AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America

v.

Robert Quido STELLA,

Defendant(s)

Case No. 2:21-mj-03333

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief. On or about the date(s) of July 15, 2021 in the county of Los Angeles in the Central District of California, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C . § 2252A	Access to view and possession of child pornography
18 U.S.C . § 2251	Production of child pornography

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

Victoria Scott
Complainant's signature

Victoria Scott, Special Agent
Printed name and title

Sworn to before me and subscribed in my presence.

Date: July 15, 2021

Patricia Donahue
Judge's signature

City and state: Los Angeles, California

Hon. Patricia Donahue, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT

I, VICTORIA J. SCOTT, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint against ROBERT QUIDO STELLA ("STELLA"), date of birth December 21, 1972, for violations of 18 U.S.C. § 2251(a) (production of child pornography) and 18 U.S.C. § 2252A(a)(5)(B) (access with intent to view and possession of child pornography) ("SUBJECT OFFENSES").

2. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and investigators. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and investigators. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all my knowledge of or investigation into this matter. Unless specifically indicated

otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. INTRODUCTION

4. I am a Special Agent ("SA") with the United States Department of Homeland Security ("DHS"), Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI") in Los Angeles, California, and I have been so employed since June 2019. I am currently assigned to HSI Ventura, which is tasked with investigating federal crimes involving child exploitation, child pornography, cybercrimes, immigration crimes, human rights violations and human smuggling, smuggling of narcotics, weapons, and other types of contraband, financial crimes, and various other violations of immigration and customs laws. I have received training in the area of child pornography and child exploitation and observed and reviewed various examples of child pornography in all forms of media, including computer media. I have also participated in the execution of numerous search warrants, many of which involved child exploitation and/or child pornography offenses.

5. Through my training and experience, I have become familiar with the methods of operation used by people who are involved with offenses involving the sexual exploitation of children. I have attended training classes and seminars concerning computer crimes and the sexual exploitation of children on the Internet. This training has given me an understanding of how people involved with offenses relating to the sexual exploitation of children use the Internet to further

those offenses. My experience in investigations in this regard has supplemented my understanding of how people involved in offenses relating to the sexual exploitation of children use the Internet to further those offenses.

III. BACKGROUND ON CHILD EXPLOITATION OFFENSES, COMPUTERS, THE INTERNET, AND DEFINITION OF TERMS

6. In this affidavit, the terms "minor," "sexually explicit conduct," "visual depiction," "producing," and "child pornography" are defined as set forth in 18 U.S.C. § 2256. The term "computer" is defined as set forth in 18 U.S.C. § 1030(e)(1).

7. Based upon my training and experience in the investigation of child pornography, and information related to me by other law enforcement officers involved in the investigation of child pornography, I know the following information about the use of computers with child pornography:

a. Computers and Child Pornography. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. Child pornographers can now produce both still and moving images directly from a common video camera and can convert these images into computer-readable formats. The use of digital technology has enabled child pornographers to electronically receive, distribute, and possess large numbers of child exploitation images and videos with other Internet users worldwide.

b. File Storage. Computer users can choose their method of storing files: either on a computer's hard drive, an

external hard drive, a memory card, a USB thumb drive, a smart phone or other digital media device, etc. (i.e., "locally") or on virtual servers accessible from any digital device with an Internet connection (i.e., "cloud storage"). Computer users frequently transfer files from one location to another, such as from a phone to a computer or from cloud storage to an external hard drive. Computer users also often create "backup," or duplicate, copies of their files. In this way, digital child pornography is extremely mobile and such digital files are easily reproduced and transported. For example, with the click of a button, images and videos containing child pornography can be put onto external hard drives small enough to fit onto a keychain. Just as easily, these files can be copied onto compact disks and/or stored on mobile digital devices, such as smart phones and tablets. Furthermore, even if the actual child pornography files are stored on a "cloud," files stored in this manner can only be accessed via a digital device. Therefore, viewing this child pornography would require a computer, smartphone, tablet, or some other digital device that allows the user to access and view files on the Internet.

c. Internet. The term "Internet" is defined as the worldwide network of computers -- a noncommercial, self-governing network devoted mostly to communication and research with roughly 4.6 billion users worldwide. The Internet is not an online service and has no real central hub. It is a collection of tens of thousands of computer networks, online services, and single user components. In order to access the Internet, an

individual computer user must use an access provider, such as a university, employer, or commercial Internet Service Provider ("ISP"), which operates a host computer with direct access to the Internet.

d. The following definitions:

i. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, 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.

ii. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

iii. "Computer hardware," as used herein, consists of all equipment that 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 central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including 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 physical keys and locks).

iv. "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.

v. "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 what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices,

chips, and circuit boards. 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 "booby-trap" protected data to make it inaccessible or unusable, as well as reverse

vi. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

vii. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), 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 anus, genitals, or pubic area of any person.

viii. A "storage medium" or "storage device" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

ix. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other 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 a permanent format.

x. A "Website" consists of textual pages of information and associated graphic images. The textual

information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

IV. SUMMARY OF PROBABLE CAUSE

8. As set forth in greater detail below, on July 13, 2020, STELLA used BitCoin to pay for access to a darkweb website called, "365 CP," the homepage of which contained images of child pornography and writing only about child sex abuse. STELLA used Coinbase, a cryptocurrency trading platform, to make his BitCoin payment and in doing so, gave his home address, his full name, email address (rob.stella1@gmail.com), phone number, and year of birth (1972). Based on that evidence, I obtained a federal search warrant for STELLA's home which my team executed today.

