23. Because several people share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described

in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

24. I submit that this affidavit supports probable cause for a warrant to search the SUBJECT PREMISES described in Attachment A and seize the items described in Attachment B.

25. Based on the foregoing, I have probable cause to believe Samuel Arthur THOMPSON has used and is using one or more computers and/or electronic storage media located in the residence located at the SUBJECT PREMISES, more fully described in Attachment A to this affidavit, to, among other things, conduct unauthorized access of computer networks belonging to the VICTIM COMPANY. Based on my training and experience, and after consulting with other FBI Special Agents that investigate similar computer intrusions, it is common practice that individuals who conduct such activity maintain physical control of instrumentalities used in the crime and/or in furtherance of the crime. Therefore, I have probable cause to believe that one or more individuals, using the residence described above, has violated Title 18, United States Code, Section 1030. Additionally, I have

probable cause to believe that fruits, evidence, and instrumentalities of violation of Title 18, United States Code, Section 1030, as more fully described in Attachment B, will be located at the SUBJECT PREMISES.

Respectfully submitted,

Frank Norris
Special Agent
Federal Bureau of Investigation

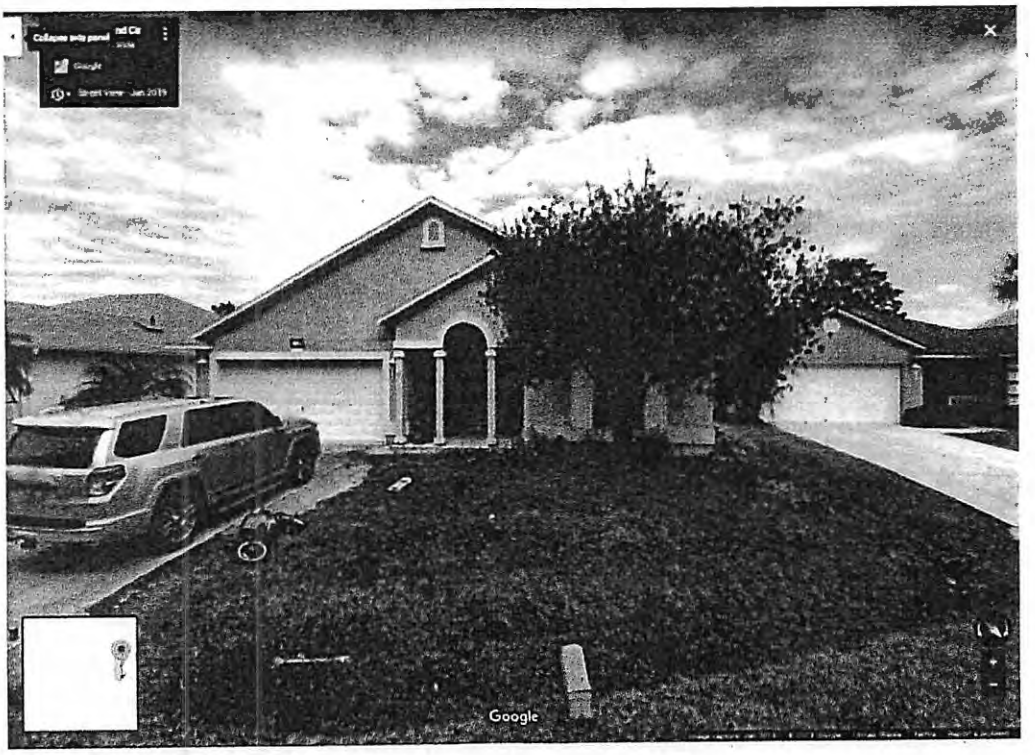
Subscribed and sworn to before me
On July 11, 2019

