AO 106 (Rev. 01/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Northern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
1 black I-PAD Air, serial # DMPLLPFPFK11; 1 silver/grey MacBook Pro serial # C02LM82AFD59; silver/grey & black WD My Passport hard drive, serial # WX51A92R0854; silver/grey & black WD My Passport hard drive, serial # WXU1EB3WVLC3, 1 black Western Digital hard drive, serial # WXK1A9003026T, 1 black micro 2GB San Disk Cruzer thumb drive; 1 terabyte, silver/grey, Transcend flash drive and black USB cable, 2 blue 4G PNY thumb drives, 1 purple, 8GB Verbatim thumb drive, 1 black Kingston MicroSD thumb drive, 1 black thumb drive w/toggles on the side, 1 purple & black Linkeys Bluetooth USB adapter, 1 orange and white thumb drive

Case No. 5:15-MJ-00154 (ATB)

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 there is now concealed on the following person or property located in the Northern District of New York *(identify the person or describe property to be searched and give its location):* See "Attachment A", which is attached to an incorporated in this Application and Affidavit.

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized):* See "Attachment B", which is attached to an incorporated inthis Application and Affidavit.

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 18 U.S.C. § 1030(a)(2), 1030(a)(5), and 1030(a)(5)(B), and the application is based on these facts:

☑ 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

Mark S. Hurley, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 04/17/2015

Judge's signature

City and state: Syracuse, New York

Hon. Andrew T. Baxter, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT

I, Special Agent Mark Hurley, being duly sworn, hereby depose and state that the following is true to the best of my information, knowledge, and belief:

INTRODUCTION AND AGENT BACKROUND

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have served in this capacity since 2011. I am currently assigned to the Albany Field Office, Syracuse Resident Agency, where I work with a team of Agents and Task Force Officers who are focused on investigating matters relating to a variety of federal crimes, including international terrorism. I have received formal training from the FBI in investigations and operations. Currently, I am responsible for, among other assignments, conducting investigations of alleged criminal violations of numerous Title 18 offenses, and in that capacity have worked on a number of investigations concerning international terrorism, violations of terrorism laws of the United States, the execution of search warrants, and the use of cell phones, social media, and other electronic devices used by subjects in those investigations. As an FBI Special Agent, I am authorized to investigate violations of the laws of the United States generally, and to execute arrest warrants issued under the authority of the United States. I have discussed the matters herein with the other Agents working on this and other associated investigations, read reports, and otherwise reviewed materials assimilated during the investigation. I have also discussed with these colleagues the use of computers and cellular phones to create, store, and use electronic data over internet-based applications, and how criminals, including terrorists and their supporters, use cellular telephones, computers and related equipment, and the internet to facilitate their crimes. My discussions have included consultations with law enforcement personnel specifically trained in these specialized areas.

2. This affidavit is in support of an application for a search warrant for digital devices the data located therein, that were seized from Chris Roberts on April 15, 2015 after Chris Roberts exited flight #3642 in Syracuse, New York. Chris Roberts had flown from Denver to Chicago on United Airlines flight #1474 on April 15, 2015, Roberts changed planes and continued to Syracuse.

3. The following statements contained in this affidavit are based on my experience and background as a Special Agent of the FBI and my work and conversations with other FBI special agents and specialists in this investigation. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I believe the information that I have set forth herein to be reliable based upon my investigation to date.

4. This investigation concerns alleged violations of Title 18 U.S.C. Sections 1030(a)(2), and 1030(a)(5), relating to unauthorized access to computers.

