# UNITED STATES DISTRICT COURT

for the

District of Columbia

In the Matter of the Seizure of
*(Briefly describe the property to be seized)*

IN THE MATTER OF THE SEIZURE OF A SERVER HELD BY AN INTERNET SERVICE PROVIDER

Case No. 26-sz-49

## APPLICATION FOR A WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

I, a federal law enforcement officer or attorney for the government, request a seizure warrant and state under penalty of perjury that I have reason to believe that the following property in the Jurisdiction of the District of Columbia is subject to forfeiture to the United States of America under U.S.C. § 18 U.S.C. § 2339B, 18 U.S.C. § 1956(h), 18 U.S.C. § 981(a)(1)(C), and 28 U.S.C. § 2461(c)

(describe the property): See Attachment A, hereby incorporated by reference.

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE.

❒ Continued on the attached sheet.

[redacted]
*Applicant's signature*

[redacted] Special Agent
*Printed name and title*

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: 08/18/2026

*Judge's signature*

City and state: Washington, D.C.

Matthew J. Sharbaugh, United States Magistrate Judge
*Printed name and title*

# UNITED STATES DISTRICT COURT
for the
District of Columbia

In the Matter of the Seizure of
*(Briefly describe the property to be seized)*

IN THE MATTER OF THE SEIZURE OF A SERVER HELD BY AN INTERNET SERVICE PROVIDER ) ) ) ) )

Case No. 26-sz-49

## WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests that certain property located in the Jurisdiction of the District of Columbia be seized as being subject to forfeiture to the United States of America. The property is described as follows:

See Attachments A-1 hereby incorporated by reference.

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

**YOU ARE COMMANDED** to execute this warrant and seize the property on or before 09/01/2026
*(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

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

An officer present during the execution of the warrant must prepare, as required by law, an inventory of any property seized and the officer executing the warrant must promptly return this warrant and a copy of the inventory to
Matthew J. Sharbaugh .
*(United States Magistrate Judge)*

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _______ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of ____________________ .

Date and time issued: 08/18/2026

*Judge's signature*

City and state: Washington, D.C.

Matthew J. Sharbaugh, United States Magistrate Judge
*Printed name and title*

## Return

| Case No.: | Date and time warrant executed: | Copy of warrant and inventory left with: |
|---|---|---|
| 26-sz-49 | | |

Inventory made in the presence of:

Inventory of the property taken:

## Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: ____________________

____________________
*Executing officer's signature*

____________________
*Printed name and title*

## **ATTACHMENT A-1**

**SUBJECT SERVER**

*IP Address:* ***45.134.141.68***

With respect to the IP Address and associated server listed above ("**SUBJECT SERVER**"), DataCamp Limited., 9 Coldbath Square, London, United Kingdom, EC1R 5HL who is the electronic service infrastructure provider for the **SUBEJCT SERVER**, shall take the following actions to effectuate the seizure of the **SUBJECT SERVER**:

1) Take all reasonable measures to redirect the domain names to substitute servers at the direction of the Federal Bureau of Investigation by associating the **SUBJECT SERVER** to the following authoritative name-server(s):
    a. ns1.fbi.seized.gov
    b. ns2.fbi.seized.gov
    c. Any new authoritative name server to be designated by a law enforcement agent in writing, including e-mail, to DataCamp Limited, the Subject provider.
2) Prevent any further modification to, or transfer of, the **SUBJECT SERVER** pending transfer of all right, title, and interest in the **SUBJECT SERVER** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **SUBJECT SERVER** cannot be made absent court order or, if forfeited to the United States, without prior consultation with the FBI.
3) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.
4) Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

The Government will display a notice on the website to which the **SUBJECT SERVER** will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

**This domain has been seized by the Federal Bureau of Investigation and Department of Justice in accordance with a seizure warrant issued by the United States District Court for the District of Columbia as part of a law enforcement action against HAMA**

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF COLUMBIA**

| | |
|---|---|
| **IN THE MATTER OF THE SEIZURE OF A SERVER HELD BY AN INTERNET SERVICE PROVIDER** | **Case No. 26-sz-49**<br><br>**Filed Under Seal** |

***Reference: USAO Ref. #2025R00808; Subject Account(s): 45.134.141.68***

## AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEIZURE WARRANT

I, [redacted] being first duly sworn, hereby depose and state as follows:

## INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a seizure warrant concerning a server supporting the website alqassam.ps with the IP address **45.134.141.68 (SERVER 68)** further described below and in Attachment A. Known and unknown actors use **SERVER 68** to support a cryptocurrency donation scheme to generate revenue for HAMAS, which is a designated Foreign Terrorist Organization ("FTO"). An electronic service provider named DataCamp Limited ("DataCamp") controls **SERVER 68**. DataCamp is headquarted in London, United Kingdom at 9 Coldbath Square. DataCamp operates a brand known as "DataPacket." DataCamp and DataPacket provide electronic services and leases servers through servers and infrastructure located in the United States, the United Kingdom and other countries, including Brazil. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that **SERVER 68** is subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A), 981(a)(1)(G)(i), and 982(a)(1) because it is property involved in transactions or attempted transactions that violate 18 U.S.C. § 1956(a)(2)(A) (International Promotional Money Laundering) done with the intent to promote the carrying on of specified unlawful activity, specifically violations of 18 U.S.C.

§ 2339B (Providing Material Support or Resources to Designated Foreign Terrorist Organizations).

2. As explained in more detail below, a known foreign person transferred funds from a place outside the United States to a place in the United States to register **SERVER 68** with the intent to promote the carrying on of a cryptocurrency donation scheme to support HAMAS. Because **SERVER 68** is subject to civil and criminal forfeiture, the Government may seize it by warrant pursuant to 18 USC § 981(b) and 21 U.S.C. § 853(f). The procedure by which the Government will seize **SERVER 68** is described in Attachment A.

3. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since September 2022. While employed by the FBI, I have investigated federal criminal violations related to high technology or cybercrime, including violations of 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1030 (Fraud and Related Activities in Connection with Computers), and 18 U.S.C. § 1956 (Money Laundering). I have gained experience through training and everyday work relating to conducting these types of investigations. Prior to becoming a special agent of the FBI, I earned a bachelor's degree in history, a master's degree in criminal justice, and served more than seven years as a communications officer in the United States Marine Corps. I have received training related to counter-terrorism investigations, computer networking, virtual currency, and cyber security.

4. Specifically, I have completed the FBI's Accelerated Cyber Training Program, which included ten virtual currency courses. I am licensed to trace virtual currency via a Blockchain Analysis Software that has provided reliable information in the past and have attended in-person training and conferences focused on such. I have obtained a competency certification associated with Blockchain Analysis Software. I have obtained a Global Information Assurance

Certification in Security Essentials and also a certification on using Open Source Intelligence investigative methods.

5. In addition to my direct experience, I have also had conversations with cyber investigators across the FBI regarding dozens of complex cases, including several involving the seizures of virtual currency accounts, bank accounts, and domains. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, analysts, witnesses, and agencies. This affidavit is intended to show that there is sufficient probable cause for the requested seizure warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

## ASSETS TO BE SEIZED

6. I make this affidavit in support of an application for a seizure warrant for a web server leased on IP Address 45.134.141.68, hereinafter referred to as **SERVER 68**. DataCamp has confirmed it leases and controls **SERVER 68**. SERVER 68 is further attached to the internet and is accessible from anywhere in the world, including the United States and the District of Columbia.

## JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1355(a), which provides that [t]he district courts shall have original jurisdiction . . . of any action or proceeding for the recovery or enforcement of any fine, penalty, or forfeiture, pecuniary or otherwise, incurred under any Act of Congress . . . .” This Court also has subject matter jurisdiction pursuant to 28 U.S.C. § 1345, which provides that “the district courts shall have original jurisdiction of all civil actions, suits or proceedings commenced by the United States.”

