

U.S. DISTRICT COURT
WESTERN DISTRICT OF LOUISIANA
RECEIVED

JUL 14 2015

TONY R. MOORE, CLERK
BY  DEPUTY

AFFIDAVIT

I, FBI Special Agent Randy J Jordan, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (hereinafter “FBI”), and have been since July 2011. I am currently assigned to the New Orleans Division, New Orleans, Louisiana. Since September 2013, I have been assigned to work primarily cases involving high technology crime. I have conducted or participated in surveillance, the execution of search warrants, and the debriefing of informants and cooperating witnesses. As an FBI agent, I am authorized to investigate violations of federal law and to execute warrants issued under the authority of the United States.

2. My training has included attending eighteen weeks FBI new agent basic training during which I received instruction on various aspects of federal investigations. In addition, I have received additional specialized training focusing on more specific aspects of cyber-crime investigations. I successfully completed the FBI’s training as a Digital Extraction Technician (DEXT). The three-week training course certified me in the forensic imaging/copying/duplication of digital evidence and trained me in the search/find/extraction functions of digital evidence. Prior to my current position as Special Agent with the FBI, I have received a Bachelors of Science in Computer Information Systems (CIS) and Business



Administration. I have a Masters in Business Administration with a concentration in Management.

3. The facts set forth in this affidavit are based on my personal knowledge, the knowledge obtained during my participation in this investigation, the knowledge obtained from other individuals, including other law enforcement personnel, review of documents and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, this affidavit does not set forth each and every fact learned by me during the course of this investigation.

TECHNICAL TERMS

1. Based on my 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 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, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.
- d. Server: A server is a centralized computer that provides services for other computers connected to it through a network. The computers that use the server's services are sometimes called “clients”. Server computers can be physically located anywhere. For example, it is not uncommon for a network's server to be located hundreds, or even thousands of miles away from the client computers.
- e. Hacked Server: A hacked server refers to a server that has been compromised by nefarious criminal hackers without the consent of the legitimate owner. Hacked servers can be used by criminals in the furtherance of multiple criminal schemes to include the operations of botnets. Criminals use hacked

servers because they do not have to provide any registration information which could be traced back to them.

- f. Malware: Malware is short for malicious software, is software used or programmed by hackers to disrupt computer operations, gather sensitive information, or gain access to otherwise private computer systems.
- g. Emails: Emails sent over the internet contain Internet Protocol (IP) addresses that can be used to determine the origin and destination of the message. The "header" of an email, which is attached to the top of every email and contains IP addresses of computers which have transmitted the email, may be used to identify the "path" through the internet the email traveled from its origin to its destination. The header will often contain the IP addresses of any and all servers from which the given email "bounced" en route to its destination. These IP addresses may be traced to determine the sender of a specific email.
- h. Zero Day exploits: Zero Day exploits are essentially newly developed malware to exploit vulnerabilities in computer operating systems or software being run on computers which can allow hackers to "hack" the computer. They are coined "zero day" because if they haven't yet been used for hacking computers, there are no discreet anti-virus signatures of other security means to detect them yet.
- i. Botnet: A botnet is a collection of Internet-connected computers (often referred to as zombie computers) whose security defenses have been breached

and control ceded to a malicious party. Each such compromised device, known as a "bot", is created when a computer is penetrated by malware. Typically, the malware directs the computer to "call back" or connect to command and control (c2) servers which are controlled by hackers. These servers can be used to control the various bots. Furthermore, the malware installed on a victim's computer often blocks access to more than 100 popular anti-virus and security programs so that the infected user cannot download the software to fight the malware.

- j. SQL: SQL stands for Structured Query Language. SQL is used to communicate with a database which stores electronic data to include forum data such as public and private posts.
- k. Proxy: A proxy, as used in this affidavit, refers to a specific proxy, known as a web proxy. Web proxies facilitate access to content on the World Wide Web and providing anonymity and are set to hide the IP or thus conceal the physical location of the primary "back-end" server. Proxies are also referred to as "Front-End" servers in this affidavit.
- l. Geo-Location: Geo-location is, in general, the process of identifying an IP address's geographical location, including its country of origin, which in turn helps identify the location of the device connected to the Internet using that IP address. Identifying an IP address's country of origin is relatively simple and accurate (approximately 95-99 percent according to an established DNS

company), because IP registrars must provide a country name when an IP range is allocated to the registrars and the registrars provide IP addresses to the public.

