

FILED

UNITED STATES DISTRICT COURT

for the
Southern District of California

APR 14 2016

CLERK US DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA
BY DEPUTY

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*Blue Apple iPhone. Model A1532, associated with no.
619-721-2979, located at FBI Evidence Control Room,
10385 Vista Sorrento Pkwy, San Diego, CA 92121

Case No.

'16MJ1082**APPLICATION FOR A SEARCH WARRANT**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Southern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 USC 956, 1117, 1119, 1341, 2261, 2314	foreign murder of US national, conspiracy to do the same, mail fraud, interstate/foreign domestic violence, transportation of stolen goods

The application is based on these facts:
See Attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

FBI Special Agent Eric Van Houten

Printed name and title

Sworn to before me and signed in my presence.

Date: 4/14/16


Judge's signature

City and state: San Diego, CA

Bernard G. Skomal, U.S. Magistrate Judge

Printed name and title

Att
X6735
04/13/16

AFFIDAVIT IN SUPPORT OF
APPLICATIONS FOR SEARCH
WARRANTS

1. I, Special Agent Eric Van Houten, being duly sworn, hereby state as follows:

2. I am a special Agent of the Federal Bureau of Investigation ("FBI") and have been employed as such since 2014. Since November 2014, I have been assigned to the FBI's Violent Crime squad in San Diego where I have both conducted and assisted in criminal investigations to include bank robberies, extortions, assaults against federal officers, and kidnappings. Between May 2008 and June 2014, I served as an Intelligence Analyst for the FBI. I hold a Bachelor of Arts degree from Purdue University with majors in Political Science and Communications with specializations in International and Public Relations and a minor in Forensic Science.

3. During my career with the FBI, I have conducted arrests, search warrants, and physical and electronic surveillance. Through my formal education and law enforcement career, I have completed training in forensic science and learned the evidentiary value of that evidence as it relates to violent crime and other criminal offenses (to include the processing of violent crime scenes and the collection of trace evidence).

4. I have spoken with other agents, as well as other law enforcement officers with experience in violent crime investigations about their experiences and the results of their investigations and interviews. Through these discussions and through my own training and experience, I know that cellular telephones and other electronic devices, to include smart phones, are frequently used to facilitate

criminal activity. In many instances, cellular telephones and smart phones are used to facilitate communication between co-conspirators through traditional audio conversations, text messages, emails, and other electronic applications. Records of these communications are often stored on the devices and may not be accessed through records obtained from service providers.

5. I am also aware that violent offenders often have electronic documents and files, which were used to aide and facilitate the commission of the crime. In many instances, these files can contain additional forensic and transactional evidence linking the subject to the victim and/or the identification of other co-conspirators. In addition, violent offenders often attempt to conceal, dispose of, or destroy evidence linking them to the crime scene and/or the victim.

6. Through training and conversations with other special agents and experts, I have learned location and/or GPS information can be electronically stored on a cellular phone and extracted for analysis. This information is relevant in violent crime investigations as this information can indicate times a particular phone was at specific place, which can corroborate or disprove a suspect's statements regarding his/her location.

7. This affidavit is offered as follow-up to previous search warrants 15MJ1718 and 15MJ3407. *See* Exhibit 1 (15MJ1718) and Exhibit 2 (15MJ4307). Search warrant 15MJ1718 was executed on June 4, 2015, to search an apartment located at 30 27th Street San Diego, California 92102, and download and search forensic evidence seized from that location. Search warrant 15MJ3407 was executed on November 30, 2015 solely to recover one deleted voicemail from an Apple iPhone belonging to Taylor LANGSTON (LANGSTON's Apple iPhone).

8. My experience as a Special Agent, my participation in the investigation of violent crimes, my conversations with other agents, and other state and local law enforcement officers familiar with violent crimes, as well as

my education and training, form the basis of the opinions and conclusions set forth below, which I have drawn from the facts set forth herein. Since this affidavit is being submitted for the limited purpose of securing a search warrant on a previously seized item, I have not included each and every fact known concerning this investigation but have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence relating to violations of Title 18, United States Code §§ 1001, 1117, 1118, 1512, 2314 and 2261, is located on the item described in Attachment B (LANGSTON's Apple iPhone). The discussions included herein are set forth in substance and not verbatim, unless otherwise noted.