8. This Court has *in rem* jurisdiction over **SERVER** 68 and venue lies in this district pursuant to 18 U.S.C. § 981(b)(3), 28 U.S.C. §§ 1355(b)(1)(B) and 1395(a), and 18 U.S.C. § 3238,

because the criminal offenses under investigation were begun or committed upon the high seas, or elsewhere out of the jurisdiction of any particular State or district, and no offender is known to have, or have had, residence within any United States district. This Court further has jurisdiction to issue a seizure of **SERVER 68** located outside of this District because this is a matter involving international terrorism pursuant to Federal Rules of Criminal Procedure 41(b)(3). This is a related matter to a prior seizure warrant authorized by the Honorable Judge G. Michael Harvey in 26-sz-45, and a search warrant authorized by the Honorable Moxila A. Upadhyaya in 26-sc-1521. Paragraphs 6-56 of this affidavit are substantially the same as information provided in the affidavits submitted in those warrants.

## SUBSTANTIVE CRIMINAL OFFENSES

6. Providing Material Support or Resources to Designated Foreign Terrorist Organizations. This investigation relates to the provision of material support to a foreign terrorist organization, in violation of 18 U.S.C. § 2339B.

7. 18 U.S.C. § 2339B(a)(1) provides, "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." "[M]aterial support or resources" is defined as

> any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel (1 or more individuals who may be or include oneself), and transportation, except medicine or religious materials.

18 U.S.C. §§ 2339A(b)(1), 2339B(g)(4).

8. Money Laundering. 18 U.S.C. § 1956(a)(1)(B)(i) makes it a crime to conduct or attempt to conduct a financial transaction, knowing that the property involved in the transaction

represents the proceeds of some form of unlawful activity, and which in fact involves the proceeds of specified unlawful activity, knowing that the transaction is designed in whole or in part to conceal the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity. This activity is commonly referred to as concealment money laundering.

9. The money laundering statute, 18 U.S.C. § 1956, also makes it a crime to conspire to engage in money laundering: "Any person who conspires to commit any offense defined in [section 1956] or section 1957 shall be subject to the same penalties as those prescribed for the offense the commission of which was the object of the conspiracy." 18 U.S.C. § 1956(h).

10. Title 18, United States Code, Section 1956(a)(2)(A) (International Promotional Money Laundering) prohibits the transportation, transmission, or transfer of monetary instruments or funds from the United States to or through a place outside the United States, or to the United States from or through a place outside the United States with the intent to promote the carrying on of a specified unlawful activity. Specified unlawful activity is defined in 18 U.S.C. § 1956(c)(7)(D) to include violations of 18 U.S.C § 2339B.

**LEGAL AUTHORITIES RELATING TO SEIZURE AND FORFEITURE**

9. Pursuant to 18 U.S.C. § 981(a)(1)(G)(i), "[a]ll assets, foreign or domestic . . . of any individual, entity, or organization engaged in planning or perpetrating any Federal crime of terrorism (as defined in 18 U.S.C. § 2332b(g)(5)) against the United States, citizens or residents of the United States, or their property, and all assets, foreign or domestic, affording any person a source of influence over any such entity or organization" are subject to forfeiture to the United States. Violations of 18 U.S.C. § 2339B are included in the definition of a Federal crime of terrorism. Section 981(a)(1)(G)(i) thus covers two categories of property: (1) all assets, foreign or

domestic, of individuals, entities, or organizations engaged in planning or perpetrating federal crimes of terrorism; and (2) all assets, foreign or domestic, that afford any person a source of influence over an entity or organization engaged in planning or perpetrating any federal crime of terrorism. *See, e.g.*, *United States v. All Petroleum-Product Cargo Aboard the Bella with Int'l Mar. Org. No. 9208124*, Civil Action No. 20-1791 (JEB), 2021 U.S. Dist. LEXIS 189395, at *12–13 (D.D.C. Oct. 1, 2021) ("The Court concludes, as a result, that Defendant Properties likely afforded Madanipour and Mobin a source of influence over the IRGC because those properties were critical to furthering the affairs of the terrorist group's enterprise. The Government thus properly brought this action for forfeiture under 18 U.S.C. § 981(a)(1)(G)(i).") (citations omitted).

10. Among the Government's forfeiture authorities, the terrorism forfeiture provision applies to the broadest range of property. Specifically, § 981(a)(1)(G)(i) provides for the forfeiture of *all* property, foreign or domestic, of a terrorist organization or that affords a source of influence to any entity or organization over a terrorist organization, irrespective of whether the property has any nexus to a crime or to the United States. *See, e.g., United States v. One Gold Ring with Carved Gemstone*, Civil Action No. 16-CV-02442 (TFH), 2019 U.S. Dist. LEXIS 195423, at *1–2 (D.D.C. Nov. 7, 2019) ("§ 981(a)(1)(G)(i) covers all property 'foreign or domestic.' That is, the statute empowers the Government to seek the forfeiture of property outside the United States, which may have never touched the United States. The broad expanse of this language is for forfeiture actions to reach all property of terrorist organizations.").

11. Property that is involved in a money laundering offense (or conspiracy to commit a money laundering offense) is subject to forfeiture under both civil and criminal authorities. Pursuant to 18 U.S.C. § 981(a)(1)(A) and (a)(1)(C), "[a]ny property, real or personal, involved in a transaction or attempted transaction in violation of section 1956, 1957 or 1960 of this title, or

any property traceable to such property," and "[a]ny property, real or personal, which constitutes or is derived from proceeds traceable to" a specified unlawful activity, such as a violation of 18 U.S.C. § 2339B, is subject to forfeiture to the United States. Similarly, 18 U.S.C. § 982(a)(1) provides that the "[t]he court, in imposing a sentence on a person convicted of an offense in violation of section 1956, 1957, or 1960 of this title, shall order that the person forfeit to the United States any property, real or personal, involved in such offense, or any property traceable to such property."

12. Property "involved in" a money laundering offense "includes the money or other property being laundered (the corpus), any commissions or fees paid to the launderer, and any property used to facilitate the laundering offense." *United States v. Puche*, 350 F.3d 1137, 1153 (11th Cir. 2003) (internal quotation omitted). "The statute sweeps broadly because 'money laundering largely depends upon the use of legitimate monies to advance or facilitate the scheme.'" *United States v. Bikundi*, 926 F.3d 761, 793 (D.C. Cir. 2019) (quoting *Puche*, 350 F.3d at 1153). Forfeitures can include untainted funds that are comingled with tainted funds derived from illicit sources. *See United States v. Casey*, 444 F.3d 1071, 1073 (9th Cir. 2006) ("It is . . . clear that Congress intended criminal forfeiture provisions to eliminate profit from certain criminal activities, including money laundering . . . ."); *United States v. Kivanc*, 714 F.3d 782, 794-95 (4th Cir. 2013) ("Consequently, when legitimate funds are commingled with property involved in money laundering or purchased with criminally derived proceeds, the entire property, including the legitimate funds, is subject to forfeiture."); *United States v. Lazarenko*, 564 F.3d 1026, 1035 (9th Cir. 2009) ("[I]n a money laundering charge, the commingling of tainted money with clean money taints the entire account. The money transferred from a commingled account does not need to be traceable to fraud, theft, or any wrongdoing at all. It is enough that the money, even if

innocently obtained, was commingled in an account with money that was obtained illegally.") (internal citations omitted). When the laundering transaction is a purchase, sale, exchange, or disbursement, the property that is bought, sold, exchanged, or otherwise the subject of the transaction is deemed to be "involved in" the offense. *See, e.g.*, *United States v. Real Prop. Identified As: Parcel 03179-005R*, 311 F. Supp. 2d 126, 130 (D.D.C. 2004) ("[T]he Court concludes that the Government has demonstrated that the aircraft was involved in a monetary transaction [a payment of specific unlawful activity proceeds to release a lien on the aircraft] involving the proceeds of specified unlawful activity. Clearly, this involvement renders the aircraft subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A).")