BACKGROUND OF INVESTIGATION

4. As part of its investigation, [REDACTED]
[REDACTED]. [REDACTED] is actually a member of the DARKODE
(*Explained below beginning at paragraph 9*) forum and has been for approximately four years. As such, [REDACTED] is a very experienced computer hacker who has extensive knowledge of criminal activity occurring over the Internet and particularly on the criminal hacking forum known as DARKODE. [REDACTED]

[REDACTED]
[REDACTED] has provided the FBI with reliable and corroborated information in regards to malicious criminal activity as it relates to RORY STEPHEN GUIDRY (GUIDRY) known on the DARKODE forum as “k@exploit.im”.

5. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED].

6. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

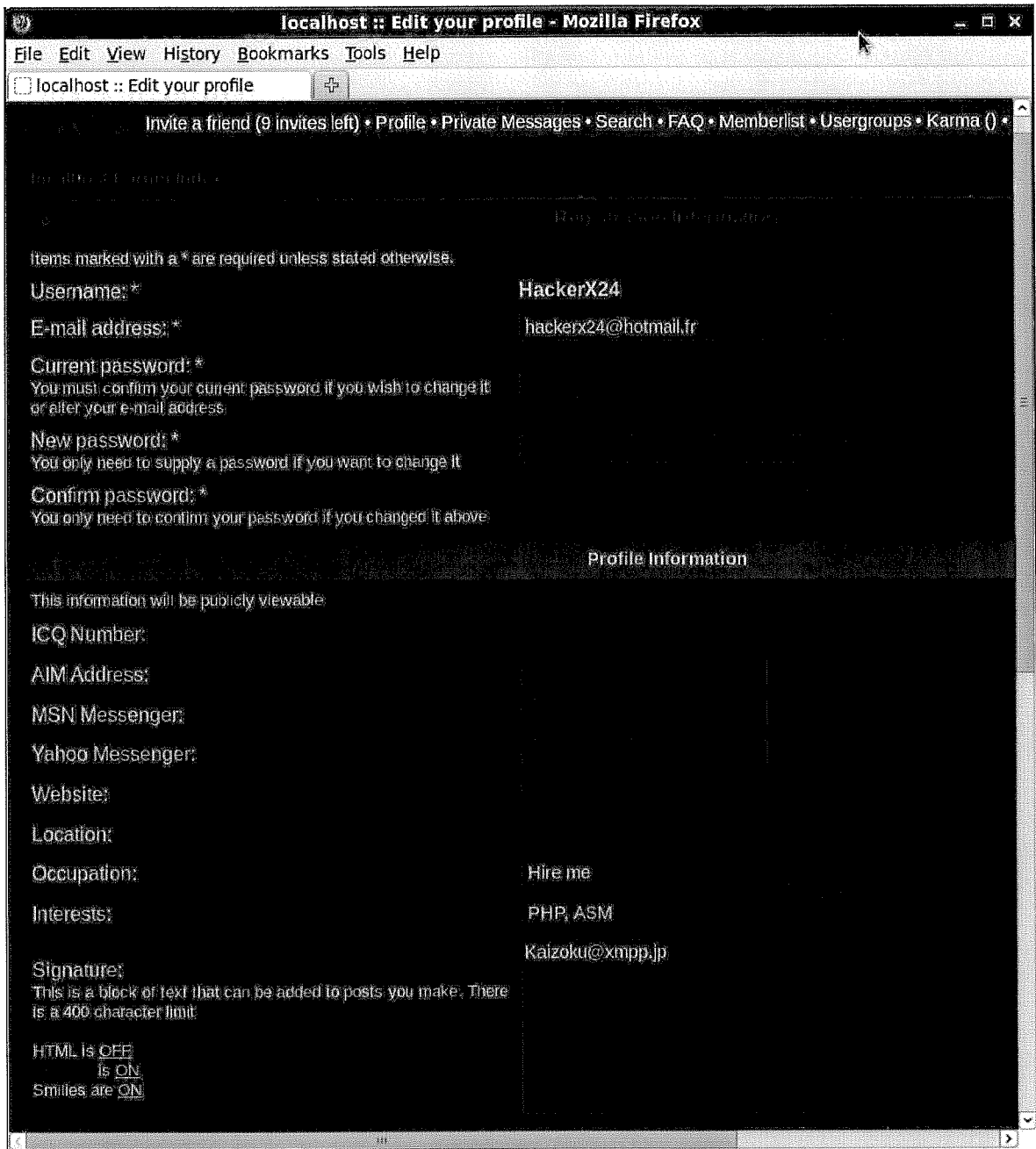
[REDACTED]