9. Today, during the warrant execution, agents found digital devices containing surreptitiously recorded videos of STELLA's minor daughter ("Daughter") and two of Daughter's minor female friends, taken from a hidden camera in the family's bathroom; the videos clearly depict the girls' nude genitalia. STELLA is a former Navy Seal, and agents also found numerous pieces of covert surveillance equipment and weapons.

V. BACKGROUND ON TOR-HIDDEN-SERVICE "365 CP" USING URL HTTP://365C7Q5JVM5C5RBZ.ONION

10. On or about May 10, 2021, I received information from HSI Cyber Crimes Center (C3) regarding an investigation initiated by German Federal Criminal Police Office, Bundeskriminalamt (BKA) into Tor-Hidden-Service "365 CP:"

a. https://365c7q5jvm5c5rbz.onion is a website platform that appears to have been developed to allow users to connect online for the purposes of viewing and/or downloading CSAM.

b. To use this website, a user first uses a Tor browser, a web browser that anonymizes a user's web traffic, to access the darknet web. The user then accesses a website's URL home page by manually typing in the weblink or clicking on a hyperlink, a simple link to enter a website. A user on the darknet web or the Internet cannot unintentionally stumble upon this website. The user must make a conscious choice to first download and use special software such as the Tor browser, and then must have the unique alphanumeric string that makes up the URL in order to find and then access the site. Based on my training and experience, Tor browser is known to be used by pedophiles as a means to mask their identities and activities.

c. When a user arrives to the website "365CP" only 12 video stills depicting child pornography with hyperlinks are displayed, along with log in and registration options. Based on my training and experience, the letters "CP" in the title of the website "365CP" likely stand for child pornography, and the display of only video stills depicting child pornography would make the purpose of the website clear to a user prior to making an account or payment.

d. When a user chooses to enter the website "365CP," the user must create an account and make a cryptocurrency payment in order to gain access to the website. After a payment

is sent, the user's account will be unlocked according to the instructions on the website.

VI. STATEMENT OF PROBABLE CAUSE

11. Based on my review of law enforcement reports, conversations with other law enforcement agents, and my own knowledge of the investigation, I am aware of the following:

A. STELLA Accessed Coinbase to pay for Child Pornography on "365 CP"

12. Based on review of reports obtained from Coinbase, I learned that on or about July 13, 2020, STELLA submitted a bitcoin transactional payment of $18.58 USD to the Bitcoin wallet "1D3aQThytRGxD8xHefdhmvJqnMvHa55qhc" to gain access to the CSAM website "365 CP."

13. Additional Coinbase information provided for STELLA's transaction included - User's ID: "5a2973778cc74c0103cff2cb, User's Email: rob.stella1@gmail.com, User's Country: United States of America, Transaction Detail Transaction Type: Send, Transaction Detail Account Name: BTC Wallet, Transaction Detail Account Currency: BTC, Transaction Detail Address: 1D3aQThytRGxD8xHefdhmvJqnMvHa55qhc, Transaction Detail Transaction ID: 5f0cdbb254f6ae0311547be2, Transaction Detail Hsh: 1c056cff5155037ac686379e6eb982a81ee7c0b938b7406df0bc54420b0a4110, Name: Robert STELLA, First Name: Robert Quido, Last Name: Stella, DOB Year: 1972, Phone Number: 619-672-9249, Street Address: 17808 Maplehurst Place, City: Canyon Country, Postal Code: 91387.

14. Within "365 CP," I observed screenshots from the start page provided by BKA via HSI C3. The screenshots included 12 video stills with hyperlinks, depicting child pornography, i.e., visual depictions of a minor engaging in sexually explicit conduct, that were visible immediately once on the website's start page. Some of the images depicted children who were prepubescent.

B. Agents Obtain and Use a Federal Search Warrant to Search STELLA's home

15. According to the California Department of Motor Vehicles ("DMV"), STELLA lists his address as 17808 Maplehurst Place, Canyon Country, California 91387.

16. On July 8, 2021, I obtained a federal search warrant, attached hereto and incorporated herein as Exhibit 1, in which I received permission to search STELLA's home for evidence of access with intent to view child pornography based on the probable cause laid forth in Exhibit 1 (and largely repeated above) regarding STELLA's payment of BitCoin to access a child pornography website.

17. Today, July 15, 2021, agents executed that warrant on STELLA's home.

C. Agents Find Surreptitiously Recorded Videos of STELLA's Naked Minor Daughter and Two Other Minor Females

18. During the execution of the search warrant, agents found numerous digital devices and conducted a preliminary field screening on those devices to determine which devices were of evidentiary value. One of those devices was a Passport External

drive, which is an external storage device, bearing serial number WXMIE83NVZ10 ("the storage drive"). All the files described in the paragraphs contained in this subsection were found on the storage drive.

19. On the storage drive, agents found a folder structure which appeared to be associated with study at a university, as the structure was labeled "\1-NU\1-Courses\HUB 650 Foundations of Behavioral Research\3-Case Study\Week4\." Based on my training and experience of both digital devices and the behavior of individuals with a sexual interest in children, I know that:

a. Individuals with a sexual interest in children will often hide their child pornography in areas of their digital devices that appear to be unrelated and innocent, for example, in a folder labeled "2019 Taxes" or "Photos from Science Lab." These labels are meant to obfuscate the folders' true contents.

b. Individuals with a sexual interest in children will also hide their child pornography in folders that are nested several folders deep in subfolders so that it would be difficult for a different user to simply stumble upon the subfolders' contents.

