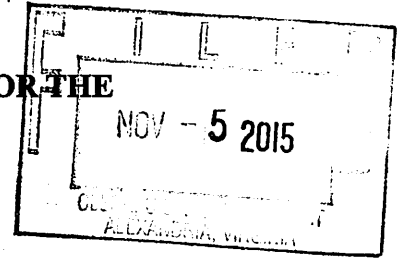


COPY

**IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA**

Alexandria Division



UNITED STATES OF AMERICA)

v.)

ARDIT FERIZI,)
a/k/a "Th3Dir3ctorY,")

Defendant.)

CRIMINAL NO. 1:15-MJ-515

AFFIDAVIT IN SUPPORT OF
REQUEST FOR EXTRADITION

AFFIDAVIT IN SUPPORT OF REQUEST FOR EXTRADITION

I, Brandon L. Van Grack, being duly sworn, hereby depose and state:

1. I am a citizen of the United States of America, residing in Washington, D.C.
2. In May 2001, I received a Bachelor's Degree from Duke University. In June 2006, I received a Juris Doctor degree from Harvard Law School. I was admitted to the Bar of the State of Maryland in December 2006 and to the Bar of the District of Columbia in April 2008. From June 2010 to the present, I have been a prosecuting attorney with the United States Department of Justice, serving as Counsel to the Assistant Attorney General for the National Security Division, as a Trial Attorney in the National Security Division, and as a Special Assistant United States Attorney (SAUSA) in the United States Attorney's Office for the Eastern District of Virginia. My duties include the investigation and prosecution of persons charged with violating the criminal laws of the United States. I have represented the United States in numerous felony cases throughout the United States, including in the United States District Court for the Eastern District of Virginia. Based upon my training and experience, I am knowledgeable about the

criminal and extradition laws and procedures in the Eastern District of Virginia and the United States.

The Complaint

3. I submit this affidavit in support of an application by the government of the United States for the extradition of ARDIT FERIZI from Malaysia to the United States to face criminal charges in the United States District Court for the Eastern District of Virginia in the criminal case identified above, United States v. Ardit Ferizi, a/k/a "Th3Dir3ctorY," 1:15-MJ-515.

4. I am the SAUSA currently assigned to this prosecution. FERIZI has been charged by complaint with several serious violations of the laws of the United States. I have obtained a certified true and accurate copy of the complaint in this case, attached as Exhibit A, which was sworn out before a United States Magistrate Judge and filed in the United States District Court for the Eastern District of Virginia.

5. Under the laws of the United States, a criminal prosecution may be commenced by the filing of a criminal complaint in a United States District Court. A criminal complaint is a written statement of essential facts constituting an offense charged and is made under oath before a United States Magistrate Judge. A criminal complaint must establish that probable cause exists to believe that an offense has been committed and that the defendant named in the complaint committed the offense. If satisfied that the complaint sets forth a sufficient factual basis to establish probable cause, the United States Magistrate Judge orders the issuance of a warrant for the arrest of the defendant named in the complaint.

6. On October 6, 2015, a criminal complaint, No. 1:15-MJ-515, was filed in the United States District Court for the Eastern District of Virginia, formally charging FERIZI with criminal offenses against the laws of the United States. An arrest warrant for FERIZI was then

issued by a United States Magistrate Judge of the Eastern District of Virginia, also on October 6, 2015. It is the practice of the United States District Court for the Eastern District of Virginia to retain the original complaint and file it with the records of the Court. Therefore, I have obtained certified copies of the complaint, which is attached as Exhibit A, and the arrest warrant, which is attached as Exhibit B. On October 12, 2015, Malaysian authorities provisionally arrested FERIZI in Kuala Lumpur, Malaysia, at the request of the United States.

7. I verify that this prosecution is not barred by any statute of limitations. Pursuant to Title 18, United States Code, Section 3282, the United States can commence a prosecution for violations of Title 18, United States Code, Sections 1030 and 1028A, within five years after the charged offenses have occurred. Additionally, pursuant to Title 18, United States Code, Section 3286, the United States can commence a prosecution for violations of Title 18, United States Code, Section 2339B, within eight years after the charged offenses have occurred. FERIZI is charged with offenses that took place in April 2015 and thereafter. Accordingly, the prosecution of FERIZI is not time-barred. A copy of the relevant provisions of Sections 3282 and 3286 is attached as Exhibit C.

8. The charges against FERIZI in the complaint are as follows:

1) Unauthorized Access to a Computer (two counts),¹ in violation of Title 18, United States Code, Section 1030, for which the maximum statutory sentence is five years;

2) Aggravated Identity Theft, in violation of Title 18, United States Code, Section 1028A, for which the maximum statutory sentence is five years; and

¹ It is common practice to list a Code Section and Offense Description one time in a criminal complaint even if there are multiple violations of the Code Section alleged in the affidavit, as is the case here for Title 18, United States Code, Section 1030.

3) Providing Material Support to a Foreign Terrorist Organization (FTO), in violation of Title 18, United States Code, Section 2339B, for which the maximum statutory sentence is 20 years and, if the death of any person results, any term of years or for life.

9. A violation of any of the charged statutory provisions constitutes a felony crime under United States law. Each of these statutes and regulations was a duly enacted law of the United States at the time the offenses were committed and is now in effect. The relevant portions of these statutes and regulations are included in Exhibit C.

Elements of the Offenses Charged

10. In order to convict FERIZI of unauthorized access to a computer, in violation of Title 18, United States Code, Section 1030(a)(2), which is the first violation of Title 18, United States Code, Section 1030 alleged in the complaint, the government would have to prove the following elements: (1) FERIZI intentionally accessed a computer without authorization or exceeded authorized access; (2) FERIZI thereby obtained information from a protected computer; and (3) FERIZI did this in furtherance of a criminal act in violation of the laws of the United States.

11. In order to convict FERIZI of making extortion threats relating to unauthorized access to a computer, in violation of Title 18, United States Code, Section 1030(a)(7), which is the second violation of Title 18, United States Code, Section 1030 alleged in the complaint, the government would have to prove the following elements: (1) FERIZI transmitted in interstate or foreign commerce a communication demanding or requesting money or other thing of value in relation to damaging a protected computer; (2) FERIZI did so with the intent to extort money or anything of value from a person, and; (3) FERIZI damaged a protected computer to facilitate the extortion.

12. In order to convict FERIZI of aggravated identity theft, in violation of Title 18, United States Code, Section 1028A(a)(2), the government would have to prove the following elements: (1) FERIZI, during and in relation to a felony violation of a federal crime of terrorism; (2) knowingly transferred, possessed, or used a means of identification of another person; (3) without lawful authority.

13. In order to convict FERIZI of providing material support to a designated FTO, in violation of Title 18, United States Code, Section 2339B, the government would have to prove the following elements: (1) FERIZI knowingly provided, attempted or conspired to provide material support or resources to Islamic State of Iraq and the Levant (ISIL); and (2) FERIZI did so knowing that ISIL was a designated FTO, that the organization engaged or engages in terrorist activity, or that the organization engaged or engages in terrorism.

Facts in Support of the Charges

14. The first charge under Title 18, United States Code, Section 1030 alleges that FERIZI gained unauthorized access to a computer. In sum, FERIZI used a computer in Malaysia to access the Victim Company's server in the United States without authorization from the Victim Company. FERIZI used malicious computer code to access the server, and obtained personal information about government military and law enforcement personnel who lived in the United States. This personal information was not publicly available, and the Victim Company treated this information as confidential. FERIZI gave this information to another person, who FERIZI knew was an ISIL member, so the ISIL member could call upon followers to find the government personnel and cause them physical harm. The United States Government, as explained elsewhere in this Request for Extradition, has designated ISIL as a FTO.

15. The second charge under Title 18, United States Code, Section 1030 alleges that FERIZI made extortion threats relating to unauthorized access to a computer. In sum, FERIZI, from Malaysia, contacted the Victim Company's computer administrator over the Internet. During those communications, FERIZI demanded the Victim Company to stop trying to remove FERIZI's malicious computer code or FERIZI would publish more of the Victim Company's confidential information. FERIZI demanded the Victim Company pay FERIZI in exchange for allowing the Victim Company to terminate FERIZI's access to the server and delete FERIZI's malicious computer code.

16. The complaint further alleges that FERIZI committed aggravated identity theft. In sum, FERIZI, without lawful authority as previously explained, possessed confidential information FERIZI obtained from the Victim Company's server, which included the means of identification of United States government military and law enforcement personnel. FERIZI transferred the means of identification to an ISIL member so it could be used during or in relation to a crime of terrorism, which is the fourth charge in the complaint.

17. Finally, the complaint alleges that FERIZI provided material support to an FTO. In sum, FERIZI provided his hacking services, skills, and the fruits of his hacking, specifically the personal information from the Victim Server, to ISIL members. Those services, property, and information, constitute material support under the law. FERIZI knew, including from conversations FERIZI had with ISIL members, that ISIL was a designated FTO, that the organization engaged or engages in terrorist activity, or that the organization engaged or engages in terrorism.