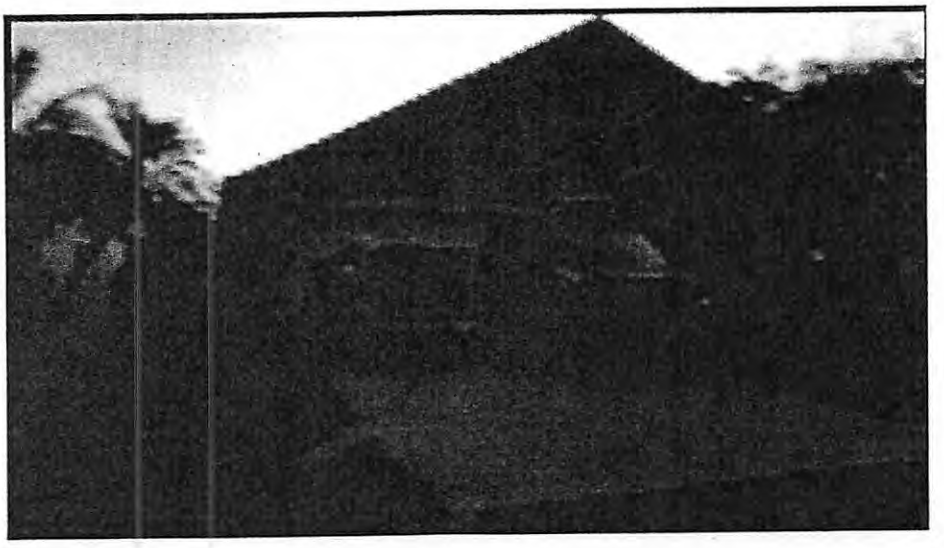
MONTE C. RICHARDSON
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Location to be searched

The location to be searched is the premises known as 113 Marsh Island Circle, Saint Augustine, Florida 32095. The location to be searched is a single story neutral-colored stucco home with light-colored trim. Photos of the location to be searched are below:





ATTACHMENT B

Property to be searched and seized

1. Computers and electronic storage media.

2. Any and all notes, documents, records, or correspondence, in any format and medium pertaining to the Jacksonville Jaguars.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

   a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

   b. Any and all computer software, including applications and programs that may be used for remote access to a computer.

   c. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of

malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

d. evidence of the lack of such malicious software;

e. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

f. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

g. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

h. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

i. evidence of the times the COMPUTER was used;

j. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

k. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

l. records of or information about Internet Protocol addresses used by the COMPUTER;

m. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

n. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Middle District of Florida

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

the premises known as 113 Marsh Island Circle, Saint Augustine, Florida 32095

Case No. 3:19-mj- 1251-MCR

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Middle District of Florida
(identify the person or describe the property to be searched and give its location):

the premises known as 113 Marsh Island Circle, Saint Augustine, Florida 32095, more particularly described in Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

see Attachment B.

YOU ARE COMMANDED to execute this warrant on or before July 23, 2019 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Monte C. Richardson.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 7/16/19 @ 10:50 a.m.

Judge's signature

City and state: Jacksonville, Florida

Magistrate Judge Monte C. Richardson
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return		
Case No.: 3:19-mj-1251-MCR	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

COMPOSITE EXHIBIT 2

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Middle District of Florida

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
a black Apple iPhone 7 with serial number F725RGL2HG and phone number (904)-813-6066

Case No. 3:19-mj- 1284 -JBT

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):* a black Apple iPhone 7 with serial number F725RGL2HG and phone number (904)-813-6066, being held at the Evidence Control Room of the Jacksonville office of the Federal Bureau of Investigation, located at 6061 Gate Parkway North, Jacksonville, Florida, as further described in Attachment A,

located in the Middle District of Florida, there is now concealed *(identify the person or describe the property to be seized)*:
see Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252(a)(2)	Receipt of child pornography
18 U.S.C. § 2252(a)(4)	Possession of and access with intent to view child pornography

The application is based on these facts:
see attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Frank Norris, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 8/2/19

Judge's signature

City and state: Jacksonville, Florida

JOEL B. TOOMEY, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

Item to be searched

The item to be searched is an Apple iPhone 7 with serial number F725RGL2HG and phone number (904)-813-6066 (the "Subject Device"). The Subject Device is black in color with two screen cracks in the bottom left corner. The Subject Device was seized from the person of Samuel Arthur THOMPSON on July 17, 2019, pursuant to a federal search warrant, during a search of the premises known as 113 Marsh Island Circle, Saint Augustine, Florida, within the Middle District of Florida. The Subject Device currently is being stored in the Evidence Control Room of the Jacksonville office of the Federal Bureau of Investigation, located at 6061 Gate Parkway North, Jacksonville, Florida, within the Middle District of Florida.

ATTACHMENT B

Items to be Seized

1. Any and all computer software, including programs to run operating systems, applications, such as word processing, graphics, and communications programs, including, but not limited to, P2P software and/or mobile applications such as Kik Messenger, 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 produce, distribute, possess or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

2. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, e-mail messages, chat logs and electronic messages) pertaining to the production, possession, receipt, or distribution of child pornography as defined in Title 18, United States Code, Section 2256(8) or to the production, possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in Title 18, United States Code, Section 2256(2).

