

AO 91 (Rev. 08/09) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Southern District of Florida

United States of America )

v. )

CHRISSANO S. LESLIE, a/k/a, "Owlcity," )

Case No. 16-6339-SNOW )

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 3/6/2016-July 27, 2016 in the county of Broward in the Southern District of Florida, the defendant(s) violated:

Table with 2 columns: Code Section, Offense Description. Rows include Title 21, United States Code, Sections 846 & 841(b)(1)(c) for Conspiracy to Traffic in Controlled Substances, and Title 18, United States Code, Sectiona 1956(h) & 1956(a)(1) for Conspiracy to Committ Money Laundering.

This criminal complaint is based on these facts: SEE ATTACHED AFFIDAVIT.

Continued on the attached sheet.

Handwritten signature of Lilita Infante, S/A, DEA. Printed name and title below.

Sworn to before me and signed in my presence.

Date: 7/27/16

Handwritten signature of Lurana S. Snow. Judge's signature.

City and state: Ft. Lauderdale, Florida Lurana S. Snow, United States Magistrate Judge

**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, Section 878.

2. This affidavit is made in support of a criminal complaint charging Chrissano LESLIE, a/k/a "Owlcity," with conspiracy to traffic 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 Alphabay Market.

6. In the course of this investigation, I have learned that the Alphabay Market website is one of many The Onion Router (“Tor”) network or “dark web” criminal marketplaces. The Alphabay 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, probable cause exists that LESLIE 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 Alphabay Market.

### **I. 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](http://www.google.com) website server) know each other’s IP address.

9. The typical user may not know the IP address of a website 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](http://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<sup>1</sup> 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.<sup>2</sup> This is problematic for anyone conducting criminal activity on the internet and wishing to remain anonymous.

#### **A. 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.

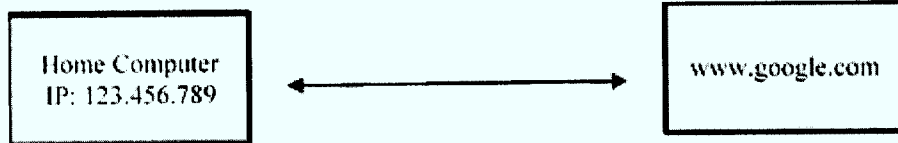
---

<sup>1</sup> 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.

<sup>2</sup> 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.

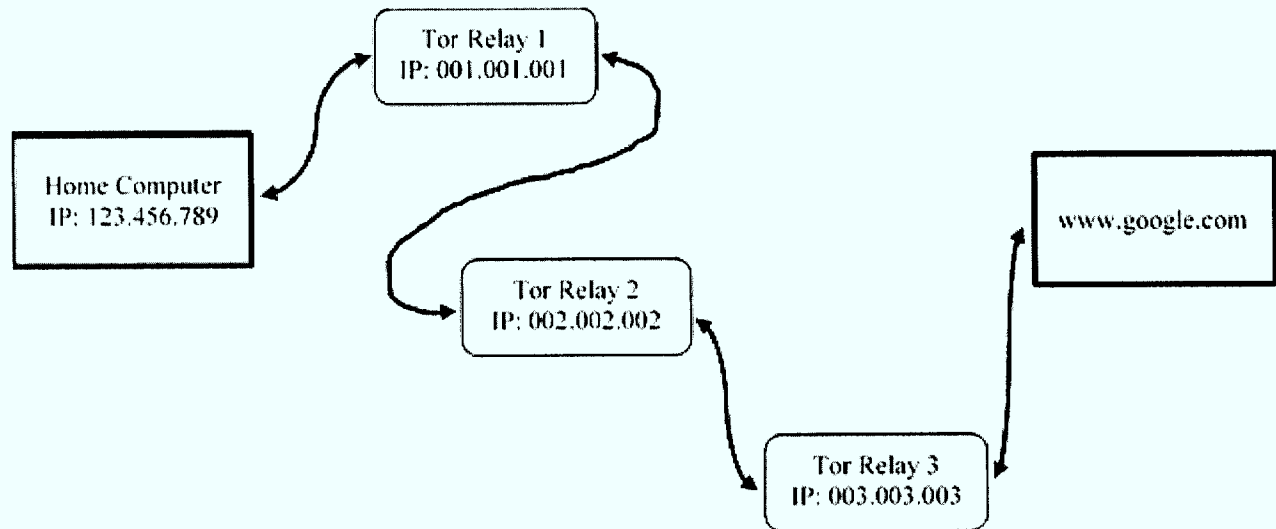
14. By way of illustration, in a standard internet communication, when a person connects to a website, that website can see that persons IP address:



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](http://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](http://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](http://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.”