18. The facts in support of the allegations in the complaint are further summarized in the Affidavit of Special Agent Kevin M. Gallagher of the Federal Bureau of Investigation, which is attached as Exhibit D.

Identification And Location Information

19. A photograph of FERIZI is attached to the affidavit of Special Agent Kevin M. Gallagher. Set forth below is relevant identification and location information for FERIZI:

Name:	Ardit FERIZI
Date of Birth:	January 12, 1995
Nationality:	Kosovar
Passport Type:	Kosovo
Number:	P00390126
Location:	Ardit FERIZI is currently in the custody of Malaysian authorities.

20. Attached hereto and incorporated herein are the following:

Exhibit A: Complaint in case number 1:15-MJ-515

Exhibit B: Arrest Warrant in case number 1:15-MJ-515

Exhibit C: Text of relevant statutes

Exhibit D: Affidavit of Federal Bureau of Investigation Special Agent Kevin M. Gallagher

Conclusion

21. This affidavit, including the exhibits, contains sufficient evidence to support the request of the United States Government that ARDIT FERIZI be extradited from Malaysia to the United States, specifically the Eastern District of Virginia, for prosecution on the above-cited offenses, and that FERIZI remain detained pending the determination of his extradition, and any appeal thereof.



Brandon L. Van Grack
Special Assistant United States Attorney
U.S. Attorney's Office, Eastern District of Virginia

Sworn to and subscribed before me
this 5th day of November, 2015

/s/



Theresa Carroll Buchanan
United States Magistrate Judge

The Hon. Theresa Carroll Buchanan
United States Magistrate Judge

EXHIBIT A

AO 91 (Rev. 08/09) Criminal Complaint

UNITED STATES DISTRICT COURT

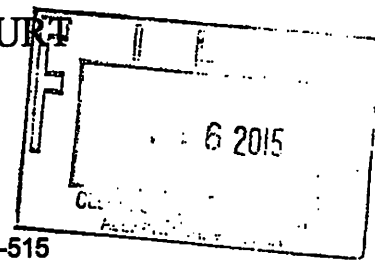
for the
Eastern District of Virginia

United States of America

v.

ARDIT FERIZI
a/k/a Th3Dir3ctorY,

Case No. 1:15-MJ-515



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) 4/01/15 to or on about 8/11/15 in the extraterritorial jurisdiction of U.S. and in the
Eastern District of Virginia, the defendant(s) violated:

Code Section

Offense Description

18 U.S.C. § 1030
18 U.S.C. § 1028A
18 U.S.C. § 2339BUnauthorized access to a computer;
Aggravated identity theft; and
Providing material support to a designated foreign terrorist group

This criminal complaint is based on these facts:

See attached affidavit.

☒ Continued on the attached sheet.

Reviewed by AUSA/SAUSA:

AUSA Lynn E. Haaland

A handwritten signature in black ink, appearing to read "Kevin M. Gallagher".

Complainant's signature

Special Agent Kevin M. Gallagher

Printed name and title

Sworn to before me and signed in my presence.

Date: 10/06/2015City and state: Alexandria, VA

A handwritten signature in black ink, appearing to read "Theresa Carroll Buchanan".

/s/

Theresa Carroll Buchanan
United States Magistrate Judge

Judge's signature

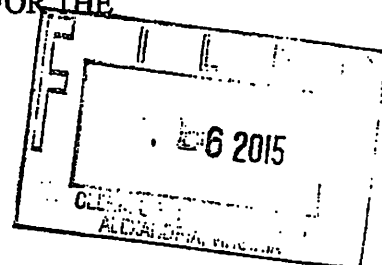
The Honorable Theresa C. Buchanan
U.S. Magistrate Judge, TCB

Printed name and title

A handwritten signature in black ink, appearing to read "Deputy Clerk".

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



UNITED STATES OF AMERICA

v.

No. 1:15mj515

ARDIT FERIZI,

a/k/a "Th3Dir3ctorY,"

Defendant.

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

Kevin M. Gallagher, being duly sworn, says:

I. INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since August 2009. I am currently assigned to the Washington Field Office. I have training in the preparation, presentation, and service of criminal complaints and arrest and search warrants, and have been involved in the investigation of numerous types of offenses against the United States, including crimes of terrorism, as set forth in 18 U.S.C. § 2331 *et seq.* Prior to my current employment, I was an independent contractor for approximately three years, working as an intelligence analyst for two other government agencies within the intelligence community. My knowledge about this investigation comes from my personal participation in this investigation, a review of documents, electronic media, e-mails, and other physical and documentary evidence, and interviews of witnesses. I have also relied on information provided to me by other agents and law enforcement officials in the United States. Where statements of others are set forth, they are set forth in substance and in part. Because this affidavit is being submitted for the limited purpose

of establishing probable cause for the requested warrant, it does not contain all information known to me or to the government relating to this investigation.

2. Ardit Ferizi, aka "Th3Dir3ctorY" ("FERIZI"), a Kosovo citizen residing in Malaysia, is believed to be the leader of a known Kosovar internet hacking group, Kosova Hacker's Security ("KHS"). In or about April 2015, FERIZI used the Twitter account @Th3Dir3ctorY to provide unlawfully obtained personally identifiable information ("PII") to an Islamic State of Iraq and the Levant ("ISIL") member, Tariq Hamayun ("Hamayun"), known as "Abu Muslim Al-Britani." In addition, between in or about June 2015 and August 11, 2015, FERIZI provided unlawfully obtained personally identifiable information ("PII") to a second known ISIL member, Junaid Hussain ("Hussain"), known as "Abu Hussain al-Britani." On August 11, 2015, in the name of the Islamic State Hacking Division ("ISHD"), Hussain posted a public hyperlink on Twitter with the title "U.S. Military AND Government personnel, including Emails, Passwords, Names, Phone Numbers, and Location Information," which provided ISIL supporters in the United States and elsewhere with the PII for over 1,000 U.S. government personnel, for the purpose of encouraging terrorist attacks against the identified individuals. Some of these individuals reside in the Eastern District of Virginia.

3. For the reasons detailed below, I submit that there is probable cause to believe that, from at least in or about April 2015 continuing through August 11, 2015, FERIZI gained unauthorized access to and obtained information from a protected computer, in violation of 18 U.S.C. § 1030. I further submit that there is probable cause to believe that, from at least in or about April 2015 continuing through on or about August 11, 2015, FERIZI used the unauthorized access to steal the means of identification and other personal information of U.S. military and other

government personnel, including their names, email addresses, passwords, and cities and states of residence, and then knowingly possessed and transferred the means of identification and other stolen information with the intent to aid or abet unlawful activity constituting a violation of federal law, particularly a felony violation enumerated in 18 U.S.C. § 2332(g)(5)(B), all in violation of 18 U.S.C. § 1028A(a)(2). Specifically, the PII stolen by FERIZI was knowingly provided to ISIL to be used by ISIL members and supporters to conduct terrorist attacks against the U.S. government employees whose names and locations were published. Prior to that, in or about April 2015, FERIZI transferred PII containing credit card information to ISIL. Based on the information contained in this Affidavit, I believe FERIZI conspired, attempted to provide, and provided, material support to ISIL, a designated foreign terrorist organization, in violation of 18 U.S.C. § 2339B.

4. I expect that FERIZI will be arrested outside of the United States and will be first brought to the Eastern District of Virginia.

II. BACKGROUND REGARDING ISIL AND JUNAID HUSSAIN

5. On October 15, 2004, the U.S. Department of State designated Al-Qa'ida in Iraq, then known as Jam'at al Tawhid wa'al-Jihad, as a Foreign Terrorist Organization ("FTO") under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist Entity pursuant to Executive Order 13224.

6. On May 15, 2014, the U.S. Department of State amended the designation of Al-Qa'ida in Iraq ("AQI") as a Foreign Terrorist Organization ("FTO") under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist Entity under Executive Order 13224 to list the name Islamic State of Iraq and the Levant ("ISIL") as its primary

name. The Department of State also added the following aliases to the ISIL listing: the Islamic State of Iraq and al-Sham (ISIS), the Islamic State of Iraq and Syria (ISIS), ad-Dawla al-Islamiyya fi al-'Iraq wa-sh-Sham, Daesh, Dawla al Islamiya, and Al-Furqan Establishment for Media Production. Although the group has never called itself "Al-Qa'ida in Iraq (AQI)", this name has frequently been used by others to describe it. To date, ISIL remains a designated FTO. In an audio recording publicly released on or around June 29, 2014, ISIL announced a formal change of its name to the Islamic State.

7. On or about September 21, 2014, ISIL spokesperson Abu Muhammad al-Adnani called for attacks against citizens, civilian or military, of the countries participating in the United States-led coalition against ISIL.

8. Junaid Hussain, also known by the *nom de guerre* or *kunya* Abu Hussain al-Britani, was a British hacker and well-known member of ISIL. On or about August 24, 2015, Hussain was killed in an airstrike in Raqqa, Syria, a city which I know ISIL considers to be its capital.¹

III. RELEVANT LAW

9. I am advised that 18 U.S.C. § 1030(a)(2)(C) provides:

Whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer . . . shall be punished [not more than five years].

