SEARCH WARRANT

IN THE CIRCUIT COURT OF THE THIRTEENTH JUDICIAL CIRCUIT

IN AND FOR HILLSBOROUGH COUNTY, FLORIDA

IN THE NAME OF THE STATE OF FLORIDA:

TO: THE CHIEF OF THE TAMPA POLICE DEPARTMENT, OR ANY DESIGNATED LAW ENFORCEMENT OFFICER THEREOF:

WHEREAS, complaint on oath and in writing, supported by affidavit has been made before me, Judge Michael Bagge-Hernandez**,** in and for Hillsborough County, Florida, by Julio Tagliani **(Affiant)**, Tampa Police Department who states:

That your Affiant has reason to believe and does believe certain premises located in Hillsborough County, Florida, described as follows, to-wit: The premises with the common street address of 10420 N Mckinley St., Apartment 7201, Tampa, FL 33612. The premises is an apartment located within the Cortland Lakecrest apartments. Apartment 7201 is located within building 7, on the second floor, on the Northeast corner of the building. The numeric “7201” is posted in black letters on a white placard to the left of the door. The premises includes any conveyances associated with or owned/leased by Raiyan Abdul Baten, A/M, 11/01/1993 and or any other known or unknown individuals reasonably believed to be associated with the residence.

And there is now being kept on/in said premises certain evidence, to- wit: .

1. Computer hardware to include any and all computer equipment used to collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes
(but is not limited to) any data-processing devices (such as central processing units, cellular devices, personal computers to include "laptop" or "notebook" or “pocket” computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, and other electronic media devices).

2. Computer input and output devices to include but not limited to keyboards, mice, scanners, printers, monitors, network communication devices, modems and external or connected devices used for accessing computer storage media.

3. Computer storage media and the digital content to include but not limited to floppy disks, hard drives, VHS tapes, USB flash drives, SD cards, DVD disks, CD-ROM disks or other magnetic, optical or mechanical storage which can be accessed by computers to store or retrieve data or images of CSAM.

4. Computer software and application software installation and operation media.

5. Computer software, hardware or digital contents related to the sharing of Internet access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address.

6. Manuals and other documents (whether digital or written) which describe operation of items or software seized.

7. Items containing or displaying passwords, access codes, usernames or other identifiers necessary to examine or operate items, software or information seized.

8. Correspondence or other documents (whether digital or written) pertaining to the possession, receipt, origin or distribution of images involving the sexual exploitation of children.

9. Correspondence or other documents (whether digital or written) exhibiting an interest in the sexual exploitation of children.

10. Items that would tend to establish ownership or use of computers and ownership or use of any Internet service accounts accessed to obtain CSAM to include credit card bills, telephone bills, correspondence and other identification documents.

11. Items that would tend to show dominion and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements and other identification documents.

12. Data maintained on the computer, or computer related storage devices such as floppy diskettes, tape backups, computer printouts, and “zip” drive diskettes, in particular, data in the form of images and/or videos and any accompanying text associated with those images, and/or log files recording the transmission, of images as they relate to violations of Florida law cited herein related to possession and distribution of CSAM.

13. Files and data on the computer that show the suspect’s ownership, possession and control at time of the offense.

14. Any and all software that may be utilized to create, receive, distribute, store, or modify the evidence sought and all software that may be used to communicate or store online communications.

15. Encrypted, deleted and unallocated files on electronic media that contain any of the information listed in previous paragraphs.

16. Notations, files or documentation containing passwords or codes necessary to unlock computer files or to access the computer or storage media.

17. In addition to digital evidence, the following physical items are authorized to be seized as evidence, instrumentalities, or fruits of violations of Florida State Statute 827.071: Any items designed or modified to resemble a minor for prohibited purposes, including any packaging, documentation, receipts, shipping materials, or correspondence relating to the purchase, shipment, or possession of such items; any accessories or items intended for use with such objects; any photographs, videos, or recordings depicting their use, display, or

possession; and any materials or items demonstrating ownership, possession, dominion, or control of the above-described property.

18. Children's clothing, including but not limited to underwear, swimsuits, sleepwear, or other garments sized or designed for minors, where the circumstances of possession indicate potential misuse; any packaging, receipts, tags, or purchase records relating to the acquisition of such clothing; any photographs, videos, or recordings depicting possession or display of such clothing in an inappropriate context; any related storage containers or paraphernalia; and any evidence demonstrating ownership, possession, dominion, or control of the above-described items.

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

During the execution of this search warrant, the law enforcement personnel are authorized to utilize user(s) biometrics such as depress the fingerprints and/or thumbprints of any person, or facial recognition or any user(s) who is located at "the Premises" during the execution of the search, and who is reasonably believed by law enforcement to be a user of a biometrics enabled device that is located at "the Premises" and falls within the scope of this search warrant.

Law enforcement personnel are authorized to direct and compel any person, who is located at "the Premises" during the execution of the search warrant, and who is reasonably believed by law enforcement to contain knowledge of a password(s) to any device(s) and/or application within the device to provide such password(s) in order to allow access to search the device(s) or application(s) pursuant to this search warrant.