IDENTIFICATION OF THE DEVICE(S) TO BE EXAMINED

5. The property listed in Attachment A is secured in the FBI Syracuse Resident Agency and were found in the possession of Chris Roberts on April 15, 2015 after Chris Roberts exited United Airline flight #3642 in Syracuse, New York. The following items were seized by the FBI from Chris Roberts on April 15, 2015 at the Syracuse airport, herein referred to collectively as "Devices.":

A. 1 black I-PAD Air, serial number DMPLLPFPFK11 with hard plastic case and Death Wish Coffee Co sticker;

B. 1 silver/grey MacBook Pro, serial number C02LM82AFD59 w/multiple stickers;

C. 1 silver/grey & black WD My Passport hard drive, serial number WX51A92R0854

D. 1 silver/grey & black WD My Passport hard drive, serial number WXU1EB3WVLC3

E. 1 black Western Digital hard drive, serial number WXK1A9003026T w/"WIN" label;

F. 1 black micro 2GB San Disk Cruzer thumb drive;

G. 1 terabyte, silver/grey Transcend flash drive and black USB cable;

H. 2 blue 4G PNY thumb drives;

I. 1 purple, 8GB Verbatim thumb drive;

J. 1 black Kingston MicroSD thumb drive;

K. 1 black thumb drive w/toggles on the side;

L. 1 purple & black Linkeys Bluetooth USB adapter;

M. 1 orange & white thumb drive,

6. I submit there is probable cause to believe that the Device(s) are or contain evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1030(a)(2), 1030(a)(5). The applied-for warrant would authorize the forensic examination of the Device(s) for the purpose of identifying electronically stored data particularly described in Attachment B.

7. In my training and experience, I know that the Device(s) all have been stored in a manner in which the contents are, to the extent material to this investigation, in substantially the same state as they were when the Device(s) first came into the possession of FBI.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

8. Based on my training and experience, your Affiant knows about the following Devices.

9. A laptop computer is a computer that contains a hard disk drive ("HDD"). An HDD, which can be internal to the computer, or an external component, is a data storage device that consists of an external circuit board, external data, power connections, and internal glass, ceramic, or magnetically charged rotating metal platters that permanently store data even when powered off. A solid-state drive ("SSD"), also known as a solid-state disk, is a data storage device that uses integrated circuit assemblies as memory to permanently store data instead of using rotating platters. Flash drives, flash cards, and thumb drives are digital storage devices that can connect to computers or other devices using the appropriate connection. These devices are capable of storing any electronic information including images, videos, word processing documents, programs and software, and web pages.

10. A tablet, or IPad, is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets can also function as wireless communication devices and can be used to access the Internet through cellular networks, "wi-fi" networks, or otherwise. Tablets typically contain programs called applications ("apps"), which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

11. Computers and digital storage devices can include all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptop computers, mobile

phones, pagers, tablets, server computers, game consoles, and network hardware and also includes any physical object upon which computer data can be recorded such as hard disk drives, RAM, floppy disks, flash memory, CDs, DVDs, and other magnetic or optical media.

12. Based on my knowledge, training, and experience, your Affiant knows that computers and digital storage devices can store information for long periods of time, even if the user has attempted to delete the information. Similarly, things that have been searched for and viewed via the Internet, apps, or other programs, can be stored for some period of time on a device. This information can sometimes be recovered with forensic tools.

13. Based on my knowledge, training, and experience, examining data stored on computers and digital storage devices can uncover, among other things, evidence that reveals or suggests who possessed or used the computer or digital storage devices.

14. There is probable cause to believe that things that were once stored on the Device(s) may still be stored there, for at least the following reasons:

A. For example, based on my knowledge, training, and experience, I know that a powered-on computer maintains volatile data. Volatile data can be defined as active information temporarily reflecting a computer's current state including registers, caches, physical and virtual memory, network connections, network shares, running processes, disks (floppy, tape and/or CD-ROM), and printing activity. Collected volatile data may contain such information as opened files, connections to other computers, passwords used for encryption, the presence of anti-forensic tools, or the presence of programs loaded in memory that would otherwise go unnoticed. Volatile data and its corresponding evidentiary value is lost when a computer is powered-off and unplugged.

B. Based on my knowledge, training, and experience, I know that digital files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a digital storage device or computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

C. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

D. Wholly apart from user-generated files, computer storage media including digital storage devices and computers' internal hard drives can contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the

storage medium that can reveal information about the Device's use and who used it including online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer or device was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

E. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." Forensic review may also disclose when and by whom the Internet was used to conduct searches, view material, and communicate with others via the Internet.