10. Also, I am advised that section 1030(a)(7) provides:

(a) Whoever with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication concerning any—threat, [to damage a protected computer, to obtain information without

¹<http://www.centcom.mil/en/news/articles/iraq-progresses-in-isil-fight-key-extremist-confirmed-dead>

access, or demand or request money or other thing of value in relation to damage to a protected computer], . . . shall be punished [not more than five years].

A “computer” is defined as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. The term “protected computer” includes a computer which is used in or affecting interstate or foreign commerce or communication. 18 U.S.C. § 1030(e)(1) and (e)(2)(B).

11. I am also advised that 18 U.S.C. § 1028A(a)(2) provides:

Whoever, during and in relation to any felony violation enumerated in section 2332(g)(5)(B) [defining Federal crimes of terrorism], knowingly transfers, possesses, or uses, without lawful authority, a means of identification [as defined in 18 U.S.C. § 1028(d)(7)] of another person. . . [shall be guilty of a separate felony].

12. Additionally, I am advised that 18 U.S.C. § 2339B provides:

Whoever knowingly provides material support or resources to a foreign terrorist organization,² or attempts or conspires to do so, shall be [guilty of a felony]. To violate this paragraph, a person must have knowledge that the organization is a designated terrorist organization (as defined in subsection (g)(6)), that the organization has engaged or engages in terrorist activity (as defined in section 212(a)(3)(B) of the Immigration and Nationality Act), or that the organization has engaged or engages in terrorism (as defined in section 140(d) (2) of the Foreign Relations Authorization Act, Fiscal Years 1988 and 1989.

“Material support or resources” means “any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safe houses, false documentation or identification, communications

² I am advised that the term “terrorist organization” means an organization designated as a terrorist organization under section 219 of the Immigration and Nationality Act. 18 U.S.C. § 2339B(g)(6). As stated above, ISIL is a designated foreign terrorist organization (“FTO”).

equipment, facilities, weapons, lethal substances, explosives, personnel (1 or more individuals who may be or include oneself), and transportation, except medicine or religious materials.

“Expert advice or assistance” means advice or assistance derived from scientific, technical or other specialized knowledge. 18 U.S.C. §§ 2339A(b)(1), (b)(3) & 2339B(g)(4).

IV. STATEMENT OF PROBABLE CAUSE

A. FERIZI IS Th3Dir3ctorY

13. On April 5, 2015, @Th3Dir3ctorY, using the name “Ardit Ferizi,” publicly tweeted a link to a June 2013 article from the InfoSec Institute,³ as shown in the screenshot below:

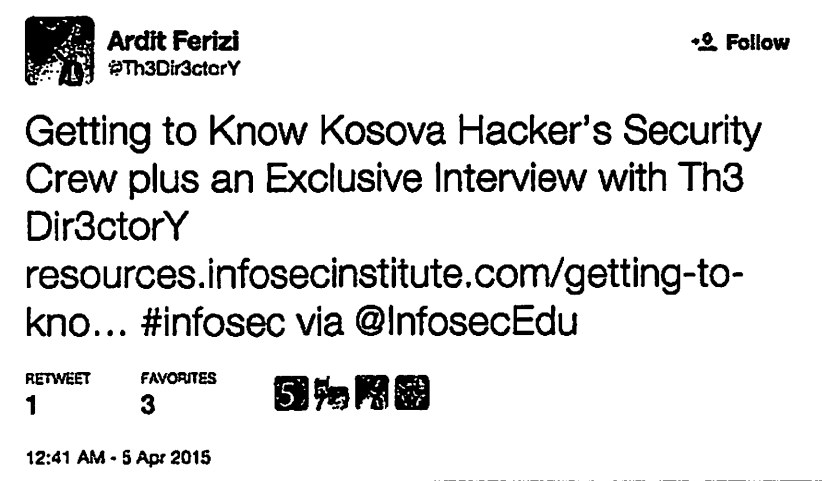


Photo: Screenshot of FERIZI/@Th3Dir3ctorY's April 5, 2015 Tweet with a link to the June 2013 InfoSec Institute Article on KHS and @Th3Dir3ctorY

14. According to the interview of Th3Dir3ctorY by the InfoSec Institute, the user of Twitter account @Th3Dir3ctorY is the leader of a group of ethnic Albanian hackers from Kosovo, calling themselves Kosova Hacker's Security ("KHS"), which is responsible for

³ The InfoSec Institute (www.infosecinstitute.com), founded in 1998 and based in Illinois, is a training institute for technology professionals focused on information assurance, information technology auditing, database, project management, coding and related vendor training. InfoSec Institute also publishes research and articles, including interviews with hacking organizations.

compromising government and private websites in Israel, Serbia, Greece, the Ukraine, and elsewhere.



Photo: Banner for "Kosova Hackers Security" (KHS)

15. According to the article, as of the time of publication, KHS claimed responsibility for having hacked more than 20,000 websites, including: 90% of Serbian government websites; Interpol, based in France (including taking its site down for two days) in October 2012; and IBM's research domain, researcher.ibm.com, located in Somers, New York, in May 2012. KHS also claimed responsibility for having posted more than 7,000 Israeli credit card numbers in January 2012. Again according to the article, hackers calling themselves "Th3Dir3ctorY" and "ThEta.Nu" also claimed responsibility for compromising Microsoft's Hotmail servers in 2011. KHS itself has confirmed its involvement in these attacks in other open sources.

16. On or about July 10, 2015, @Th3Dir3ctorY posted a tweet identifying himself as "Owner of Kosova Hacker's Security, Pentagon Crew," and again used the name Ardit Ferizi:



Photo: Screenshot of @Th3Dir3ctorY's Twitter profile as of July 10, 2015

17. According to Twitter records, the @Th3Dir3ctorY account was registered on September 1, 2012, using Microsoft email account lajmetal@hotmail.com, from an Internet Protocol⁴ address allocated to IPKO Telecommunications LLC in Albania, a telecommunications company that provides services in the adjacent country of Kosovo. This registration information is consistent with @Th3Dir3ctorY's association with KHS, an organization which claims to be associated with Kosovo. Moreover, the investigation has revealed that FERIZI is a citizen of Kosovo.

⁴ Devices directly connected to the internet are identified by a unique number called an Internet Protocol, or IP, address. This number is used to route information between devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address so that the responding device knows where to send its response. In other words, an IP address is similar to a phone number, and indicates the online identity of the communicating device. IP addresses are allocated by an international organization, the Internet Assigned Numbers Authority.

18. Based on my investigation, I know that FERIZI currently resides in Malaysia on a student visa and that, as of spring 2015, FERIZI was studying at Limkokwing University in Malaysia. I believe that FERIZI entered Malaysia in or about early 2015.

19. IP logs for Twitter account @Th3Dir3ctorY reveal that all logins to @Th3Dir3ctorY between June 15, 2015 and August 14, 2015 originated with internet service providers ("ISPs") in Malaysia.

B. ABU MUSLIM AL-BRITANI, A MEMBER OF ISIL, IS THE USER OF TWITTER ACCOUNT @MUSLIM_SNIPER_D

20. The Twitter account @Muslim_Sniper D came to the attention of the FBI following the May 2015 shooting incident at the "Draw Mohammad Contest" in Garland, Texas. On May 3, 2015, two roommates from Phoenix, Arizona, Elton Simpson and Nadir Soofi, fired at a security guard outside the contest venue. Garland police fired back, and when one of the two men pulled out what appeared to be a hand grenade, police shot and killed both men. Based on my investigation, including my review of publicly available social media postings, I believe that Simpson and Soofi were supporters of ISIL.

21. Twitter records demonstrate that the user of @Muslim_Sniper D had been in communication with @atawaakul, a Twitter account believed to have been used by Simpson, prior to the May 3, 2015 incident, and that the two users had discussed issues of "security."

22. According to those records, the user of @Muslim_Sniper_D publicly identified himself as "Tariq Hamayun." According to my investigation, Hamayun, 37 years old, was a car mechanic who volunteered for the Taliban and fought in Pakistan before joining ISIL in Syria.

Twitter records confirm that @Muslim_Sniper_D, originated from an ISP providing service in Raqqah, Syria.

23. On April 21, 2015, Hamayun, using Twitter account @Muslim_Sniper_D, published a tweet that read: "God Willingly will be making the best Electronics LAB in the Islamic state, would be producing sophisticated IEDs."

24. On April 22, 2015, Hamayun, using Twitter account @Muslim_Sniper_D, published a tweet that read: "IEDs is my favourite weapon after Sniping, u hit the enemy & disappear in thin air just like a Ghost. Its [sic] a Must."