20. Here, where there the files are contained in a subfolder that is five subfolders deep and the subfolders are labeled in a manner which would suggest unrelated and innocent study at a university, I believe the following files were purposefully hidden.

21. Within that folder structure on the storage device, agents found 17 videos, between 14 seconds and 3 minutes long, as well as what appeared to be approximately 430 screen captures, or video stills, from those videos and other videos which we have not yet located.

a. Some of the videos appear to be taken from about waist height in the family's bathroom. Several of those videos, taken over about a 20-minute period on March 5, 2018, capture Daughter undressing to complete nakedness, entering the shower (which is not visible in the video), exiting the shower, and getting dressed. The Daughter does not appear to be aware that she was being taped. The video depicts a clear, level image, indicating that the recording device was kept completely still during the filming; although it is possible for a person holding a camera to keep the camera very still, based on my training and experience, I know that when videos are this clear and level, it indicates the video was taken from a stationary device, often not held by a person. Such filming is consistent with, although not exclusive to, surreptitious recording devices. The video does not contain any other content, including a person filming. Daughter was born in 2005, and is currently 15 years old. If the creation date is accurate, then Daughter was approximately 12 years old when it was taken. Even if the date is incorrect, given that Daughter is still a minor, the videos were taken when Daughter was a minor.

b. Agents also discovered what appears to be approximately 24 screen captures taken over a one-minute and

twenty-second period on March 14, 2018, depicting a minor female sitting on the toilet and then standing up to redress; as she redresses, her pants and underwear are pulled down thereby clearing exposing her nude external genitalia.

c. Another series appears to be approximately 104 screen captures taken over an 18-minute period on May 16, 2018, from a video which agents have not yet located; I believe these 104 stills were taken from the same video because they are sequentially date-and-time stamped and have a mark on the top left corner indicating they were taken from a camera. The stills depict Daughter and her minor female friend having a sleepover in STELLA's home office. The camera is angled at a mattress on the floor, and the video captures the two girls socializing, completely clothed.

d. Agents located a three-minute video taken over about a 3-minute period on April 5, 2018, which also appears to be taken from about waist height in the family's bathroom. The video captures another minor female (this would be the third victim now) pulling down her underwear, sitting on the toilet (thereby exposing her buttocks), wiping herself, standing up (thereby exposing her external genitalia), and entering the shower. The girl does not appear to be aware that she was being taped. Like the video of Daughter in the bathroom, the video depicts a clear, level image, indicating - possibly - surreptitious recording. The video does not contain any other content, including a person filming.

D. Agents Also Find Numerous Pieces of Covert Surveillance Equipment and Illegal Weapons

22. During the search, agents found numerous pieces of covert surveillance equipment, including but not limited to the following:

a. In Daughter's bedroom, agents found a surreptitious camera hidden inside what appeared to be a smoke detector in Daughter's ceiling; the device had no components to detect smoke.

b. In STELLA's office, agents found a clock that was enabled with wi-fi that had a camera hidden inside.

c. In STELLA's bedroom, in the drawer of a small armoire next to his bed which he said was his side of the bed, agents found a functional USB-charger that also concealed a hidden camera.

d. In a shed in the backyard, agents found:

i. Covert cameras that are designed to be pushed through the open buttonhole of a shirt to disguise the recording device, commonly referred to as pinhole cameras;

ii. An empty box for a camera hidden in a coat hook;

iii. Memory cards that appeared to fit these and other devices;

iv. A Xaver 400 Through Wall Vision device which had a sticker affixed to it stating, "Operation of this device is restricted to law enforcement, emergency rescue, and firefighter personnel. Operation by any other party is a

violation of 47 U.S.C. 301 and could subject the operator to serious legal penalties." Using the internet, I looked up this device on the manufacture's website which said this device allows the operator to locate people behind walls and barriers using ultra-wideband sensor technology;

v. 11 simunition (i.e., simulated munitions) grenades, which are explosive devices containing gun powder and which I understand are illegal in the state of California; and

vi. Multiple tactical vests, and several thick metal plates which are inserted into tactical vests to stop projectiles such as bullets.

23. STELLA is a former United States Navy Seal. STELLA's last position was the Chief of an intelligence unit.

E. STELLA Admits He Accessed the "365 CP" Website, But Denies Looking at Child Pornography

24. During a consensual, non-*Mirandized* interview, STELLA admitted he had accessed the 365 CP website. STELLA further admitted that he liked and looked for teen porn, but that his preferred age range was 18 or 19 years-old.