15. As further described in Attachment B, this application seeks permission to locate not only electronically stored information on the Device(s) that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device(s) were used, the purpose of the use, who used the Device(s), and when. There is probable cause to believe that this forensic electronic evidence might be on the Device(s) because:

A. Data on the storage medium can provide evidence of a file that was once on the storage media but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the

attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer or device was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created. This information can be recovered months or even years after they have been downloaded onto the storage medium, deleted, or viewed. Bash history is a log detailing all commands entered by a user when operating in a Unix/Linux environment. The bash history is maintained on an operating system unless manually deleted by a user. Plist is a file that stores users settings on a Unix/Linux operating system. Plist files are the equivalent of registry files in a Windows operating system. I know that these sorts of artifacts provide evidence of what a computer was used for, by whom and when.

B. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

C. A person with appropriate familiarity with how a digital storage device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

D. The process of identifying the exact electronically stored information on storage media that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer or digital storage device and the application of knowledge about how a

computer or digital storage device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

E. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

F. Your Affiant knows that when an individual uses an electronic device to aid in the commission of a crime, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: information about devices attached to computers, and information about who used the devices and when and where.

G. Your Affiant also knows that those who engage in criminal activity will attempt to conceal evidence of the activity by hiding files, encrypting them, or by giving them deceptive names such that it is necessary to view the contents of each file to determine what it contains.

16. Your Affiant recognizes the prudence requisite in reviewing and preserving in its original form only such records applicable to the violations of law described in this Affidavit and in Attachment B in order to prevent unnecessary invasion of privacy and overbroad searches. Your Affiant advises it would be impractical and infeasible for the Government to review the mirrored images of digital devices that are copied as a result of a search warrant issued pursuant to this Application during a single analysis. Your Affiant has learned through practical

experience that various pieces of evidence retrieved from digital devices in investigations of this sort often have unknown probative value and linkage to other pieces of evidence in the investigation until they are considered within the fluid, active, and ongoing investigation of the whole as it develops. In other words, the weight of each individual piece of the data fluctuates based upon additional investigative measures undertaken, other documents under review and incorporation of evidence into a consolidated whole. Analysis is content-relational, and the importance of any associated data may grow whenever further analysis is performed. The full scope and meaning of the whole of the data is lost if each piece is observed individually, and not in sum. Due to the interrelation and correlation between pieces of an investigation as that investigation continues, looking at one piece of information may lose its full evidentiary value if it is related to another piece of information, yet its complement is not preserved along with the original. In the past, your Affiant has reviewed activity and data on digital devices pursuant to search warrants in the course of ongoing criminal investigations. Your affiant has learned from that experience, as well as other investigative efforts, that multiple reviews of the data at different times is necessary to understand the full value of the information contained therein, and to determine whether it is within the scope of the items sought in Attachment B. In order to obtain the full picture and meaning of the data from the information sought in Attachments A and B of this application, the Government would need to maintain access to all of the resultant data, as the completeness and potential of probative value of the data must be assessed within the full scope of the investigation. As such, your Affiant respectfully requests the ability to maintain the whole of the data obtained as a result of the search warrant, and to maintain and to review the data in the control and custody of the Government and law enforcement at times deemed necessary during the investigation, rather than minimize the content to certain communications

deemed important at one time. As with all evidence, the Government will maintain the evidence and mirror images of the evidence in its custody and control, without alteration, amendment, or access by persons unrelated to the investigation.

17. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, copying and reviewing the contents of the Device(s) consistent with the warrant. The warrant I am applying for would authorize a later examination and perhaps repeated review of the Device(s) or information from a copy of the Device(s) consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device(s) to human inspection in order to determine whether it is evidence described by the warrant.

INVESTIGATION

18. A Special Agent with the FBI interviewed Chris Roberts on February 13, 2015 and March 5, 2015 to obtain information about vulnerabilities with In Flight Entertainment (IFE) systems on airplanes. Chris Roberts advised that he had identified vulnerabilities with IFE systems on Boeing 737-800, 737-900, 757-200 and Airbus A-320 aircraft. Chris Roberts furnished the information because he would like the vulnerabilities to be fixed.