C. FERIZI'S TRANSFER OF PII TO ISIL MEMBER ABU MUSLIM AL-BRITANI

25. On or about April 26-27, 2015 there was a Twitter exchange between the accounts @Muslim_Sniper_D and @Th3Dir3ctorY. During this exchange, FERIZI, as the user of @Th3Dir3ctorY, provided Hamayun, the user of @Muslim_Sniper_D, with screen shots of what appears to be unlawfully obtained credit card information belonging to 27 Americans, 18 British and 22 French citizens, including: names; addresses; zip codes; birth dates; and credit card information, such as the type, number, expiration date and Card Verification Value. Based on the context of this exchange, I believe that FERIZI provided this information intending it to be used by and for ISIL.

26. In the conversation, FERIZI asked the user of @Muslim_Sniper_D to confirm that he was "speaking with britani :) abu britani :)" to which Hamayun replied, "Yes brother/Im muslim al britani." Hamayun moreover confirms his association with "Abu Hussain Al-Britani," which is, as described above, the *nom de guerre* of ISIL member Junaid Hussain, who was based in Syria. Hamayun told FERIZI that Abu Hussain al Britani (Junaid Hussain) "is my friend he told

me a lot about u.” This exchange indicates that as of on or about April 26, 2015, FERIZI and Hussain were already in communication with one another.

27. At the end of this exchange, the user of @Muslim_Sniper_D, Hamayun, wrote the following message to the user of Twitter account @Th3Dir3ctorY, FERIZI:

“Pliz [sic] brother come and join us in the Islamic state.” (Emphasis added.)

D. FERIZI’S TRANSFER OF PII TO ISIL MEMBER ABU HUSSAIN AL-BRITANI

28. On August 11, 2015, Hussain, using Twitter account @AbuHussain_16, re-tweeted a post from the Twitter account @IS_Hacking_Div, which had, in the name of the Islamic State Hacking Division (“ISHD”), publicly tweeted a link to PII belonging to approximately 1,351 U.S. military and other government employees. As detailed below, there is probable cause to believe that FERIZI provided these 1,351 names to ISIL.

29. On or about June 13, 2015, FERIZI accessed without authorization a protected computer, namely a server (“Victim Server”) belonging to an identified internet hosting company (the “Hosting Company”), which maintained the website belonging to a U.S. retailer that sells goods via the internet to customers in multiple states (“Victim Company”). The Victim Server is physically located in Phoenix, Arizona. Some of the customers whose information was obtained reside in EDVA. Based on my conversations with other FBI agents, it is a dedicated server, meaning that no companies other than the Victim Company utilize this server. The Victim Server is leased by the Victim Company and owned by the Hosting Company.

30. FERIZI subsequently used his unauthorized access to the Victim Server to obtain the PII of approximately 100,000 people. Sometime between June 13, 2015 and August 11, 2015, FERIZI provided the PII of approximately 1,351 U.S. military and other government personnel to

ISIL, intending it to be used by and for ISIL, and knowing that ISIL would use the PII against the U.S. personnel, including to target the U.S. personnel for attacks and violence. Earlier, in or about March 2015, ISHD, acting in the name of ISIL, posted a “Kill List” including the purported names and addresses of 100 American service members.

31. On August 11, 2015, Hussain re-posted the following tweet by IHSD:

“NEW: U.S. Military AND Government HACKED by the Islamic State Hacking Division!”



Photo: Screenshot of @AbuHussain_16 (Abu Hussain Al Britani) Twitter profile as of August 11, 2015

32. The tweet contained a hyperlink to a 30-page document. The beginning of the document warned the “Crusaders” who were conducting a “bombing campaign against the muslims” . . . that “we are in your emails and computer systems, watching and recording your every move, we have your names and addresses, we are in your emails and social media accounts, we are extracting confidential data and passing on your personal information to the soldiers of the khilafah, who soon with the permission of Allah will strike at your necks in your own lands!” The next 27 pages of the document contained the names, e-mail addresses, e-mail passwords, locations,

and phone numbers for approximately 1,351 U.S. military and other government personnel. The final three pages of the document contained what appear to show (i) credit card numbers and addresses for three federal employees and (ii) Facebook exchanges between U.S. military members. One of the Facebook exchanges includes what appears to be a discussion between two service members ("Service Member-1" and "Service Member 2"). Under this exchange, the creator of the document wrote, "Went to Iraq and returned in a body bag – Hell is the abode of the disbelievers . . ." Based on my review of public-source documents, I know that Service Member-1, a veteran of combat in Iraq and Afghanistan, was in fact killed in 2008, albeit in an accident after returning to the United States.

E. FERIZI'S FIRST KNOWN OFFER OF HACKING-RELATED ASSISTANCE TO ISIL ASSOCIATES

33. The April 26-27, 2015 communication in which FERIZI sent PII to Hamayun was not the first in which FERIZI communicated with ISIL members/supporters and offered them his computer expertise. On April 19, 2015, using @Th3Dir3ctorY, FERIZI posted a publicly available tweet directed to ISIL-affiliated accounts, which read: "@the_traveler01 @ksasisti @AbuBakrSShani brother wait till im [sic] making the script which u can upload and never get deleted (DEDICATED SERVERS)" [.]

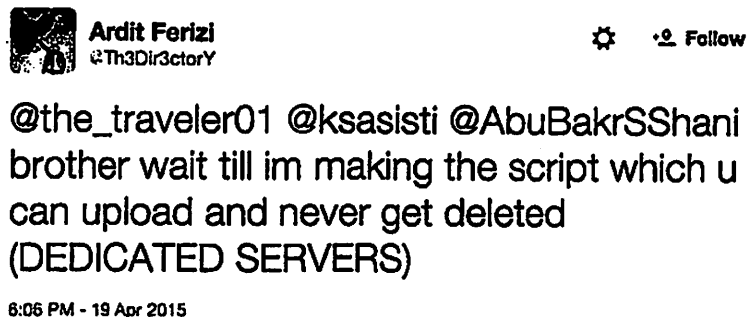


Photo: Screen shot of the April 19, 2015 Tweet by FERIZI aka @Th3Dir3ctorY showing FERIZI's intent to support ISIL.

34. I believe this tweet reflects FERIZI's intention to create and provide a "script," or computer program aimed at assisting ISIL to publicly post communiqués and/or propaganda in a fashion which would supposedly make it difficult for such content to be removed by service providers or law enforcement.

35. All three accounts referenced in the above tweet by @Th3Dir3ctorY have been suspended by Twitter (date unknown). Based on searches of cached tweets, all appear to contain pro-ISIL messages, possibly explaining the suspensions. For example, on April 18, 2015, according to a public posting on pastebin⁵ (<http://pastebin.com/NBAs8mcU>), Twitter user @the_traveler01, utilizing the name "Abu Naseeha," was suspended by Twitter after posting the Al-Furqan/ISIL video of beheadings of Christians and Kurdish Pershmerga. On April 18, 2015, Twitter user @AbuBakrSShani "re-tweeted" the following by @Liberation_X, a pro-ISIL Twitter account: "RT @Liberation_X Egypt Sinai 3high ranking army commanders join islamic state in

⁵ Pastebin is a web application where users can store plain text. They are most commonly used to share short source code snippets for review via Internet Relay Chat.

Sinai.” In April 2015, @ksasisti tweeted: “Mawahideen⁶ of Shaytat tribe denounce & declare their enmity to the people from their blood who've allied with Assad,” followed by another tweet which read: “They also ask Sh Abubakr Baghdad⁷ to let them fight the filth from their tribe who allied with Bashar Assad.”

F. FERIZI IS THE SOURCE OF THE HACKED PII HE SENT TO ISIL

36. On August 13, 2015, an employee of the Victim Company reported an unauthorized access to their website. More specifically, the employee contacted an FBI agent and informed the agent that an account using the username “KHS,” which I believe to be an acronym for Kosova Hackers Security, had access to customer details from their databases. According to the Victim Company, customer information stored in the database included: names, addresses, cities, states, countries, phone numbers, email accounts, and usernames and passwords.

37. On August 17, 2015, the FBI was provided with an exchange between an employee of the Victim Company and technicians at the Hosting Company that owns the server on which the Victim Company’s website resides.

38. According to the exchange, beginning as early as June 13, 2015, an unauthorized user gained access to the Victim Company’s website, and created a user account with the initials KHS.

39. During an exchange that occurred on July 15, 2015, the Hosting Company technician verified to the Victim Company that the Hosting Company was witnessing ongoing

⁶ *Mawahideen* is an alternate spelling for “mujahedeen” or “mujahideen,” a term used to describe guerrilla fighters in Islamic countries, especially those who are fighting against non-Muslim forces. In this instance, I believe it is used to refer to those who fight for ISIL.

⁷ Abu Bakr al Baghdadi is the leader of ISIL.

outbound cyber-attacks against their infrastructure. The Hosting Company verified that the attacks were originating from the account utilizing username "KHS" and provided information about the account, discussed below.