Which is being kept and used in violation of the Laws of the State of Florida, to-wit: F.S.S. **827.071 and 828.126 the law(s) prohibiting: Possession of CSAM and sexual activities involving animals and subject to seizure pursuant to F.S.S. 933.02.**

That the facts tending to establish the grounds for this application and the probable cause of Affiant believing that such facts exist are contained in an affidavit for search warrant, sworn to pursuant to Florida law on this date by Julio Tagliani**.** The affidavit for search warrant made by **Julio Tagliani** is hereby incorporated by reference and made a part of this search warrant as if repeated in full, and a copy is attached.

And it appears to the Court that the Affiant is a reputable citizen of the **State of Florida.** The

facts set forth in said affidavit show and constitute probable cause for the issuance of this warrant and the Court being satisfied of the existence of said grounds set forth in said application, or that there is probable cause to believe in their existence.

NOW THEREFORE, you are commanded with such proper and necessary assistance as may be necessary, in the day-time or in the nighttime, or on Sunday, as the exigencies of the occasion may demand or require, to enter and search the aforesaid premises for the described in this warrant: and if the same or any part thereof be found, you are hereby authorized to seize and secure same, giving proper receipt therefore and delivering a duplicate copy on said premises. And you are further directed to bring said property so found before any County or Circuit Judge having jurisdiction of this offense to be disposed of according to law.

WITNESS my hand and seal this 28th day of October, 2026

Wednesday, 28 October 2026
08:45:59

Wednesday, 28 October 2026
08:45:59

Michael Bagge-Hernandez

Judge in and for Hillsborough County, Florida

AFFIDAVIT FOR SEARCH WARRANT

IN THE CIRCUIT COURT OF THE THIRTEENTH JUDICIAL CIRCUIT

IN AND FOR HILLSBOROUGH COUNTY, FLORIDA

STATE OF FLORIDA

COUNTY OF HILLSBOROUGH

BEFORE ME, Judge Michael Bagge-Hernandez , in and for Hillsborough County, Florida, personally or by sworn attestation, came Julio Tagliani (Affiant), Tampa Police Department who, being first duly sworn, deposes and says: That Affiant is employed within said State of Florida and has reason to believe and does believe that those certain premises located in Hillsborough County, Florida, described as follows, to-wit:

The premises with the common street address of 10420 N Mckinley St., Apartment 7201, Tampa, FL 33612. The premises is an apartment located within the Cortland Lakecrest apartments. Apartment 7201 is located within building 7, on the second floor, on the Northeast corner of the building. The numeric “7201” is posted in black letters on a white placard to the left of the door. The premises includes any conveyances associated with or owned/leased by Raiyan Abdul Baten, A/M, 11/01/1993 and or any other known or unknown individuals reasonably believed to be associated with the residence.

Being the premises owned by or registered to: Raiyan Abdul Baten, A/M, 11/01/1993 OR ANY JOHN OR JANE DOE WHOSE NAMES ARE UNKNOWN TO YOUR AFFIANT, but currently located at the common street address 10420 N Mckinley St., Apartment 7201, Tampa, FL 33612.

And there is now being kept on or in said premises certain evidence, to-wit: 1. Computer hardware to include any and all computer equipment used to collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes (but is not limited to) any data-processing devices (such as central processing units, cellular devices, personal computers to include "laptop" or "notebook" or “pocket” computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, and other electronic media devices).

2. Computer input and output devices to include but not limited to keyboards, mice, scanners, printers, monitors, network communication devices, modems and external or connected devices used for accessing computer storage media.

3. Computer storage media and the digital content to include but not limited to floppy disks, hard drives, VHS tapes, USB flash drives, SD cards, DVD disks, CD-ROM disks or other magnetic, optical or mechanical storage which can be accessed by computers to store or retrieve data or images of CSAM.

4. Computer software and application software installation and operation media.

5. Computer software, hardware or digital contents related to the sharing of Internet access

over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address.

6. Manuals and other documents (whether digital or written) which describe operation of items or software seized.

7. Items containing or displaying passwords, access codes, usernames or other identifiers necessary to examine or operate items, software or information seized.

8. Correspondence or other documents (whether digital or written) pertaining to the possession, receipt, origin or distribution of images involving the sexual exploitation of children.

9. Correspondence or other documents (whether digital or written) exhibiting an interest in the sexual exploitation of children.

10. Items that would tend to establish ownership or use of computers and ownership or use of any Internet service accounts accessed to obtain CSAM to include credit card bills, telephone bills, correspondence and other identification documents.

11. Items that would tend to show dominion and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements and other identification documents.

12. Data maintained on the computer, or computer related storage devices such as floppy diskettes, tape backups, computer printouts, and “zip” drive diskettes, in particular, data in the form of images and/or videos and any accompanying text associated with those images, and/or log files recording the transmission, of images as they relate to violations of Florida law cited herein related to possession and distribution of CSAM.

13. Files and data on the computer that show the suspect’s ownership, possession and control at time of the offense.

14. Any and all software that may be utilized to create, receive, distribute, store, or modify the evidence sought and all software that may be used to communicate or store online communications.

15. Encrypted, deleted and unallocated files on electronic media that contain any of the information listed in previous paragraphs.

16. Notations, files or documentation containing passwords or codes necessary to unlock computer files or to access the computer or storage media.

17. In addition to digital evidence, the following physical items are authorized to be seized as evidence, instrumentalities, or fruits of violations of Florida State Statute 827.071: Any items designed or modified to resemble a minor for prohibited purposes, including any packaging, documentation, receipts, shipping materials, or correspondence relating to the purchase, shipment, or possession of such items; any accessories or items intended for use with such objects; any photographs, videos, or recordings depicting their use, display, or possession; and any materials or items demonstrating ownership, possession, dominion, or

control of the above-described property.

