UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

No. 17mj02572-JG

UNITED STATES OF AMERICA

v.

JOSHUA J. KELLY,
a/k/a, "USTOUS,"

Defendant.
_____/

CRIMINAL COVER SHEET

1. Did this matter originate from a matter pending in the Northern Region of the United States Attorney's Office prior to October 14, 2003? ____ Yes __X__ No

2. Did this matter originate from a matter pending in the Central Region of the United States Attorney's Office prior to September 1, 2007? ____ Yes __X__ No

Respectfully submitted,

WIFREDO A. FERRER
UNITED STATES ATTORNEY

BY: _____

FRANCISCO R. MADERAL
ASSISTANT UNITED STATES ATTORNEY
Fla. Bar. No. 41481
99 N. E. 4th Street
Miami, Florida 33132-2111
TEL (305) 961-9159
FAX (305) 530-7976
francisco.maderal@usdoj.gov

AO 91 (Rev. 08/09) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Southern District of Florida

United States of America
v.
JOSHUA J. KELLY, a/k/a, "USTOUS,"

Case No. 17mj02572-JG

Defendant(s)

CRIMINAL COMPLAINT

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

On or about the date(s) of 9/2016-12/2016 in the county of Miami-Dade in the Southern District of Florida, the defendant(s) violated:

Code Section	*Offense Description*
Title 21, United States Code, Sections 846 & 841(b)(1)(c)	Conspiracy to Distribute Controlled Substances
Title 18, United States Code, Sectiona 1956(h) & 1956(a)(1)	Conspiracy to Committ Money Laundering

This criminal complaint is based on these facts:

SEE ATTACHED AFFIDAVIT.

☑ Continued on the attached sheet.

Complainant's signature

Lilita Infante, S/A, DEA
Printed name and title

Sworn to before me and signed in my presence.

Date: April 25 2017

Judge's signature

City and state: Miami, Florida

Jonathan Goodman, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT

I, LILITA INFANTE, Special Agent with the Drug Enforcement Administration, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18 of the United States Code. That is, I am an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516(1), and in Title 21, United States Code, Sections 846 and 878.

2. This affidavit is made in support of a criminal complaint charging Joshua J. KELLY, a/k/a, "USTOUS," with conspiracy to distribute in narcotics in violation of Title 21, United States Code, Section 846, and conspiracy to launder money, in violation of Title 18, United States Code, Section 1956(h).

3. I have not necessarily included in the affidavit each and every fact known to me about the matters set forth herein, but only those facts and circumstances that I believe are sufficient to establish probable cause for the Court to sign a criminal complaint.

4. The statements contained in this affidavit are based upon my investigation, information provided by other sworn law enforcement officers and on my experience and training as a federal agent and the experience and training of other federal agents.

PROBABLE CAUSE

5. This application stems from an ongoing criminal investigation into drug dealers operating on criminal online marketplace websites, including a website known as the Valhalla Market.

6. In the course of this investigation, I have learned that the Valhalla Market website is one of many The Onion Router ("Tor") network or "dark web" criminal marketplaces. The Valhalla Market is designed to promote the anonymous sale of illegal items, such as narcotics, in exchange for Bitcoin and other, peer-to-peer crypto-currencies (also known as, virtual currencies).

7. As set forth in more detail below, probably cause exists that KELLY is trafficking in narcotics and laundering in the proceeds of his activities using the Bitcoin and the dark web, in conspiracy with the unknown administrator(s) of the Valhalla Market.

A. THE TOR NETWORK AND THE "DARK WEB"

8. The Internet is a global network of computers and other devices. Devices directly connected to the Internet are identified by their unique IP address. This number is used to route information between devices. Generally, when one device contacts a second device, the first device must be directed to the IP address of the second device. Moreover, when the first device contacts the second device, the first device provides its own IP address to the second device, so that the second device knows where to direct its response. Accordingly, the two connected devices (for instance, a home computer and the www.google.com website server) know each other's IP address.

9. The typical user may not know the IP address of a websites he visits. Typically, a user will type the domain name of the website—which commonly corresponds to a plain-language name for the website, *e.g.,* www.google.com—into the Uniform Resource Locator ("URL") bar at the top of their web browsers. This domain name will be transmitted to a Domain Name System ("DNS") server, which then translates the domain name into the appropriate numerical IP address, and thereby allows the user to connect with the requested website.

10. However, if a user knows of a unique IP address for a particular website, generally[1] the user can type that IP address directly into the URL bar and access the website in that manner.