40. According to the "Password last set" entry, which states "6/13/2015 7:28:19 AM," I believe the account was created on or before June 13, 2015. According to the "Last logon" entry, at 7/15/2015 11:32:01 AM, I believe KHS had accessed the Victim Server as recently as the day of the exchange between the Victim Company and the Hosting Company.

```
C:\Users\Administrator>net user KHS
User name KHS
Full Name KHS
Comment
User's comment
Country code 000 (System Default)
Account active Yes
Account expires Never
Password last set 6/13/2015 7:28:19 AM
Password expires Never
Password changeable 6/13/2015 7:28:19 AM
Password required Yes
User may change password Yes
Workstations allowed All
Logon script
User profile
Home directory
Last logon 7/15/2015 11:32:01 AM
Logon hours allowed All
Local Group Memberships *Administrators *Users
Global Group memberships *None
```

41. The Hosting Company also identified that the file being run by KHS on July 15, 2015 was DUBrute.exe, located at the following directory:

C:\Users\KHS\Desktop\DUBrute v2.2 + VNC - Scanner GUI v1.2DUBrute v2.2

42. On August 19, 2015, the Victim Company contacted an FBI agent to report a threatening message it had received. The message, which was from an "Albanian Hacker," with a contact email khs-crew@live.com, threatened the Victim Company for deleting the hacker's "files" from their server. From my experience, I believe that the user of khs-crew@live.com was referring to the DUBrute.exe malware placed on the server which granted the user KHS unfettered access to information stored on the Victim Server.

43. The following is an excerpt of the email sent from an employee of the Victim Company to the FBI:

...I work for [owner of Victim Company] for his store [Victim Company].

The server was hacked again today and left a note on main page...⁸

Hi Administrator,

Is third time that your deleting my files and losing my Hacking JOB on this server !
One time i alert you that if you do this again i will publish every client on this Server!
I don't wanna do this because i don't win anything here !
So why your trying to lose my access on server haha ?
Why you're spending your time with one thing that you can't do ?
Please don't do the same mistake again because bad things will happen with you!
i didn't touch anything on your webhosting files please don't touch my files!
Want to contact me ?
Here : khs-crew@live.com

Greetings from an Albanian Hacker !

#SkyNet
#KHS

⁸ "Main page" refers to the primary page of the website operated by the Victim Company.

44. On August 20, an employee of the Victim Company wrote an email to khs-crew@live.com, identifying him/herself as an employee of the Victim Company, stating: "Please dont attack our servers." In response, the user of khs-crew@live.com wrote:

2BTC: 1f5Vgj7wMU9ofZWZno9ABsLSQ7XXkLsrG and will leave your server also make a report for method how am getting access to your servers :)

(Emphasis added.)

45. The employee replied "2 bitcoin mean? didnt get you whats that?" On August 21, 2015, the user of khs-crew@live.com sent a message to the Victim Company including information on what Bitcoins were and instructions on where the Victim Company should transmit the Bitcoin to:

**<https://en.wikipedia.org/wiki/Bitcoin>
When i get money here : 1f5Vgj7wMU9ofZWZno9ABsLSQ7XXkLsrG
I will make full report for server and method .. i will protect and remove all bugs on your shop !**

I believe that KHS demanded the two Bitcoin, worth approximately \$500, for KHS to relinquish his access to the Victim Server and to provide a report to the administrator on the method he was using to gain that access.

46. In August, the Victim Company provided the FBI with consent to review all information related to the Victim Company's website, which is stored on the Victim Server owned by the Hosting Company.

47. FBI review of the image of the Victim Server reveals an originating IP address of 210.186.111.14. This is an IP assigned to a Malaysian-based ISP that is frequently used by FERIZI. The image shows that on July 8, 2015 at approximately 3:15 Universal Time Coordinate (UTC), the Victim Server was showing signs of a Structured Query Language (SQL) injection

attack. I learned from speaking with other FBI agents that SQL injection is a technique often used against retailer websites that inserts malicious code into a database entry field, thereby causing, for example, the database to send its content to the attacker. I believe that KHS has used this method of hacking in the past.

48. Records for Facebook account 100003223062873, associated with the vanity name "ardit.ferizi01," believed to be used by FERIZI, reveal that the account was accessed from the same IP responsible for the aforementioned SQL injection attack on the Victim Server on July 7, 2015 at approximately 06:49 UTC, the day prior to the initial unauthorized intrusion, and July 8, 2015 at approximately 12:34UTC, which is roughly six hours after the initial unauthorized intrusion.

49. Furthermore, FBI analysis of the Facebook records reveal over 1200 discrete actions attributed to IP 210.186.111.14 occurring between July 6, 2015 and July 13, 2015 including, but not limited to, account Logins, Session Terminations and sent messages.

50. Twitter records demonstrate that the @Th3Dir3ctorY account, attributed to FERIZI, was logged into from the same IP responsible for the SQL injection attack on the Victim Server at approximately 17:15 UTC the day prior to the initial unauthorized intrusion and at approximately 17:09 UTC on July 8, 2015, approximately 13 hours after the initial unauthorized intrusion.

51. Furthermore, FBI analysis of Twitter records reveal at least nine total logins to @Th3Dir3ctorY from IP 210.186.111.14 between July 5, 2015 and July 13, 2015.

52. FBI review of the Victim Server revealed that the full names, email addresses, passwords, and cities and states of residence for the 1,351 U.S. military and other government

personnel included in the release by Hussain and the ISHD on August 11, 2015 were found on the Victim Server.

53. On September 10, 2015, FERIZI sent himself, via Facebook, a file called contact.csv. FBI analysis shows that the data from file contact.csv (100,001 PII records) was imported into a spreadsheet and subsequently truncated to remove the trailing string characters followed by the "|" (pipe)" symbol, so that the data could be compared against normal email address formats. For example, the data row firstnamelastname@gmail.com|22483m was truncated to remove "|22483m," thus leaving "firstnamelastname@gmail.com," which could then be used to compare against any matching email addresses from those posted online by ISIL on August 11, 2015. Utilizing this process, the records from the .csv file were reduced from approximately 100,000 to 98,890 records. The data was subsequently sorted and records not following normal email formats (e.g., suffix "@xxx.xxx") were removed. Any records not having a prefix before the @xxx.xx, were likewise removed. Additionally, all duplicative records were subsequently eliminated. There were 8,475 duplicate records, leaving 91,525 unique email addresses contained in the .csv file. The records from the Victim Server belonging to 1,351 customers of the Victim Company were then imported into the spreadsheet for comparison. In a similar manner, any duplicate email address records were eliminated, leaving 1,351 records which were subsequently compared against the 91,525 remaining email addresses contained in the .csv. Of the 1,351 unique records posted by ISIL on August 11, 2015, 1,089 records matched those records contained in the .csv file and 262 records did not match.

54. Furthermore, a review of the Facebook records revealed a conversation between FERIZI and another Facebook user, account "Butrint Komoni," on or about August 22, 2015, in

which Facebook account Butrint Komoni asked FERIZI: “what happened with the [Victim Company’s website]” to which FERIZI replied, “the network came in :3. I called you man.” I believe FERIZI is confirming his unauthorized access to the Victim Server.

55. Given the above, I believe that FERIZI, the user of the Facebook account 100003223062873, obtained the PII belonging to the U.S. military and other government personnel by unlawfully accessing the Victim Server and provided that information to ISIL for ISIL’s use, including publication and for use against the owners of the PII.

V. CONCLUSION

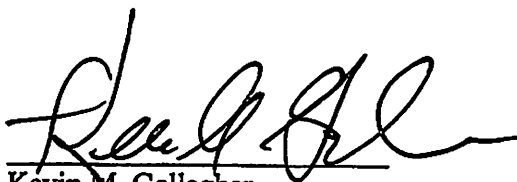
56. Based upon the facts detailed above, I respectfully submit that there is probable cause to believe that from on or about April 2015 to August 11, 2015, out of the jurisdiction of any particular State or district, Ardit FERIZI:

- a. Intentionally accessed the Victim Server, a protected computer, without authorization and exceeded authorized access to the Victim Server, and thereby obtained information from a protected computer, and the offense was committed in furtherance of a criminal act in violation of the laws of the United States, specifically, the criminal act of providing material support to a designated foreign terrorist organization as prohibited by 18 U.S.C. § 2339B, all in violation of Title 18, United States Code, Section 1030(a)(2) and (c)(2)(B)(ii);
- b. With intent to extort from persons money and other things of value, transmitted in interstate and foreign commerce a communication containing a threat to cause damage to a protected computer and threat to obtain

information from a protected computer without authorization and to impair the confidentiality of information obtained from a protected computer without authorization, all in violation of Title 18, United States Code, Section 1030(a)(7) and (c)(3)(A);

- c. Knowingly transferred, possessed and used, without lawful authority, a means of identification of another person (consisting of, among other things, names, birth dates, and credit card information) during and in relation to a felony violation enumerated in section 2332b(g)(5)(B), that is, providing material support to ISIL, a designated foreign terrorist organization as prohibited by 18 U.S.C. § 2339B, knowing that the means of identification belonged to another actual person, in violation of Title 18, United States Code, Section 1028A(a)(2).

- d. Knowingly provided and conspired and attempted to provide material support to ISIL, a designated foreign terrorist organization, namely, property and services, including himself as personnel, expert advice and assistance in computer hacking, and the PII of U.S. military and government personnel, in violation of 18 U.S.C. § 2339B.