18. Children's clothing, including but not limited to underwear, swimsuits, sleepwear, or other garments sized or designed for minors, where the circumstances of possession indicate potential misuse; any packaging, receipts, tags, or purchase records relating to the acquisition of such clothing; any photographs, videos, or recordings depicting possession or display of such clothing in an inappropriate context; any related storage containers or paraphernalia; and any evidence demonstrating ownership, possession, dominion, or control of the above-described items.
.

Which is being kept and used in violation of the Laws of the State of Florida, to-wit: F.S.S. 827.071 and 828.126 the law(s) prohibiting: Possession of CSAM and sexual activities involving animals and subject to seizure pursuant to F.S.S. 933.02.

That the facts tending to establish the grounds for this application and the probable cause of Affiant believing that such facts exist are as follows:

The Affiant Julio Tagliani, a law enforcement officer of the Tampa Police Departmentbeing properly sworn states:

The Affiant is an Investigative Law Enforcement Officer as defined in Florida State Statute 934.02, and is making this application pursuant to his official duties.

1. Your Affiant, Detective Julio Tagliani, is a sworn member of the Tampa Police Department and currently holds the position of Police Detective in and for Hillsborough County, City of Tampa, Florida, assigned to the Internet Crimes Against Children (ICAC)squad, having held that position since August 2024. Your Affiant is also a Task Force Officer with the Federal Bureau of Investigations (FBI), assigned to the Violent Crimes Against Children (VCAC) squad having held that position since September 2022. In September 2023, Your Affiant was promoted to Detective, where he was assigned to the Special Victims Unit. Prior to being promoted to Detective, your Affiant was assigned to the Internet Crimes Against Children (ICAC) squad where he held that position since February 2020. Prior to being employed by the Tampa Police Department, your Affiant was employed as a Deputy Sheriff in and for Hernando County, Florida, having held that position since November 2006. Your Affiant transferred to the Vice and Narcotics Bureau in 2009. Your Affiant's responsibilities included investigating narcotics complaints or "tips". Your Affiant has authored over 100 search warrants and has been involved in several hundred investigations. Your Affiant currently holds the position of Police Detective assigned to the Tampa Police Department's Major Crimes Bureau, Internet Crimes Against Children (ICAC) squad, is responsible for investigating child pornography related offenses, sexual batteries, lewd molestations, child abuse/neglect and other various crimes against children of crimes of a lewd manner. Your Affiant has successfully completed the law enforcement academy at the Withlacoochee Technical Institute which operates under the regulations of the Florida Justice Standards and Training Commission (CJSTC). Affiant has received specialized training and on-the-job experience in successful child abuse investigations, sex offense investigations and Internet Crimes Against Children (ICAC) investigations. Your Affiant has completed ICAC courses for investigating child pornography. Training certifications include, Interviews and Body Language Techniques, Crisis Intervention Training, Investigative Interviews, Intercept of Secure Communications, GPS Tracking Systems, Basic Safe Locks, Internet Protocol Networks, Router Configuration, Data Analysis, Investigative Techniques, Electronic and

Technical Surveillance Training, Death, Injury, Sexual Violence Scene For First Responders, Search and Seizure Investigations, Basic Computer Skills for Law Enforcement, Identifying and Seizing Electronic Evidence, Online Undercover, Cell Phone Investigations, Search Warrants and Digital Evidence, ICAC BitTorrent Investigations, Determining & Evaluating: True Victims, False Allegations & Statements, Undercover Chat Concepts, BDFA-Windows Acquisition, Child Sex Crimes Investigations, Searching for the Digital Evidence at Your Crime Scene, ICAC-Search and Seizure: Data Driven Warrants, Cellebrite Certified Operator, and Cellebrite Certified Physical Analyst.

2. Your Affiant is a member of the Central Florida Internet Crimes Against Children (ICAC) Task Force. The Internet Crimes Against Children Task Force program helps State and Local Law Enforcement Agencies develop an effective response to cyber enticement and child pornography cases. This help encompasses forensic and investigative components, training, and technical assistance, victim services, and community education. The ICAC program is a national network of 61 coordinated task forces representing over 3,000 Federal, State, and Local law enforcement and prosecutorial agencies. These agencies are engaged in proactive investigations, forensic investigations, and criminal prosecutions. One of the programs that aids in the detection and investigation of cyber enticement and child pornography cases is the Cyber Tip line/Cyber Tips. The Cyber Tip line is operated by the National Center for Missing and Exploited Children (NCMEC) and in partnership with the FBI, Immigration and Customs Enforcement, U.S. Postal Inspection Service, U.S. Secret Service, military criminal investigative organizations, U.S. Department of Justice, Internet Crimes Against Children Task Force program, as well as other state and local law enforcement agencies. The National Center for Missing & Exploited Children (NCMEC) opened in 1984 to serve as the nation’s clearinghouse on issues related to missing and sexually exploited children. Today NCMEC is authorized by Congress to perform 22 programs and services to assist law enforcement, families and the professionals who serve them. One of the Congressional Authorized functions of NCMEC (42 U.S.C. §5773) is to Operate a Cyber Tip line to provide online users and electronic service providers an effective means of reporting Internet-related child sexual exploitation in the areas of :possession, manufacture, and distribution of child pornography; online enticement of children for sexual acts; child prostitution; sex tourism involving children; extra familial child sexual molestation; unsolicited obscene material sent to a child; misleading domain names; and misleading words or digital images on the Internet, and subsequently to transmit such reports, including relevant images and information, to the appropriate international, Federal, State, or local law enforcement agency for investigation. Reports to the Cyber Tip line are made by the public and Electronic Service Providers (ESP). ESPs are required by law to report apparent child pornography to law enforcement via the Cyber Tip line (18 U.S.C. §2258A). When the Cyber Tip line receives a report, they are triaged to help ensure children in imminent danger get first priority. Analysts review reports and examine and evaluate the content, add related information that may be useful to law enforcement, use publicly available search tools to determine the geographic location of the apparent criminal act, and provide all information to the appropriate law enforcement agency for potential investigation.