FACTS SUPPORTING PROBABLE CAUSE

9. On May 2, 2015, United States citizen Jake Clyde MERENDINO (DOB: 09/22/63) was found dead in Baja California Norte, Mexico on the highway between Rosarito and Ensenada at kilometer 48.7, near a location known as Los Arenales. MERENDINO's vehicle, a Range Rover registered to him and bearing Texas license plate FPJ6119, was found near his body.¹

10. On May 11, 2015, Henk TYSMA, owner of California Baja Rent-a-Car in Spring Valley, California, established telephonic contact with the U.S. consulate in Tijuana, Mexico, after seeing a news piece on the MERENDINO homicide. MERENDINO, a United States Citizen and former resident of Beaumont, Texas, had been a long time customer at TYSMA's rental car company and would frequently rent cars to drive down to Mexico, where he was planning on retiring.

¹ MERENDINO's body was found approximately 10 meters from his Range Rover in a small valley with blood evidence located approximately 3 meters from the vehicle. Mexican law enforcement officials assessed that the initial confrontation occurred in the driver's seat of the vehicle, and continued outside to the rear of the vehicle, where a major confrontation occurred approximately 2-3 meters behind the vehicle, and MERENDINO was stabbed approximately 20 times in the chest and suffered multiple slash wounds across the neck. Mexican law enforcement officials have not yet located a murder weapon.

TYSMA also established telephonic contact with FBI San Diego on May 11, 2015, to report MERENDINO's death.

11. TYSMA reported that MERENDINO arrived at California Baja Rent-a-Car in Spring Valley on April 29, 2015, at approximately 10:00 am with United States Citizen David Enrique MEZA (DOB: 06/13/90). The two rented a 2013 Ford Explorer bearing California license plate 7AOM662 and left in both the rental car and MERENDINO's Range Rover.

12. It is my understanding that MERENDINO and MEZA met on-line in July 2013 and thereafter entered into a consensual romantic relationship. At the time they met, MERENDINO lived in Texas and MEZA in San Diego.

13. On April 29, 2015, MERENDINO and MEZA travelled south into Mexico in order for MERENDINO to complete the purchase of a \$300,000 condominium at Palacio del Mar, at kilometer 50 ½ on the highway between Rosarito and Ensenada. MERENDINO and MEZA crossed back into the U.S. on April 29, 2015, at 2:45 pm² and checked into the Hercor Hotel, 692 H Street, Chula Vista, California.

14. On May 1, 2015, MERENDINO and MEZA checked out of the Hercor Hotel in Chula Vista, California and returned the rental car at approximately 12:13 pm. After returning the rental car in Spring Valley, MERENDINO and MEZA both left the rental car agency in MERENDINO's Range Rover and returned to Mexico, MERENDINO in his Range Rover and MEZA on MEZA's motorcycle. At 1:00 pm, MERENDINO in his Range Rover and MEZA on MEZA's motorcycle were photographed passing through the Playas de Tijuana toll booth,

² All border crossings from Mexico into the United States referenced herein are based on official entries in the Treasury Enforcement Communications System (TECS), a database utilized by the U.S. Customs and Border Protection Agency.

which is the route from San Diego to Rosarito. MERENDINO was wearing a dark short-sleeve shirt with a light-colored stripe on the sleeve, and MEZA was wearing a red helmet, a black leather jacket and blue jeans. At 1:15 pm, MEZA drove through the Rosarito toll booth wearing the same red helmet, black leather jacket and jeans. MEZA was followed by MERENDINO at 1:16 pm, wearing the same shirt and driving the Range Rover.