13. Title 18, United States Code, Section 981(a)(1)(C) subjects to civil forfeiture "[a]ny property, real or personal, which constitutes or is derived from proceeds" of any "specified unlawful activity." The term "specified unlawful activity" is defined in 18 U.S.C. § 1956(c)(7) and 1961(1) and it includes, among other crimes, Providing Material Support to a Foreign Terrorist Organization, in violation of 18 U.S.C. § 2339B.

14. In addition, 28 U.S.C. § 2461(c) provides that, "[i]f a person is charged in a criminal case with a violation of an Act of Congress for which the civil or criminal forfeiture of property is authorized," then the Government can obtain forfeiture of property "as part of the sentence in the criminal case."

15. This application seeks a seizure warrant under both civil and criminal authorities because the Target Properties consist of a transferrable group of web domains that can easily be placed beyond process if not seized by a warrant.

16. Pursuant to 18 U.S.C. § 981(b), property subject to forfeiture under § 981 may be seized via a civil seizure warrant issued by a judicial officer "in any district in which a forfeiture

action against the property may be filed," if there is probable cause to believe the property is subject to forfeiture. Section 982(b)(1) incorporates the procedures in 21 U.S.C. § 853 (other than subsection (d)) for criminal forfeiture proceedings. Section 853(f) of Title 21 permits the Government to request the issuance of a seizure warrant for property subject to criminal forfeiture.

## DEFINITIONS

11. **Virtual Currency**: Virtual currencies are digital tokens of value circulated over the Internet. Virtual currencies are typically not issued by any Government or bank like traditional fiat currencies, such as the U.S. dollar, but rather are generated and controlled through computer software. Different virtual currencies operate on different blockchains, and there are many different, widely used virtual currencies currently in circulation. Bitcoin (or BTC) and ether (ETH) are currently the most well-known virtual currencies in use. BTC exists on the Bitcoin blockchain and ETH exists on the Ethereum network. Typically, a virtual currency that is "native" to a particular blockchain cannot be used on a different blockchain. Thus, absent technological solutions those native assets are siloed within a specific blockchain. For instance, ETH (the native token on the Ethereum network) cannot be used on other networks unless it is "wrapped" by smart contract code. This wrapping process results in what is called Wrapped ETH or WETH.

12. **Blockchain**: Many virtual currencies publicly record all of their transactions on what is known as a blockchain. The blockchain is essentially a distributed public ledger, run by the decentralized network of computers, containing an immutable and historical record of every transaction utilizing that blockchain's technology. The blockchain can be updated multiple times per hour and records every virtual currency address that has ever received that virtual currency and maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

13. **Blockchain Explorer**: These explorers are online tools that operate as a blockchain search engine allowing users the ability to search for and review transactional data for any address on a particular blockchain. A blockchain explorer is software that uses application programming interface and blockchain nodes to draw data from a blockchain and uses a database to arrange and present the data to a user in a searchable format.

14. **Smart Contract:** Smart contracts are computer programs stored on a blockchain that run when predetermined conditions are met. Typically, they are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement. The Ethereum network is designed and functions based on smart contracts.

15. **Stablecoins**: Stablecoins are a type of virtual currency whose value is pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. dollar, or to a different virtual currency. Stablecoins achieve their price stability via collateralizations (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.

16. **Tether (USDT)**: Tether ("USDT") is a virtual currency that resides on multiple blockchains. The value of USDT is tied to the value of the U.S. dollar; therefore, one unit of USDT is represented to be backed by one U.S. dollar in Tether Limited's reserves, making it what is known as a "stablecoin." USDT is hosted on the Ethereum and Tron blockchains, among others. USDT is issued by Tether Limited, a company that controls the smart contracts and treasury for USDT, which is domiciled in the British Virgin Islands. Because Tether manages the smart contracts for USDT, it can blacklist addresses containing USDT.

17. **Tron (TRX)**: Tron is a blockchain network built to host decentralized applications with high speed, scalability and low fees. TRX is the native token used to power the network.

TRC20 is a network protocol used for smart contracts, often enabling USDT transfers via the Tron blockchain.

18. **Virtual Currency Address**: Virtual currency addresses are the particular virtual locations to which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of letters and numbers.

19. **Private Key**: Each virtual currency address is controlled through the use of a unique corresponding private key, a cryptographic equivalent of a password, which is needed to access the address. Only the holder of an address's private key can authorize a transfer of virtual currency from that address to another address.

20. **Virtual Currency Wallet**: There are various types of virtual currency wallets, including software wallets, hardware wallets, and paper wallets. A virtual currency wallet allows users to store, send, and receive virtual currencies. A virtual currency wallet can hold many virtual currency addresses at the same time.

21. Wallets that are hosted by third parties are referred to as "hosted wallets" because the third party retains a customer's funds until the customer is ready to transact with those funds. Conversely, wallets that allow users to exercise total, independent control over their funds are often called "unhosted" wallets.

22. **Virtual Currency Bridge**: A blockchain bridge, otherwise known as a cross-chain bridge, connects two blockchains and allows users to send virtual currency from one chain to the other.

23. **Virtual Currency Exchanges (VCEs)**: VCEs are trading and/or storage platforms for virtual currencies, such as BTC and ETH. There are generally two types of VCEs: centralized exchanges and decentralized exchanges, which are also known as "DEXs." Many VCEs also store

their customers' virtual currency in virtual currency wallets. As previously stated, these wallets can hold multiple virtual currency addresses associated with a user on a VCE's network. Because VCEs act as money services businesses, they are legally required to conduct due diligence of their customers (*i.e.*, KYC checks) and to have anti-money laundering programs in place (to the extent they operate and service customers in the United States).

24. **Blockchain Analysis**: As previously stated, while the identity of a virtual currency address owner is generally anonymous, law enforcement can identify the owner of a particular virtual currency address by analyzing the blockchain (*e.g.*, the Bitcoin blockchain). The analysis can also reveal additional addresses controlled by the same individual or entity. "For example, when an organization creates multiple [BTC] addresses, it will often combine its [BTC] addresses into a separate, central [BTC] address (*i.e.*, a "cluster"). It is possible to identify a 'cluster' of [BTC] addresses held by one organization by analyzing the [BTC] blockchain's transaction history. Open source tools and private software products can be used to analyze a transaction." *United States v. Gratkowski*, 964 F.3d 307, 309 (5th Cir. 2020).

25. In addition to using publicly-available blockchain explorers, law enforcement uses commercial services offered by several different blockchain-analysis companies to investigate virtual currency transactions. These companies analyze virtual currency blockchains and attempt to identify the individuals or groups involved in transactions. Through numerous unrelated investigations, law enforcement has found the information provided by these tools to be reliable.

26. **Decentralized Finance (DeFi)**: Decentralized Finance, or DeFi, is an umbrella term for financial services on public blockchains, primarily the Ethereum network. The Ethereum network's native virtual currency is ETH. Ethereum was the first blockchain that offered various decentralized services within its network. To make these services possible, the Ethereum network

allows other tokens besides ETH to run within the network. These tokens are known as ERC-20 tokens.

27. DeFi is a term used to describe a financial system that operates without the need for traditional, centralized intermediaries. Instead, DeFi platforms offer an alternative financial system that is open for anyone to use, and that allows centralized intermediaries to be replaced by decentralized applications (or dApps). With DeFi, one can do most of the things that banks support—earn interest, borrow, lend, buy insurance, trade derivatives, trade assets, etc.—but it is faster than using traditional banks and does not require paperwork or a third party. DeFi is global, peer-to-peer (*i.e.*, directly between two people rather than routed through a centralized system), pseudonymous, and open to the public.