19. During these conversations, Mr. Roberts stated the following:

A. That he had exploited vulnerabilities with IFE systems on aircraft while in flight. He compromised the IFE systems approximately 15 to 20 times during the time period 2011 through 2014. He last exploited an IFE system during the middle of 2014. Each of the compromises occurred on airplanes equipped with IFE systems with video monitors installed in the passenger seatbacks.

B. That the IFE systems he compromised were Thales and Panasonic systems. The IFE systems had video monitors installed in the passenger seatbacks.

C. That he was able to exploit/gain access to, or "hack" the IFE system after he would get physical access to the IFE system through the Seat Electronic Box (SEB) installed under the passenger seat on airplanes. He said he was able to remove the cover for the SEB under the seat in front of him by wiggling and squeezing the box.

D. After removing the cover to the SEB that was installed under the passenger seat in front of his seat, he would use a Cat6 ethernet cable with a modified connector to connect his laptop computer to the IFE system while in flight.

E. He then connected to other systems on the airplane network after he exploited/gained access to, or "hacked" the IFE system. He stated that he then overwrote code on the airplane's Thrust Management Computer while aboard a flight. He stated that he successfully commanded the system he had accessed to issue the "CLB" or climb command. He stated that he thereby caused one of the airplane engines to climb resulting in a lateral or sideways movement of the plane during one of theseflights. He also stated that he used Vortex software after compromising/exploiting or "hacking" the airplane's networks. He used the software to monitor traffic from the cockpit system.

F. Roberts said he used Kali Linux to perform penetration testing of the IFE system. He used the default IDs and passwords to compromise the IFE systems. He also said that he used VBox which is a virtualized environment to build his own version of the airplane network. The virtual environment would replicate airplane network, and that he used virtual machine's on his laptop while compromising the airplane network.

20. On February 13, 2015 and February 23, 2015 Special Agents with the FBI in Denver advised Chris Roberts that accessing airplane networks without authorization is a violation of federal statute, and that Roberts may be prosecuted for obtaining access to airplane networks or scanning airplane networks. Chris Roberts advised that he understoodand he would not access airplane networks.

21. On February 23, 2015 the following tweet was made by on Chris Roberts' Twitter account Sidragon1: "Two very civilized but direct warnings in the last week to not mess with certain things means I'll be modifying a few upcoming talks".

22. On April 15, 2015 United Airlines advised the FBI that Chris Roberts tweeted the following message from Twitter account Sidragon1: "Find myself on a 737/800, lest see Box-IFE-ICE SATCOM, ? Shall we start playing with EICAS messages? 'PASS OXYGEN ON' Anyone ? :)".

23. The following conversation was on Twitter account Sidragon1 in response to the tweet about Roberts' being on a 737/800: RafalLos tweeted "...aaaaaand you're in jail. :)" followed by a tweet from Chris Roberts @Sidragon1 of "There IS a distinct possibility that the course of action laid out above would land me in an orange suite rather quickly :) ".

24. United Airlines advised that Chris Roberts was traveling on a United Airlines flight #1474 from Denver to Chicago on April 15, 2015. His seat was 3A. The aircraft tail number was 3260.

25. On April 15, 2015 a Senior Manager with United Airlines' Cyber Security Intelligence Department, advised that United Airlines flight #1474 was equipped with a Thales IFE system with seatback monitors. Two SEBs are installed in each row. One SEB is installed

on each side of the airplane aisle. A SEB is installed under seat 2A and a SEB is installed under seat 3A.

26. A Senior Manager with United Airlines' Cyber Security Intelligence Department advised the FBI that EICAS refers to the Engine Indication Crew Alerting System. The EICAS provides the pilots with information about the airplane engines.

27. According to a Senior Manager with United Airlines' Cyber Security Intelligence Department , the portion of Chris Roberts' tweet "PASS OXYGEN ON" may refer to the passenger oxygen masks on the aircraft. ICE is a possible acronym for In Flight Communications Equipment or Integrated Communications Equipment.

28. I know the acronym IFE refers to the In Flight Entertainment system and SATCOM is a reference to satellite communications system which are installed on some aircraft.