3. The Central Florida ICAC Task Force receives NCMEC Cyber tips within central Florida, and then disseminates them to the appropriate law enforcement agency for investigation. The Cyber Tip line reporting mechanism assists law enforcement and prosecutors in their detection, investigation and prosecution of child sexual exploitation crimes. The Cyber Tip line helps make law enforcement’s efforts more efficient and maximizes the limited resources available in the fight against child sexual exploitation. The value of the Cyber Tip

line as a source of leads for law enforcement has been greatly enhanced by collaboration with ESPs.

Probable Cause:

1. Probable Cause
On October 1, 2026, your Affiant was assigned this case for follow up, in reference to a NCMEC (National Center for Missing and Exploited Children) cyber tip regarding the online possession/distribution of apparent child pornography. Your Affiant reviewed cyber tip 255726211 and all of its supporting content. According to NCMEC, the cyber tip was received on 08-21-2026 at 17:14:02 UTC from Dropbox, after Dropbox discovered that someone uploaded apparent CSAM (Child Sexual Abuse Material) to Dropbox's servers on 08-20-2026 at 17:14:02 UTC.

The cyber tip lists the following suspect information:
Email Address: raiyanabdulbaten@gmail.com (Verified 03-12-2013 12:55:37 UTC)
Screen/User Name: Raiyan Abdul Baten
ESP User ID: 49034115

The cyber tip lists several IP addresses that were used to access the Dropbox account. One of those IP addresses was 47.200.20.147 on 06-19-2026 at 16:16:55 UTC.

The cyber tip lists the following file of apparent child pornography that was discovered on Dropbox's servers:
Filename: video_2026-07-23_15-11-18.mp4
MD5: 8752513ad6bad6bceac5c61866ecf15e

Your Affiant reviewed the file, and it can be described as follows:
The file is a color video that is twenty-four minutes and twenty-four seconds in length. The video depicts a [redacted] that is approximately [redacted] It is evident that [redacted] is a child based on [redacted] small size, [redacted] and childlike face. The [redacted] removes [redacted] and has the [redacted] and performing oral sex on the child. The file constitutes CSAM as defined in Florida State Statutes.

This case was originally assigned to the Hillsborough County Sheriff's Office, and through legal process, they determined that IP address 47.200.20.147 was utilized by Frontier Communications at 10420 McKinley Dr. Apt 7301, Tampa, FL 33612, with the account holder being Raiyan Abdul Baten, 11/01/1993.

This address is the jurisdiction of the Tampa Police Department, so the case was reassigned to the Tampa Police.
An inquiry through DHSMV, (Department of Highway Safety and Motor Vehicles), for 10420 McKinley Dr. Apt 7301, Tampa, FL revealed a Raiyan Abdul Baten, A/M, 11/01/1993.

Raiyan Baten has a tan 2011 Toyota Corolla bearing FL registration 19DLWU registered to him.
On October 5, 2026, your Affiant authored a search warrant for the Dropbox account identified by the Email Address: raiyanabdulbaten@gmail.com, Screen/User Name: Raiyan

Abdul Baten, ESP User ID: 49034115. The search warrant was reviewed and signed by the Honorable Judge Leslie Schultz-Kin and served to Dropbox via their online portal.

On October 15, 2026, Dropbox responded to the search warrant with 6 zipped folders, 384 GB in size. The folders were parsed through Axiom.

On October 22, 2026, at approximately 0500 hours, I responded to 10420 N McKinley Ave, Tampa, Fl 33612 for the purpose of conducting surveillance. Upon arrival, your Affiant observed Raiyan's tan 2011 Toyota Corolla bearing FL registration 19DLWU parked in a parking spot adjacent to the door that leads to apartment 7301.

On the same date, your Affiant reviewed the contents of the Dropbox return, and discovered the following items of evidence:

13 files of bestiality. An example of one of the files, is the file identified by the filename 0_553.mp4. The file is a 28-minute compilation [redacted] having sexual intercourse with various different dogs. The file is if violation of Florida State Statutes.

The file can be found at the file path:

file-data-part-3.zip\49034115\File Data Part 3\Dropbox Folder\Screenshots\New folder (2)\0_553.mp4
Several files that show domain, including selfie style photos of Raiyan Baten and his work documents as a professor at USF.
There were thousands of files of adult pornography.

On October 26, 2026, your Affiant authored a search warrant for 10420 N McKinley Dr, Apartment 7301, Tampa, Florida, 34612. The search warrant was reviewed and signed by the Honorable Judge Frances Perrone.

