FILED
UNITED STATES DISTRICT COURT
ALBUQUERQUE, NEW MEXICO

SEP 18 2012

MATTHEW J. DYKMAN
CLERK

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of New Mexico

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

2540 FIREWHEEL AVENUE SW, LOS LUNAS, NM 87031, described in Attachment A, incorporated herein by reference.

Case No. 12MR852

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 to Affidavit, incorporated herein by reference.

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

See Attachment B to Affidavit, incorporated herein by reference.

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:

Code Section	*Offense Description*
18 U.S.C. 1030	Fraud and related activity in connection with Computers
18 U.S.C. 2511	Interception and disclosure of wire, oral, or electronic communications prohibited

The application is based on these facts:

See attached affidavit, incorporated herein by reference.

- ☑ 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

Michael Boady, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 09/18/2012

Judge's signature

City and state: ALBUQUERQUE, NEW MEXICO

Alan C. Torgerson
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO

IN THE MATTER OF THE SEARCH OF: 2540 FIREWHEEL AVENUE SW, LOS LUNAS, NM 87031	Case No. 12MR852

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Michael Boady, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the SUBJECT PREMISES known as 2540 FIREWHEEL AVENUE SW, LOS LUNAS, NM 87031, hereinafter "SUBJECT PREMISES," further described in Attachment A, for the items described in Attachment B.

2. I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws. I have been a Special Agent (SA) with the Federal Bureau of Investigation ("FBI") for over eight years. I have participated in investigations of computer crimes, crimes against children on the Internet and, among other things, have conducted or participated in surveillance, the execution of search warrants, and debriefings of informants. Through my training, education and experience, I have become familiar with the manner in which computers, computer equipment, software, and electronically stored information are used in furtherance of criminal activity.

AFT

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. As set forth herein, there is probable cause to believe that at the SUBJECT PREMISES, there exists evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. § 2511 (Interception and disclosure of wire, oral, or electronic communications prohibited) and Title 18 U.S.C. § 1030 (Fraud and related activity in connection with Computers).

PROBABLE CAUSE

4. On or about June 21, 2012, Susana Martinez ("Martinez"), the Governor of the State of New Mexico, contacted the Albuquerque Division of the FBI to report a suspected computer intrusion. During subsequent interviews with Governor Martinez as well as Jay McCleskey ("McCleskey"), a political consultant to Governor Martinez, the FBI determined that the allegations warranted further investigation.

5. During the course of investigation, the FBI has learned that on or about July 18, 2009, in connection with Governor Martinez' 2010 gubernatorial campaign, one of Martinez' early supporters, David Hiss ("Hiss"), created and registered an internet domain designated as www.susana2010.com (the "Domain"). Hiss created the Domain, with the intent to donate it to Martinez' gubernatorial campaign, using the domain registrar GoDaddy.com ("GoDaddy"). The Domain was registered for a period of two years. As such, the domain registration was set to expire on or about July 18, 2011.

6. Among other purposes, throughout the course of the 2010 gubernatorial campaign, Martinez and her staff used the Domain to communicate with one another, and with

AEF

individuals outside the campaign, via email. To that end, each member of Martinez' staff, as well as Martinez herself, maintained an email address at the Domain, (*e.g.*, Susana@susana2010.com).

7. The Domain was controlled by means of username and password. Only the individual or individuals who had access to the username and password associated with the Domain were able to make substantive changes to the Domain. Such changes included, but were not limited to, creating new email accounts associated with the Domain, adding or removing substantive content from the website associated with the Domain, and directing incoming email to a certain mail server. Furthermore, only an individual with access to the username and password would have the ability to renew the Domain upon its expiration in July 2011.