Kevin M. Gallagher
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me
this 6 day of ~~September~~ ^{Oct}, 2015



/s/
Theresa Carroll Buchanan
United States Magistrate Judge

The Hon. Theresa Carroll Buchanan
United States Magistrate Judge

True Copy, Teste:
Clerk, U.S. District Court



Deputy Clerk

EXHIBIT B

9914307

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

United States of America

v.

ARDIT FERIZI
a/k/a Th3Dir3ctorY,

Defendant

Case No. 1:15-MJ-515

UNDER SEAL

RECEIVED
UNITED STATES MARSHAL
2015 OCT -6 PM 3:23
EASTERN DISTRICT
OF VIRGINIA
ALEXANDRIA DIVISION

ARREST WARRANT

To: Any authorized law enforcement officer

YOU ARE COMMANDED to arrest and bring before a United States magistrate judge without unnecessary delay
(name of person to be arrested) Ardit Ferizi
who is accused of an offense or violation based on the following document filed with the court:

☐ Indictment ☐ Superseding Indictment ☐ Information ☐ Superseding Information ☒ Complaint
☐ Probation Violation Petition ☐ Supervised Release Violation Petition ☐ Violation Notice ☐ Order of the Court

This offense is briefly described as follows:

18 U.S.C. § 1030, Unauthorized access to a computer;
 18 U.S.C. § 1028A, Aggravated identity theft; and
 18 U.S.C. § 2339B, Providing material support to a designated foreign terrorist group

Date: 10/06/2015City and state: Alexandria, VA

/s/
 Theresa Carroll Buchanan
 United States Magistrate Judge

Issuing officer's signature

Honorable Theresa C. Buchanan, U.S. Magistrate Judge

Printed name and title

Return

This warrant was received on (date) _____, and the person was arrested on (date) _____
 at (city and state) _____

Date: _____
 Arresting officer's signature _____

Printed name and title

INFORMATION
 COPY ONLY
 NOTICE BEFORE ARREST, VALID
 THROUGH NOV. ORIGINAL
 HELD BY U.S. MARSHAL

EXHIBIT C

18 U.S.C. § 1028A

Title 18, United States Code, Section 1028A provides:

(a) Offenses.--

* * *

(2) Terrorism offense.--Whoever, during and in relation to any felony violation enumerated in section 2332b(g)(5)(B), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person or a false identification document shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 5 years.

18 U.S.C. § 1030

Title 18, United States Code, Section 1030 provides:

(a) Whoever--

* * *

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

* * *

(C) information from any protected computer;

* * *

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any—

(A) threat to cause damage to a protected computer;

(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

(C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;

shall be punished as provided in subsection (c) of this section.

* * *

(c) The punishment for an offense under subsection (a) or (b) of this section is--

(1)(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if—

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds \$5,000...

(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph...

18 U.S.C. § 2339B

Title 18, United States Code, Section 2339B provides:

(a) Prohibited activities.--

(1) Unlawful conduct.--Whoever knowingly provides material support or resources to a foreign terrorist organization, or attempts or conspires to do so, shall be fined under this title or imprisoned not more than 20 years, or both, and, if the death of any person results, shall be imprisoned for any term of years or for life. To violate this paragraph, a person must have knowledge that the organization is a designated terrorist organization (as defined in subsection (g)(6)), that the organization has engaged or engages in terrorist activity (as defined in section 212(a)(3)(B) of the Immigration and Nationality Act), or that the organization has engaged or engages in terrorism (as defined in section 140(d)(2) of the Foreign Relations Authorization Act, Fiscal Years 1988 and 1989).

* * *

(g)(6) [T]he term "terrorist organization" means an organization designated as a terrorist organization under section 219 of the Immigration and Neutrality Act.

18 U.S.C. § 3282

Title 18, United States Code, Section 3282 provides:

(a) In general.--Except as otherwise expressly provided by law, no person shall be prosecuted, tried, or punished for any offense, not capital, unless the indictment is found or the information is instituted within five years next after such offense shall have been committed.

18 U.S.C. § 3286

Title 18, United States Code, Section 3286 provides:

(a) Eight-year limitation.--Notwithstanding section 3282, no person shall be prosecuted, tried, or punished for any noncapital offense involving a violation of any provision listed in section 2332b(g)(5)(B), or a violation of section 112, 351(e), 1361, or 1751(e) of this title, or section 46504, 46505, or 46506 of title 49, unless the indictment is found or the information is instituted within 8 years after the offense was committed. Notwithstanding the preceding sentence, offenses listed in section 3295 are subject to the statute of limitations set forth in that section.

EXHIBIT D

**IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA**

Alexandria Division

UNITED STATES OF AMERICA)	
)	CRIMINAL NO. 1:15-MJ-515
v.)	
ARDIT FERIZI,)	AFFIDAVIT IN SUPPORT OF
a/k/a "Th3Dir3ctorY,")	REQUEST FOR EXTRADITION
)	
Defendant.)	

I, Kevin M. Gallagher, being duly sworn, depose, and state:

1. I am a citizen of the United States.
2. I am a Special Agent with the Federal Bureau of Investigation (FBI) assigned to the Washington Field Office. I have been employed by the FBI for approximately six years.
3. The FBI is one of the agencies within the United States government responsible for the enforcement of federal criminal laws. As an agent with the FBI, I have training in the preparation, presentation, and service of criminal complaints and arrest and search warrants, and have been involved in the investigation of numerous types of offenses against the United States, including crimes of terrorism.
4. Based on my training and experience as an agent with the FBI, I am familiar with the means and methods of those who commit computer and identity theft-related crimes, and those who provide material support to Foreign Terrorist Organizations (FTOs).
5. My duties have included conducting an investigation of the above-named defendant in the criminal case captioned United States v. Ardit Ferizi, a/k/a "Th3Dir3ctorY, 1:15-MJ-515. As the lead investigator, I am familiar with the facts and circumstances of the

investigation from my personal participation in this investigation and information provided to me by other law enforcement officials involved in this investigation.

I. BACKGROUND

A. Identification of FERIZI as “Th3Dir3ctorY”

6. The investigation has revealed that the defendant, Ardit FERIZI, is a leader of a known Kosovar internet hacking group called Kosova Hacker’s Security (KHS), which provided unlawfully obtained personally identifiable information (PII) to the Islamic State of Iraq and the Levant (ISIL), as described below.

7. On April 5, 2015, the user of Twitter account @Th3Dir3ctorY, using the name “Ardit Ferizi,” publicly tweeted a link to a June 2013 article from the InfoSec Institute,¹ as shown in the screenshot below:

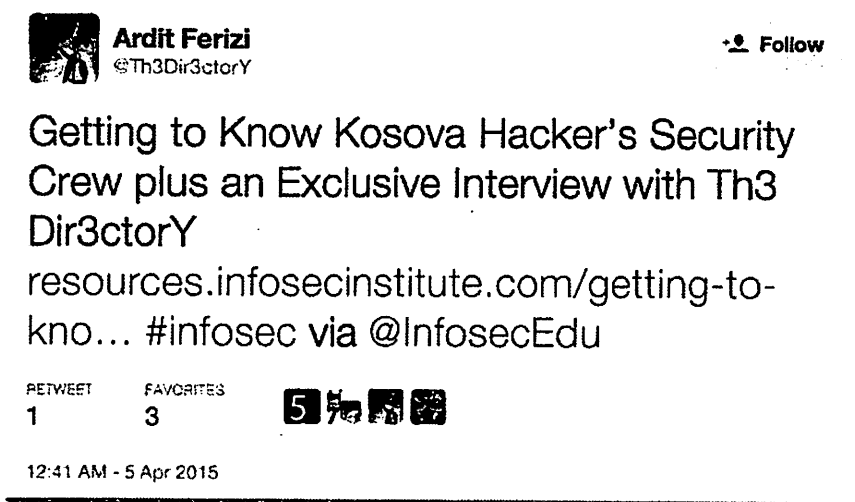


Photo: Screenshot of FERIZI/@Th3Dir3ctorY’s April 5, 2015 Tweet with a link to the June 2013 InfoSec Institute Article on KHS and @Th3Dir3ctorY

¹ The InfoSec Institute (www.infosecinstitute.com), founded in 1998 and based in Illinois, United States, is a training institute for technology professionals focused on information assurance and related training. InfoSec Institute also publishes research and articles, including interviews with hacking organizations.

8. According to the interview of “Th3Dir3ctorY” by the InfoSec Institute, the user of Twitter account @Th3Dir3ctorY is the leader of a group of ethnic Albanian hackers from Kosovo, calling themselves Kosova Hacker’s Security, which is responsible for compromising government and private websites in Israel, Serbia, Greece, the Ukraine, and elsewhere.