On October 28, 2026, your Affiant learned that Riayan Baten moved from 10420 N McKinley Dr, Apartment 7301, Tampa, FL 33612 to 10420 N Mckinley Dr. Apartment 720, Tampa, FL 33612.

Your Affiant contacted the Tampa Electric Company, who confirmed that the electric account for Raiyan Baten was moved from 10420 N McKinley Dr, Apartment 7301, Tampa, FL 33612 to 10420 N Mckinley Dr. Apartment 7201, Tampa, FL 33612 on October 9, 2026.

Your Affiant seeks this search warrant for Raiyans current apartment at 10420 N Mckinley Dr. Apartment 7201, Tampa, FL 33612.

2. Computer Evidence Disclosure

Your Affiant knows from training and experience that digital evidence is not limited to computers. Your Affiant has been involved in numerous cases where persons with an interest in child exploitation materials can access the Internet, display images of CSAM and communicate with other individuals with the same interest using digital communications devices to include cellular telephones, email devices and personal digital assistants. These devices are frequently found to contain chat communications in the form of short message

service (SMS) messages as well as enabling Internet and digital cellular network access.

Your Affiant knows from training and experience that searches and seizures of evidence from computers and other Internet access devices require agents to seize most or all electronic items (hardware, software, passwords and instructions) to be processed later by a qualified digital evidence expert in a controlled environment. Digital storage media may include but is not limited to floppy disks, hard drives, tapes, DVD disks, CD-ROM disks or other magnetic, optical or mechanical storage which can be accessed by computers or other electronic devices to store or retrieve data or images of CSAM, which can store the equivalent of thousands of pages of information. Users may store information or images in random order with deceptive file names, which requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process renders it impractical to attempt this kind of data search on site.

Your Affiant knows from training and experience that searching digital evidence systems for criminal evidence requires experience in the computer and cellular telephone field and a properly controlled environment in order to protect the integrity of the evidence and recover even "hidden", erased, compressed, password-protected, or encrypted files. Since digital evidence is extremely vulnerable to tampering or destruction (either from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

Your Affiant knows from training and experience that computers and other digital communication devices contain volatile memory that contains information only while the device is in a powered on and/or running state. Your Affiant knows that powering off the device may result in the loss of the volatile information. Your Affiant also knows that adding an external evidence storage device will cause minor changes to the state of the computer but will allow for the best effort in fully capturing the state of the running evidence. Your Affiant knows that this capture of information requires technical expertise to ensure the resulting data can be examined by all subsequent investigators. Your Affiant knows that this captured information may include current and recent use of the computer, use of encryption, use of other communications devices, routes of Internet and other digital communications traffic and passwords, encryption keys or other dynamic details relevant to use of the system.

Your Affiant knows from training and experience that in order to fully retrieve data from a computer or other digital communications system, the analyst needs all magnetic storage media as well as the storage devices. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware access software or drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) as well as documentation, items containing or displaying passwords, access codes, usernames or other identifiers necessary to examine or operate items, software or information seized or to activate specific equipment or software.

Your Affiant knows from training and experience that persons trading in, receiving, distributing, or possessing images involving the exploitation of children or those interested in the actual exploitation of children often communicate with others through correspondence or other documents (whether digital or written) which could tend to identify the origin of the images as well as provide evidence of a person’s interest in CSAM or child exploitation.

Your Affiant knows from training and experience that files related to the exploitation of children found on computers and other digital communications devices are usually obtained from the Internet or from cellular data networks using application software which often leaves files, logs or file remnants which would tend to show the method of location or creation of the images, search terms used, exchange, transfer, distribution, possession or origin of the files.

Your Affiant knows from training and experience that digital software or hardware exists that allows persons to share digital access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address. The most common type of equipment that allows for this type of access is a router. Examination of these items can reveal information about the authorized or unauthorized use of Internet connection at the residence. In the case of unauthorized access of a wireless network, the router is the instrumentality of the crime. The router can be interrogated and data may be retrieved that can lead to the discovery of the computer responsible for the unauthorized access and subsequent criminal activity.

Your Affiant knows from training and experience that a cell phone can operate as a router by utilizing wireless Wi-Fi hotspot technology. A Wi-fi hotspot allows a cell phone to act as a router by sharing internet access wirelessly with other electronic devices. In these instances, the connected devices share the cell phones IP address. The cellphone which is acting as a Wi-fi hotspot can be interrogated and data may be retrieved that can lead to the discovery of the computer or device responsible for the criminal activity.

Your Affiant knows from training and experience that computers or other digital devices used to access the Internet usually contain files, logs or file remnants which would tend to show ownership and use of the device as well as ownership and use of Internet service accounts used for the Internet or cellular data network access.

Your Affiant knows from training and experience that digital crime scenes usually include items or digital information that would tend to establish ownership or use of digital devices and Internet access equipment and ownership or use of any Internet service or digital cellular service accounts to participate in the exchange, receipt, possession, collection or distribution of CSAM.

Your Affiant knows from training and experience that persons with an interest in the exploitation of children frequently have trophies from victims, items for the grooming of children as well as collections of clothing and toys related to the exploitation of children.

Your Affiant knows from training and experience that search warrants of residences involved in computer or digitally related criminal activity usually produce items that tend to establish ownership or use of digital devices and ownership or use of any Internet service accounts accessed to obtain CSAM to include credit card bills, telephone bills, correspondence and other identification documents.