8. After the Domain was donated to the campaign, then-campaign manager Jamie Estrada ("Estrada") maintained the username and password associated with the Domain. During the gubernatorial campaign, Governor Martinez caught Estrada reading her emails from the susana2010.com domain, which led to him being removed from the campaign prior to the election in 2010. On December 23, 2009, in an e-mail sent by Estrada to McCleskey he expressed his frustration regarding the decision and stated the following:

> "*...I can't understand how she wouldn't think there are political consequences for treating me poorly and unfairly.*"

9. Around that same time, on or about December 27, 2009, Governor Martinez sent an email to Estrada which included the following text:

ACT

> "*Please submit immediately all information you have that pertains to this campaign, to include, but not limited to...[a]ny and all usernames and passwords to any account or any service, to include, Vonage, Verizon, Wells Fargo, or any account that belongs to this campaign...any and all data that is part of the campaign...please provide all of the above data on Mo[n]day, December 28, 2009, no later than 5:00pm. I will expect that you will not keep any electronic copies or hard copies of any of the campaign data.*"

10. Following her election as Governor in November 2010, Martinez and her political staff continued to use email accounts linked to the Domain for certain communications. On or about July 18, 2011, however, Martinez' staff began receiving reports that emails sent to addresses at the Domain were bouncing back to the sender. Members of Martinez' staff soon determined that the emails were not being delivered as intended, because the Domain had expired.

11. As mentioned above, the Domain was registered with GoDaddy, a company located in Scottsdale, Arizona. GoDaddy allows a domain registrant a grace period of 42 days[1] in which to re-register a domain name before it is cancelled and released to the public for purchase. On or about July 18, 2011, the day it was discovered that the domain had expired, members of Martinez' staff made efforts to re-register the Domain, but were unsuccessful. However, no one on the staff had access to the username and password associated with the Domain. What further complicated the situation, GoDaddy does not permit anyone to re-register a domain without the username and password or proof that you are the original registrar, to prevent hijacking of a domain name.

---

[1] http://support.godaddy.com/help/article/608/what-is-your-process-for-handling-expired-domain-names

ACT

12. At the time, neither Governor Martinez nor the members of her staff could recall who registered the domain originally. Eventually, members of Martinez' staff contacted Estrada in an effort to obtain the username and password associated with the Domain, but Estrada declined to provide this information. The staff was, therefore, unable to re-register the Domain.

13. Having been unsuccessful in their attempts to re-register the Domain, Martinez' staff simply transitioned their political communications to a new domain designated as "susanapac.com." Martinez and her staff made efforts to alert all potential contacts of the corresponding change in email addresses. Following this change, Martinez and her staff believed that the Domain had simply expired and was no longer in use.

14. However, in and around June 2012, local media outlets obtained and published an email from Hanna Skandera ("Skandera"), the Cabinet Secretary for the Department of Education, to Martinez's susana2010.com email account. The email was originally sent on or about May 2, 2012 to several individuals including two of Martinez' staffers accounts at the Domain. The release of this email prompted Martinez and her staff to believe that the Domain had not in fact expired, but had been re-registered by someone unaffiliated with Martinez' political organization. The individual who re-registered this domain apparently redirected incoming emails into a different account unassociated with the Domain.

15. According to McCleskey, he and Governor Martinez suspected Estrada may have been the one who renewed the domain and redirected it, so they sent attorney, Pat Rogers ("Rogers") to confront Estrada. When Rogers confronted Estrada, he immediately presented him with a printout from David Hiss, the original registrant. The printout appeared to be an email

AT

from Hiss to jamie@jamieestrada.com, which was dated August 17, 2009, and included the GoDaddy account details including the username and password for the Domain account.

16. McCleskey advised that Rogers made a comment to him about how readily Estrada had that email printout, like he expected to be contacted about the Domain. Moreover, Estrada denied that he renewed the Domain or had any knowledge of who had may have accessed it.

17. When the FBI interviewed Hiss, he advised that he did not renew the Domain in 2011 nor was he aware of anyone else who had done so. Moreover, Hiss advised that he contacted GoDaddy and informed them of the situation. GoDaddy investigated the situation and determined that someone had fraudulently used his credentials to re-register the Domain within the 42 day grace period, therefore, GoDaddy returned the Domain to Hiss' control.