9. According to the article, as of the time of publication, KHS claimed responsibility for having hacked more than 20,000 websites, including: 90 percent of Serbian government websites; Interpol, based in France (including taking its site down for two days) in October 2012; and IBM’s research domain, researcher.ibm.com, located in Somers, New York, in May 2012. Again according to the article, hackers calling themselves “Th3Dir3ctorY” and “ThEta.Nu” also claimed responsibility for compromising Microsoft’s Hotmail servers in 2011. KHS itself has confirmed its involvement in these attacks in other open sources.

10. On or about July 10, 2015, the user of Twitter account @Th3Dir3ctorY posted the below tweet identifying himself as “Owner of Kosova Hacker’s Security, PentagonCrew,” and again used the name “Ardit Ferizi”:

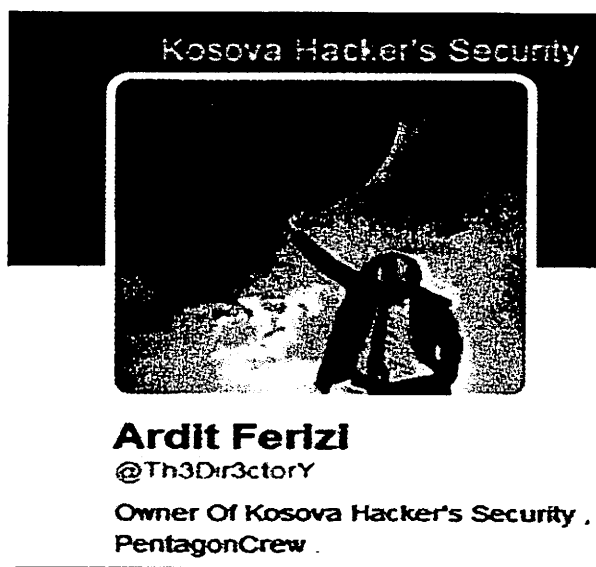


Photo: Screenshot of @Th3Dir3ctorY's Twitter profile as of July 10, 2015

11. According to Twitter records, the Twitter account @Th3Dir3ctorY was registered on September 1, 2012, using Microsoft email account lajmetal@hotmail.com, from an Internet Protocol² address allocated to IPKO Telecommunications LLC in Albania, a telecommunications company that provides services in the adjacent country of Kosovo. This registration information is consistent with @Th3Dir3ctorY's association with KHS, an organization which claims to be associated with Kosovo. As discussed below, FERIZI's passport was issued by the Government of Kosovo.

12. The FBI's investigation, including information provided to the FBI by the Royal Malaysian Police, has revealed that FERIZI currently resides in Malaysia on a Student Pass and that, as of Spring 2015, FERIZI was studying at Limkokwing University in Malaysia. FERIZI appears to have entered Malaysia in early 2015.

13. IP logs for Twitter account @Th3Dir3ctorY reveal that all logins to @Th3Dir3ctorY between June 15, 2015, and August 14, 2015, originated with Internet Service Providers (ISPs) in Malaysia.

B. ISIL is a Foreign Terrorist Organization

14. On October 15, 2004, the U.S. Department of State designated Al-Qa'ida in Iraq (AQI), then known as Jam'at al Tawhid wa'al-Jihad, as an FTO under Section 219 of the Immigration and Nationality Act (see Exhibit C), and as a Specially Designated Global Terrorist

² Devices directly connected to the Internet are identified by a unique number called an Internet Protocol (IP) address. This number is used to route information between devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address so that the responding device knows where to send its response. In other words, an IP address is similar to a phone number, and indicates the online identity of the communicating device. IP addresses are allocated by an international organization, the Internet Assigned Numbers Authority.

Entity pursuant to Executive Order 13224.

15. On May 15, 2014, the U.S. Department of State amended the designation of AQI as an FTO under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist Entity under Executive Order 13224 to list the name “Islamic State of Iraq and the Levant” as its primary name. The Department of State also added the following aliases to the ISIL listing: the Islamic State of Iraq and al-Sham (ISIS), the Islamic State of Iraq and Syria (ISIS), ad-Dawla al-Islamiyya fi al-‘Iraq wa-sh-Sham, Daesh, Dawla al Islamiya, and Al-Furqan Establishment for Media Production. Although the group described herein has never called itself “Al-Qa’ida in Iraq,” this name has frequently been used by others to describe it. To date, ISIL remains designated as an FTO. In an audio recording publicly released on or around June 29, 2014, ISIL announced a formal change of its name to the Islamic State.

16. On approximately September 21, 2014, ISIL spokesperson Abu Muhammad al-Adnani called for attacks against citizens, civilian or military, of the countries participating in the United States-led coalition against ISIL.

II. EVIDENCE

17. The evidence obtained from various sources, including witness statements, electronic media, and social media records demonstrates that, in or about June 2015, FERIZI accessed without authorization a protected computer, namely a server (the “Victim Server”) belonging to an identified Internet hosting company (the “Hosting Company”), which maintained the website belonging to a U.S. retailer that sells goods via the Internet to customers in multiple states (“Victim Company”). The Hosting Company informed the FBI that the compromised server was a dedicated server, meaning that no companies other than the Victim Company utilized the server. The Victim Server is leased by the Victim Company and owned by the Hosting

Company. The Victim Server is located in the United States.

18. Information provided by the Victim Company to the FBI in August 2015 revealed that, beginning as early as June 13, 2015, the user “KHS,” which refers to “Kosova Hacker’s Security” (discussed above), had access to customer details from their database, including: names, addresses, cities, states, countries, phone numbers, email accounts, and usernames and passwords. Additionally, the Victim Company reported to the FBI that an “Albanian hacker,” using `khs-crew@live.com`, believed to be FERIZI, threatened the Victim Company for deleting the hacker’s “files” from the Victim Server. The “Albanian hacker” threatened to “publish every client” on the Victim Server if the Victim Company terminated his access. The Victim Company responded to the user of `khs-crew@live.com` requesting that its servers not be attacked. In response, the user of `khs-crew@live.com` demanded two Bitcoin, worth approximately \$500, to report the method he was using to gain access to the Victim Server, to “protect and remove all bugs” from the server, and to terminate his access to the Victim Server.

19. IP information obtained from the Victim Server reveals that a Malaysian IP address was used to conduct a Structured Query Language (SQL) injection attack³ on the Victim Server on July 8, 2015. Records obtained from Facebook for an account attributed to “ardit.ferizi01” and Twitter records for account @Th3Dire3ctory (discussed above), which are believed to be used by FERIZI, reveal that these accounts were accessed from the same Malaysian IP address the day before and hours after the SQL attack on July 8, 2015. FERIZI also accessed the Facebook and Twitter accounts from that Malaysian IP address on multiple other occasions between July 5, 2015

³ A SQL injection is a technique often used against retailer websites that inserts malicious code into a database entry field thereby causing, for example, the database to send its contents to the attacker.

and July 13, 2015.

20. On August 11, 2015, in the name of the Islamic State Hacking Division (ISHD), known ISIL member Junaid Hussain, also known as “Abu Hussain al-Britani,” now deceased, posted a public hyperlink on Twitter with the title “U.S. Military AND Government personnel, including Emails, Passwords, Names, Phone Numbers, and Location Information,” which provided ISIL supporters in the United States and elsewhere with the PII belonging to 1,351 U.S. military and other government personnel to be used to target the U.S. personnel for attacks and violence. An FBI review of the Victim Server revealed that the full names, email addresses, passwords, and cities and states of residence for the 1,351 U.S. government personnel included in the release by Hussain and ISHD on August 11, 2015 were found on the Victim Server. Additionally, records from the Facebook account associated with “ardit.ferizi01” revealed that FERIZI sent himself a “.csv” file containing 91,525 unique email addresses. Of the 1,351 unique records posted by ISIL on August 11, 2015, 1,089 records matched those records contained in the “.csv” file.

21. Twitter records demonstrate that earlier, on approximately April 26 and/or 27, 2015, the users of Twitter accounts @Muslim_Sniper_D and @Th3Dir3ctorY participated in a Twitter exchange during which FERIZI, as the user of @Th3Dir3ctorY, provided Tariq Hamayun, the user of @Muslim_Sniper_D, an ISIL member located in Syria, with screen shots of what appears to be unlawfully obtained credit card information belonging to 27 Americans, 18 British and 22 French citizens. This information included names; addresses; zip codes; birth dates; and credit card information such as the type, number, expiration date and Card Verification Value. During the exchange, the user of Twitter account @Muslim_Sniper_D confirmed that Abu Hussain al-Britani (Junaid Hussain) was Hamayun’s friend and that “he [Abu Hussain al-Britani]

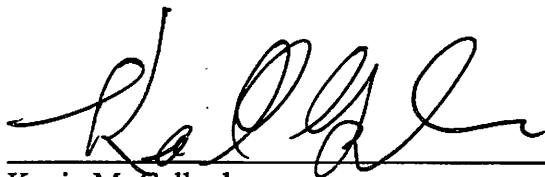
had “told me [Hamayun] a lot about u [FERIZI],” indicating that, as of the date of the exchange FERIZI and Hussain were already in communication with one another. At the end of this exchange, the user of @Muslim_Sniper_D, Hamayun, wrote the following message to the user of Twitter account @Th3Dir3ctorY, FERIZI: “Pliz [sic] brother come and join us in the Islamic state.”