15. As the condominium at Palacio del Mar was not yet habitable, MERENDINO and MEZA rented a room together at Bobby's By The Sea, located near kilometer 43 on the highway between Rosarito and Ensenada, Mexico. They checked in at approximately 3:36 pm on May 1, 2015. MERENDINO appeared in the lobby between 7:00 pm and 8:00 pm to open a bottle of wine. At approximately 10:30 pm, a motorcycle was heard departing the hotel. At 11:01 pm, MEZA entered the U.S. on MEZA's motorcycle bearing California license plate 22J6784.

16. On May 2, 2015, at around 1:00 am, hotel security observed MERENDINO departing the hotel in his Range Rover. MERENDINO told the security guard that he was going to help a friend stranded on the road. At approximately 3:33 am, MERENDINO's body was found on the highway between Rosarito and Ensenada, five minutes from Bobby's By The Sea. MERENDINO was still wearing the dark-colored short-sleeve t-shirt with a light-colored stripe on the sleeve.

17. On May 2, 2015, at 3:57 am, MEZA crossed into the U.S. on MEZA's motorcycle. MEZA's pregnant girlfriend, Taylor Marie LANGSTON (DOB: 07/06/95), crossed into the U.S. twenty-five minutes later at 4:22 am in a black Sport Utility Vehicle with no license plates. I believe that this black SUV with no

license plate is MEZA's SUV and suspect that the plates were removed to disguise the identity of the registered owner of the SUV (MEZA).

18. At approximately 7:00 pm on May 2, 2015, according to hotel staff, MEZA and LANGSTON returned to the hotel in a black SUV without license plates --which I again believe to be MEZA's SUV-- and picked up a number of personal items from the room at Bobby's By The Sea, where MERENDINO and MEZA had been staying.

19. Mexican officials reported to the FBI that MERENDINO's iPhone, iPad, laptop computer and \$15,000 diamond-studded Rolex watch were missing. They were not found on MERENDINO's body, in the hotel room at Bobby's By The Sea or in MERENDINO's condominium.

20. On May 3, 2015, at 12:55 am, MEZA and LANGSTON crossed into the U.S. in MEZA's SUV, this time bearing plate number CA 7KSW212. MEZA's SUV, with California license plate 7KSW212, is assigned to a 2012 Hyundai Tucson SUV registered to MEZA at 1309 Pequena Street, San Diego, CA 92154. MEZA's parents live at this address.

21. Mexican law enforcement officials investigating MERENDINO's death identified Boston-based attorney Carron HAIGHT as a close friend of MERENDINO's who had drawn up MERENDINO's Last Will and Testament in 1998 ("1998 Will") when they were both residing in Texas.

22. HAIGHT confirmed that she had been close friends with MERENDINO since the late 1990s. HAIGHT also reported that she had been named Executrix of MERENDINO's 1998 Will and had filed an Application for Probate and Letters Testamentary on May 8, 2015, in Galveston, Texas.

23. An associate of MEZA's in Mexico showed Mexican law enforcement officials a holographic will alleged to be handwritten and executed by MERENDINO on December 12, 2014 on Hercor Hotel letterhead in Chula Vista, California, which named MEZA sole heir and beneficiary of MERENDINO's estate ("2014 Will"). See Exh. 3.

24. On May 12, 2015, MEZA and LANGSTON were observed at the United Parcel Service ("UPS") office located on Market Street in San Diego, California sending a copy of the 2014 Will to HAIGHT in Boston. See Exh. 4.

25. On May 17, 2015, MEZA filed an Original Answer and Contest in the Probate Court of Galveston County, Texas contesting the 1998 Will filed by HAIGHT and filing the 2014 Will.

26. On December 22, 2015, a Grand Jury in the United States District Court, Southern District of California indicted both MEZA and LANGSTON for Interstate or Foreign Domestic Violence Resulting in Murder, in violation of Title 18, U.S.C. Sec. 2261(a)(1) (MEZA); Conspiracy to Obstruct Justice, in violation of Title 18, U.S.C. Sec. 1512(k) (MEZA and LANGSTON); Obstruction of Justice, I violation of Title 18, U.S.C. Sec. 1512(c)(2) (LANGSTON); and False Statement to a Federal Officer, in violation of Title 18, U.S.C. Sec. 1001 (LANGSTON).