18. After the email was released to the media, Governor Martinez and McCleskey took steps to learn who might have re-registered the Domain and, by extension, who might be receiving any emails sent to accounts at the Domain. Through their own investigation using open-source information, Martinez and her staff learned that the Domain was renewed on July 29, 2011, only ten days after it had expired. Because of GoDaddy's policy allowing a 42-day grace period, this timing strongly indicates that the Domain was renewed by either the original registrant or someone who had access to the username and password.

19. The FBI obtained information from GoDaddy, relating to the registration history of the Domain. These records confirmed that the Domain was in fact re-registered on or about

ACT

July 29, 2011, approximately ten days after it had initially expired. The records received from GoDaddy further indicate that the individual who re-registered the Domain did so using Hiss' credentials which were originally associated with the account.

20. Information provided by GoDaddy indicated that the Domain was re-registered by an individual who was assigned GoDaddy Shopper ID 29407762 and provided the following subscriber information:

Name: Sylvia Tacori

Address: 1644 E. Evans, Denver, Colorado 80210

Login Name: stac303

Phone Number: 303-416-6156

Email Address: sylviatacori@gmail.com

21. Investigation has determined that the subscriber information provided by the registrant above was fictitious. Investigative databases were unable to identify anyone by the name of Sylvia Tacori. Additionally, the address of 1644 E. Evans, Denver, Colorado 80210 is the location of a Chipotle restaurant. Lastly, the method of payment used to pay for the renewal of the Domain was a Green Dot Prepaid debit card, which was purchased on April 28, 2010 at a Walmart Rite Aid store located in the Washington, D.C. area. In my training and experience, Green Dot cards are commonly used by individuals attempting to conceal their identity since money can be put on them and they cannot be traced.

22. Information provided by GoDaddy for Shopper ID 29407762, which is the Sylvia Tacori account, had several pieces of information which are pertinent to the case and assisted

AFT

with identifying the individual controlling the account. According to GoDaddy, the Domain was re-registered on 7/29/2011 and accessed from IP address 216.184.15.250, between 10:48 and 11:20am Arizona time. Investigation has determined that the IP address is associated with the Flying Star restaurant located at 8001 Menaul Blvd NE, Albuquerque, NM 87110. This signifies that the subject connected to the free wireless at Flying Star either with a personal laptop and/or cell phone to access the Sylvia Tacori GoDaddy account.

23. Another significant piece of information provided by GoDaddy, that assisted with the identification of the subject who created the Sylvia Tacori account that renewed the Domain was found in the notes for the Shopper ID 29407762, which included the following text:

> *7/31/2011 6:28:43 PM / Customer / Client IP: onlinestor:90575589-Profile Update REQUESTOR_IP:97.224.178.242.*
>
> *7/31/2011 6:28:43 PM / Customer / Client IP: calendar:90575580-Profile Update REQUESTOR_IP:97.224.178.242.*
>
> *7/31/2011 6:28:43 PM / Customer / Client IP: email:90575579-Profile Update REQUESTOR_IP:97.224.178.242.*

24. The above lines are significant because they show that the person who renewed the Domain and controls the Sylvia Tacori account logged in and updated the profile information from IP address 97.224.178.242 at 6:28pm Arizona time. Investigation determined that the IP address associated with 97.224.178.242 was a cell phone assigned to the following Verizon Wireless customer:

> *Name: Jamie P. Estrada*
>
> *Address: 4830 25th Road N, Arlington, VA 22207*
>
> *Cell number: 575-386-9654*

ACT

Home Number: 703-465-0889

This signifies that Estrada, using his cell phone internet service has logged into the GoDaddy account that was used to re-register the Domain in the name of Sylvia Tacori.