3. In any format and medium, all originals, files, and copies of images and/or videos depicting child pornography as defined in Title 18, United States Code, Section 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in Title 18, United States Code, Section 2256(2), or child erotica.

4. 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 device or by other means for the purpose of distributing or receiving child pornography as defined in Title 18, United States Code, Section 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in Title 18, United States Code, Section 2256(2).

5. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in Title 18, United States Code, Section 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the production, receipt, transmission, or possession of child pornography as defined in Title 18, United States Code, Section 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of websites or file sharing networks on the Internet that contain child pornography or that cater to those with an interest in child pornography.

8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail 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.

9. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.

10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, 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.

11. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, images, videos, e-mail messages, chat logs and electronic messages, and other digital data files), which show the identity of the users of any of the electronic storage media described herein.

12. Any and all diaries, notes, e-mail messages, chat logs and electronic messages, other digital data files reflecting personal contact with minors, sexual activity with minors, and/or any other activities with minors visually depicted while

engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

13. Any and all documents, records, or correspondence, in any format or medium (including email messages, chat logs and electronic messages, and other digital data files), pertaining to the identity of any and all owners and/or users of this Samsung mobile telephone.

AFFIDAVIT

I, Frank Norris, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent (SA) with the Federal Bureau of Investigation ("FBI") and have been so employed since March 2018. I am an investigative or law enforcement officer of the United States within the meaning of Rule 41(a)(2)(C) of the Federal Rules of Criminal Procedure. I am currently assigned to the Cyber Task Force of the Jacksonville, Florida, Division of the FBI, where I conduct a variety of investigations in the area of cyber-crimes. Prior to this assignment, I was employed as a Staff Operation Specialist ("SOS") for the FBI for approximately 2 years. As an SOS, I worked investigations pertaining to violent crimes, white collar crimes, counter intelligence, domestic terrorism, cyber-crimes, cyber-crimes related to national security. Prior to working for the FBI, I received a Bachelor's degree in Criminal Justice and in Political Science and also received a Master's Degree in Information Systems. 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 financial and non-financial motivated computer intrusions and Internet-enabled fraud. Since becoming a Special Agent, I have worked with experienced Special Agents who also investigate financial and non-financial motivated computer intrusions and Internet-enabled fraud. Since becoming a Special Agent, I also have worked with experienced Special Agents who investigate child exploitation offenses. In the performance of my duties, I have investigated and

assisted in the investigation of matters involving the unauthorized access of a computer network, fraud facilitated through the use of the Internet, nation state computer intrusions, and computer intrusions for the purposes of financial gain. I have participated in the execution of numerous search warrants, including search warrants in cyber investigations.

2. The statements contained in this affidavit are based on my personal knowledge as well as on information provided to me by other law enforcement officers, including FBI Special Agents with experience investigating child exploitation offenses. This affidavit is being submitted for the limited purpose of securing a search warrant, 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 evidence of violations of federal law is present in the device to be searched.

REQUESTED WARRANT

3. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search an Apple iPhone 7 with serial number F725RGL2HG and phone number (904)-813-6066 (the "Subject Device"), as further described in Attachment A, for the items described in Attachment B. The Subject Device was seized from the person of Samuel Arthur THOMPSON on July 17, 2019, pursuant to a federal search warrant, during a search of the premises known as 113 Marsh Island Circle, Saint Augustine, Florida, within the Middle District of Florida. The Subject Device currently is being stored in the

Evidence Control Room of the Jacksonville office of the FBI, located at 6061 Gate Parkway North, Jacksonville, Florida, within the Middle District of Florida.

STATUTORY AUTHORITY

4. THOMPSON is the subject of an FBI investigation into violations of Title 18, United States Code, Sections 2252(a)(2), receipt of child pornography, and 2252(a)(4), possession of and access with intent to view child pornography, and there is probable cause to believe that the Subject Device contains fruits, instrumentalities, and evidence of such violations as well as contraband.