11. In addition, publicly available databases can be easily searched to obtain the IP address for any known URL and the registered owner and location of any IP address. Thus, with additional inquiry, most any URL or IP address can be traced to its owner and physical location.[2] This is problematic for anyone conducting criminal activity on the internet and wishing to remain anonymous.

B. User Anonymity Provided by the Tor Network

12. The Onion Router (Tor) network is a special network of computers distributed around the world designed to conceal the true IP addresses of the users of the network. Every communication sent through Tor is directed through numerous relays within the network—and wrapped in a layer of encryption at each relay—such that the end recipient of the communication has no way of tracing the communication back to its true originating IP address.

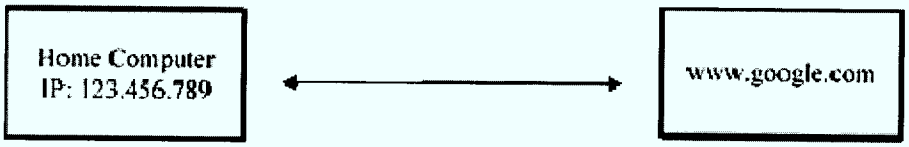
---

[1] The server or virtual server with a particular IP address can host multiple websites, in which case entering that particular IP address would not direct a user to a single website. However, if an IP address is associated with a single website, entering the IP address as described above would direct the user to that particular website.

[2] Private individuals operating home computers usually do not own and register their own IP address; instead, they subscribe to broadband accounts with ISPs, such as Comcast or AT&T, which in turn assign or lease an IP address to them (the subscriber). Nevertheless, the IP address can usually be traced to its assigned user at a given point in time using the ISPs records of which subscriber was assigned which IP address and when.

13. In order to access the Tor network, anyone can simply download the Tor browser software and use it to access the internet. The user simply inputs a website IP address or URL into the Tor browser and the Tor browser automatically encrypts and routes the communication through several relays and then out to the destination so that the destination website can only see the IP address of the last (or "exit") relay and not the IP address of the device actually connecting to the destination website.

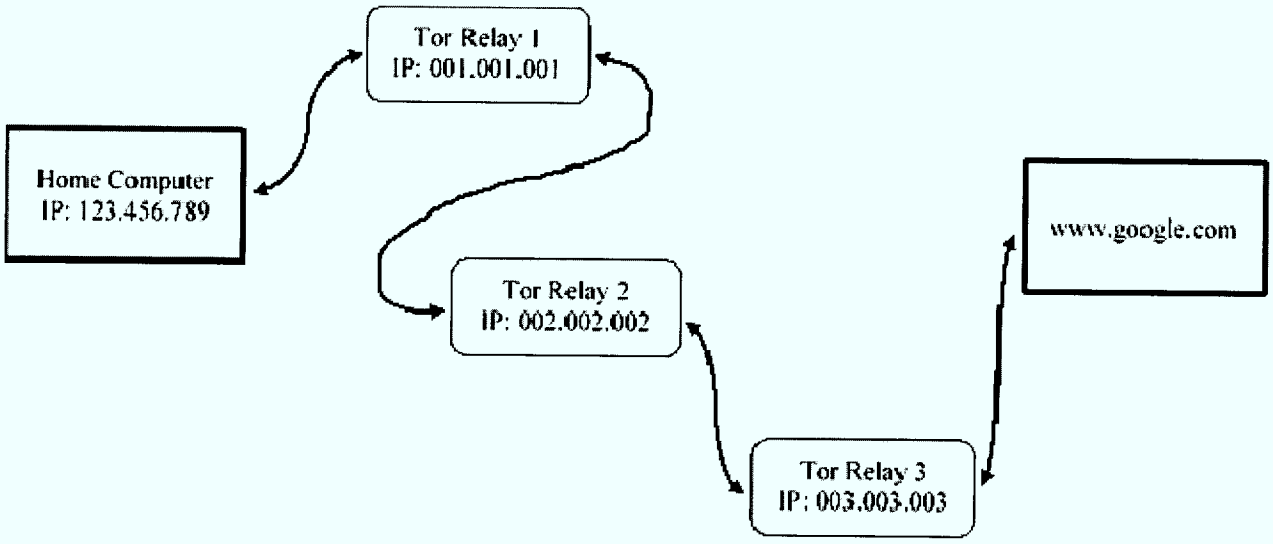
14. By way of illustration, in a standard internet communication, when a person connects to a website, that website can see that persons IP address:



In this illustration of a standard internet connection, the website www.google.com can see the home computer IP address (123.456.789) and, of course, the user of the home computer knew the URL, and therefore the IP address, of www.google.com, which the user had to type into his browser to connect to the website in the first place. Thus, each users' IP address is known to the other, and the owner and location of both can later be traced.