25. Further investigation determined that Estrada previously lived at that address and still maintains that phone number. For example, Estrada has a Facebook account (www.facebook.com/JamieEstradaNM) and a Google Mail account jpestrada@gmail.com, both of which are registered in Estrada's name and associated with the 575-386-9654 number. Additionally, on December 25, 2009, Estrada sent a text message to McCleskey from the 575-386-9654 number with the following text:

"*Its Jamie,..my new permanent cell # is 575-386-9654.*
Sent from my Verizon Wireless Blackberry"

26. On September 6, 2012, the writer received compliance from Verizon which included cell site information, IP sessions, and call logs which detailed the use of the cell phone. Based on that compliance, it appears that Estrada uses the cell phone quite regularly to access the internet as well as making phone calls. In a one month period, there were two cell towers which Estrada's phone was used to connect to the internet and/or make phone calls from more than any others. The first, was cell tower #890, which is located at 320 Gold Ave SW, Albuquerque, NM 87102. According to the logs, in one month, Estrada connected to this cell tower over 200 times. This makes sense because Estrada is the Vice President at DW Turner[2], a local public relations

[2] http://www.dwturner.com/Jamie_Estrada.aspx

ACT

company which is located at 400 Gold Ave SW, 12th Floor, Albuquerque, NM 87102, which according to Google Maps is 98 feet away from the tower.

27. The second cell tower that was most frequently accessed by Estrada's cell phone was cell tower #427, which is located at 1000 Main St., Los Lunas, NM 87031. In one month, Estrada connected to this cell tower 150 times. This tower is the closest one to Estrada's residence of 2540 Firewheel Ave SW, Los Lunas, NM 87031, the SUBJECT PREMISES, and is less than 2 miles away.

28. The information provided by Verizon shows that the "First Servicing Cell Face" for the connections between Estrada's cell phone and cell tower #427 were almost always a "3". This is significant because a three (3) represents a person who is beaconing in the direction between South and Northwest of the cell tower (e.g. between the 6 and 10 on a clock). A direct line between Estrada's residence and the cell tower would be consistent with someone who is connecting to this cell tower from cell face "3".

29. Information provided by Verizon advised that on December 24, 2009, Estrada updated his Verizon account associated with the 575-386-9654 number, to reflect his current place of residence as 2540 Firewheel Ave SW, Los Lunas, NM 87031, the SUBJECT PREMISES. Investigative databases and publically available information confirm that Estrada's primary place of residence is at the SUBJECT PREMISES, where he resides with his wife Kristina Estrada.

RCT

30. On September 17, 2012, the FBI conducted surveillance on the SUBJECT PREMISES, and observed Estrada leaving the residence in a vehicle registered to him. Moreover, the FBI observed Estrada driving his vehicle and arriving at a parking garage that is adjacent to Estrada's place of work.

31. Based on my training and experience, it is common for people to use their cell phone to access the internet directly, or in some cases, people use the internet connection provided by their cell phone service to access the internet with their computer, which is commonly known as "tethering". Tethering is defined as "the process of using a cell phone or smartphone as a modem for a personal computer of some sort - typically a laptop computer."[3]

32. On July 29, 2011, between 11:10am and 11:20am Arizona time, while using the wireless internet connection from the Flying Star restaurant described above, the individual who re-registered the Domain executed a sequence of commands to cause all incoming email messages intended for Governor Martinez and/or her staff to be directed to an account hosted by Google through the use of a service called Google Apps. This was done by changing the mail exchanger record (MX record) associated with the Domain from an IP address associated with a company called YumaSol to an IP address associated with Google. Although the precise location of which the incoming mail messages were directed is unknown, the individual who re-registered the Domain provided the email address SYLVIATACORI@GMAIL.COM (herein referred to as "SYLVIATACORI").

---

[3] http://www.mobileburn.com/definition.jsp?term=tether

AEG

33. Based in part on the information provided above, on July 20, 2012, the Honorable Judge Robert Hayes Scott, District of New Mexico, issued a search warrant for the SYLVIATACORI account. During a review of the SYLVIATACORI account, the FBI found several emails that further substantiated the belief that the Domain was re-registered by the person who maintained the SYLVIATACORI account and that the person who re-registered it directed all incoming emails to a 'Google Apps' account.