28. **Recovery Address:** In the context of email accounts, a "recovery address" is an email account address which is provided by the subscriber at the time an email account is registered with a service provider. The recovery address is often used in the process of registration, during which the subscriber must access the recovery account and take some action in order to confirm their control of the address. In the event that an email account becomes locked or the password is forgotten, the recovery address is often used as a means to regain access to the email account. Because the recovery address is known to the subscriber at the time of registration for an email account, and often used in the process of confirming the registration of the email account, and because the recovery account can be used to gain control of an email account, the person who controls the recovery account is typically the same person who controls the email account. Therefore, it is reasonable to assume that if several accounts have the same recovery address, they likely belong to the same person or persons.

## BACKGROUND OF THE INVESTIGATION

### I. HAMAS and the al-Qassam Brigades

29. Harakat al-Muqawamah al-Islamiyya, commonly known as HAMAS, was founded in 1987 as an outgrowth of the Palestinian branch of the Muslim Brotherhood. From its inception, HAMAS's stated purpose has been to create an Islamic Palestinian state throughout Israel by eliminating the State of Israel through violent holy war, or jihad. HAMAS has not only directed its violence and terrorism against Israeli targets in furtherance of that goal; HAMAS's leaders have also assailed the United States and American citizens, in retaliation for and in an effort to weaken American support for Israel's right to exist and defense of that right. HAMAS has murdered and injured dozens of Americans as part of its campaign of violence and terror.

30. HAMAS carries out terrorist attacks and armed conflict through the Izz al-Din al-Qassam Brigades (the "al-Qassam Brigades"), its military wing. The al-Qassam Brigades conduct suicide bombings and other terrorist attacks within Israel, Gaza, and the West Bank, and have done so for decades. These attacks have included large-scale bombings against Israeli civilian targets, small-arms attacks, improvised roadside explosives, and rocket attacks.

31. On October 8, 1997, the United States State Department, located in Washington D.C., designated HAMAS as a Foreign Terrorist Organization ("FTO") under Section 219 of the Immigration and Nationality Act. On October 31, 2001, the State Department also designated HAMAS as a Specially Designated Global Terrorist under Executive Order 13224. The Secretary of State has also listed the following aliases for HAMAS: Islamic Resistance Movement, Harakat al-Muqawama al-Islamiya, Students of Ayyash, Students of the Engineer, Yahya Ayyash Units, Izz Al-Din Al-Qassim Brigades, Izz Al-Din Al-Qassim Forces, Izz Al-Din Al Qassim Battalions,

Izz al-Din Al Qassam Brigades, Izz al-Din Al Qassam Forces, and Izz al-Din Al Qassam Battalions. To date, HAMAS remains a designated FTO.

## II. The October 7 HAMAS Attacks

32. On or about October 7, 2023, HAMAS and other terrorist groups, including the Palestinian Islamic Jihad ("PIJ"), another designated FTO,[1] launched a surprise assault into Israel ("the October 7 HAMAS Attacks"). HAMAS began by firing thousands of rockets, and then HAMAS militants crossed into Israel. The militants infiltrated Israeli towns and army bases and took civilian and soldier hostages, many of whom they brought back to Gaza. Israel formally declared war on HAMAS in response to the attack and began a ground invasion of the Gaza Strip on or about October 27, 2023. According to news reports, the HAMAS assault that began on or about October 7, 2023, killed approximately 1,200 people, including American citizens. HAMAS also took more than 250 people hostage, also including American citizens. HAMAS publicly took credit for the attacks.

33. In connection with the initiation of the October 7 HAMAS Attacks, on or about October 7, 2023, the now deceased supreme military commander of the al-Qassam Brigades, Mohammed al-Masri, a/k/a "Mohammed Deif," a/k/a "al Khalid al-Deif," issued a recorded message in which he "announce[d] the 'Al-Aqsa Flood' operation," and identified himself as "commander-in-chief of the Brigades of the martyr Ezeddine al-Qassam."

---

[1] On October 8, 1997, the United States Secretary of State designated Palestine Islamic Jihad – Shaqaqi Faction as a Foreign Terrorist Organization under Section 219 of the Immigration and Nationality Act. On January 23, 1995, the Department of the Treasury also designated PIJ as a Specially Designated Terrorist under Executive Order 12947. The Secretary of State has also listed the following aliases for PIJ: PIJ-Shaqaqi Faction, PIJ, Islamic Jihad in Palestine, Abu Ghunaym Squad of the Hizballah Bayt Al-Maqdis, Al-Quds Squads, Al-Quds Brigades, Saraya Al-Quds, Al-Awdah Brigades.

34. Also on or about October 7, 2023, al-Masri stated in a message broadcast on al-Aqsa TV that the al-Qassam Brigades leadership had "decided to put an end to all the crimes of the occupation, and the time during which it was rampant without accountability has ended." He stated that in the first minutes of the October 7 attacks, HAMAS launched 5,000 missiles and artillery shells, and asserted that the "Al-Aqsa Flood" operation was launched in response to what al-Masri described as "crimes committed by the Israeli occupation and colonial settlers," and American and Western support for and international silence regarding the occupation. He also instructed, "Today, whoever has a weapon should pull it out, this is its time, and whoever has no weapon should get his axe, Molotov cocktail, his truck, his bulldozer, or his car."

35. On or about October 8, 2023, the day after the October 7 HAMAS Attacks had begun, Ali Baraka, HAMAS's head of National Relations Abroad who is effectively responsible for HAMAS's foreign relations,[2] appeared in a video interview aired on a Russian television outlet. During the interview, Baraka conveyed that "[a] limited number of HAMAS leaders knew . . . about the attack and its timing." Baraka stated that HAMAS's social activities had actually been a ruse, to "make them [*i.e.*, Israel and the international community] think that HAMAS was busy with governing Gaza, and that it wanted to focus on the 2.5 million Palestinians" living there, when "[a]ll the while, under the table, HAMAS was preparing for this big attack." In fact, Baraka stated that HAMAS had "been preparing for this [*i.e.*, the October 7 HAMAS Attacks] for two years."

[2] From 2011 to 2019, Baraka was HAMAS's representative in Lebanon. Baraka is based principally in Lebanon. On or about December 13, 2023, the U.S. Department of the Treasury, Office of Foreign Assets Control ("OFAC") designated Baraka as a Specially Designated Global Terrorist under Executive Order 13224. In announcing the designation, OFAC noted that, when he held the position of HAMAS's representative to Lebanon, Baraka "met with international diplomats based in Lebanon on behalf of Hamas and spoke in support of violent campaigns" and that "[a]ccording to [] Baraka's public statements, Hamas has long drawn on money and training from Iran and Iranian proxies like Hizballah while bolstering forces in Gaza."

In response to a question about the HAMAS-held hostages, Baraka stated, "There are also prisoners in the U.S. We want them. Of course. There are HAMAS members sentenced for life in the U.S. We want them too. Of course. We demand that the U.S. free our sons from prisons."

36. The October 7 HAMAS attacks marked the beginning of what has become the Israel-HAMAS war. A ceasefire agreement between Israel and HAMAS was reached on or about January 15, 2025, and went into effect on or about January 19, 2025. On or about March 18, 2025, the Israeli Prime Minister's Office released a statement indicating that he had authorized "the renewal of military action" against HAMAS.[3] Between on or about October 7, 2023, and on or about February 26, 2025, numerous hostages taken by HAMAS have died in captivity or been released as part of a ceasefire deal with Israel. On or about October 2025, a mediated agreement between HAMAS and Israel was scheduled to go into effect, securing the release of final surviving groups of hostages and scaling up UN aid delivery. Sporadic security incidents continue to occur in the Gaza Strip.

