SEALED

UNITED STATES DISTRICT COURT

for the
District of Arizona

COPY

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

417 N. Loma Vista Circle, Unit #202,
Mesa, Arizona, 85213

Case No. 17-6138MB

(Filed Under Seal)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

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

AS FURTHER DESCRIBED IN ATTACHMENT A-1.

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

AS SET FORTH IN ATTACHMENT B AND ATTACHMENT C.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before 5/3/17
(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m.
☐ at any time in the day or night as I find reasonable cause has been established.

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

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Any United States Magistrate Judge on Criminal duty in the District of Arizona.

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (*check the appropriate box*) ☐ for ____ days (*not to exceed 30*)
☐ until, the facts justifying, the later specific date of _____.

Date and time issued: Apr. 19, 2017 @ 4:45 p.m.

Judge's signature

David K. Duncan

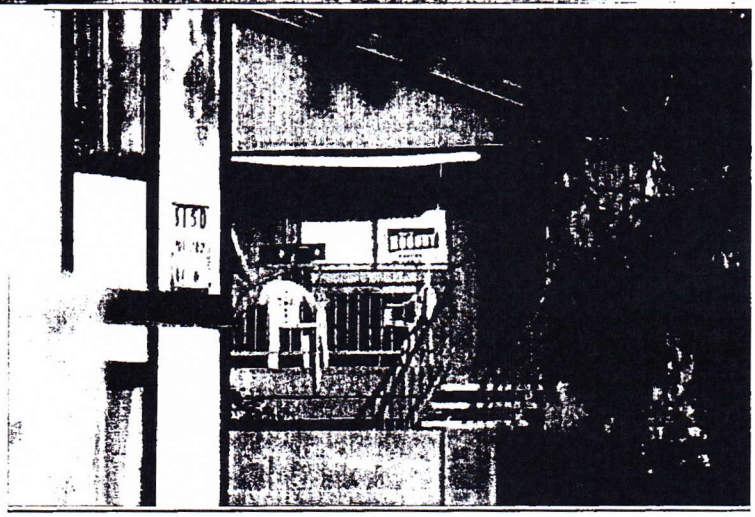
City and State: Phoenix, Arizona

Honorable John Z. Boyle, United States Magistrate Judge
Printed name and title

ATTACHMENT A-1

DESCRIPTION: LOCATION TO BE SEARCHED:

AN APARTMENT UNIT located at **417 N. Loma Vista Circle, Unit #202, Mesa, Arizona, 85213** (hereinafter referred to as "**LOMA VISTA RESIDENCE**"). This is a multi-unit, two-story apartment complex located on the northeast corner of the intersection of N. Loma Vista Circle / E. Cicero Street. Specifically, Unit #202 is located on the second story, far south end of the complex. Unit #202 is the first unit located at the top of the most southern staircase. The front door to the unit faces west and has a tan in color metal security door. At the time of this writing, there is a piece of white paper in the front window to the unit with the numbers "#202" printed in black.



ATTACHMENT B

THINGS TO BE SEARCHED FOR AND SEIZED

EVIDENCE, FRUITS, AND INSTRUMENTALITIES OF CRIMINAL OFFENSES

Agents are authorized to search for and seize evidence of violations of Title 18 U.S.C. §1956(a)(3)(B) and (C) (Conceal or disguise the nature, location, source, or ownership of proceeds of unlawful activity being represented by a law enforcement officer)(Avoid transaction reporting requirements), Title 18 U.S.C. §1960 (Operation of unlicensed money transmitting business), and Title 21 U.S.C. §846 (Conspiracy to Distribute a Controlled Substance);

1. Heroin, Cocaine, Methamphetamine, or any other illicit drug.

2. United States Currency or currency of any nation, coins, precious metals, Digital currency including Bitcoin, Ethereum, Dash, or other digital coin "altcoin", and any other financial instruments believed to be proceeds of money laundering or drug sales, including any containers, devices, or secret compartments capable of holding the same.

3. Bank documents and records, financial documents and records, and any and all records and documents relating to any bank or financial transactions, including ~~but not limited to~~: digital Bitcoin transactions, correspondence, signature cards and applications for all credit card accounts, investment accounts, and retirement accounts; copies of monthly, quarterly, yearly and/or periodic account statements for all such accounts; copies of check journals, check ledgers, checkbooks, deposit

tickets, deposit items, credit memos, debit memos, canceled checks, loan applications, and/or any related financial statements, and/or mortgage and/or promissory notes for all such accounts; copies of loan ledger accounts; copies of annual loan statements; application for bank drafts, cashier's checks, and foreign drafts, with associated copies of canceled checks, check registers, safe deposit box records and keys, wire transfer receipts, money order receipts and purchases, and records relating to employment, wages earned and paid, business income earned, and other compensation records.

4. Books, records, receipts, notes, ledgers, correspondence and other papers relating to the transportation, ordering, purchase, and distribution of controlled substances, or the laundering of proceeds.

5. Any and all monetary related customer lists, dealer lists, or any notes containing the individual names of such persons, telephone numbers and/or addresses of these customers or dealers, any corresponding records of accounts receivable, money paid or received, drug supplied or received, cash supplied or received, and digital currency supplied or received.