VII. TRAINING & EXPERIENCE ON INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

25. As set forth above, there is probable cause to believe that STELLA conducted a bitcoin transactional payment to log into the "365 CP" website to access child pornography and surreptitiously produced child pornography of Daughter and other female victims. Based on my training and experience, and the training and experience of other law enforcement officers experienced in investigating crimes involving the sexual

exploitation of children with whom I have had discussions, I have learned that individuals who view and possess multiple images of child pornography, including on web-based bulletin boards and file-sharing programs, are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or in other visual media; or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children often use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children may possess and maintain "hard

copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etcetera, in the privacy and security of their home or some other secure location. Individuals who keep hard copies typically retain them for many years.

d. More recently, individuals who have a sexual interest in children or images of children typically maintain their collections in a digital or electronic format. They typically maintain these collections in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence or inside the collector's vehicle, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials (including through digital distribution via the Internet); 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 child pornography. These individuals often maintain possession of these items for long periods of time.

f. Individuals who access hidden and embedded child pornography-related bulletin boards, and other forums such as newsgroups and IRC chatrooms, are typically more experienced

child pornography collectors. These individuals likely would have gained knowledge about such forums through online communications with other individuals who have a sexual interest in children or images of children.

g. Individuals who have a sexual interest in children or images of children frequently prefer not to be without their child pornography for a prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

h. Child pornography received via computer is extremely mobile. Through computer technology, digital files are easily reproduced and transported. For example, with the click of a button, images and videos containing child pornography can be put onto thumb drives so small that they fit onto a keychain. Just as easily, these files can be copied onto floppy disks or compact disks, and/or stored on iPods, Blackberries, or cellular telephones. Because someone at the SUBJECT PREMISES likely collects and values child pornography, which is easily-stored and duplicated, there is probable cause to believe that evidence of a child pornography collection will be found in the SUBJECT PREMISES.

26. .

VIII. TRAINING & EXPERIENCE IN COMPUTER-RELATED SEXUAL EXPLOITATION INVESTIGATIONS

27. Based on my training and experience, and the training and experience of other law enforcement officers experienced in

investigating crimes involving the sexual exploitation of children with whom I have had discussions, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Individuals with an interest in child pornography can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when a photograph is taken, it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera can be stored on a removable memory card in the camera. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive on the camera. The video files can then be easily transferred from the camcorder to a computer.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to

literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the methods of distributing and receiving child pornography. Child pornography can be transferred via electronic mail or through FTPs to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., Instant Messaging), and easy access to the Internet, the computer is a preferred method for distributing and receiving child pornography.

d. 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 (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media

storage devices can easily be concealed and carried on an individual's person.

e. The Internet affords individuals many different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals can also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services, as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

28. As is the case with most digital technology, communications via a computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (temporary files or ISP client software, among others). 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. Such

information is often maintained indefinitely until overwritten by other data.

IX. CONCLUSION

29. For all the reasons described above, there is probable cause to believe to believe that STELLA committed the SUBJECT OFFENSES.

Victoria Scott
Special Agent
Homeland Security Investigations

UNITED STATES MAGISTRATE JUDGE

The magistrate judge has viewed the images/videos described in paragraph 21 (a-d) above that the affiant alleges are lascivious. The images/videos were provided to the magistrate judge on a labeled disk. The images/videos are in a password-protected folder on the disk. After the magistrate judge viewed the images/videos, the disk was placed inside a sealed envelope and the magistrate judge initialed across the seal. The affiant has taken custody of the envelope and will maintain custody until all appeals have been exhausted.

UNITED STATES MAGISTRATE JUDGE

Exhibit 1

AO 93C (Rev. 8/18) Warrant by Telephone of Other Reliable Electronic Means (USAO rev. 12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)*	)	Case No. 2:21-MJ-03211
The premises located at 17808 Maplehurst Place, Canyon Country, California 91387	)	
Described further in Attachment A	)	

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

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 Central District of California *(identify the person or describe the property to be searched and give its location)*:

See 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

Such affidavit(s) or testimony are incorporated herein by reference [and attached hereto].

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(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.

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 the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

Date and time issued: 07/08/2021 at 1:02pm

Judge's signature

City and state: Los Angeles, CA

Hon. Maria A. Audero

Printed name and title

AUSA: Christopher Brunwin- 213-894-4242

AO 93C (Rev. 8/18) Warrant by Telephone of Other Reliable Electronic Means (Page 2)

Return

Case No.:	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

ATTACHMENT A

PREMISES TO BE SEARCHED

The SUBJECT PREMISES is located at 17808 MAPLEHURST PLACE, CANYON COUNTRY, CALIFORNIA 91387. The SUBJECT PREMISES is on the south side of Maplehurst Place, two houses west of Partridge Drive. It is a two-story gray brick and beige stucco residence with a three-car garage and dark gray shingles on the roof. The number "17808" is above the garage door. The front entry is on the west side/right side of the residence.

ATTACHMENT B

ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 2252A(a)(5)(B) (access with intent to view and possession of child pornography) (the "Subject Offenses"), namely:

a. Child pornography, as defined in 18 U.S.C. § 2256(8).

a. Any digital device used to facilitate the above-listed violations and forensic copies thereof.

b. With respect to any digital device used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device 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, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, 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;

iii. evidence of the attachment of other devices;

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

v. evidence of the times the device was used;

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

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device'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.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as

telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

A. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 120-day period without first obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

c. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

d. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

e. The team searching the digital data also may use sophisticated tools, such as forensic hashing tools, to identify child pornography (including, but not limited to, "Encase" and "Forensic Tool Kit," or "FTK"). Forensic hashing is the process of using a mathematical function, often called an algorithm, to generate a numerical identifier for data (such as a particular file). If the data is changed, even very slightly (such as the addition or deletion of a comma or a period), the identifier should change. A hash value can be thought of as a "digital fingerprint" for data. The team searching digital devices in this case will also use a "hash set," which contains the hash values of image and video files associated with known identified victims of child pornography to determine whether these files are stored within digital devices. Because this "hash set" is constantly being updated as investigations result in the rescue of children depicted in child pornography images/videos, it will

not contain the hash values of all currently identified image and video files. The team searching the digital devices will only use search protocols specifically selected to identify items to be seized under this warrant.