27. Also on Tuesday, December 22, 2015, the Court issued arrest warrants for MEZA and LANGSTON.

28. On December 23, 2016, MEZA and LANGSTON were arrested and taken into custody at their Imperial Beach apartment without incident.

29. On June 4, 2015, at MEZA's apartment, a blue Apple iPhone was seized and later identified as belonging to LANGSTON. The initial forensic examination

results of this iPhone did not produce a list of Apple iPhone applications located on the phone, nor did the results identify any possible location or GPS information.

30. I am on the FBI San Diego Violent Crimes squad. My squad-mate FBI Special Agent Benjamin Inman downloaded LANGSTON's Apple iPhone consistent with the dictates of search warrants 15MJ1718 and 15MJ3407 using Cellebrite technology. The time limitations of these search warrants have lapsed. To the extent that there were additional records of applications and location and/or GPS information, it was not downloaded using Cellebrite and remains on LANGSTON's Apple iPhone.

31. The San Diego Regional Computer Forensics Laboratory (RCFL) makes highly trained digital forensic examiners available to support federal, state, and local investigations through impartial and objective analysis of digital evidence. Through recent conversations with experts in the Regional Computer Forensics Laboratory (RCFL), I have been told that the RCFL has additional tools beyond Cellebrite, which could potentially identify and extract location information stored on Langston's iPhone, as well as identify relevant Apple iPhone applications that could also hold location information. Although the original forensic analysis using Cellebrite provided relevant investigative material, RCFL experts have informed me that a Cellebrite search alone probably did not provide

an in-depth analysis of all of the information forensically available from LANGSTON's Apple iPhone. RCFL has agreed to assist me with searching LANGSTON's Apple iPhone for location and/or GPS data if I obtain a search warrant.

32. I am therefore requesting a warrant, so an RCFL expert can forensically enter LANGSTON's Apple iPhone and identify available location and/or GPS information, through applications or otherwise, which would reflect the phone's location at and/or around the time of MERENDINO'S death, as well as any historical location information which would indicate trips with or without MEZA to Mexico leading up to the murder on May 2, 2015. Additional forensic examination is needed to fully identify the presence --or lack thereof-- of this information, which an initial search, solely using Cellebrite, was unable to determine. The original Cellebrite analysis did not produce a list of applications currently downloaded to the Apple iPhone, which is needed to further investigate the extent that location information was stored and/or captured. I believe that additional forensic examination of LANGSTON's Apple iPhone will produce records, evidence, fruits and instrumentalities relating to violations of Title 18, United States Code, §§ 1001, 1117, 1118, 1512, 2314, and 2261.

PROCEDURES FOR ELECTRONICALLY STORED INFORMATION ON CELL PHONES

33. It is not possible to determine the nature and types of services to which the device is subscribed and the nature of the data stored on the device until one accesses the device. Cellular devices today can be simple cellular telephones and text message devices, can include cameras, can serve as personal digital assistants and have functions such as calendars and full address books and can be mini-computers allowing for electronic mail services, web services and rudimentary word processing. An increasing number of cellular service providers now allow for their subscribers to access their device over the internet and remotely destroy all of the data contained on the device. For that reason, the device may only be powered in a secure environment or, if possible, started in "flight mode" which disables access to the network. Unlike typical computers, many cellular telephones do not have hard drives or hard drive equivalents and store information in volatile memory within the device or in memory cards inserted into the device. Current technology provides some solutions for acquiring some of the data stored in some cellular telephone models using forensic hardware and software. Even if some of the stored information on the device may be acquired forensically, not all of the data subject to seizure may be so acquired. For devices that are not subject to forensic data acquisition or that have potentially relevant data stored that is not subject to such acquisition, the examiner must inspect the device manually and record the process and the results using digital photography. This process is time and labor intensive and may take weeks or longer.