15. Similarly, any person monitoring the internet traffic at a point between the two would see the connection between IP 123.456.786 and www.google.com and know that those two devices were communicating.

16. On the other hand, in the case of a Tor network communication, when a person connects to a website, the traffic is encrypted and routed through multiple relays, and that website cannot see that persons IP address:



In this illustration of a Tor network connection, the website www.google.com cannot see the home computer IP address (123.456.789); instead it only sees the IP address of the device it is directly connected to, the third (or "exit") Tor relay, with IP address 003.003.003, which IP address cannot be traced back to the home computer user.

17. In addition, any person monitoring the internet traffic at a point between the home computer and www.google.com and would not know that those two devices were communicating. Instead, depending on the monitoring point, that person would only see the direct connections between the home computer and first (or "entry") Tor relay, between the first and second, or second and third Tor relays, or between the third (or "exit") Tor relay and www.google.com.

18. As with a standard internet connection, the user must have known the URL or IP address of the website in order to have directed a connection to it through the Tor network.

Accordingly, although the IP address of the user is hidden from the website, the IP address of the website must be known to the user—the anonymity is only one-way.

19. The Tor network addresses this problem through a feature known as "hidden services."

C. Hidden Services: Website Anonymity Provided by the Tor Network

20. To achieve true, two-way anonymity, the Tor network also enables websites to operate inside the network in a manner that conceals the true IP address of the computer server hosting the website. Such "hidden services" operating on Tor have complex web addresses, generated in a computer algorithm, ending in ".onion." Unlike a standard URL, there is no way to retrieve a website server's true IP address from its .onion Tor address alone.

21. This alleviates the need for a Tor network user to know the true IP address of a website. Rather the user can direct his Tor browser to the .onion address, reach the website, and neither the user nor the website knows the other's IP address—two-way anonymity is achieved. This network of anonymous users and websites is the "Dark Web."

22. Criminals have taken advantage of the Dark web to create websites with online marketplaces dedicated to the trafficking of controlled substances and other illicit goods. Websites such as www.deepdotweb.com maintain an overview of illegal marketplaces operating on the Dark Web, and how-to guides such as: "How to Buy Drugs Online from Darknet Markets."[3]

[3] https://www.deepdotweb.com/2015/12/30/buy-drugs-online-from-darknetmarkets/

D. Description of the Valhalla Market

23. Valhalla provides an infrastructure that allows buyers and sellers to conduct transactions online, in a manner similar to well-known online marketplaces such as eBay. Like eBay:

a. Valhalla functions as an intermediary between buyers and sellers. Sellers create accounts on Valhalla to advertise their products, such as narcotics or hacked computer passwords, and buyers create accounts to browse sellers' products and purchase them; in this regard, Valhalla's website interface is similar to well-known online marketplaces;

b. Valhalla performs moderator and maintenance services, such as receiving complaints, providing technical assistance, and allowing customers to post reviews of Valhalla vendors. Valhalla also provides a means by which its users can communicate with its administrators and operators; and

c. Valhalla charges a commission from every transaction as a percentage of the sale price.

24. However, unlike legitimate online marketplaces, Valhalla is dedicated and designed to facilitate the sale of illegal narcotics and drug paraphernalia. For example:

a. Illegal drugs, such as methamphetamines, heroin, and cocaine, are openly advertised and sold and are immediately and prominently visible on the Valhalla website.

b. The Valhalla website is specifically designed to facilitate illegal commerce by working to ensure the anonymity of its administrators, as well as of the buyers and sellers who participate in commerce on the website. The website is designed to achieve this anonymity primarily by operating as a hidden service on the Tor network.

c. To further promote anonymity, purchases are made primarily in bitcoin (or other virtual currency) using Valhalla's escrow services, i.e., a buyer transfers funds from his or her own account or virtual-currency wallet into an Valhalla account or wallet, and Valhalla subsequently transfers the funds to the seller's account or wallet upon satisfaction of the terms of sale. In doing so, Valhalla also provides a "tumbling" or "mixing" service which essentially scrambles multiple buyer-seller Bitcoin transactions together in order to conceal the bitcoin payments from buyer to seller or commission payments to the administrator. Thus, there is no direct bitcoin transaction between the buyer and the seller.