f. When searching a digital device pursuant to the specific search protocols selected, the search team shall make and retain notes regarding how the search was conducted pursuant to the selected protocols.

g. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

h. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

i. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

j. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of items to be seized, the government may retain

forensic copies of the digital device but may not access data falling outside the scope of the items to be seized (after the time for searching the device has expired) absent further court order.

k. The government may retain a digital device itself until further order of the Court or one year after the conclusion of the criminal investigation or case (whichever is latest), only if the device is determined to be an instrumentality of an offense under investigation or the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending). Otherwise, the government must return the device.

l. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, VICTORIA J. SCOTT, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the United States Department of Homeland Security ("DHS"), Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI") in Los Angeles, California, and I have been so employed since June 2019. I am currently assigned to HSI Ventura, which is tasked with investigating federal crimes involving child exploitation, child pornography, cybercrimes, immigration crimes, human rights violations and human smuggling, smuggling of narcotics, weapons, and other types of contraband, financial crimes, and various other violations of immigration and customs laws. I have received training in the area of child pornography and child exploitation and observed and reviewed various examples of child pornography in all forms of media, including computer media. I have also participated in the execution of numerous search warrants, many of which involved child exploitation and/or child pornography offenses.

2. Through my training and experience, I have become familiar with the methods of operation used by people who are involved with offenses involving the sexual exploitation of children. I have attended training classes and seminars concerning computer crimes and the sexual exploitation of children on the Internet. This training has given me an understanding of how people involved with offenses relating to

the sexual exploitation of children use the Internet to further those offenses. My experience in investigations in this regard has supplemented my understanding of how people involved in offenses relating to the sexual exploitation of children use the Internet to further those offenses.

II. PURPOSE OF AFFIDAVIT

3. This affidavit is made in support of an application for a warrant to search the residence located at 17808 Maplehurst Place, Canyon Country, California 91387, as further described in Attachment A, which is attached hereto and incorporated herein by reference, and to seize evidence, fruits, and instrumentalities, as specified in Attachment B, which is also attached hereto and incorporated by reference, of violations of 18 U.S.C. § 2252A(a)(5)(B) (access with intent to view and possession of child pornography) ("SUBJECT OFFENSES").

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and investigators. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. BACKGROUND ON CHILD EXPLOITATION OFFENSES, COMPUTERS, THE INTERNET, AND DEFINITION OF TERMS

5. In this affidavit, the terms "minor," "sexually explicit conduct," "visual depiction," "producing," and "child pornography" are defined as set forth in 18 U.S.C. § 2256. The term "computer" is defined as set forth in 18 U.S.C. § 1030(e)(1).

6. Based upon my training and experience in the investigation of child pornography, and information related to me by other law enforcement officers involved in the investigation of child pornography, I know the following information about the use of computers with child pornography:

a. Computers and Child Pornography. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. Child pornographers can now produce both still and moving images directly from a common video camera and can convert these images into computer-readable formats. The use of digital technology has enabled child pornographers to electronically receive, distribute, and possess large numbers of child exploitation images and videos with other Internet users worldwide.

b. File Storage. Computer users can choose their method of storing files: either on a computer's hard drive, an external hard drive, a memory card, a USB thumb drive, a smart phone or other digital media device, etc. (i.e., "locally") or on virtual servers accessible from any digital device with an Internet connection (i.e., "cloud storage"). Computer users

frequently transfer files from one location to another, such as from a phone to a computer or from cloud storage to an external hard drive. Computer users also often create "backup," or duplicate, copies of their files. In this way, digital child pornography is extremely mobile and such digital files are easily reproduced and transported. For example, with the click of a button, images and videos containing child pornography can be put onto external hard drives small enough to fit onto a keychain. Just as easily, these files can be copied onto compact disks and/or stored on mobile digital devices, such as smart phones and tablets. Furthermore, even if the actual child pornography files are stored on a "cloud," files stored in this manner can only be accessed via a digital device. Therefore, viewing this child pornography would require a computer, smartphone, tablet, or some other digital device that allows the user to access and view files on the Internet.

c. Internet. The term "Internet" is defined as the worldwide network of computers -- a noncommercial, self-governing network devoted mostly to communication and research with roughly 4.6 billion users worldwide. The Internet is not an online service and has no real central hub. It is a collection of tens of thousands of computer networks, online services, and single user components. In order to access the Internet, an individual computer user must use an access provider, such as a university, employer, or commercial Internet Service Provider ("ISP"), which operates a host computer with direct access to the Internet.

d. Internet Service Providers ("ISP"). Individuals and businesses obtain access to the Internet through ISPs. ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customer's behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or businesses that have subscriber accounts with them. Those records often include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, and other information both in computer data and written record format.