5. This investigation concerns alleged violations of Title 18, United States Code, Section 2252, relating to material involving the sexual exploitation of minors. Based upon my training and experience, I know the following:

a. Title 18, United States Code, Section 2252(a) in pertinent part prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing or accessing with intent to view any visual depiction of minors engaging in sexually explicit conduct using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mails.

b. Under Title 18, United States Code, Section 2252(a)(2), it is a federal crime for any person to knowingly receive or distribute, by any means including by computer, any visual depiction of minors engaging in sexually explicit conduct using any means or

facility of interstate or foreign commerce or that has been mailed or shipped or transported in or affecting interstate or foreign commerce. That section also makes it a federal crime for any person to knowingly reproduce any visual depiction of minors engaging in sexually explicit conduct for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails.

c. Under Title 18, United States Code, Section 2252(a)(4), it is also a crime for a person to knowingly possess or knowingly access with intent to view, one or more books, magazines, periodicals, films, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that have been mailed, or have been shipped or transported using any means or facility of interstate or foreign commerce or in and affecting interstate or foreign commerce, or which were produced using materials which have been mailed or so shipped or transported, by any means including by computer.

DEFINITIONS

6. The following definitions apply to this Affidavit:

a. "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, illegal or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child pornography," as used herein, includes the definitions in Title 18, United States Code, Sections 2256(8) and 2256(9) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct). *See* Title 18, United States Code, Sections 2252 and 2256(2).

c. "Visual depictions" include undeveloped film and videotape, data stored on computer disk or by electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in permanent format. *See* Title 18, United States Code, Section 2256(5).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or

oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. *See* Title 18, United States Code, Section 2256(2).

e. "Computer," as used herein, is defined pursuant to Title 18, United States Code, Section 1030(e)(1), as "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."

f. "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).

g. "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.

h. 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).

i. "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.

j. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet and is associated with a physical address. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) may assign a unique and different number to a computer at different times that it accesses the Internet. IP addresses might also be static, if an ISP assigns a

user's computer a particular IP address which is used each time the computer accesses the Internet.

k. "Wireless telephone" (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device. Many wireless telephones are minicomputers or "smart phones" with immense storage capacity.

l. A "digital camera" is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

m. A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

COMPUTERS AND CHILD PORNOGRAPHY

7. Based upon my training and experience, as well as conversations with other experienced law enforcement officers and computer forensic examiners, I know 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 significant skill 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 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.

8. The development of computers has radically changed the way that child pornographers manufacture, obtain, distribute and store their contraband. Computers basically serve five functions in connection with child pornography: access, production, communication, distribution, and storage.

9. 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, proliferation and widespread use of digital cameras, images and videos 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, as well as "smart" phones such as the Apple iPhone, have the capacity to store images and videos indefinitely, and memory storage cards used in these cameras are capable of holding hundreds 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.

10. 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.

11. 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.

12. 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.

13. 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 my training and experience, as well as conversations with other law enforcement officers and computer forensic examiners, I know that these electronic "chat logs" often have great evidentiary value in child pornography investigations, as they can record communication in transcript form, often 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 communications, 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

14. Based upon my training and experience, as well as conversations with other experienced law enforcement officers, I know that searches and seizures of evidence from computers commonly require agents 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 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:

a. Computer storage devices (e.g., hard drives, compact disks ("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; and

b. 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, so it is difficult to know before a search which expert should analyze the system and its data. 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[1], 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.

---

[1] Based on my training and experience, as well as conversations with other law enforcement officers and computer forensic examiners, I know that computer forensic techniques can often recover files, including images and videos of child pornography, that have long been "deleted" from computer media by a computer user.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

15. Based on my experience, training, and conversations with other experienced agents who investigate cases involving the sexual exploitation of children, I know that certain common characteristics are often present in individuals who collect child pornography. I have 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 my training and experience, and conversations with other experienced agents who investigate cases involving the sexual exploitation of children, I know that the following traits and characteristics are often present in individuals who collect child pornography:

a. 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.

b. Many individuals who collect child pornography also collect other sexually explicit 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 meet the legal

definition of child pornography but which nonetheless fuel their deviant sexual fantasies involving children.

c. 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 in children 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.

d. Some individuals who collect child pornography maintain books, magazines, newspapers and other writings (which may be written by the collector), in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals often do not destroy these materials because of the psychological support that they provide.

e. Some 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.

f. 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 like-minded 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. 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. Based on my training and experience, as well as my conversations with other experienced law enforcement officers who conduct child exploitation investigations, I know that individuals who possess, receive, and/or distribute child pornography by computer devices using the Internet, including "smart" phones, often maintain and/or possess the items listed in Attachment B.