[REDACTED]

7. This membership list is compiled within the DARKODE forum server through the use of “membership forms” that the DARKODE administrators require prior to admission into the forum. On the form, an email address (hereinafter “REGISTRATION EMAIL”) is to be provided by each member for registration into the forum (as seen in the following member profile screen shot), which shows the user’s forum moniker, as well as that user’s contact information as shown immediately below:

1 [REDACTED]

[REDACTED]



8. [REDACTED] provided Pittsburgh FBI with GUIDRY's email account, k@exploit.im, which is associated with the membership list for DARKODE and indicated that k@exploit.im (GUIDRY) is an active member of the criminal hacking forum and that he/she uses and has control of the associated REGISTRATION EMAIL.

EXPLANATION OF DARKODE FORUM

9. DARKODE is a well-known, exclusive, invitation-only criminal hacking forum which maintains an electronic public posting area as well as a private messaging (PM) area. Based on information provided by [REDACTED], as well as information gathered from private security researchers and foreign law enforcement, the FBI has learned that the forum has a formalized hierarchy with varying levels of membership access to the contents of the forum. To become a member of the forum, an individual must be “sponsored” by an existing member, and sent a formal invitation. The proposed member is then required to post a resume’, usually in the form of an introductory statement, to the already approved and active forum membership, in essence espousing what the new member’s criminal cyber skills are and what he/she would contribute to the forum membership.

10. Once approved for membership, the new member is typically initially assigned a lower-tier status within the forum, hereinafter referred to as “Level 0.” Members can progress from this introductory Level 0, to Levels 1, 2 or 3. Level 3 members, as explained later, are considered the “Administrators” of the forum, the top-level individuals with the greatest level of access to the information stored within the forum and the maintainers of the technical operations of the forum, including membership control and access.

11. DARKODE members use the forum to conduct criminal business and trade. DARKODE members utilize the forum to setup buys and/or offer and arrange the sale of hacker products, including, but not limited to malware, Zero Day Exploits and hacked servers. They also seek out and offer various expert services to each other, often in

furtherance of some criminal hacking activity, such as finding another hacker who has special knowledge or has other hacker apparatus (such as malware) they need.

Background providing the connection between the moniker ‘k@exploit.im’ and RORY

RORY STEPHEN GUIDRY

12. On July 8, 2015, FBI Task Force Officer (TFO) Charles Riley, Austin Police Department (APD) Detective e-mailed FBI Special Agent (SA) Scott Kibbey a copy of APD Police Report (General Occurrence # 2014-5032454) regarding a no-knock search warrant conducted by APD at the residence of RORY STEPHEN GUIDRY, 105 Prospector Lane, Liberty Hill, Texas, 78642 on October 9, 2014. The search warrant was part of an APD investigation regarding GUIDRY allegedly conducting a Distributed Denial of Service (DDoS) attack against a website owned by Austin PC Tech (APT) in Austin, Texas.