e. IP Addresses. An Internet Protocol address ("IP Address") is a unique numeric address used to connect to the Internet. An IPv4 IP Address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). In simple terms, one computer in a home may connect directly to the Internet with an IP Address assigned by an ISP. What is now more typical is that one home may connect to the Internet using multiple digital devices simultaneously, including laptops, tablets, smart phones, smart televisions, and gaming systems, by way of example. Because the home subscriber typically only has one Internet connection and is only assigned one IP Address at a time by their ISP, multiple devices in a home are connected to

the Internet via a router or hub. Internet activity from every device attached to the router or hub is utilizing the same external IP Address assigned by the ISP. The router or hub "routes" Internet traffic so that it reaches the proper device. Most ISPs control a range of IP Addresses. The IP Address for a user may be relatively static, meaning it is assigned to the same subscriber for long periods of time, or dynamic, meaning that the IP Address is only assigned for the duration of that online session. Most ISPs maintain records of which subscriber was assigned which IP Address during an online session.

f. IP Address - IPv6. Due to the limited number of available IPv4 IP addresses, a new protocol was established using the hexadecimal system to increase the number of unique IP addresses. An IPv6 consists of eight sets of combination of four numbers 0-9 and/or letters A through F. An example of an IPv6 IP address is 2001:0db8:0000:0000:0000:ff00:0042:8329.

g. The following definitions:

i. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

ii. "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 necessarily obscene

or do not necessarily depict minors engaging in sexually explicit conduct.

iii. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, 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.

iv. "Cloud-based storage," as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user's computer or other local storage device) and is made available to users over a network, typically the Internet. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to

access the file. Access is typically free and readily available to anyone who has an Internet connection.

v. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

vi. "Computer hardware," as used herein, consists of all equipment that 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 central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including 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 physical keys and locks).

vii. "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.

viii. "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 what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. 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 "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

ix. "Encryption" is the process of converting data into a code in order to prevent unauthorized access to the data.

x. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be

directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

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

xii. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

xiii. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a.

xiv. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

xv. "Remote computing service," as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

xvi. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), 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 anus, genitals, or pubic area of any person.

xvii. A "storage medium" or "storage device" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

xviii. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other 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 a permanent format.

xix. A "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

IV. SUMMARY OF PROBABLE CAUSE

7. As set forth in greater detail below, Robert Quido STELLA ("STELLA"), who resides at the SUBJECT PREMISES, has been linked to an online community of individuals who use the darknet[1] with the intent to access child pornography and to sexually abuse children. STELLA used the darknet weblink Uniform Resource Locator ("URL") "365c7q5jvm5c5rbz.onion" to knowingly access "365 CP", a Child Sex Abuse Material ("CSAM") website on approximately July 13, 2020. At the time the child pornography was accessed, STELLA used Coinbase, a cryptocurrency exchange platform, to make a bitcoin transactional payment on July 13, 2020 to the wallet "1D3aQThytRGxD8xHefdhmvJqnMvHa55qhc" to gain access to "365 CP". Additionally, STELLA provided the SUBJECT PREMISES, his full name Robert Quido STELLA, email address rob.stella1@gmail.com, phone number ending in -9249, and year of birth 1972, in his transactional payment.

8. I reviewed screen captures of the Tor-Hidden-Service "365 CP" start page, which contained twelve images containing

[1] The darknet is an overlay network within the Internet that can only be accessed with specific software, configurations, or authorization. The darknet often uses a unique customized communication protocol and is most often used for file hosting and peer-to-peer file sharing with the intent of being anonymous and secure.

child pornography, also referred to as "CSAM." Based on my training and experience, a visitor to this start page would know the contents of the site before making a payment to access the site. Based on these facts, and as further set forth believe, there is probable cause to believe that evidence, fruits, or instrumentalities of the SUBJECT OFFENSES will be found at the SUBJECT PREMISES.

V. BACKGROUND ON TOR-HIDDEN-SERVICE "365 CP" USING URL HTTP://365C7Q5JVM5C5RBZ.ONION

9. On or about May 10, 2021, I received information from HSI Cyber Crimes Center (C3) regarding an investigation initiated by German Federal Criminal Police Office, Bundeskriminalamt (BKA) into Tor-Hidden-Service "365 CP:"

a. https://365c7q5jvm5c5rbz.onion is a website platform that appears to have been developed to allow users to connect online for the purposes of viewing and/or downloading CSAM.

b. To use this website, a user first uses a Tor browser, a web browser that anonymizes a user's web traffic, to access the darknet web. The user then accesses a website's URL home page by manually typing in the weblink or clicking on a hyperlink, a simple link to enter a website. A user on the darknet web or the Internet cannot unintentionally stumble upon this website. The user must make a conscious choice to first download and use special software such as the Tor browser, and then must have the unique alphanumeric string that makes up the

URL in order to find and then access the site. Based on my training and experience, Tor browser is known to be used by pedophiles as a means to mask their identities and activities.

c. When a user arrives to the website "365CP" only 12 video stills depicting child pornography with hyperlinks are displayed, along with log in and registration options. Based on my training and experience, the letters "CP" in the title of the website "365CP" likely stand for child pornography, and the display of only video stills depicting child pornography would make the purpose of the website clear to a user prior to making an account or payment.

d. When a user chooses to enter the website "365CP," the user must create an account and make a cryptocurrency payment in order to gain access to the website. After a payment is sent, the user's account will be unlocked according to the instructions on the website.