34. One such email was received on July 29, 2011, the same day that the domain was re-registered, which included the following text:

> *"Hello Google Apps admin,*
>
> *We're excited to help you offer powerful communication and sharing tools to susana2010.com with Google Apps!*
>
> *To learn how to setup and deploy Google Apps, visit our getting started resource center for tips and instructions:*
>
> *http://www.google.com/a/help/intl/en/admins/resources/setup/*
>
> *Step 1: Sign in to the administrative control panel. Here you can manage your user accounts and customize Google Apps. To access the control panel, visit:*
>
> *http://www.google.com/a/susana2010.com/*
>
> *If you haven't already signed in and created your administrator account, you can click here:*
>
> *<https://www.google.com/a/cpanel/standard/setup/susana2010.com/GWe8zjEBAAA.5aPjWGdcYiEwMRajjuwVAw.2HKCxUvwbN8WMj6ahzVfgQ?hl=en>*
>
> *Step 2: Verify domain ownership. Before we can fully activate your services, you will need to verify ownership of susana2010.com. From the control panel, you can verify by either uploading an HTML file or creating a special CNAME record. Verifying ownership does not cause any change to your existing services.*

AZ

To find more information or get in touch, visit our Help Center at http://www.google.com/support/a. Please do not reply to this email; replies are not monitored.

Sincerely,

The Google Apps Team"

35. The above email shows that the owner of the SYLIVATACORI account also setup a Google Apps account which allowed that person to gain full control of the domain including the ability to accept all emails addressed to the Domain, using the administrative control panel located at http://www.google.com/a/susana2010.com.

36. On or about June 29, 2012, the public was made aware of the FBI's ongoing investigation, when the media posted an article entitled "Gov. Martinez alleges hacking of campaign email", which included the following text:

"*New Mexico Gov. Susana Martinez has asked the FBI to investigate whether a campaign email system was hacked to obtain correspondence involving her and her top advisers, a spokesman for the governor said Friday.*"

37. Information provided by Google advised that shortly after, on July 15, 2012, around 19:00 UTC, the SYLVIATACORI account was deleted by the registrant, believed to be Estrada. According to Google, the IP address used to access the account and delete it was 198.22.122.160, which is associated with Best Buy. In addition to deleting the SYLIVATACORI account, the subject also deleted the Google Apps account which is believed to have been used to store all of the incoming emails intended for Governor Martinez and her staff at the Domain.

AT

38. According to Best Buy, they have a free and open wireless connection available for any of their customers, which could even be accessed from the parking lot if someone has a cell phone and/or laptop with them that has that functionality.

39. Reviews of several email accounts, domains, and social media accounts which are registered in the name Jamie Estrada and believed to be maintained and accessed by him identified that the accounts were accessed those accounts on a regular basis from two primary internet sources, Comcast Communications and City Link Fiber Holdings, LLC.

40. Information provided by Comcast confirms that Estrada has High Speed Internet Service that is registered at the SUBJECT PREMISES, and is assigned the Comcast user identification estrada575@comcast.net. The Comcast account is active and is being paid for with a credit card that is associated with Estrada. Based on my training and experience, a person who has an internet connection at their residence typically has at least one computer or similar device that allows them to access the internet. Furthermore, computers and similar devices that are likely to be at the SUBJECT PREMISES could have been used in furtherance of the above described criminal activity and may have information stored therein, that would be considered evidence of the captioned case.

41. Information provided by City Link Fiber Holdings, LLC advised that the registrant of the IP address which accessed several of Estrada's personal accounts is assigned to DW Turner, a public relations firm located at 400 Gold Avenue SW, 12th Floor, Albuquerque, NM 87102. As mentioned above, Estrada is employed at DW Turner.