13. On July 9, 2015, TFO Riley e-mailed SA Kibbey a zip file containing all the Jabber (instant messaging platform) chat logs found on GUIDRY’s computer. TFO Riley included a file hash listing which contained the location of each log. The chat logs were divided into two subfolders, “duckylord@priv.in” and “k@exploit.im”, indicating that GUIDRY used both monikers to chat via the Jabber client. The “k@exploit.im” folder contained a folder [REDACTED] with chat logs between k@exploit.im and [REDACTED], indicating that GUIDRY had communicated with [REDACTED] utilizing the k@exploit.im moniker on the Jabber client.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

BOTNET Explained

17. A botnet is a number of Internet computers which are compromised by a malicious actor to use at the actors discretion. The infected computers or bots can be programmed to redirect transmissions to a specific computer, for malicious activity. If a computer is part of a botnet, it's infected with a type_of_malware. The bot (infected computers) contacts a remote server — or just gets into contact with other nearby bots (infected computers) — and waits for instructions from whoever is controlling the botnet, in this regards k@exploit.im (GUIDRY). This allows an attacker to control a large number of computers for malicious purposes.

18. Computers in a botnet may also be infected with other types of malware, like keyloggers that record your financial information and send it to a remote server. What makes a computer part of a botnet is that it's being controlled remotely along with many other computers. The botnet's creators, in this regards k@exploit.im (GUIDRY), can decide what to do with the botnet, for instance he could direct the bots to download additional types of malware, and even have the bots act together to conduct malicious activity.

BOTNET Purpose (Maliciously)

19. Botnets can be used for many different purposes, they allow hundreds of thousands of different computers to act in unison and all are controlled by one person the malicious hacker. The following explains the many uses of a botnet:

- For profit, by infecting as many computers as possible to build the structure of the botnet, then renting access of the botnet to other malicious actors.

- Because botnets infect hundreds of thousands of different computers to act in unison, a botnet could be used to perform a distributed denial-of-service (DDoS) attack on a system. Hundreds of thousands of computers would bombard a system with traffic at the same time, overloading it and causing it to perform poorly or become unreachable.
- A botnet could also be used to send spam emails. Email spam, also known as junk email or unsolicited bulk email (*UBE*), is a subset of electronic spam involving nearly identical messages sent to numerous recipients by email. Clicking on links in spam email may send users to phishing web sites or sites that are hosting malware. Spam email may also include malware as scripts or other executable file attachments.
- Botnets can also just be used to distribute other malware. The bot software essentially functions as a Trojan, downloading malware to a system after obtain access. The people in charge of a botnet might direct the computers on the botnet to download additional malware, such as keyloggers, adware, and even nasty ransomware like CryptoLocker.

How BOTNETS Are Controlled

20. Botnets can be controlled in several different ways. The most basic way for a botnet to be controlled is for each bot to connect to a remote server. For example, each bot might download a file from <http://example.com/bot> every few hours, and the file would tell them what to do. Such a server is generally known as a command-and-control server. Alternately, the bots might connect to an Internet relay chat (IRC) channel hosted on a server somewhere and wait for instructions. Some botnets may communicate in a distributed, peer-

to-peer way. Bots will talk to other nearby bots, which talk to other nearby bots, which talk to other nearby bots, and so on. There's no one, identifiable, single point where the bots get their instructions from.

21. Below is a technical analysis of the server [REDACTED] k@exploit.im

[REDACTED] utilized as a command-and-control server for his botnet.

Summary of Technical Analysis Report of Virtual Private Server 80.242.123.196

Background:

The Investigative Analysis Unit (IAU) performed analysis on a snapshot of a Virtual Private Server (VPS) with Internet Protocol (IP) address 80.242.123.196, referred to as "the server" for the remainder of this document. The server [REDACTED] "k@exploit" on March 3, 2015, through the time the Technical Analysis Report was written on June 26, 2015.

Botnet:

The server contained source code in the C programming language and compiled binary executables for both a botnet Command and Control (CnC) server and client malware that connects back to the IP address of the server. The client malware appears to have been compiled for a variety of computer architectures including mipsel, PowerPC, arm, mips, and sh4.