VI. STATEMENT OF PROBABLE CAUSE

10. Based on my review of law enforcement reports, conversations with other law enforcement agents, and my own knowledge of the investigation, I am aware of the following:

A. STELLA Accessed Coinbase to pay for Child Pornography on "365 CP"

11. Based on review of reports obtained from Coinbase, I learned that on or about July 13, 2020, STELLA submitted a bitcoin transactional payment of $18.58 USD to the Bitcoin wallet "1D3aQThytRGxD8xHefdhmvJqnMvHa55qhc" to gain access to the CSAM website "365 CP."

12. Additional Coinbase information provided for STELLA's transaction included - User's ID: "5a2973778cc74c0103cff2cb, User's Email: rob.stella1@gmail.com, User's Country: United States of America, Transaction Detail Transaction Type: Send, Transaction Detail Account Name: BTC Wallet, Transaction Detail Account Currency: BTC, Transaction Detail Address: 1D3aQThytRGxD8xHefdhmvJqnMvHa55qhc, Transaction Detail Transaction ID: 5f0cdbb254f6ae0311547be2, Transaction Detail Hsh: 1c056cff5155037ac686379e6eb982a81ee7c0b938b7406df0bc54420b0a4110, Name: Robert STELLA, First Name: Robert Quido, Last Name: Stella, DOB Year: 1972, Phone Number: 619-672-9249, Street Address: 17808 Maplehurst Place, City: Canyon Country, Postal Code: 91387.

13. Within "365 CP," I observed screenshots from the start page provided by BKA via HSI C3. The screenshots included 12 video stills with hyperlinks, depicting child pornography, i.e., visual depictions of a minor engaging in sexually explicit conduct, that were visible immediately once on the website's start page.

B. Identification of Robert Quido STELLA at the SUBJECT PREMISES

14. According to the California Department of Motor Vehicles ("DMV"), STELLA lists his address as the SUBJECT PRESMISES.

15. As of May 17, 2021, according to Accurint - an information database operated by LexisNexis which consolidates

public records, including addresses, phone numbers, driver's licenses, property deed transfers, corporate information, and other property records - STELLA is associated with the SUBJECT PREMISES and appears to reside at the SUBJECT PREMISES. Accurint reports also show the phone number 619-672-9249 is associated to the SUBJECT PREMISES.

16. On May 19, 2021, I served a Federal Grand Jury Subpoena on Verizon for subscriber information for phone number 619-672-9249. On May 27, 2021, Verizon responded to the subpoena with the subscriber name as Robert STELLA, and the subscriber address as the SUBJECT PREMISES.

17. On MAY 13, 2021, I conducted surveillance at the SUBJECT PREMISES and observed two vehicles parked in the driveway: a black Chevrolet sport utility vehicle bearing California license plate 8LNH985, and a dark blue Toyota Highlander bearing California handicap license plate 65097DV. According to the California Department of Motor Vehicles ("CA DMV"), both vehicles are registered to STELLA at the SUBJECT PREMISES.

VII. TRAINING & EXPERIENCE ON INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

18. As set forth above, there is probable cause to believe that an individual at the SUBJECT PREMISES conducted a bitcoin transactional payment to log into the "365 CP" website to access child pornography. Based on my training and experience, and the training and experience of other law enforcement officers

experienced in investigating crimes involving the sexual exploitation of children with whom I have had discussions, I have learned that individuals who view and possess multiple images of child pornography, including on web-based bulletin boards and file-sharing programs, are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or in other visual media; or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children often use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children may possess and maintain "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etcetera, in the privacy and security of their home or some other secure location. Individuals who keep hard copies typically retain them for many years.

d. More recently, individuals who have a sexual interest in children or images of children typically maintain their collections in a digital or electronic format. They typically maintain these collections in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence or inside the collector's vehicle, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials (including through digital distribution via the Internet); 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 child pornography. These individuals often maintain possession of these items for long periods of time.

f. Individuals who access hidden and embedded child pornography-related bulletin boards, and other forums such as newsgroups and IRC chatrooms, are typically more experienced child pornography collectors. These individuals likely would have gained knowledge about such forums through online communications with other individuals who have a sexual interest in children or images of children.

g. Individuals who have a sexual interest in children or images of children frequently prefer not to be without their child pornography for a prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

h. Child pornography received via computer is extremely mobile. Through computer technology, digital files are easily reproduced and transported. For example, with the click of a button, images and videos containing child pornography can be put onto thumb drives so small that they fit onto a keychain. Just as easily, these files can be copied onto floppy disks or compact disks, and/or stored on iPods, Blackberries, or cellular telephones. Because someone at the SUBJECT PREMISES likely collects and values child pornography, which is easily-stored and duplicated, there is probable cause to believe that evidence of a child pornography collection will be found in the SUBJECT PREMISES.

19. Furthermore, even if a person deleted any images of child pornography that may have been possessed or distributed, there is still probable cause to believe that there will be evidence of the illegal activities - that is, the possession, receipt, and/or distribution of child pornography - at the SUBJECT PREMISES or on his person. Based on my training and experience, as well as my conversations with digital forensic experts, I know that remnants of such files can be recovered months or years after they have been deleted from a computer device. Evidence that child pornography files were downloaded and viewed can also be recovered, even after the files themselves have been deleted, using forensic tools. Because remnants of the possession, distribution, and viewing of child pornography is recoverable after long periods of time, searching the SUBJECT PREMISES could lead to evidence of the child exploitation offenses.