16. As stated in substance above and based upon my training and experience, as well as my conversations with other experienced law enforcement officers, I know that individuals who collect and trade child pornography often do not willfully dispose of their child pornography collections, even after contact with law enforcement officials.

17. Based on my training and experience, as well as my conversations with other experienced law enforcement officers, I also know that, with the development of faster Internet download speed and the growth of file-sharing networks and other platforms through which individuals may trade child pornography, some individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis. However, as referenced above, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices using forensic tools. Furthermore, even in instances in which an individual engages in a cycle of

downloading, viewing, and deleting images, a selection of favorite images involving a particular child or act is often maintained on the device.

18. Based on my training and experience, as well as my conversations with other experienced law enforcement officers, I know that within the last several years, individuals who have a sexual interest in minor children have used the internet and internet-enabled devices with increasing frequency to make contact with and attempt to establish relationships with potential child victims. These individuals may perceive that the internet provides some degree of anonymity and safety from prosecution. Because more and more children are using the internet and internet enabled devices, these individuals potentially expose more and more child victims to online sexual exploitation. These individuals may contact potential child victims through social networking websites such as Facebook and Twitter, or may engage in online conversations with children through text messaging and email. During these online conversations, photographic images and links to internet websites can be easily exchanged between the individual and the targeted child. Based on my training and experience, as well as my conversations with other experienced law enforcement officers, I know that when such an individual uses text messaging, email, or other websites to have online contact with children, the internet-enabled device used, whether it is a computer, a cellular telephone, a "smart" phone such as an "iPhone," or a tablet such as an "iPad," often saves and maintains evidence of such contacts. This evidence can often be extracted and examined by a trained forensic examiner.

PROBABLE CAUSE

19. I and other agents of the FBI began investigating THOMPSON as the subject in a computer intrusion case in or about December 2018. During the investigation of the computer intrusion case, I and other FBI agents developed probable cause to believe that THOMPSON had intentionally accessed a protected computer or computer network without authorization.

20. On July 11, 2019, I applied for and obtained a federal warrant to search the premises known as 113 Marsh Island Circle, Saint Augustine, Florida 32095, which is THOMPSON's residence, for evidence related to the intentional access of a protected computer or computer network without authorization. *See* Case No. 3:19-mj-1251-MCR (the "Computer Intrusion Warrant"). The Computer Intrusion Warrant was executed on July 17, 2019, by me and other special agents of the FBI. The Computer Intrusion Warrant authorized the search and seizure of "computers and electronic storage media," with the term "computer" defined to include "all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware." A certified copy of the application and accompanying affidavit and attachments for the Computer Intrusion Warrant is attached as Composite Exhibit 1. The facts and information contained therein are incorporated by reference.

21. Upon executing the Computer Intrusion Warrant at THOMPSON's residence on July 17, 2019, SA JulianCarl Slaughter seized the Subject Device from THOMPSON inside the residence. The Subject Device was in THOMPSON's hand upon SA Slaughter seizing it. THOMPSON provided me with the security code to unlock the Subject Device. The Subject Device subsequently was placed into the Evidence Control Room of the Jacksonville office of the FBI, located at 6061 Gate Parkway North, Jacksonville, Florida, for later review for the purpose of identifying evidence of the computer intrusion.

22. On July 29, 2019, FBI Task Force Officer Roger Prendergast began analyzing the Subject Device for evidence of the computer intrusion as outlined above. TFO Prendergast informed me that, during his review, he discovered one image that he suspected of being child pornography. I reviewed the image, which is a front view of a nude prepubescent male, based on the lack of arm, body, and pubic hair and the male's child-like facial features and child-sized arms and legs. In the image, the child is gripping his own erect penis and the child's genitalia appears to be the focal point of the image. I and TFO Prendergast consulted with SA Jonathan McDonald regarding this image. SA MacDonald has been assigned to the FBI Jacksonville Violent Crimes Against Children Task Force for over ten years. In that capacity, SA MacDonald investigates crimes against children, including child pornography offenses, under the auspices of the FBI's "Innocent Images" National Initiative. During the course of his duties, SA MacDonald has executed search warrants and investigated cases involving the advertisement and solicitation for,

possession, collection, receipt, and production of child pornography. SA McDonald reviewed the image of suspected child pornography described above and advised me that, based on his training and experience, the image discovered by TFO Prendergast during his review of the Subject Device and described above constitutes child pornography pursuant to Title 18, United States Code, Section 2256, because the image depicts a minor child engaged in sexually explicit conduct, that is, the lascivious exhibition of his genitalia and masturbation. At that point, I and other agents ceased reviewing the contents of the Subject Device and advised Assistant United States Attorney Laura Cofer Taylor of the child pornography image that had been found on the Subject Device. AUSA Taylor instructed me to tell FBI agents to cease the search and forensic examination of the Subject Device and that a search warrant authorizing the further search of the Subject Device for evidence, fruits, and instrumentalities of the possession of child pornography would be sought later from this Court. Thus, all examination of the Subject Device ceased.