The client malware was configured to download and execute the file <http://142.11.230.18/b.php>. Analysis of "b.php" showed that the file executes shell code to download updated client malware from 80.242.123.196.

The server was configured to use the Apache web server software to allow infected systems to download updated client malware. The Apache access log, which contains a list of each request to the web server, was found to contain 167,934 unique IP addresses.

SSH Brute Force:

The botnet appears to have the ability to perform SSH brute force scans, which means it can attempt to connect to various systems using a list of usernames and passwords in an attempt to guess the login credentials.

A log file was discovered that appears to contain IP addresses, usernames, and passwords of successful SSH brute force attempts. The file contains 14,093 rows with 6,903 unique IP addresses.

Botnet Management:

Management of the botnet server was configured to be accessible via a Tor hidden service. A Tor hidden service hides the real IP address of the server from the clients and hides the real IP address of the clients from the server.

The management console was configured to be accessible using the Tor address dqvs5sqrovwrxsqzq.onion.

Analysis of bot IP addresses communicating with the server controlled by k@exploit (GUIDRY)

An IP Geolocation search on a list of IP addresses that communicated with the Virtual Private Server (VPS) with Internet Protocol (IP) address 80.242.123.196 provided to the hacker known as k@exploit (GUIDRY). The IP addresses in the list at some point had

connections with the server operated by k@exploit (GUIDRY). There were 2,036 identified bot IP addresses in the U.S. that communicated with the CNC server.

The Geolocation database identified 63 of the IP addresses as being in Louisiana. A sample of the Louisiana bot IP addresses is listed below:

IP Address	City	Domain	Region	Company
99.195.57.241	VILLEPLATTE	CENTURYTEL.NET	LA	CENTURY TELEPHONE ENT
98.80.18.143	SHREVEPORT	BELLSOUTH.NET	LA	SHV ADSL CBB
98.67.239.215	SHREVEPORT	BELLSOUTH.NET	LA	SHV ADSL CBB
98.179.214.62	LAFAYETTE	COX.NET	LA	COX COMMUNICATIONS
98.125.82.47	MONROE	CENTURYTEL.NET	LA	CENTURY TELEPHONE ENT

Analysis of an SSH log file from the server controlled by k@exploit (GUIDRY).

An analysis on the 420 U.S. IP addresses from the file that appears to contain successful Secure Shell (SSH) brute force attempts, from the server operated by k@exploit (GUIDRY). The list of IP addresses shows GUIDRY attempted to establish unauthorized SSH connections. It is unknown how many of the IP addresses GUIDRY successfully connected to.

Secure Shell is a secure, encrypted network connection that allows someone to establish a connection with the command line of another computer over an unsecured network. SSH sessions typically involve remotely executing commands and/or transferring data between the client and the server.

Within those results, five IP addresses traced back to Louisiana. They are listed below.

IP Address	City	Domain	Region	Company
173.218.194.106	BASTROP	SUDDENLINK.NET	LA	SUDDENLINK COMMUNICATIONS
98.67.116.222	SHREVEPORT	BELLSOUTH.NET	LA	SHV ADSL CBB
67.148.229.141	MONROE	QWEST.NET	LA	QWEST COMMUNICATIONS INTERNATIONAL INC.
65.157.10.223	MONROE	QWEST.NET	LA	QWEST COMMUNICATIONS INTERNATIONAL INC.
76.72.97.75	LAFAYETTE	LUSFIBER.NET	LA	LAFAYETTE CONSOLIDATED GOVERNMENT

There were 64 IP addresses belonging to .MIL networks present in the list. A sample of the results is listed below. The full list is attached.