VIII. TRAINING & EXPERIENCE IN COMPUTER-RELATED SEXUAL EXPLOITATION INVESTIGATIONS

20. Based on my training and experience, and the training and experience of other law enforcement officers experienced in investigating crimes involving the sexual exploitation of children with whom I have had discussions, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Individuals with an interest in child pornography can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when a photograph is taken, it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera can be stored on a removable memory card in the camera. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive on the camera. The video files can then be easily transferred from the camcorder to a computer.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the methods of distributing and receiving child pornography. Child pornography can be transferred via electronic mail or through FTPs to anyone with access to a computer and modem. Because of the proliferation of

commercial services that provide electronic mail service, chat services (i.e., Instant Messaging), and easy access to the Internet, the computer is a preferred method for distributing and receiving child pornography.

d. 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 (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person.

e. The Internet affords individuals many different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals can also use online resources to retrieve and store child pornography, including services offered

by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services, as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

21. As is the case with most digital technology, communications via a computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (temporary files or ISP client software, among others). 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. Such information is often maintained indefinitely until overwritten by other data.

IX. TRAINING & EXPERIENCE ON DIGITAL DEVICES[2]

22. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. A person who connects to the Internet must use a computer or mobile device, such as a tablet or wireless telephone, to facilitate that access. Furthermore, in my training and experience, these devices typically travel with a subject or remain in SUBJECT PREMISES. It is therefore reasonable to believe that computers, tablets, wireless telephones, and other electronic storage media may be present in SUBJECT PREMISES. Further, because it is possible to store certain mobile devices, such as removable storage media and wireless telephones, in a pocket, it is reasonable to believe that mobile devices may be found on the persons.

b. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the

---

[2] As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

c. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

d. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

e. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading

filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

f. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

g. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

h. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

23. The search warrant requests authorization to use the biometric unlock features of the devices seized, based on the

following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. As noted above, I know that most homes with Internet capability use only one IP address. That IP address, in turn, is often shared by many devices that access the Internet using a wireless modem. Accordingly, if there are multiple digital devices discovered during a search of the SUBJECT

PREMISES, any of those devices could have been used to access the Internet and download the files discussed above.

d. Thus, if while executing the warrant, law enforcement personnel encounter a digital device within the scope of the warrant that may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to, with respect to residents of the SUBJECT PREMISES, who are located at the SUBJECT PREMISES during the execution of the search: (1) depress the person's thumb- and/or fingers on the device(s); and (2) hold the device(s) in front of the face of the person with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

24. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

X. REQUEST FOR SEALING OF APPLICATION/AFFIDAVIT

25. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant affidavit. I believe that sealing is necessary because the items and information to be seized is relevant to an ongoing investigation into criminal conduct involving minor victims and as far as I am aware, the targets of this investigation remain unaware that they are being investigated. Disclosure of the search warrant affidavit at this time would seriously jeopardize the investigation, as such

disclosure may provide an opportunity to destroy evidence, change patterns of behavior, or allow flight from prosecution. Further, based upon my training and experience, I have learned that online criminals often search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on this continuing investigation and may severely jeopardize its effectiveness

XI. CONCLUSION

26. For all the reasons described above, there is probable cause to believe to believe that evidence, fruits, and instrumentalities of the SUBJECT OFFENSES, as described in Attachment B will be found in a search of the SUBJECT PREMISES, as described in Attachment A of this affidavit.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 8th day of July, 2021.

MAA
UNITED STATES MAGISTRATE JUDGE

Magistrate Judge Case Initiating Documents

2:21-mj-03211 USA v. Warrant

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

Notice of Electronic Filing

The following transaction was entered by Brunwin, Christopher on 7/7/2021 at 3:39 PM PDT and filed on 7/7/2021

Case Name: USA v. Warrant
Case Number: 2:21-mj-03211
Filer: USA
Document Number: 1

Docket Text:
APPLICATION for Search Warrant filed by Plaintiff USA. (Not for Public View pursuant to the E-Government Act of 2002) (Attachments: # (1) Proposed Warrant) (Attorney Christopher M Brunwin added to party USA(pty:pla)) (Brunwin, Christopher)

2:21-mj-03211-1 Notice has been electronically mailed to:

2:21-mj-03211-1 Notice has been delivered by First Class U. S. Mail or by other means BY THE FILER to :

The following document(s) are associated with this transaction:

Document description: Main Document
Original filename:N:\Brunwin, Christopher\7.7.21\Application for a Search Warrant (004).pdf
Electronic document Stamp:
[STAMP cacdStamp_ID=1020290914 [Date=7/7/2021] [FileNumber=32237076-0]
[6c8c80acce92b3d6f5a8dbe4886d97c9ab18de5af3f2597080e267d118922576c753
32ceff1ded45ffcc0f249745bd096e127fa77363613af894d3e85652c1e1]]
Document description: Proposed Warrant
Original filename:N:\Brunwin, Christopher\7.7.21\Warrant Search and Seizure Warrant (003).pdf
Electronic document Stamp:
[STAMP cacdStamp_ID=1020290914 [Date=7/7/2021] [FileNumber=32237076-1]
[af8f21d500a51bde96562eb0452658a1d611c730bd74c1d603b7aba30c20d5e19c62
49839f37d9b06cb38b40c5dc5bcc9b060431449d912cf24e029e81356553]]