23. After a forensic image of the Subject Device was created by FBI CART Forensic Examiner SA Robert McCallum, the device was secured in the secured evidence storage compartment in the FBI CART office.

24. Based on my review of a publicly available website maintained by the Florida Department of Law Enforcement ("FDLE"), THOMPSON is a registered sex offender residing at 113 Marsh Island Circle, Saint Augustine, Florida 32095-9644. According to FDLE, THOMPSON was convicted on April 22, 1998, of Sexual Abuse 2nd and Sodomy 2nd in Mobile, Alabama. I have also reviewed court

documents relating to this conviction, and learned that the Sexual Abuse 2nd count was based upon THOMPSON fondling the penis of a child older than 12 and younger than 16, and the Sodomy 2nd count was based upon THOMPSON performing oral sex on a child older than 12 and younger than 16.

CONCLUSION

25. Based on the foregoing, I have probable cause to believe that fruits, evidence, instrumentalities, and contraband, including visual depictions of child pornography, and information and data related to the receipt and possession of child pornography, are currently contained in the item listed and described above, that is, the Subject Device, in violation of Title 18, United States Code, Sections 2252(a)(2) and 2252(a)(4).

26. I submit that this affidavit supports probable cause for a warrant to search the Subject Device described in Attachment A for fruits, evidence, instrumentalities, and contraband set forth in Attachment B and respectfully request this Court issue a warrant authorizing such search.

Frank Norris
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
On August 21, 2019

JOEL B. TOOMEY
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Item to be searched

The item to be searched is an Apple iPhone 7 with serial number F725RGL2HG and phone number (904)-813-6066 (the "Subject Device"). The Subject Device is black in color with two screen cracks in the bottom left corner. The Subject Device was seized from the person of Samuel Arthur THOMPSON on July 17, 2019, pursuant to a federal search warrant, during a search of the premises known as 113 Marsh Island Circle, Saint Augustine, Florida, within the Middle District of Florida. The Subject Device currently is being stored in the Evidence Control Room of the Jacksonville office of the Federal Bureau of Investigation, located at 6061 Gate Parkway North, Jacksonville, Florida, within the Middle District of Florida.

ATTACHMENT B

Items to be Seized

1. Any and all computer software, including programs to run operating systems, applications, such as word processing, graphics, and communications programs, including, but not limited to, P2P software and/or mobile applications such as Kik Messenger, 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 produce, distribute, possess or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

2. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, e-mail messages, chat logs and electronic messages) pertaining to the production, possession, receipt, or distribution of child pornography as defined in Title 18, United States Code, Section 2256(8) or to the production, possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in Title 18, United States Code, Section 2256(2).

3. In any format and medium, all originals, files, and copies of images and/or videos depicting child pornography as defined in Title 18, United States Code, Section 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in Title 18, United States Code, Section 2256(2), or child erotica.

4. 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 device or by other means for the purpose of distributing or receiving child pornography as defined in Title 18, United States Code, Section 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in Title 18, United States Code, Section 2256(2).

5. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in Title 18, United States Code, Section 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the production, receipt, transmission, or possession of child pornography as defined in Title 18, United States Code, Section 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of websites or file sharing networks on the Internet that contain child pornography or that cater to those with an interest in child pornography.

8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail 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.

9. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.

10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, 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.

11. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, images, videos, e-mail messages, chat logs and electronic messages, and other digital data files), which show the identity of the users of any of the electronic storage media described herein.

12. Any and all diaries, notes, e-mail messages, chat logs and electronic messages, other digital data files reflecting personal contact with minors, sexual activity with minors, and/or any other activities with minors visually depicted while

engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

13. Any and all documents, records, or correspondence, in any format or medium (including email messages, chat logs and electronic messages, and other digital data files), pertaining to the identity of any and all owners and/or users of this Samsung mobile telephone.