34. Following the issuance of this warrant, I will collect the subject cellular telephone and subject it to analysis. All forensic analysis of the data contained within the telephone and its memory cards will employ search protocols

directed exclusively to the identification and extraction of data within the scope of this warrant.

35. Based on the foregoing, identifying and extracting data subject to seizure pursuant to this warrant may require a range of data analysis techniques, including manual review, and, consequently, may take weeks or months. The personnel conducting the identification and extraction of data will complete the analysis within ninety (90) days, absent further application to this court.

**PROCEDURES FOR ELECTRONICALLY STORED INFORMATION
(COMPUTERS AND OTHER ELECTRONIC STORAGE DEVICES)**

36. With the approval of the Court in signing this warrant, agents executing this search warrant will employ the following procedures regarding computers and other electronic storage devices, including electronic storage media and cell phones, that may contain data subject to seizure pursuant to this warrant:

Forensic Imaging

a. After securing the premises, or if sufficient information is available pre-search to make the decision, the executing agents will determine the feasibility of obtaining forensic images of electronic storage devices while onsite. A forensic image is an exact physical copy of the hard drive or other media. A forensic image captures all the data on the hard drive or other media without the data being viewed and without changing the data. Absent unusual circumstances, it is essential that a forensic image be obtained prior to conducting any search of the data for information subject to seizure pursuant to this warrant. The feasibility decision will be based upon the number of devices, the nature of the devices, the volume of data to be imaged, the need for and availability of computer forensics specialists, the availability of the imaging tools required to suit the number and

nature of devices found, and the security of the search team. The preference is to image onsite if it can be done in a reasonable amount of time and without jeopardizing the integrity of the data and the agents' safety. The number and type of computers and other devices and the number, type, and size of hard drives are of critical importance. It can take several hours to image a single hard drive - the bigger the drive, the longer it takes. As additional devices and hard drives are added, the length of time that the agents must remain onsite can become dangerous and impractical.

b. If it is not feasible to image the data on-site, computers and other electronic storage devices, including any necessary peripheral devices, will be transported offsite for imaging. After verified images have been obtained, the owner of the devices will be notified and the original devices returned within forty-five (45) days of seizure absent further application to this court.

Identification and Extraction of Relevant Data

c. After obtaining a forensic image, the data will be analyzed to identify and extract data subject to seizure pursuant to this warrant. Analysis of the data following the creation of the forensic image can be a highly technical process requiring specific expertise, equipment and software. There are thousands of different hardware items and software programs, and different versions of the same programs, that can be commercially purchased, installed, and custom-configured on a user's computer system. Computers are easily customized by their users. Even apparently identical computers in an office or home environment can be different with respect to configuration, including permissions and access rights, passwords, data storage, and security. It is not unusual for a computer forensic

examiner to have to obtain specialized hardware or software, and train with it, in order to view and analyze imaged data.

d. Analyzing the contents of a computer or other electronic storage device, even without significant technical challenges, can be very challenging. Searching by keywords, for example, often yields many thousands of hits, each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant hit does not end the review process for several reasons. The computer may have stored metadata and other information about a relevant electronic record – e.g., who created it, when and how it was created or downloaded or copied, when it was last accessed, when it was last modified, when it was last printed, and when it was deleted. Keyword searches may also fail to discover relevant electronic records, depending on how the records were created, stored, or used. For example, keywords search text, but many common electronic mail, database, and spreadsheet applications do not store data as searchable text. Instead, the data is saved in a proprietary non-text format. Documents printed by the computer, even if the document was never saved to the hard drive, are recoverable by forensic programs because the printed document is stored as a graphic image. Graphic images, unlike text, are not subject to keyword searches. Similarly, faxes sent to the computer are stored as graphic images and not as text. In addition, a particular relevant piece of data does not exist in a vacuum. To determine who created, modified, copied, downloaded, transferred, communicated about, deleted, or printed the data requires a search of other events that occurred on the computer in the time periods surrounding activity regarding the relevant data. Information about which user had logged in, whether users share passwords, whether the computer was connected to other computers or networks, and whether the user accessed or used other programs or services in the

time period surrounding events with the relevant data can help determine who was sitting at the keyboard.