AET

TECHNICAL TERMS

42. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, floppy disks, flash memory, CD-ROMs, and several other types of magnetic or optical media not listed here.

ACT

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

43. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

44. *Probable cause.* I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer 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 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.

b. 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

ACY

addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—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.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. Based on review of the evidence related to this investigation, I am aware that computer equipment was used to generate and store documents and records used in the above mentioned fraud schemes.

45. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer in the SUBJECT PREMISES because:

A24

a. Data on the storage medium 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). 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 was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

RG

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer 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 and the application of knowledge about how a computer 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 computer 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. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. When an individual uses a computer to commit fraud, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received;

ACT

notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

46. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of the SUBJECT PREMISES for information that might be stored on storage media often requires agents to seize physical storage media and later review the media consistent with the warrant. In lieu of removing storage media from the SUBJECT PREMISES, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on SUBJECT PREMISES could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

ACF

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the SUBJECT PREMISES. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

47. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), when officers executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for would permit officers either to seize or to image-copy storage media that reasonably appear to contain some or all of the evidence described in the warrant, and then later examine the seized storage media or image copies consistent with the warrant. The examination may require searching authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

ACT

CONCLUSION

48. I submit that this affidavit supports probable cause for a warrant to search the SUBJECT PREMISES described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,

Michael Boady
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on September 18, 2012:

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is 2540 FIREWHEEL AVE. SW, LOS LUNAS, NM 87031, including any vehicles located on the property that are owned or operated by JAMIE ESTRADA. The property is further described as a two-story single family home, with stucco walls that are a variant of pink in color. The number "2540" is on the North of the two-car garage at approximately eye level. The house has a two-car garage next to a one-car garage as seen in the image below:

AR4

ATTACHMENT B

1. All records, in any form, relating to violations of Title 18 U.S.C. § 2511 (Interception and disclosure of wire, oral, or electronic communications prohibited) and Title 18 U.S.C. § 1030 (Fraud and related activity in connection with Computers), involving JAMIE ESTRADA including:

a. Usernames, passwords, and other account information for email accounts, Google Apps accounts, domain accounts, accounts for credit, debit, or gift cards, and online storage accounts;

b. Records which are related to the use of computer programs to re-direct email from one domain to another;

c. All records and/or communications related to the susana2010.com and susanapac.com domains or the hi-jacking thereof;

d. All bank records, checks, credit or debit card bills, account information, and other financial records from June 2011 to the present.

e. Records relating to the provision of internet and phone service;

f. Any receipts or evidence showing business conducted at Best Buy stores and/or Flying Star restaurants from June 2011 to the present.

g. Records showing the technical or computer knowledge.

2. Any and all Green Dot Pre-paid credit/debit cards.

3. Any computers or electronic media that were or may have been used as a means to commit the offenses described on the warrant.

AEF

4. For any computer, computer hard drive, or other physical object upon which computer data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

c. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

d. evidence of the times the COMPUTER was used;

e. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

f. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

g. contextual information necessary to understand the evidence described in this attachment.

5. Records and things evidencing the use of computers and/or the internet to commit the fraud activity described in the Search Warrant Affidavit, including:

a. routers, modems, and network equipment used to connect computers to the Internet;

ARF

b. records of Internet Protocol addresses used;

c. records of wireless internet connections to Best Buy, Flying Star, and/or City Link Fiber Holdings, LLC.

d. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

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).

6. Any and all statements for credit cards, debit cards, and bank accounts, which include transactions from June 1, 2011 to the present.

7. Any and all documents, printouts, hand written statements, electronic communications, and in whatever form related to the following:

a. The Susana2010.com domain

b. Communications with GoDaddy.com and DomainsByProxy.com

c. The SusanaPAC.com domain.

8. Any and all records in whatever form related to Sylvia Tacori, SylviaTacori@gmail.com, and/or Google Voice number 303-416-6156.

ACT