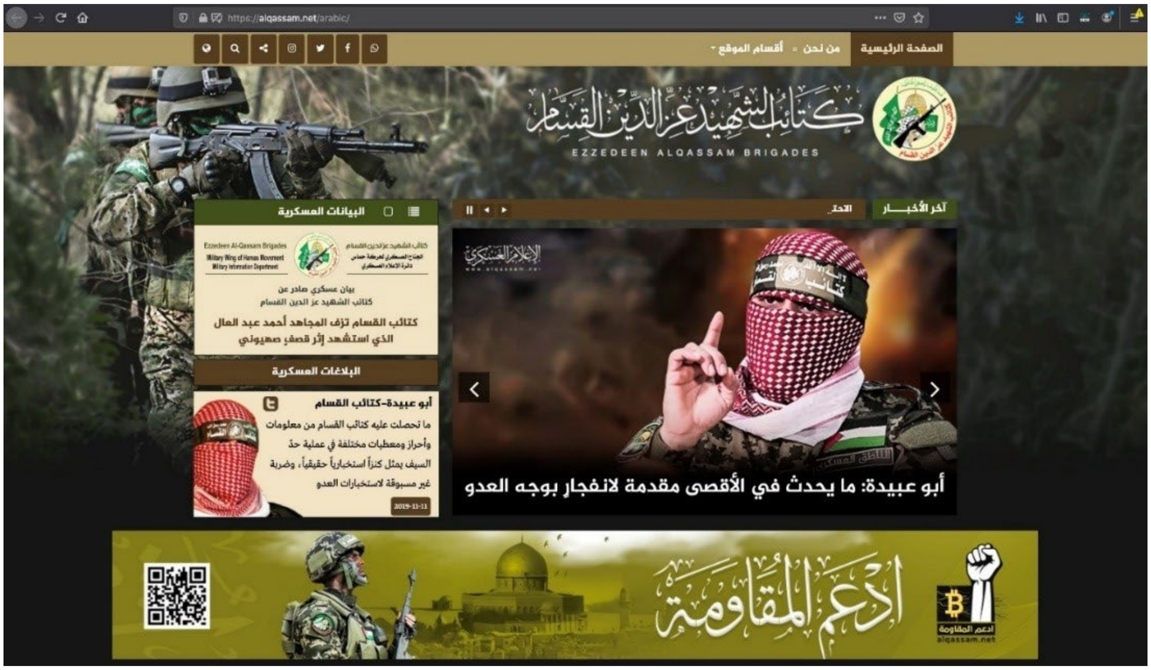
## III. The History of HAMAS Virtual Currency Financing

37. Beginning in or about early 2019, HAMAS, through the al-Qassam Brigades, tested virtual currency fundraising by soliciting donations on its Telegram channel before shifting to direct fundraising through its official websites: alqassam.net, alqassam.ps, and qassam.ps.[4]

38. The al-Qassam Brigades boasted that bitcoin donations were untraceable and would be used for violent causes. Their websites offered video instruction on how to anonymously make

[4] I know these to be official websites for the al-Qassam Brigades based on a previous investigation and subsequent United States Department of Justice announcement. *See* https://www.justice.gov/archives/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns.

donations, in part by using unique bitcoin addresses generated for each individual donor. However, such donations were pseudoanonymous. Through leveraging blockchain analysis, federal authorities seized virtual currency accounts, while also covertly seizing and operating the infrastructure behind alqassam.net.[5]




Above: Bitcoin donation advertisement on alqassam.net

39. In or around April 2023, HAMAS announced that it would stop receiving funds via bitcoin due to donor safety concerns. Statements on the website then called for donations to continue through other means.

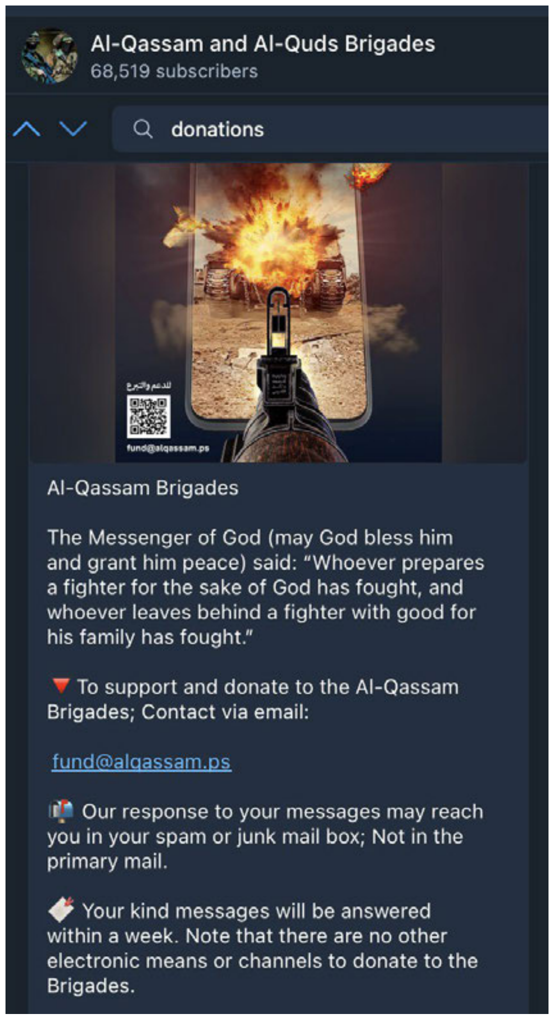
## PROBABLE CAUSE

### Finding Messaging and Donation Addresses

40. In or around February 2025, FBI Albuquerque identified a terrorist financing

5 Information obtained via the U.S. Department of Justice, *available at* https://www.justice.gov/archives/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns

network soliciting donations to the al-Qassam Brigades via virtual currency. On or about February 6, 2025, an FBI Confidential Human Source (hereinafter referred to as "CHS-1"), who is located in the United States and has provided reliable information in the past, alerted me to a Telegram post asking supporters to send an email to an address associated with the al-Qassam Brigades, fund[@]alqassam.ps, in order to donate.




<u>Above</u>: Post from the al-Qassam Brigades asking for support

Fund[@]alqassam.ps's email address is also posted at the bottom of the al-Qassam Brigades website, https://alqassam.ps/arabic/. I know this to be an official website for the al-Qassam

Brigades based on a previous investigation and subsequent United States Department of Justice announcement.[6]


Above: Contact information shown on alqassam.ps/arabic/

On or about February 10, 2025, CHS-1 emailed fund[@]alqassam.ps asking how the CHS could donate to the al-Qassam Brigades. Several hours later, CHS-1 received a response from fund[@]alqassam.ps in Arabic, roughly translated to the following:

> *In the name of Allah, the Most Gracious, the Most Merciful*
>
> *"Go forth, whether light or heavy, and strive with your wealth and your lives in the cause of Allah. That is better for you, if you only knew." [At-Tawbah: 41]*
>
> *Dear sister/s: May Allah protect and care for you*
>
> *Peace, mercy, and blessings of Allah be upon you,*
>
> *May Allah reward you for your keenness to perform the duty of support and assistance to your mujahid brothers in Gaza; and we ask Allah Almighty to accept from you your efforts and giving. If you do not have experience in dealing with digital currencies, you can seek the help of a friend inside or outside your country, or go to a money transfer office or exchange in your country that has digital currencies, and show only the wallet information from this message; To transfer the support amount to it; it is necessary not to inform the party that will undertake the transfer on your behalf of our identity; to preserve your security.*
>
> *Attached is the address and data of our current digital currency wallet; which is received from all other platforms:*