Your Affiant knows from training and experience that search warrants of residences usually reveal items that tend to show dominion and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements and other identification documents.

3. Characteristics of CSAM Collectors and Downloaders

Based upon your Affiant's knowledge, experience, and training in child exploitation and CSAM investigations, there are certain characteristics common to many individuals involved in the receipt and collection of CSAM. In the past, collectors of CSAM often possessed and maintained "hard copies" of CSAM material such as pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. CSAM collectors typically retained pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and video tapes for many years. With the advent of technology, collectors of digital CSAM often maintain their digital or electronic collections in a format that is safe, secure and private, such as a computer and/or back-up storage discs or other forms of data storage devices. CSAM collectors also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other CSAM distributors/collectors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in CSAM. Collectors of CSAM prefer not to be without their CSAM for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of CSAM throughout the world. Alternatively, those who download and possess CSAM either feel guilty because of the actions they have committed or they are afraid of being caught so they will delete the files of CSAM after viewing them. Computers and other digital media maintain deleted files and records of CSAM that was downloaded or viewed. That data can often be retrieved from a computer or digital device even after significant time has passed since the data was deleted.

4. Analysis of seized items

Your Affiant hereby requests the Court’s permission to seize the following items, and to conduct an off-site search and analysis, or to delegate the search and analysis to an off-site computer forensic analyst, of the aforementioned items 1 through 18. In addition to the seizure of the aforementioned Property, the Court gives permission to seize the computer hardware (and associated peripherals) and software and to conduct an off site analysis of the hardware and software for the evidence described, if, upon arriving at the scene, the law enforcement officers executing the search conclude that it would be impractical to search the computer hardware on site for this evidence. Your Affiant is aware that the recovery of data by a computer forensic analyst takes significant time, and much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the “return” inventory will be satisfied by a list of only the tangible items recovered from “the premises”.

5. Language to compel password

As discussed herein, based on training and experience your Affiant believes that digital devices will be found during the search. Your Affiant knows from training and experience and a review of publicly available materials that Apple Inc., Motorola, HTC, and Samsung, among other companies, produce devices that can be unlocked by the user with a numerical or an alpha-numerical password, or, for some newer versions of the devices, with the use of "biometrics" in the form of a fingerprint placed on a fingerprint sensor or a form of facial

recognition. Each company has a different name for its biometric features; for example, Apple's is called "Touch ID" or "Face ID". Once a user has set up the Biometric features in the security settings of the device, the user can unlock the device by placing a finger or thumb on the device's fingerprint sensor or use their face using the device's camera. If that device recognizes the biometric, the device unlocks.

a) Most devices can be set up to recognize multiple fingerprints or faces, so that different fingerprints or face, not necessarily from the same person, will unlock the device. Due to your Affiant's training and experience, users of devices with biometric features often enable that feature, because it unlocks the phone more quickly than the entry of a passcode or password but still offers a layer of security.

b) In some circumstances, biometric sensors will not work, and a passcode must be entered to unlock the device. For example, with Apple, Touch ID or Face ID will not work if (1) more than 48 hours have passed since the device has been unlocked, (2) the device has been turned on or restarted, (3) the device has received a remote lock command, or (4) five attempts to match a biometric have been unsuccessful. Other brands have similar restrictions. Your Affiant does not know the passcodes of the devices likely to be found at the Subject Premises. Your Affiant also knows these security feature times can changes as software updates are installed on devices from the manufacturers or in the form of updates by the user(s).

c) Your Affiant is also aware biometric sensors and/or passcodes are also used as a secondary security feature on devices for individual applications. Some of these applications use biometrics or passcodes by default, which are set by the manufacturer. Other applications can use biometrics or passcodes when chosen by the user(s) to enable these security features. Some of these applications enable biometrics once the device leaves a "familiar location" such as work or home.

d) For these reasons, while executing the warrant, Law Enforcement will likely need to use the biometrics of any user(s) of any biometric enabled device(s) to attempt to gain access to that device while executing the search warrant.

e) This affidavit seeks a warrant granting the authority to compel the use of biometrics to include fingerprint and/or thumbprint and/or facial recognition of every person who is located at "the Premises" during the execution of the search and who is reasonably believed by law enforcement to be a user of biometric enabled device or application that is located at the Subject Premises and falls within the scope of the warrant. The government may not be able to obtain the contents of the devices if those biometrics are not used to access the devices at the time of the search.

f) Although your Affiant does not know which of the fingers are authorized to access on any given fingerprint biometric enabled device, your Affiant knows based on training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors. Your affiant also knows the facial recognition can fail to recognize a face due to many reasons such changes in appearance and in any event, all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

g) The warrant seeks the authority to compel the owner of a device located at “the Premises” and that falls within the scope of the warrant to provide their password. Pursuant to State v. Stahl, 41 Fla. L. Weekly D2706 (Fla. 2nd DCA) the Second District Court of Appeal found that because the passcode combination was sought only for its content, and would not require the owner to acknowledge that the phone contained evidence of a crime, the passcode did not rise to the level of testimony within the protection of the Fifth Amendment.

h) Your affiant is aware manufacturers have now implemented a new feature commonly referred to as "Inactivity Reboot". This feature was implemented with Apple iOS 18. Beginning with iOS 18, Apple has added an inactivity reboot timer into the operating system that is tied only to the device’s lock state. This means that when the device has been locked for a period of three days (72 hours), the device reboots. Apple and Android devices are known to use "File Based Encryption". When a device restarts, a large portion of the device data which includes a large portion of user data is now encrypted. This data if often not accessible without the user password or passcode and potentially can never be accessed without the password or passcode.