29. On April 15, 2015 Chris Roberts changed aircraft after arriving in Chicago and flew to Syracuse, New York on United Airlines flight #3642. United Airlines flight #3642 was not equipped with an IFE system.

30. United Airlines aircraft with tail number 3260 flew from Chicago to Philadelphia on April 15, 2015. The flight number was 1607. The flight arrived at gate D13 at Philadelphia International Airport on April 15, 2015.

31. On April 15, 2015, a Special Agent with the FBI inspected the SEBs in the first class cabin on United Airlines 737 aircraft, flight 1607 at gate D13 at the Philadelphia International Airport. A Special Agent with the FBI advised that the SEBs under seats 2A and 3A showed signs of tampering. The SEB under 2A was damaged. The outer cover of the box was open approximately ½ inch and one of the retaining screws was not seated and was exposed.

32. At that time, we then knew: (1) that the Seat Electronics Box (SEB) for the IFE aboard the aircraft on which Roberts had flown from Denver to Chicago on April 15, 2015 showed signs of tampering in the location where Roberts had been seated; (2) that Roberts had sent social media messages during that flight indicating he was about to access without authorization that aircraft's IFE; (3) that Roberts had previously claimed in his conversations with the FBI on February 13, 2015 and March 5, 2015 that he had been able to and did use special equipment in his possession to "hack" into the IFE systems on aircraft previously and had claimed that he had connected to other systems on the aircraft network; and (4) that agents and technical specialists with the FBI believed that he may have just done that again or attempted to do so using the equipment then in his possession as witnessed by the FBI. We further knew that Roberts had reservations to travel by air from Syracuse back to Denver on April 17, 2015. Considering all of this information, we believed that Roberts had the ability and the willingness to use the equipment then with him to access or attempt to access the IFE and possibly the flight control systems on any aircraft equipped with an IFE system, and that it would endanger public safety to allow him to leave the Syracuse airport that evening with that equipment. Accordingly, we confiscated the above-referenced equipment at that time.

33. On April 15, 2015, Special Agents with the FBI interviewed Roberts at the Syracuse Airport after he arrived in Syracuse on United Airlines flight #3642. Chris Roberts had the following items in his possession upon arrival in Syracuse: 1 black I-PAD Air, serial number DMPLLPFPFK11with hard plastic case and Death Wish Coffee Co sticker; 1 silver/grey MacBook Pro serial number C02LM82AFD59 w/multiple stickers; silver/grey & black WD My Passport hard drive, serial number WX51A92R0854; silver/grey & black WD My Passport hard drive, serial number WXU1EB3WVLC3, 1 black Western Digital hard drive, serial number

WXK1A9003026T w/ "WIN" label; 1 black micro 2GB San Disk Cruzer thumb drive; 1 terabyte, silver/grey, Transcend flash drive and black USB cable; 2 blue 4G PNY thumb drives; 1 purple, 8GB Verbatim thumb drive; 1 black Kingston MicroSD thumb drive; 1 black thumb drive w/toggles on the side; 1 purple & black Linkeys Bluetooth USB adapter, 1 orange and white thumb drive.

34. Chris Roberts asked the interviewing Agents when Roberts was interviewed if the interview was in response to Roberts' tweet on April 15. Roberts advised during the interview that he did not compromise the airplane network on the United Airlines flight from Denver to Chicago. Chris Roberts advised that the thumb drives in his possession contained virtual machines and malware to compromise networks. He described the content as "nasty."

35. A virtual machine is a secondary operating system that runs on a primary operating system with hardware emulation. A user is able to run several concurrent virtual machines with different operating systems on one computer. Virtual machines can be stored and operated from different storage media such as USB drives, external hard drives, CDs/DVDs, or an internal hard drive.

36. During the interview on April 15, 2015 Chris Roberts voluntarily showed the FBI wiring schematics related to multiple airplane models. The schematics were on Roberts' MacBook Pro.

37. Chris Roberts advised during the interview on April 15, 2015 that his MacBook Pro had been powered on since his flight from Denver to Chicago. The screen is locked on the MacBook Pro but the computer has remained on since being seized by the FBI on April 15, 2015.