III. IDENTIFICATION

22. On October 12, 2015, FERIZI was detained by the Royal Malaysia Police on the provisional arrest warrant request from the United States and he remains in custody pending extradition proceedings.


23. According to his passport, a copy of which was provided to the FBI by the Royal Malaysia Police following his detention, ARDIT FERIZI is a citizen of Kosovo, born on January 12, 1995, in the city of Gjakova. The FBI was informed by the Royal Malaysia Police that FERIZI entered Malaysia using Kosovo Passport number is P00390126, a copy of which has been attached as Exhibit 1.

24. Attached to this affidavit as Exhibit 2 is a photograph that was obtained from the Facebook account associated with "ardit.ferizi01." This photograph was viewed by an FBI agent who personally observed ARDIT FERIZI following his detention by the Royal Malaysia Police on the provisional arrest warrant request from the United States. The FBI agent confirmed to me that the person in Exhibit 2 is ARDIT FERIZI, the person detained by the Royal Malaysia Police, whose criminal conduct is described in this affidavit and who has been charged in this case.



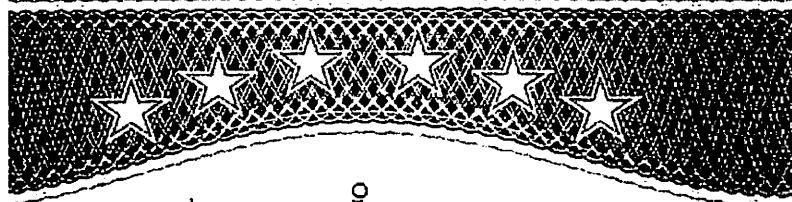
Kevin M. Gallagher
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me
this 5 day of November, 2015

 /s/
Theresa Carroli Buchanan
United States Magistrate Judge

The Hon. Theresa Carroll Buchanan
United States Magistrate Judge

EXHIBIT 1



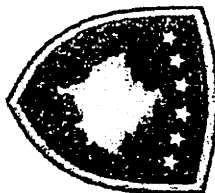
REPUBLIKA E KOSOVËS
РЕПУБЛИКА КОСОВО
REPUBLIC OF KOSOVO

Kjo pasaportë është pronë e Shtetit
të Kosovës.
Мдајтеси i saj është сhtetas i Republikës
së Kosovës.

Овај пасоу је власништво државе Косово.
Носилац овог пасоуа
је држављанин Републике Косово.

This passport is the property
of the state of Kosovo
The holder of this passport is a citizen of the
Republic of Kosovo.

REPUBLIKA E KOSOVËS
РЕПУБЛИКА КОСОВО
REPUBLIC OF KOSOVO



PASAPORTË
ПАСОУ
PASSPORT



69

VIZAT - BM3E - VISAS

SOCIAL VISIT

VIZAT - BM3E - VISAS



SINGLE ENTRY VISA



Visa No:

SR131/14

Date:

02/04/2014

SEEN AT THE OFFICE OF THE
EMBASSY OF MALAYSIA
BELGRADE, REPUBLIC OF SERBIA

Good for a SINGLE JOURNEY to

Malaysia. This VISA must be used

before 02/04/2014. Provided with

Passport remains valid.

CONULAR OFFICER
BELGRADE

NOT PERMITTED TO ENGAGE IN ANY EMPLOYMENT
PROFESSIONAL OCCUPATION IN MALAYSIA.

Fee Paid: RM 5.00 Receipt No: PH97615

VIZAT - BIJE - VISAS

MALAYSIA IMMIGRATION DEPARTMENT
MALAYSIA IMMIGRATION DEPT.
KUALA LUMPUR
19 AUG 2014
FID No. 1
Passport No. J88398126
Date of entry 19/08/2014
Date of expiry 26/09/2014

Visas and stamps in chronological order

SOCIAL VISIT VIZAT - BIJE - VISAS

SRB SINGLE ENTRY VISA
Visa No. SR 231/14 Date 26/09/2014
STEN AT THE OFFICE OF THE
EMBASSY OF MALAYSIA
BELGRADE, REPUBLIC OF SERBIA
Good for a SINGLE JOURNEY to
Malaysia. This visa must be used
before 26/09/2014. Validity 14
days from issuance date.
NOT ADMITTED TO ENTER IN ANY EMPLOYMENT
OR PROFESSIONAL OCCUPATION IN MALAYSIA
CONSULAR OFFICER
BELGRADE

Visas and stamps in chronological order

Tice Paid: EUR 5000 Receipt No: EH.13.113

The validity of data on 5039 MAR 2015
is hereby amended to 17 MAR 2015

12 FEB 2015

of Negara Indragresen (Negri Solanigor)



MAIL ADDRESS

Receipt No : HWT-D000439
For Paid Post : 24YR 60.00
Vide : 24YR 2A 00

1 2 MAR 2015

14215

Good for any number of journeys in Malaysia until 30 September 1964.

Immigration Regulations 1963
STUDENT'S PASS [Reg.13(3)]



Director General
FBIHQ 370-49 JAC

Name : FERIZ ARDIT
Gender : MALE
Nationality : REPUBLIC OF KOSOVO

Page No : 1639123

Subject to Regulation 13(7) International Regulations 1963, the subject is permitted to enter and reside in MYTH MALLASIA until 1968-1973 as a student for the purpose of studying at MANAGEMENT & SCIENCE UNIVERSITY ONLY. 17C, ALOR A JEN KORESTRAN, 1202 OFF PERSIANAN BUKAN KINYOVA 12, BUKIT ALAM, 40100, SELANGOR, SELANGOR. 1

Ref No :
Date Of Issue :
Place Of Issue :

12 BENJALAN, 40100, SELANGOR
12 MAR 2015

See Page 10

KOSFERIZI<ARDIT<<<<<<<<<<<<<<<<<<<<<<<<<<<<
J3901262K0S9512014M18112831509164<<<<<<<<

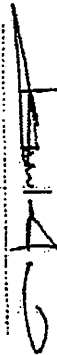
VIZAT - BN3E - VISAS

VIZAT - BN3E - VISAS

Special Pass No. VE0051A96636

Valid till. 9.04.15 issued

Ref. BVPSTU/1202/40098911/1



b/p. Ketua Pengarah Imigrasi
Malaysia

AUTHORITY:
TPPI

11 MAR 2015

12

13

VIZAT - BM3E - VISAS

VIZAT - BM3E - VISAS

Special Pass No. VE0654394542

Valid till 06.01.2015 issued

Ref: BVPSTU/140121100098741/1

[Signature]
Dip. Ketua Pengadilan Tinggi
Majlis

AUTHORITY:
TPPIK

08 APR 2015

14

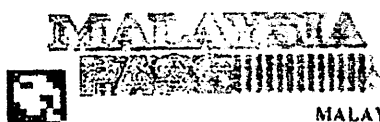
Visas and stamps in chronological order

15

Visas and stamps in chronological order

Visas and stamps in chronological order

VIZAT - ВИЗЕ - VISAS



Director General
VP HQ, JEDF3761560

MALAYSIA IMMIGRATION
[Section 3(1), Passport Act 1966]
MULTIPLE ENTRY VISA

Receipt No : H076031198
 Fee Paid Price : MYR 60.00
 Date : MYR 22.02

Good for any member of your family's physiology and mind. 06 MAY 2016
 100% natural and 100% pure. 100% natural and 100% pure.

Immigration Regulations 1963
STUDENT'S PASS (Reg 13(5))

DOM 19

Name	PERKID ARDIT	Passport No	1-P0000154
Gender	MALE		
Date of Birth	REPUBLIC OF KOSOVO		
Place of Birth	Subject to Registration (201) (among other Registrations) P.02, the subject is permitted to enter and remain in WEST MALAYSIA until 01 MAY 2018 on a condition that the purpose of staying at UNIVERSITI TEKNOLOGI KREATIF (UNIKOM) LANGKAT, PULAU TIAU, 01200 TERENGGANU, MALAYSIA, KAMPUNG MELANGKAT, 20 LANGKAT		
Ref No	STP2017101010000000		
Date of Issue	01 MAY 2018		
Place of Issue	IMMIGRATION OFFICE OF PUTRAJAYA		

TSKOSFERIZI<ARDIT<<<<<<<<<<<<<<<<<<<<<<<<<<<<
P003901262K0S9512014M18112831605066<<<<<<<<

SECRET

Useful properties:

а постои профитна је дјела за објектима који је имао посматрати

immediately upon their return

EXHIBIT 2



Ardit Ferizi

Follow Jul 29 · 🌐

In Cyberjaya

Like Share

👍 7 people like this.



Galuh Irmia Cahyaningtyas

August 1 at 9:30am · Like · 🌐

Sponsored 🌐



Come home to Verizon

www.verizonwireless.com

Get 10 gigs for \$80/mo and \$15/mo
line + taxes & fees