**B. 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](http://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.”<sup>3</sup>

---

<sup>3</sup> <https://www.deepdotweb.com/2015/12/30/buy-drugs-online-from-darknetmarkets/>

### C. Description of the Alphabay Market

23. Alphabay 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. Alphabay functions as an intermediary between buyers and sellers. Sellers create accounts on Alphabay 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, Alphabay's website interface is similar to well-known online marketplaces;

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

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

24. However, unlike legitimate online marketplaces, Alphabay is dedicated and designed to facilitate the sale of illegal narcotics, drug paraphernalia, firearms, and counterfeit and fraud-related goods and services. For example:

a. Illegal drugs, such as methamphetamines, heroin, and cocaine, are openly advertised and sold and are immediately and prominently visible on the Alphabay website. Some of the item categories listed on the Alphabay website are: "Fraud," "Drugs & Chemicals," "Counterfeit Items," "Weapons," and "Software & Malware";

b. The Alphabay 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 Alphabay's escrow services, i.e., a buyer transfers funds from his or her own account or virtual-currency wallet into an Alphabay account or wallet, and Alphabay subsequently transfers the funds to the seller's account or wallet upon satisfaction of the terms of sale. In doing so, Alphabay 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 Alphabay website, *i.e.*, the administrator(s), is unknown.

**D. "OWLCITY" Vendor on Alphabay and Other Dark Web Markets**

26. Since at least July of 2015, agents with the DEA have been investigating a narcotics vendor, known as "OWLCITY," appearing on several criminal Dark Web marketplaces. On several occasions, DEA agents have made undercover online purchases of controlled substances from OWLCITY and received the purchased narcotics, to include fentanyl, heroin, and alpha-PVP, via U.S. Mail, shipped to undercover mailboxes. For instance:

a. On July 23, 2015, DEA agents purchased 2.5 grams of Alpha-PVP from vendor "OWLCITY" on the Agora Marketplace for .1716 bitcoins; and,

b. On October 23, 2015, DEA agents purchased .4 grams of heroin from vendor "OWLCITY" on the Abraxas Marketplace for .3606 bitcoins. In the product listing,

“OWLCITY” stated: “Finally Ive [sic] gotten some very good dope which ive [sic] tested myself.”

27. In both instances, the controlled substances were shipped via United States Priority Mail with South Florida return addresses.

**E. LESLIE & Leslie Residence Associated with “OWLCITY”**

28. On February 26, 2016, DEA agents received information from the U.S. Postal Service (USPS) that the tracking status of the Priority Mail package that OWLCITY sent to complete the October 23, 2015 heroin order was queried online on the U.S. Postal Service website from an IP address assigned by AT&T to an account associated with the Leslie Residence.

29. A query with the Florida Department of Highway Safety and Motor Vehicles revealed that LESLIE is associated with the Leslie Residence.

30. On or around March 3, 2016, DEA agents observed OWLCITY as a listed vendor on the Alhabay Market. OWLCITY’s Alhabay user profile displayed “Positive feedback (last 12 months): 98%,” and OWLCITY listed numerous controlled substances for sale, including: “Xanax Bars,” “Methylone,” “Modafinil Pills,” “Cocaine,” “Heroin,” and “Furanyl-Fentanyl (UNCUT).”

31. On OWLCITY’s Alhabay vendor profile, the DEA agents observed a listing that stated “1G China White Heroin Sample.” Acting in an undercover capacity, the DEA agents placed an order for ten (10) grams of China White Heroin and made a bitcoin payment corresponding to approximately \$510.00.

32. The DEA agents instructed OWLCITY to ship the drugs, that same day, March 3, 2016, to an undercover mailbox, using U.S. Priority Mail. Subsequently, the DEA agents

received a private message on Alphabay from OWLCITY confirming the order and stating that the package would be shipped by midday and to expect a tracking number within 24 hours.

33. Meanwhile, that same day, March 3, 2016, at approximately 9:00 AM, DEA agents and Miramar Police Department detectives established surveillance at the Leslie Residence, and a vehicle registered to LESLIE parked in the apartment complex parking lot.