Your Affiant is aware that the recovery of data by a computer forensic analyst takes significant time, and much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. In compliance with FSS 933.05 any such warrant shall be returned within 10 days after issuance thereof, except that a search warrant issued for a computer, a computer system, or an electronic device, as those terms are defined in s. 815.03, which is in the actual possession of a law enforcement agency at the time such warrant is issued shall be returned to the court within 45 days after issuance thereof. For this reason, the “return” inventory provided at the premises will contain a list of only the tangible items recovered from “the Premises.” An additional return will be provided to the court within 45 days to include the tangible items and evidence obtained during forensic extractions.

WHEREFORE, Affiant makes this Affidavit and Application for Search Warrant and prays for the issuance of a Search Warrant in due form of law commanding the Chief of Police of the Tampa Police Department or any designated Officer thereof, the Commissioner of the Florida Department of Law Enforcement, or any of his duly constituted special agents, and the Sheriff of Hillsborough County, Florida, or any of his duly constituted deputies, members of the Tampa Bay Regional Operations Center Cyber High-Tech Crime Task Force, the Director of the Homeland Security Investigations, or any of their duly constituted Special Agents, and the Director of the Federal Bureau of Investigation, or any of their duly constituted Special Agents, with any proper and necessary assistance, including forensic computer analyst experts, to search “the Premises” above described and the curtilage thereof, or persons located within “the Premises” and the curtilage reasonably believed to be connected with said illegal activity, for “the Property” 1 through 16, heretofore described, and to search “the Property” described above and to seize and safely keep same, either in the daytime or in the nighttime, or on Sunday, as the exigencies of the occasion may demand, in order that the evidence may be procured to be used in the prosecution of such person or persons who have unlawfully used, possessed, or are using or possessing the same in violation of the laws of the State of Florida.

WHEREOF, your Affiant makes this affidavit and prays the issuance of a search warrant in due form of law for the search of the above described premises for the said property, heretofore described, and for the seizure and safe keeping thereof, subject to the order of this Honorable Court, by the duly constituted officers of the law.

Under penalty of purgery, I declare that I have read the foregoing affidavit and the facts as stated are true.

Julio Tagliani

Tampa Police Department

AFFIANT

STATE OF FLORIDA

COUNTY OF HILLSBOROUGH

I am a law enforcement officer as defined in s. 943.10, Florida Statutes, and, pursuant to s.117.10, Florida Statutes, I am authorized to administer oaths when engaged in the performance of official duties. The foregoing instrument was acknowledged before me on this 28th day of October, 2026 by the individual whose name and signature appear above, and who is personally known to me and who did take an oath.

Gregory Van Heyst

-

Tampa Police Department

WITNESS my hand and seal this 28th day of October, 2026

Wednesday, 28 October 2026
08:45:59

Wednesday, 28 October 2026
08:45:59

Michael Bagge-Hernandez

SEARCH WARRANT

IN THE CIRCUIT COURT OF THE THIRTEENTH JUDICIAL CIRCUIT

IN AND FOR HILLSBOROUGH COUNTY, FLORIDA

IN THE NAME OF THE STATE OF FLORIDA:

TO: THE CHIEF OF THE TAMPA POLICE DEPARTMENT, OR ANY DESIGNATED LAW ENFORCEMENT OFFICER THEREOF:

WHEREAS, complaint on oath and in writing, supported by affidavit has been made before me, Judge Frances Perrone**,** in and for Hillsborough County, Florida, by Julio Tagliani **(Affiant)**, Tampa Police Department who states:

That your Affiant has reason to believe and does believe certain premises located in Hillsborough County, Florida, described as follows, to-wit: The premises with the common street address of 10420 N Mckinley Dr., Apartment 7301, Tampa, FL 33612. The premises is an apartment located within the Cortland Lakecrest apartments. Apartment 7301 is located within building 7, on the third floor, on the Northeast corner of the building. The numeric “7301” is posted in black letters on a white placard to the left of the door. The premises includes any conveyances associated with or owned/leased by Raiyan Abdul Baten, A/M, 11/01/1993 and or any other known or unknown individuals reasonably believed to be associated with the residence.

And there is now being kept on/in said premises certain evidence, to- wit: .

1. Computer hardware to include any and all computer equipment used to collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes (but is not limited to) any data-processing devices (such as central processing units, cellular devices, personal computers to include "laptop" or "notebook" or “pocket” computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, and other electronic media devices).

2. Computer input and output devices to include but not limited to keyboards, mice, scanners, printers, monitors, network communication devices, modems and external or connected devices used for accessing computer storage media.

3. Computer storage media and the digital content to include but not limited to floppy disks, hard drives, VHS tapes, USB flash drives, SD cards, DVD disks, CD-ROM disks or other magnetic, optical or mechanical storage which can be accessed by computers to store or retrieve data or images of CSAM.

4. Computer software and application software installation and operation media.

5. Computer software, hardware or digital contents related to the sharing of Internet access

over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address.

6. Manuals and other documents (whether digital or written) which describe operation of items or software seized.
7. Items containing or displaying passwords, access codes, usernames or other identifiers necessary to examine or operate items, software or information seized.