e. It is often difficult or impossible to determine the identity of the person using the computer when incriminating data has been created, modified, accessed, deleted, printed, copied, uploaded, or downloaded solely by reviewing the incriminating data. Computers generate substantial information about data and about users that generally is not visible to users. Computer-generated data, including registry information, computer logs, user profiles and passwords, web-browsing history, cookies and application and operating system metadata, often provides evidence of who was using the computer at a relevant time. In addition, evidence such as electronic mail, chat sessions, photographs and videos, calendars and address books stored on the computer may identify the user at a particular, relevant time. The manner in which the user has structured and named files, run or accessed particular applications, and created or accessed other, non-incriminating files or documents, may serve to identify a particular user. For example, if an incriminating document is found on the computer but attribution is an issue, other documents or files created around that same time may provide circumstantial evidence of the identity of the user that created the incriminating document.

f. Analyzing data has become increasingly time-consuming as the volume of data stored on a typical computer system and available storage devices has become mind-boggling. For example, a single megabyte of storage space is roughly equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is roughly equivalent of 500,000 double-spaced pages of text. Computer hard drives are now being sold for personal computers capable of storing up to 2 terabytes (2,000 gigabytes) of data. And, this data may be stored in a variety of formats or encrypted (several new commercially available

operating systems provide for automatic encryption of data upon shutdown of the computer). The sheer volume of data also has extended the time that it takes to analyze data. Running keyword searches takes longer and results in more hits that must be individually examined for relevance. And, once reviewed, relevant data leads to new keywords and new avenues for identifying data subject to seizure pursuant to the warrant.

g. Based on the foregoing, identifying and extracting data subject to seizure pursuant to this warrant may require a range of data analysis techniques, including hashing tools to identify data subject to seizure pursuant to this warrant, and to exclude certain data from analysis, such as known operating system and application files. The identification and extraction process, accordingly, may take weeks or months. The personnel conducting the identification and extraction of data will complete the analysis within one-hundred twenty (120) days of this warrant, absent further application to this court.

h. All forensic analysis of the imaged data will employ search protocols directed exclusively to the identification and extraction of data within the scope of this warrant.

Genuine Risks of Destruction

i. Based upon my experience and training, and the experience and training of other agents with whom I have communicated, electronically stored data can be permanently deleted or modified by users possessing basic computer skills. In this case, only if the subject receives advance warning of the execution of this warrant, will there be a genuine risk of destruction of evidence.

//

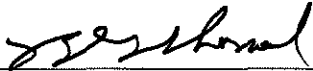
CONCLUSION

37. In conclusion, based upon the information contained in this affidavit, I have reason to believe that applications and location/GPS information contained in LANGSTON's Apple iPhone may constitute relevant records, evidence, fruits and instrumentalities relating to violations of Title 18, United States Code, §§ 1001, 1117, 1118, 1512, 2314, and 2261.



Special Agent Eric Van Houten, FBI

Subscribed and sworn to before me
this 14 day of April, 2016.



Bernard G. Skomal
United States Magistrate Judge

ATTACHMENT A

The item to be searched is a blue Apple iPhone, Model A1532, associated with no. 619-721-2979 (LANGSTON's Apple iPhone), located at the FBI Evidence Control Room, 10385 Vista Sorrento Parkway, San Diego, CA 92121.

ATTACHMENT B

Authorization is sought to search for and seize evidence that relates to the violation of 18 USC Sections §§ 1001, 1117, 1118, 1512, 2314 and 2261. This authorization includes the search of electronic data to include deleted data, remnant data and slack space. The search of computers and computer media, to include cell phones, will be conducted in accordance with the "Procedures For Electronically Stored Information" provided in the affidavit submitted in support of this warrant.

The item listed in Attachment A will be searched for communications, records, or data including, but not limited to, all location information or GPS data information stored in this iPhone or within any of its applications from March 1, 2015, to May 5, 2015.