34. Around approximately, 4:30 PM, surveillance agents observed LESLIE exit the Leslie Residence wearing a backpack, enter his vehicle and drive to a post office located in Hollywood, Florida. Around approximately 5:30 PM, agents observed LESLIE exit his vehicle wearing the same backpack and enter the post office. Agents then observed LESLIE retrieve five parcels from the backpack and hand them to the clerk at the counter. Agents observed LESLIE pay for the shipping, take his receipt, and exit the post office.

35. On the same date, a postal inspector entered the USPS post office located in Hollywood, Florida after LESLIE departed. The postal inspector located the five parcels LESLIE left at the post office. The parcels included a parcel addressed to the same name and address to which the undercover DEA agents instructed OWLCITY to ship the ordered heroin (hereinafter referred to as the "UC Parcel") and four additional parcels which resembled the UC Parcel in size, weight, location of origin and exterior appearance.

36. On March 10, 2016, agents opened the UC Parcel and executed a search warrant on the remaining four parcels. The UC Parcel contained white powdery substance suspected to be heroin. The remaining parcels all contained white powdery substances and/or pills.

37. Later laboratory analysis revealed that the UC Package in fact contained a 9.9 grams of a mixture of several controlled substances including Fentanyl, and that the remaining four packages included Alpha-PVP, Cocaine, MDMA, and Alprazolam (Xanax).

### F. Tor Network Activity from the Leslie Residence

38. In order to determine whether LESLIE, and/or some other narcotics-trafficking co-conspirator, was accessing criminal, Dark Web marketplaces from the Leslie Residence, law enforcement began monitoring the internet traffic to and from the IP address associated with the Leslie Residence.

39. 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.

40. For example, monitoring the IP connections of a computer connecting to Alphabay through Tor, will not reveal any specific IP address associated with Alphabay. Rather such monitoring could<sup>4</sup> 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.

41. 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>.

---

<sup>4</sup> 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.

42. 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.

43. On March 14, 2016, the DEA obtained a pen/trap order for all internet traffic to and from the AT&T IP address associated with the Leslie Residence. The pen/trap order results obtained through May 13, 2016 reveal frequent internet connections from the Leslie Residence 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 Alphabay, through the Tor network, from a computer located within Leslie Residence.

44. Although DEA has ceased monitoring the IP routing information from the Leslie Residence, LESLIE was seen at the Leslie Residence as recently as July 22, 2016 and the OWLCITY vendor account was seen active on Alphabay as of July 17, 2016.

#### **G. LESLIE Computer Repair Coincides with OWLCITY Inactivity**

45. On July 12, 2016, DEA agents observed LESLIE drive from the Leslie Residence and to a shopping center and then exit his vehicle with a black laptop computer which he dropped off at a computer repair shop. Records revealed that LESLIE picked up the lap top on July 13, 2016.

46. On or around July 14, 2016 agents logged into a dark web marketplace on which OWLCITY was known to operate as a vendor and observed that OWLCITY had not been active since July 11, 2016, which corresponded to the time period during which LESLIE had left the laptop for repairs.

### **E. Search of Leslie Residence**

47. On July 27, 2016, a search warrant was executed at the Leslie Residence. At the initiation of the search LESLIE ran to the bathroom within the residence in a failed attempt to flush what appeared to be controlled substances.

48. Pursuant to the search, DEA recovered pills and powders, which appear to be controlled substances, both in that bathroom and in a room identified as LESLIE's. DEA also recovered several computers and USPS packaging and shipping materials in LESLIE's bedroom, as well as at least one bitcoin cold storage wallet.

CONCLUSION

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


a. Chrissano LESLIE, did, at least from March 3, 2016 through July 27, 2016, conspire with the unknown administrator(s) of Alphabay, to possess with intent to distribute controlled substances, including Fentanyl, Alpha-PVP, MDMA, and cocaine, in violation of Title 21, United States Code, Sections 846 and 841(b)(1)(c); And that

b. Chrissano LESLIE, did, at least from March 3, 2016 through July 27, 2016, conspire with the unknown administrator(s) of Alphabay, 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

Sworn to and subscribed before me this 27  
day of July, 2016.

  
\_\_\_\_\_  
HONORABLE LURANA S. SNOW  
UNITED STATES MAGISTRATE JUDGE

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF FLORIDA

No. 16-6339-SNOW

UNITED STATES OF AMERICA

v.

CHRISSANO S. LESLIE,  
a/k/a, "Owlcity,"

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