[6] Information obtained via the U.S. Department of Justice, *available at* https://www.justice.gov/archives/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns

*Current wallet address:*

*TSWL3euRjZWXiFJgzuV9tYAGiwShtPWkZK*

*Please make sure to copy only the letters without any spaces before and after the letters; and it is preferable to extract the address from the code below:*

*Network Type:*

*Trc20*

*Currency Type:*

*USDT*

*Important Notes:*
*1. You can notify us of the value of the support and donation amount upon completion of the transfer process; to follow up on the receipt, God willing.*

*2. The wallet address is changed periodically to preserve your safety; therefore, the address is only valid for one transfer and support process; therefore, it is necessary to communicate via this email for any other new transfer process.*

*3. It is preferable not to use the "BINANCE" platform to transfer support; and not to enter any data indicating our official name so that your wallet is not blocked and for your safety as well (entering any fictitious data as the recipient of the transfer); You can transfer through the application: trust wallet, RedotPay, OKX, Kast, BYBIT...*

*Note: "BINANCE" can be used to purchase currencies only, then use another application to complete the transfer process.*

*4. We hope to circulate the official email for support and donations to the Al-Qassam Brigades: fund[@]alqassam.ps and published on the official website of the Brigades https://alqassam.ps; with the necessity of alerting our honorable audience that our response to their messages may reach them in the "junk" or "spam" mailbox and not in the Inbox; due to our access restriction policies.*

*May Allah write you the reward and reward you with all good,*

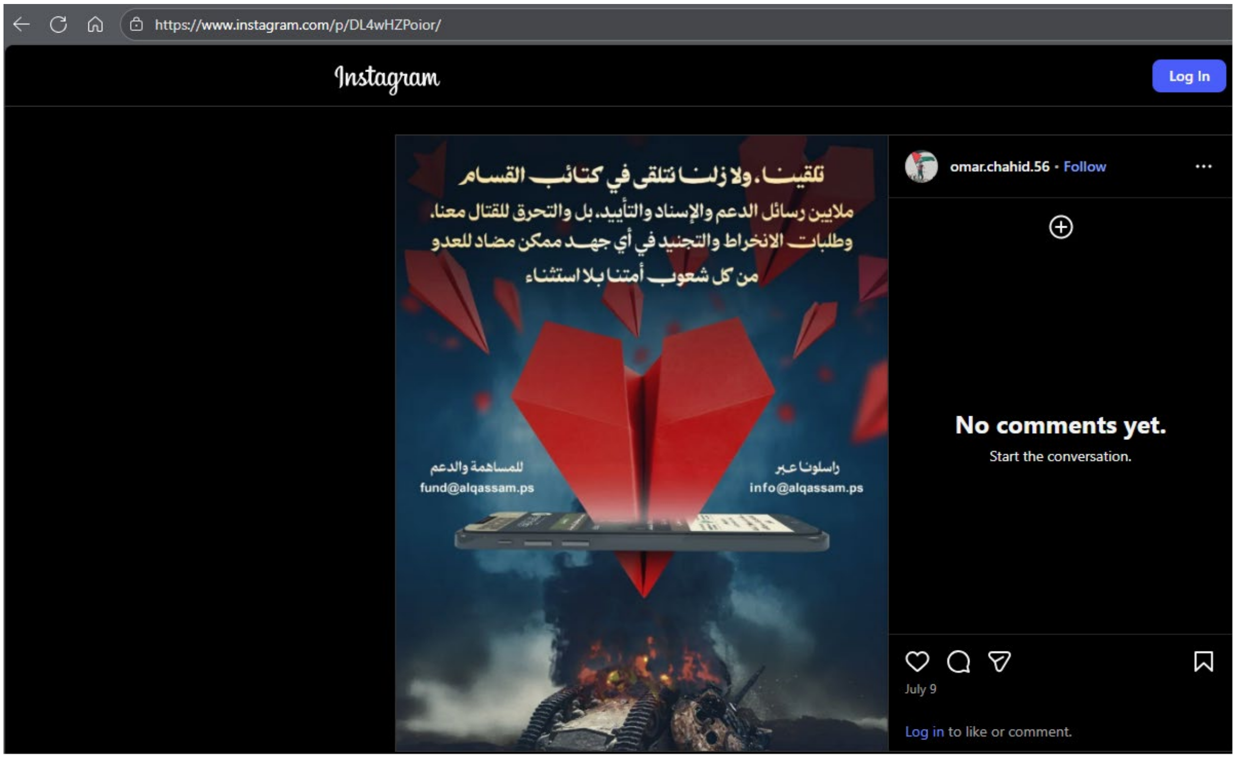
*And we ask you to pray for your brothers in Gaza and Palestine*

41. Based on my training and experience, I know that terrorists and cyber criminals often look for ways to obfuscate their online activity. Per the above message, the al-Qassam Brigades recommend donors avoid sending funds directly from Binance accounts. I have conducted in-depth virtual currency investigations and know Binance to be a commonly used exchange for users across the globe. However, I also know Binance maintains Know-Your-Customer (KYC) requirements to prevent fraudulent or illicit activity. Based on my training and experience, I also know other solutions listed, including Trust Wallet and Bybit, are commonly utilized to obfuscate the identity of the sender. By recommending these transfer solutions, the al-Qassam Brigades are seeking to receive funding while still attempting to protect the identities of their donors. Furthermore, I know USDT is a stablecoin that is widely used around the globe for different purposes, including, among other things, to finance criminal activities; and TRC20 is often chosen as a network because of its fast transaction speeds and low fees.

42. The FBI conducted virtual currency tracing and blockchain analysis on the USDT address that CHS-1 identified, TSWL3euRjZWXiFJgzuV9tYAGiwShtPWkZK, hereinafter referred to as "Donation Address 1". Over the course of several months, I continued to investigate this network through similar methods, receiving different virtual currency addresses that multiple FBI sources collected to identify additional HAMAS donation addresses. Based on blockchain analysis, I assess that this financing network has been operating since in or around October 2024 and received over $3,000,000 in donations through in or around November 2025. As recently as in or around February 2026, the fund[@]alqassam.ps email sent multiple FBI Confidential Human Sources emails with instructions on how to donate to the group.

43. On or about July 9, 2025, an Instagram post from an account "omar.chahid.56" showed a graphic appearing to represent a demolished tank, with hearts falling through a cell phone

below Arabic writing. Also included on either side of the graphic were fund[@]alqassam.ps and info[@]alqassam.ps.




Above: Screenshot of an Instagram post on or about Jul 9, 2025

Machine translation showed the above image to read:

> *We in the Qassam Brigades have received, and continue to receive, millions of messages of support, and even eagerness to fight alongside us, as well as requests to join and enlist in any possible effort against the enemy from all the peoples of our nation without exception.*
> *To contribute and support: fund[@]alqassam.ps*
> *Contact us via: info[@]alqassam.ps*

44. At the time, research on alqassam.ps showed the internet service provider associated with the domain's IP address to be Amnpardaz Soft Corporation, an internet service provider located in Tehran, Iran. Hamas leaders have repeatedly thanked Iran for its military and financial support for many years. Based on this information, it is reasonable to believe that Iranian support and internet infrastructure has enabled HAMAS to operate this financing network.

Additionally, hosting infrastructure in Iran allows HAMAS to protect it from being taken offline by a service provider linked to the U.S. or a U.S. ally.

45. Alqassam.ps is also included in official propaganda videos and photos for the al-Qassam Brigades:


Above: Al-Qassam imagery showing alqassam.ps in the banner

46. A release from the Palestinian Information Center claimed that al-Qassam's only website address is "alqassam.ps".[7] In your affiant's training and experience, this website is known to be affiliated with the al-Qassam Brigades, and any contact information posted on the website is controlled by the al-Qassam Brigades or affiliates of HAMAS. Furthermore, in your affiant's training and experience, responses from alqassam.ps are coming from members of the al-Qassam Brigades – an armed and militant affiliate of HAMAS.