6. Papers, tickets, notes, receipts, and other items relating to domestic and international travel, including ~~but not limited to~~, appointment calendars, receipts, notes, letters, airline tickets, bus tickets, food receipts, hotels, and/or other lodging receipts, related correspondence, envelopes, and opened and unopened mail.

7. Books, records, invoices, receipts, correspondence, records of real estate transactions

and documents showing ownership of real estate, vehicles, bank statements and related records, passbooks, money drafts, letters of credit, money orders, bank drafts, cashiers' checks, bank checks, loan applications, safe deposit box keys, money wrappers, and other items evidencing the obtaining, secreting, transfer, and/or concealment of assets and the obtaining, secreting, transfers, concealment and/or expenditure of money.

8. Address and/or telephone books, Rolodex indices and any papers reflecting names, addresses, telephone numbers, pager numbers, fax numbers and/or telex numbers of co-conspirators, sources of supply, customers, financial institutions, and other individuals or businesses with whom a financial relationship exists or which indicate a criminal association between co-conspirators.

9. Indicia of occupancy, residency, rental and/or ownership of the premises described herein, including, utility and telephone bills, canceled envelopes, rental purchase or lease agreements, and keys.

10. Indicia of ownership or control over any vehicles or aircraft including, ~~but not limited to,~~ titles, registrations, receipts, repair bills, and keys belonging to that vehicle.

11. Items and/or documents evidencing the expenditure of the proceeds of money laundering or drug distribution including, ~~but not limited to~~, real estate, vehicles, aircraft, clothing, furniture, jewelry, art work, and electronic equipment.

12. Copies of income tax returns, workpapers, profit and loss statements, and related correspondence concerning Thomas COSTANZO or Peter STEINMETZ and any

other entities under the name of Thomas COSTANZO, Peter STEINMETZ, Morpheus Titania, or Amideo.

13. Items used for identification, including identification cards under fictitious names, and any other type of false identifying documents.

14. Any telephone, cellular telephone, tablet, computer, USB storage device, electronic digital currency storage devices, or digital display device found in the locations to be searched, including any electronically stored data found in the same, including, ~~but not limited to, d~~ata regarding outgoing calls, incoming calls, missed calls, phone book memory data, contact names and numbers, call details including call history, electronic mail (email) messages, text messages and text message history, encrypted messaging applications, virtual currency applications, crypto-currency wallet applications, and all digital images, as well as listening to, noting and recording any messages or recordings left on any telephone answering device or recording device found in the location to be searched.

15. ~~Firearms and ammunition, including handguns, pistols, revolvers, rifles, shotguns, machine-guns and other weapons purchased with illegal proceeds and/or used~~ to protect and facilitate illegal currency transactions, ~~and any records or receipts~~ pertaining to firearms and ammunition~~.~~

16. Photographs, identification cards, address books or similar items which indicate a criminal association between co-conspirators.

17. Packaging material, shipping material, shipping labels, shipping postage, and any other paraphernalia related to the use and/or distribution of controlled substances.

18. Drug paraphernalia or other items used for possessing, processing, testing, packaging, weighing, transporting, concealing, purchasing, selling, or ingesting illegal controlled substances.

19. Safes or storage containers where co-conspirators would store, place, or keep records, documents, and/or information of illegal business transactions.

20. For any computer, computer hard drive, external hard drives, disk, USB data stick, electronic digital currency storage device, or other physical object upon which computer data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

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

    b. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

    c. Evidence of the lack of such malicious software;

d. Evidence of communication on TOR darknet websites and the use of the digital crypto-currency Bitcoin or other "Altcoin";

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

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

g. Evidence of the times the COMPUTER was used;

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

i. Documentation and manuals that may be necessary to access the COMPUTER or conduct an examination of the COMPUTER;

j. Contextual information necessary to understand the evidence described in this attachment;

k. Computer software which may have been used to create, access, modify or to otherwise interact with the stored files. Computer software is digital information which can be interpreted by a computer and any of its related components to direct the way they work. It commonly includes the operating systems, applications (like word-processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs;

l. Any peripheral equipment used to facilitate the transmission, creation, display, encoding or storage of records, including word processing equipment,

modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners.

m. Records and things evidencing the use of the Internet to facilitate the distribution of illicit drugs and laundering of monetary instruments, including:

i. Routers, modem, and network equipment used to connect computers to the Internet;

ii. Records of Internet Protocol addresses used;

iii. Records of 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.

As used herein, the terms "records," "documents," and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); and any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing).

Furthermore, all electronic items listed above may be searched, examined, and/or imaged by investigators forensically to obtain information related to items described above. Reference is made to ATTACHMENT C for further information on the technical examination of electronic devices.

ATTACHMENT C

TECHNICAL TERMS

1. Based on your Affiants training and experience, I use the following technical terms to convey the following meanings:

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

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

c) Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, floppy disks, flash memory, CD-ROMs, and several other types of magnetic or optical media not listed here.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

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

3. Your Affiant submits that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

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

   b) Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In

addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

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

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

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

a) Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a

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

b) Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

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

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

e) Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

5. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss

of the data either from accidental or intentional destruction. This is true because of the following:

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

b) Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

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

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