25. The true identity of the individual or individuals who control and operate the Valhalla website, *i.e.*, the administrator(s), is unknown.

E. "USTOUS" Vendor on Valhalla and Other Dark Web Markets

26. Since at least October of 2015, agents identified a narcotics vendor, known as "USTOUS," appearing on numerous dark web marketplaces, including Alphabay, Valhalla, and Middle Earth. On several occasions, DEA agents have made undercover online purchases of heroin, alpha-PVP ("Flakka") and MDMA from "USTOUS" and received the drugs via U.S. Mail, shipped to undercover mailboxes in Miami, Florida. For instance:

a. On October 14, 2015, DEA agents purchased one half of a gram of heroin from "USTOUS" on the Middle Earth Market for 0.2749 bitcoins. In the description, USTOUS stated: "Half Gram Uncut Raw H Number 3;" and,

b. On December 6, 2016, DEA agents purchased 10 pills of alpha-PVP and 10 pills of MDMA from "USTOUS" on the Valhalla Market for 0.05250935 BTC and 0.07679129 BTC respectively. In the description for alpha-PVP, USTOUS stated: "Blue Wrecked Benz Mega Speed Press," containing "Ethylone, A-PVP, Hexadron and AMP salts." In

the description for the MDMA, USTOUS stated: "Zen Sea Blue Ferraris," containing "awesome combo of MDMA and Benzo."

27. In both instances, the controlled substances were shipped via United States Priority Mail to Miami, Florida with respective return addresses in Saint Louis and Festus, Missouri. Laboratory results have confirmed the items referenced in paragraph (a) contained heroin and the items referenced in paragraph (b) contained alpha-PVP and MDMA.

28. "USTOUS" has conducted thousands of transactions on numerous Dark Web marketplaces, including: Alphabay Market with at least 7,519 transactions, Valhalla with at least 140 transactions, Middle Earth Market with at least 159 transactions.[4] On all of these marketplaces, "USTOUS" advertised dangerous opioids, synthetic drugs and Schedule II controlled substances for sale, including: fentanyl, heroin, methamphetamine, alpha-PVP and oxycodone.

---

[4] DEA was able to confirm that "USTOUS" is the same vendor on Valhalla and Alphabay Market by confirming that in each instance "USTOUS" was advertising the same public encryption key and signature. Persons who are involved with Dark Web narcotics trafficking utilize public key encryption to communicate with other purchasers and sellers on the marketplace in order, for instance, to provide information such as a shipping address. If the message was not encrypted, it would be visible by the administrators of the Dark Web marketplace, and by law enforcement, if the marketplace server was ever located and seized. Public key encryption allows the sender of a message to encrypt that message using a long passcode known as a public key, which the recipient of the message publicly provides to anyone wishing to communicate with them. That message, in turn, can only be decrypted by the recipient using a corresponding private key known only to them. The most commonly used encryption is that known as Pretty Good Privacy (PGP) encryption. Almost all Dark Web marketplace vendor profiles advertise a public PGP key for this purpose; the PGP key, therefore, doubles as a unique fingerprint visible across dark web platforms.

29. Regarding Valhalla in particular, a review of "USTOUS's" profile obtained on December 5, 2016 revealed that USTOUS distributed controlled substances on Valhalla at least from September 2016 to December 2016.

F. KELLY & KELLY Business Associated with "USTOUS"

30. Since the time of the first controlled purchase from "USTOUS" on October 14, 2015, DEA and other law enforcement agents have been able to identify KELLY as "USTOUS" by analyzing the shipping records associated with the drug package shipped to DEA via the United States Postal Service (USPS).

31. USPS records revealed that the first undercover drug purchase was shipped using postage purchased at "Endicia.com," an online company which allows its customers to print their own stamps and shipping labels.

32. Endicia.com records revealed that the Endicia.com account used by "USTOUS" to ship the drugs to UC agents was accessed from IP address 97.91.242.30 belonging to internet service provider Charter Communications and used Vanilla prepaid debit cards to purchase $9,433 worth of postage for shipments all over the United States from September 9, 2015 to September 8, 2016. A Subpoena of Charter Communications revealed that the IP address 97.91.242.30 is being utilized exclusively by internet service subscriber HEADY WAREZ with service address located at 1802 Broadway St., Cape Girardeau, MO. A public database search revealed that HEADY WAREZ is a smoke shop business owned by KELLY.