**Alqassam[.]ps Network Infrastructure**

47. Based on recent WhoIs lookups, as of July 24, 2026, 216.106.177.172 ("Server

[7] Information obtained via the Palestinian Information Center, available at https://english.palinfo.com/o_post/QB-Our-only-website-address-is-alqassam-ps/

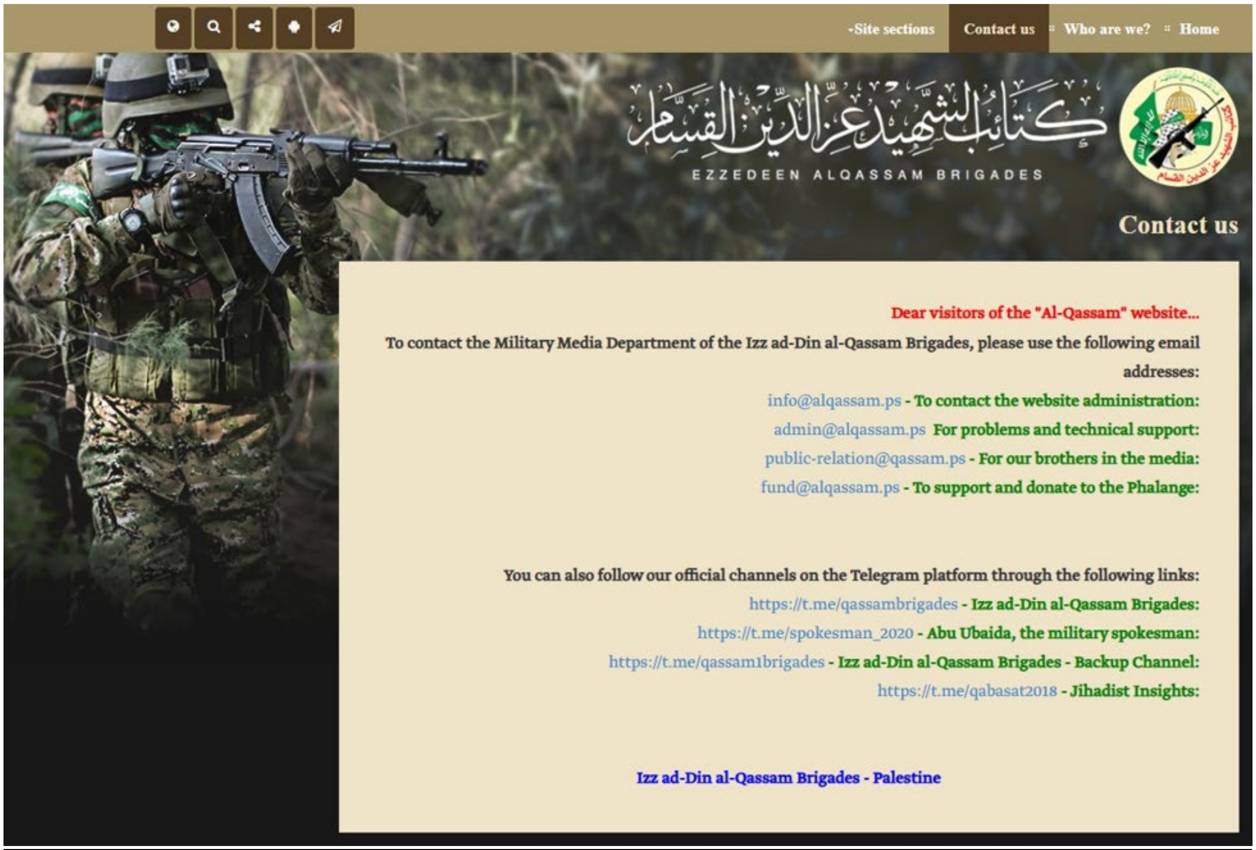
172”) supported the domain alqassam[.]ps. However, previously, the alqassam[.]ps domain was supported by the IP address 216.152.156.133 (“Server 133”). Both Server 133 and Server 172 were owned by [redacted] an internet service provider with datacenters located in the United States. [redacted] and Server 133 became associated with alqassam.ps on May 26, 2026. As noted earlier, the previous registrar for alqassam[.]ps was Amnpardaz Soft Corporation, an Iran-based internet service provider. Amnpardaz Soft Corporation was the previous registrar for alqassam[.]ps from January 24, 2024, until at least April 13, 2026 [redacted] responded to a court order and confirmed that alqassam[.]ps was associated with Server 133. [redacted] urther confirmed that the IP address 216.152.156.133 was assigned to a dedicated server, owned by [redacted] ocated in a data center in Atlanta, Georgia [redacted] records also confirmed that 216.152.156.133 was a static IP assigned to alqassam.ps [redacted]

[redacted]

[redacted]

50. On July 16, 2026, I conducted open-source research and found that alqassam.ps was still active and accessible. A machine-translated screenshot of the "Contact Us" page on alqassam.ps showed the same contact information used to support the global terror financing

campaign I am investigating. Furthermore, several Telegram channels were listed, including one that provides "Jihadist Insights".




Above: Screenshot of the "Contact Us" page on alqassam.ps (taken July 16, 2026)

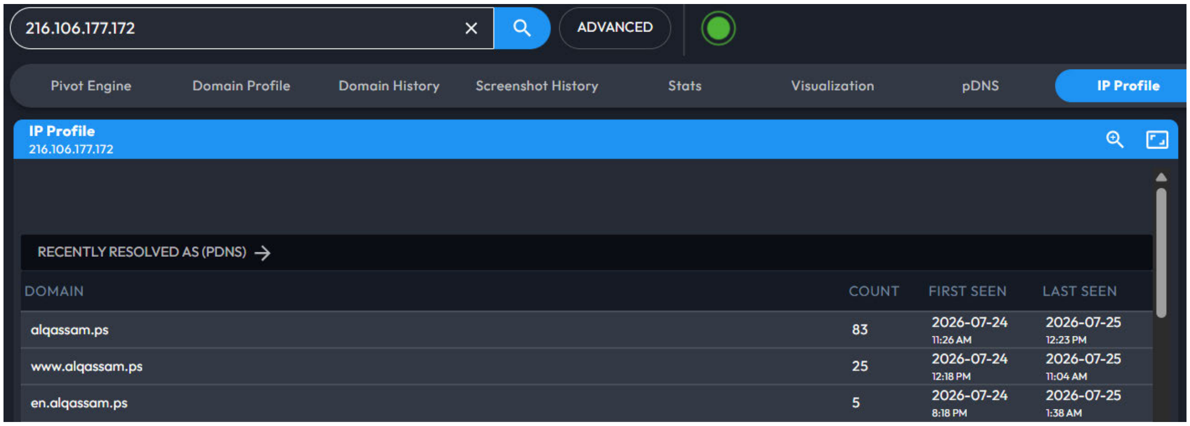
[redacted]

[redacted]

[redacted]

[redacted]

55. On July 24, 2026, I conducted an updated WhoIs lookup search and found that the alqassam[.]ps domain resolved to the IP address 216.106.177.172 ("Server 172").