IP Address	City	Domain	Region	Company
132.17.105.21	MONTGOMERY	AF.MIL	AL	754TH ELECTRONIC SYSTEMS GROUP
164.184.53.145	WASHINGTON		DC	DIA
215.89.214.141	COLUMBUS	USMC.MIL	OH	DOD NETWORK INFORMATION CENTER
6.210.135.167	FORT HUACHUCA	ARMY.MIL	AZ	HEADQUARTERS, USAISC
160.150.32.255	COLUMBIA	ARMY.MIL	SC	HEADQUARTERS, USAISC
128.49.44.56	SAN DIEGO	NAVY.MIL	CA	NAVY NETWORK INFORMATION CENTER (NNIC)

205.72.133.236	VIRGINIA BEACH	NAVY.MIL	VA	NAVY NETWORK INFORMATION CENTER (NNIC)
----------------	-------------------	----------	----	--

BOTNETS Profits Explained

22. The cost of a botnet is contingent largely upon the physical location of the malware-infected system controlled by the botnet. A botnet containing only American or European machines is worth more than one with machines from less prosperous nations. American machines are more valuable because American consumers have more “online purchasing power” than their international counterparts. Below shows an approximation of the profits which can be made, from a botnet if the hacker sells access to his botnet, by the number of infected systems purchasing hackers would be able to utilized if purchased:

<i>Number of Infected systems for sale in EUROPE</i>	<i>Price of infected system</i>
1,000	\$50
5,000	\$225
10,000	\$400

<i>Number of Infected systems for sale in CANADA</i>	<i>Price of infected system</i>
1,000	\$80
5,000	\$350

[REDACTED]

[REDACTED]

24. [REDACTED] and k@exploit.im (GUIDRY)

shows where GUIDRY discusses selling infected systems from the botnet which he owns online beginning at 12:55:44 PM. GUIDRY lays out his pricing model which shows four different uses of his botnet operation. Based on your affiants investigative knowledge and


intelligence obtained, the approximated analysis of the price chart at the time listed in the chat (1:26:19 PM) is as follows:

- ‘Installs’ refer to GUIDRY utilizing his botnet to install (infect) malware on systems for malicious activities.
- ‘Updates’ refer to GUIDRY utilizing his botnet to allow infected systems of other hackers to connect to his botnet to obtain updates of malware or obtain new malware for malicious activities.
- ‘Loads’ refer to GUIDRY utilizing his botnet to load malware onto systems for malicious activities.
- ‘IE traffic’ refer to GUIDRY allowing his botnet to be used for web (Internet) automated surfing, which allows his botnet to automatically obtain information from websites for malicious activities.

25. In conclusion, the information set forth above establishes that RORY STEPHEN GUIDRY, aka K@exploit.im utilizes the DARKODE forum in furtherance of his criminal activities, specifically violations of 18 U.S.C. § 1030(a)(2) and (4), Accessing a Computer and Obtaining Information, and Accessing a Computer to Defraud and Obtain Value. Furthermore, based on the foregoing, your affiant has probable cause to believe that RORY STEPHEN GUIDRY, aka K@exploit.im is continually conducting cyber malicious criminal activity on the Internet to date. GUIDRY is an intelligent malicious hacker who implements operational security, using techniques which attempt to hide his criminal cyber activities from law enforcement. Based on my investigative knowledge and similar cases of this nature within law enforcement, GUIDRY likely masked the use of his Internet Protocol

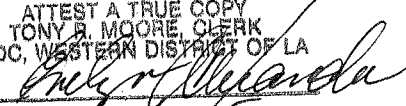
(IP) address which links back to his residence by utilizing the TOR network. The Onion Router (TOR) directs Internet traffic through a free, worldwide, volunteer network consisting of more than six thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Using TOR makes it more difficult for Internet activity to be traced back to the user: this includes "visits to Web sites, online posts, instant messages, and other communication forms".

Respectfully submitted,


Special Agent Randy J. Jordan
Federal Bureau of Investigation

Subscribed and sworn to before me on the 13th day of July 2015, at Lafayette, Louisiana.


PATRICK J. HANNA
United States Magistrate Judge

ATTEST A TRUE COPY
TONY B. MOORE, CLERK
USDC, WESTERN DISTRICT OF LA
BY 
DATE 7/13/2015