38. On April 15, 2015 the FBI seized digital evidence in possession of Chris Roberts. Roberts photographed the items that were seized. A photograph of the seized items were then tweeted on Chris Roberts' Twitter account Sidragon1 with the following caption "Bye bye electronics, all encrypted....and all now in custody/seized".

CONCLUSION

39. Based on the investigation described above, probable cause exists to believe that inside the Device(s) (described on Attachment A), will be found evidence, fruits, and instrumentalities of a violation of Title 18, United States Code, Sections 1030(a)(2), 1030(a)(5) an 1030(a)(5)(B). (described on Attachment B).

40. I, therefore, respectfully request that the attached warrant be issued authorizing the search and seizure of the items described in Attachment A for the items listed in Attachment B.

I declare under penalty of perjury that the foregoing is true and correct to the best of my information, knowledge, and belief.

Mark Hurley, Special Agent, FBI

SUBSCRIBED and SWORN before me this 17th day of April, 2015

Hon. Andrew T. Baxter
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

1 black I-PAD Air, serial number DMPLLPFPFK11with hard plastic case and Death Wish Coffee Co sticker; 1 silver/grey MacBook Pro serial number C02LM82AFD59 w/multiple stickers; silver/grey & black WD My Passport hard drive, serial number WX51A92R0854; silver/grey & black WD My Passport hard drive, serial number WXU1EB3WVLC3, 1 black Western Digital hard drive, serial number WXK1A9003026T w/ "WIN" label; 1 black micro 2GB San Disk Cruzer thumb drive; 1 terabyte, silver/grey, Transcend flash drive and black USB cable; 2 blue 4G PNY thumb drives; 1 purple, 8GB Verbatim thumb drive; 1 black Kingston MicroSD thumb drive; 1 black thumb drive w/toggles on the side; 1 purple & black Linkeys Bluetooth USB adapter, 1 orange and white thumb drive.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED

For the Device(s) listed and described in Attachment A, the following items, that constitute evidence of the commission of, contraband, the fruits of crime, or instrumentalities of violations of Title 18, United States Code, Sections 1030(a)(2); 1030(a)(5)(A); and 1030(a)(5)(B).

1. Software programs used for mapping, compromising or monitoring computer networks including Kali Linux, Metasploit, Wireshark, fdXplorer, ParaView software, VxWorks, Nmap, Vector Canoe and Vortex software.

2. Virtualizing software including Virtual Box and VMWare.

3. Bash history on native or virtualized Linux machines.

4. All files related to connection settings including connection logs, registry lists, and plists.

5. All electronic email, attachments, chat logs, Twitter posts, FaceTime logs and Skype logs or other communications discussing airplane systems or how to access a airplane's computer systems or that would reveal who used the devices and when.

6. Powerpoint presentations, photographs, images, and screenshots containing information about airplane networks, airplane wiring schematics and In Flight Entertainment systems.

7. Documentation about In Flight Entertainment systems, airplane manuals, and airplane networks.

8. Records pertaining to airline travel.

9. Volatile memory to include encryption keys and passwords.

10. Usernames and passwords for In Flight Entertainment systems and airplane networks.

11. Mac Addresses.

12. Records of internet activity including search terms pertaining to violations of 18 U.S.C. §§ 1030(a)(2) or 1030(a)(5), or that show who used, owned, possessed, or controlled the Device(s)

13. Evidence of who used, owned, or controlled the Device(s) to commit or facilitate the commission of the crimes described, or at the time the things described in this warrant were created, edited, or deleted, including photographs, videos, logs, call logs, phonebooks, address books, contacts, IP addresses, registry entries, configuration files, saved usernames and passwords, documents, calendars, browsing history, search terms, metadata, user profiles, e-mail, e-mail contacts, messages (text or voice), instant messaging logs, file structure and correspondence.

14. Evidence of software that may allow others to control the Device(s), such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security provisions or software designed to detect malicious software or unauthorized use of the device, and evidence of the lack of such malicious software

DEFINITIONS:

15. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical

form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).