Above: WhoIs lookup showing IP address 216.106.177.172 (Server 172) resolving to alqassam.ps

On July 25, 2026, I conducted Domain Name System ("DNS") lookups to confirm alqassam[.]ps resolved to Server 172. I found that the previously assigned IP address, 216.152.156.133, no longer resolved to any active domain. However, the IP address for Server 172 (216.106.177.172) did resolve to alqassam[.]ps. This search is shown below:

[redacted]

[redacted] Thus, HAMAS used Server 172 to promote a scheme designed to provide material support to a terrorist organization in violation of 18 U.S.C. § 2339B and HAMAS purchased Server 172 by moving money from outside the United States into or through the United States (*i.e.*, the payments to [redacted] to lease Server 172 for alqassam.ps). These actions violated 18 U.S.C. §§ 2339B and 1956(a)(2)(A) (International Promotional Money Laundering) and mean that Server 172 was subject to civil seizure and forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) and (b). As part of this scheme, HAMAS actors leveraged US-based networking infrastructure in order to bypass delivery restrictions and ensure information could reach supporters across the globe.

57. On July 30, 2026, the FBI served seizure warrant 26-sz-45, which was issued by this court, seizing the GTHost server (Server 172) hosting alqassam[.]ps.

**United States Operations Targeting AlQassam[.]ps**

58. On March 27, 2025, June 26, 2025, and October 15, 2025, investigators used information from multiple CHSs to identify, trace, and seize approximately $560,000 in virtual currency intended to support Hamas' Al Qassam Brigades. In conjunction with these seizures, the FBI's Albuquerque Field Office worked with CHSs to identify and seize the domains

Alaqsaflood.org and Host.alaqsaflood.org – two domains used to operate the fundraising and communication functions of AlQassam[.]ps. These seizures occurred in conjunction with Server 172 – which the Al Qassam Brigades used to host and control content on AlQassam.ps. The FBI's capture of the domains and servers enabled it to obtain additional donations intended for Hamas. Using related sources and methods the FBI also obtained information for thousands of individuals who used or had been contact with the Al Qassam website and either donated or attempted to donate to the terrorist organization using cryptocurrency and other traditional means.

**<u>SERVER 68 and DataCamp Limited</u>**

59. On August 4, 2026, pursuant to legal process [redacted] provided the FBI with records showing that the Al-Qassam Brigades terrorist financing campaign was supported by a server with IP address 45.134.141.68 ("**SERVER 68**"). WhoIs lookups, as of August 5, 2026, showed that **SERVER 68** was geolocated to São Paulo, Brazil, but owned by DataCamp Limited, an internet service provider with datacenters located in the United States.

[redacted]

[redacted]

[redacted]

[redacted]

61. As noted earlier, from January 24, 2024 until at least April 13, 2026, the previous registrar for alqassam[.]ps was Amnpardaz Soft Corporation, an Iran-based internet service provider.

62. On August 6, 2026, I conducted open-source research using publicly available repositories, finding that **SERVER 68** held certificates for csguard[.]ir.

## 45.134.141.68

Regular View | >_ Raw Data | Timeline | Whois

### General Information

| | |
|---|---|
| Hostnames | csguard.ir<br>unn-45-134-141-68.datapacket.com |
| Domains | csguard.ir datapacket.com |
| Country | Brazil |
| City | São Paulo |
| Organization | Datacamp Limited |
| ISP | Datacamp Limited |
| ASN | AS60068 |

```
X509v3 Subject Key Identifier:
    1C:19:64:C2:A6:9E:34:F9:1C:41:C4:A9:26:73:F2:BD:12:53:F4:A7
X509v3 Authority Key Identifier:
    BB:20:CA:47:0B:FE:D7:E5:9C:F9:8F:09:2A:A3:8C:37:45:B1:BC:D8
Authority Information Access:
    CA Issuers - URI:http://ye1.i.lencr.org/
X509v3 Subject Alternative Name:
    DNS:*.csguard.ir, DNS:csguard.ir
X509v3 Certificate Policies:
    Policy: 2.23.140.1.2.1
```

<u>Above</u>: Screenshots from publicly available repositories showing csguard[.]ir associated with **SERVER 68**

[redacted]

[redacted]

63. More open source database and internet communications research revealed that **SERVER 68** broadcasts Secure Sockets Layer (SSL) certificates for the alqassam[.]ps name server, csguard[.]ir. These certificates enable secure connections to the name server, which allows resolution of web traffic for individuals seeking to access alqassam[.]ps and find ways to fund the Al-Qassam Brigade [redacted]

64. In your affiant's training and experience, these connections confirm SERVER 68 is being used to provide material support to HAMAS, and that that funds originating outside the United States from HAMAS actors were used to purchase and retain **SERVER 68**, and that this server was involved in an international money laundering offense (*i.e.*, these funds travelled from/to a place outside the United States to/from/through a place inside the United States and were used to promote the carrying on of a terrorist financing campaign). Specifically, HAMAS used this server to promote a scheme designed to provide material support to a terrorist organization in violation of 18 U.S.C. § 2339B and HAMAS purchased **SERVER 68** by moving money from

outside the United States into or through the United States. These actions violate 18 U.S.C. § 2339B and 18 U.S.C. § 1956(a)(2)(A) (International Promotional Money Laundering) and mean that **SERVER 68** is subject to civil seizure and forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) and (b), and criminal seizure pursuant to Rule 41(b)(3) and 18 U.S.C. § 982(a)(1).

65. Based on the evidence discussed above, I have probable cause to believe HAMAS actors used **SERVER 68** to coordinate a terror financing campaign and solicit material support for the FTO. Through my training and experience, I know that global terrorist organizations frequently use electronic media to seek support, and that email and web traffic are used to communicate with individuals who may not be physically co-located. Furthermore, I believe these actors have knowingly provided technical and other material support to ensure delivery of cryptocurrency donation instructions to HAMAS supporters around the world, in violation of 18 U.S.C. § 2239B. Thus, **SERVER 68** is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(G)(i) and (b) and 21 U.S.C. § 853(f), and seizure pursuant to Rule 41(b)(3).

## SEIZURE PROCEDURE

66. As detailed in Attachment A, upon execution of the seizure warrant, the registrar for **SERVER 68** shall be directed to restrain and lock **SERVER 68** pending transfer of all right, title, and interest in **SERVER 68** to the United States upon completion of forfeiture proceedings, to ensure that changes to **SERVER 68** cannot be made absent court order or, if forfeited to the United States, without prior consultation with the FBI.

67. In addition, upon the FBI's seizure of **SERVER 68**, the Government will direct DataCamp to associate **SERVER 68** with a new authoritative name server(s) to be designated by

a law enforcement agent. The Government will display a notice on the website to which **SERVER 68** will resolve indicating that the site has been seized pursuant to a warrant issued by this court.

68. Neither a restraining order nor an injunction is sufficient to guarantee the availability of the **SERVER 68** for forfeiture. By seizing **SERVER 68** and redirecting it to another website, the Government will prevent third parties or the terrorist actors from acquiring it (or reacquiring it) and using it to commit additional crimes.

## CONCLUSION

69. Based on the information contained in this affidavit, I submit that there is probable cause to believe that HAMAS transferred funds originating from outside the United States to/through the United States to purchase **SERVER 68** and that HAMAS used these assets to promote and facilitate providing material support to a designated foreign terrorist organization. Accordingly, **SERVER 68** is therefore subject to civil forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A), criminal forfeiture pursuant to 18 U.S.C. § 982(a)(1), and criminal seizure pursuant to Rule 41(b)(3), and I respectfully request that the Court issue a seizure warrant for **SERVER 68**.

70. Because the warrant will be served on an electronic service provider, which controls the equipment hosting **SERVER 68**, at a time convenient to them, and the provider will transfer control of **SERVER 68** to the Government, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

71. Finally, and in order to protect the ongoing investigation and in consideration that much of the information set forth above is not otherwise publicly available, I respectfully request that this Affidavit be filed and kept under seal until further order of this Court.

Respectfully submitted,

[redacted]

Special Agent
Federal Bureau of Investigation

Subscribed and sworn pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on August 18, 2026, 2026.

MATTHEW J. SHARBAUGH
UNITED STATES MAGISTRATE JUDGE