33. A search of Missouri Department of Revenue revealed that KELLY lists the aforementioned HEADY WAREZ address as his residential and mailing address on his Missouri driver's license.

34. On August 19, 2016, DEA agents conducted a trash pull at the HEADY WAREZ trash bin. During the trash pull, agents recovered 26 pieces of paper with various handwritten acronyms, colors and numbers, such as "10 yellow Benz", "85 Xan", "10 OC 40 orange", "6 D&G." These acronyms closely matched "USTOUS" drug listings on Valhalla Market and Alphabay Market, such as, "300mg GOLD BENZ SPEED BALL," "OC 40 Dark Orange Formula # 3.3 (new FENT BLEND!), "D&G Trio of Terror Blue RC (cocaine like + small DXE) presses," "WHITE DICES XANAX PRESS 3 BENZO COMBO." Based on my training and experience, as well as the listing descriptions provided by "USTOUS", the acronym "Benz" stands for controlled substance benzodiazepine, OC 40 stands for Oxycodone 40mg, "Xan" stands for Xanax.

G. Tor Network Activity from HEADY WAREZ

35. In order to determine whether KELLY, or some other narcotics-trafficking co-conspirator, was accessing criminal, Dark Web marketplaces from the HEADY WAREZ internet connection, law enforcement began monitoring the internet traffic to and from the IP address associated with HEADY WAREZ Charter Communications internet service.

36. As discussed above, because of the anonymity provided by the Tor network such monitoring would not reveal the ultimate IP address of devices communicated with through the Tor network. However, such monitoring could reveal connections to computers generally associated with the Tor network as relays (or "Tor Nodes") which are the computers and servers designated by the administrators of the Tor network to route communications through the encrypted Tor network.

37. For example, monitoring the IP connections of a computer connecting to Valhalla through Tor, will not reveal any specific IP address associated with Valhalla. Rather such

monitoring could[5] reveal connections to computers generally associated with the Tor network as "Tor Nodes," which are the computers and servers designated by the administrators of the Tor network to route communications through the encrypted Tor network.

38. A computer attempting to connect to the Tor network must know how to contact a Tor Node in order to initiate a Tor network session, and Tor Node IP addresses are publicly available, open source information on websites such as: https://exonerator.torproject.org.

39. Therefore, monitoring the traffic of the IP address of someone suspected of using the Tor network could reveal connections to IP addresses publicly associated with computers and servers known to operate as Tor Nodes.

40. On January 26, 2017, the DEA obtained a pen/trap order for all internet traffic to and from the Charter Communications IP address utilized by HEADY WAREZ. The pen/trap order results obtained through March 27, 2017 reveal internet connections from the HEADY WAREZ IP address to known Tor Nodes and, therefore, the Tor network, which is consistent with someone logging on to the criminal, Dark Web marketplaces, such as Valhalla, through the Tor network, from a computer located within HEADY WAREZ business location.

H. KELLY Residence Associated with "USTOUS"

41. On August 5, 2016, a United States Postal Inspector (USPI) informed DEA agents that a parcel from Shanghai, China was destined for Joshua KELLY at 2806 Lynwood Hills Drive, Cape Girardeau, Missouri a single-family home (hereinafter "KELLY Residence"). From August 2016 to January 2017, DEA agents conducted multiple surveillances of Joshua KELLY

---

[5] This would not necessarily be the case if the person was adding an additional layer of anonymity, such as a virtual private network (VPN) connection, between them and the Tor network.

at the KELLY Residence. On August 9, 2016, DEA agents conducted a trash pull at the trash receptacle belonging to the KELLY Residence. Inside the trash receptacle, agents seized multiple pieces of paper with various handwritten acronyms, colors and numbers, such as "7 OC 40 Orange," "3 D&G" and "6 Yellow Benz," matching "USTOUS" drug listings and similar to the ones found previously in the trash receptacle at HEADY WAREZ. In addition, the trash contained a shipping label created with the same Endicia.com shipping account that was utilized by "USTOUS" to mail drugs to DEA agents. The destination name and address matched the Endicia.com records of shipment on August 5, 2016. Also seized from the trash were a syringe containing liquid THC, miscellaneous mail, to include a package addressed to HEADY WAREZ, a handwritten note to "Joshua," mylar bags and vacuum sealed bags with traces of marijuana. The vacuum sealed bags matched the bags that contained the drugs received by DEA agents in the mail from "USTOUS."