8. Correspondence or other documents (whether digital or written) pertaining to the possession, receipt, origin or distribution of images involving the sexual exploitation of children.

9. Correspondence or other documents (whether digital or written) exhibiting an interest in the sexual exploitation of children.

10. Items that would tend to establish ownership or use of computers and ownership or use of any Internet service accounts accessed to obtain CSAM to include credit card bills, telephone bills, correspondence and other identification documents.

11. Items that would tend to show dominion and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements and other identification documents.

12. Data maintained on the computer, or computer related storage devices such as floppy diskettes, tape backups, computer printouts, and “zip” drive diskettes, in particular, data in the form of images and/or videos and any accompanying text associated with those images, and/or log files recording the transmission, of images as they relate to violations of Florida law cited herein related to possession and distribution of CSAM.

13. Files and data on the computer that show the suspect’s ownership, possession and control at time of the offense.

14. Any and all software that may be utilized to create, receive, distribute, store, or modify the evidence sought and all software that may be used to communicate or store online communications.

15. Encrypted, deleted and unallocated files on electronic media that contain any of the information listed in previous paragraphs.

16. Notations, files or documentation containing passwords or codes necessary to unlock computer files or to access the computer or storage media.

17. In addition to digital evidence, the following physical items are authorized to be seized as evidence, instrumentalities, or fruits of violations of Florida State Statute 827.071: Any items designed or modified to resemble a minor for prohibited purposes, including any packaging, documentation, receipts, shipping materials, or correspondence relating to the purchase, shipment, or possession of such items; any accessories or items intended for use with such objects; any photographs, videos, or recordings depicting their use, display, or possession; and any materials or items demonstrating ownership, possession, dominion, or control of the above-described property.

18. Children's clothing, including but not limited to underwear, swimsuits, sleepwear, or other garments sized or designed for minors, where the circumstances of possession indicate potential misuse; any packaging, receipts, tags, or purchase records relating to the acquisition of such clothing; any photographs, videos, or recordings depicting possession or display of such clothing in an inappropriate context; any related storage containers or paraphernalia; and any evidence demonstrating ownership, possession, dominion, or control of the above-described items.

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

THE COURT FURTHER FINDS:

During the execution of this search warrant, the law enforcement personnel are authorized to utilize user(s) biometrics such as depress the fingerprints and/or thumbprints of any person, or facial recognition or any user(s) who is located at "the Premises" during the execution of the search, and who is reasonably believed by law enforcement to be a user of a biometrics enabled device that is located at "the Premises" and falls within the scope of this search warrant.

Law enforcement personnel are authorized to direct and compel any person, who is located at "the Premises" during the execution of the search warrant, and who is reasonably believed by law enforcement to contain knowledge of a password(s) to any device(s) and/or application within the device to provide such password(s) in order to allow access to search the device(s) or application(s) pursuant to this search warrant.

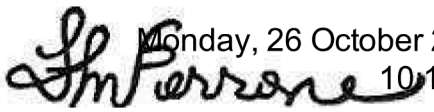
Which is being kept and used in violation of the Laws of the State of Florida, to-wit: F.S.S. **827.071 and 828.126 the law(s) prohibiting: Possession of Child Pornography and Sexual Activities Involving Animals and subject to seizure pursuant to F.S.S. 933.02.**

That the facts tending to establish the grounds for this application and the probable cause of Affiant believing that such facts exist are contained in an affidavit for search warrant, sworn to pursuant to Florida law on this date by Julio Tagliani**.** The affidavit for search warrant made by **Julio Tagliani** is hereby incorporated by reference and made a part of this search warrant as if repeated in full, and a copy is attached.

And it appears to the Court that the Affiant is a reputable citizen of the **State of Florida.** The facts set forth in said affidavit show and constitute probable cause for the issuance of this warrant and the Court being satisfied of the existence of said grounds set forth in said application, or that there is probable cause to believe in their existence.

NOW THEREFORE, you are commanded with such proper and necessary assistance as may be necessary, in the day-time or in the nighttime, or on Sunday, as the exigencies of the occasion may demand or require, to enter and search the aforesaid premises for the evidence described in this warrant: and if the same or any part thereof be found, you are hereby authorized to seize and secure same, giving proper receipt therefore and delivering a duplicate copy on said premises. And you are further directed to bring said property so found before any County or Circuit Judge having jurisdiction of this offense to be disposed of according to law.

WITNESS my hand and seal this 26th day of October, 2026



Monday, 26 October 2026
10:11:47

Monday, 26 October 2026
10:11:47

Frances Perrone

Judge in and for Hillsborough County, Florida

IN THE THIRTEENTH JUDICIAL CIRCUIT IN AND FOR HILLSBOROUGH COUNTY, FLORIDA

STATE OF FLORIDA,
COUNTY OF HILLSBOROUGH:

SEARCH WARRANT RETURN

I, Detective Julio Tagliani, received the within search warrant on the 26th day of October, A.D., 2026 and executed the same to Synchronoss Technologies, 200 Crossing Boulevard Bridgewater, NJ 8807, on the 26th day of October, A.D., 2026. On the 28th Day of October, A.D., 2026, Synchronoss responded with the following information:

48.3 GB of Data

Julio Tagliani, Detective

SWORN TO and SUBSCRIBED before me this 29th day of October 2026.

72270

Notary Public **Law Enforcement Officer**