42. On August 16, 2016, DEA agents conducted another trash pull at the KELLY Residence trash receptacle. During the trash pull, agents recovered a Vanilla prepaid debit card bearing the same card number as the one used by the "USTOUS" Endicia.com shipping account to purchase stamps. In addition, agents recovered multiple pieces of paper with various handwritten acronyms, colors and numbers, such as "10 OC 40 Orange" and "75 Xan," matching "USTOUS" drug listings and similar to the ones found previously in the trash receptacle at HEADY WAREZ and the KELLY Residence.

43. Other items seized from the KELLY Residence trash include multiple parcels from China and Canada, Ziploc bags containing residue of cellulose, and an envelope containing residue of calcium sulfate. Based on my training and experience, cellulose is used to

manufacture pharmaceutical tablets to make tablets hard and stable, giving them "bulk", and assisting in absorption. Calcium sulfate is used as a binding material for tablets.

44. On August 23, 2016, DEA agents conducted another trash pull at the KELLY Residence, resulting in the seizure of a Ziploc bag containing alpha-PVP ("Flakka") residue, vacuum sealed and mylar bags, receipts from HEADY WAREZ and KELLY's bank account deposit slips.

I. KELLY Residence # 2 Intercepted Shipment

45. On February 28, 2017, DEA agents observed a moving truck departing the KELLY Residence and arriving at 2053 Stevens Drive in Cape Girardeau, MO [hereinafter KELLY Residence # 2.]

46. On March 1, 2017, DEA agents observed a vehicle registered to KELLY parked in the driveway of KELLY Residence # 2 and another vehicle registered to Jeanette KELLY – KELLY's mother.

47. A public utility check on the KELLY Residence revealed that all utilities were changed from KELLY's name to the name of the landlord of the KELLY Residence. The utilities at KELLY Residence # 2 were registered under Jeanette KELLY on February 27, 2017.

48. On March 28, 2017, Homeland Security Investigations agents intercepted a parcel from Singapore destined for Jeannette KELLY at KELLY Residence # 2. A border search of the parcel revealed 2 round die molds and 4 metal parts for a pill press with a letter V, numbers 48-12, letter A and numbers 215. A search of pharmaceutical markings revealed that V 48-12 is the marking used by Oxycodone manufacturer Qualifest Pharm on 30mg Oxycodone tablets and the marking A 215 is used by Oxycodone manufacturer Actavis on 30mg Oxycodone pills.

49. Records from KELLY's personal Ebay buyer account indicate that in the past, KELLY purchased a TDP-5 tablet press, powder mixers and multiple die molds for Oxycodone, Norco, and Xanax.

J. Bitcoin Analysis

50. Analysis of KELLY's financial records revealed that KELLY has a bitcoin account with Coinbase—a bitcoin wallet host and exchanger. KELLY's Coinbase account is linked to his personal checking account and his business checking account under the business name Ligons & Kelly Enterprise.LLC at Wood & Huston Bank. Coinbase records revealed that in the span of three months from September 7th, 2015 to December 14th, 2015, KELLY received bitcoins equivalent to $42,161.62 from external bitcoin addresses, exchanged them to United States dollars and transferred to the aforementioned linked bank accounts. Analysis of the bitcoin block chain revealed that the majority of the external addresses that sent bitcoins to KELLY's Coinbase account belonged to dark web markets, such as Alphabay Market and Abraxas Market.

CONCLUSION

51. Based on the foregoing, probable cause exists that:

a. Joshua J. KELLY, did, at least from September 2016 to December 2016, conspire with the unknown administrator(s) of Valhalla, to distribute controlled substances, including alpha-PVP, MDMA, heroin, oxycodone and fentanyl in violation of Title 21, United States Code, Section 846.

b. Joshua J. KELLY, did, at least from September 2016 to December 2016 conspire with the unknown administrator(s) of Valhalla, to knowingly conduct financial transactions, in bitcoins, involving the proceeds of unlawful narcotics trafficking activities, knowing that the transaction was designed to conceal and disguise the nature of the proceeds, in violation of Title 18, United States Code, Section 1956(h) and 1956(a)(1).

Respectfully submitted,

LILITA INFANTE, SPECIAL AGENT
DRUG ENFORCEMENT ADMINISTRATION

The contents of this written affidavit were subscribed and sworn before me on April 25, 2017.

HONORABLE JONATHAN GOODMAN
UNITED STATES MAGISTRATE JUDGE