



U.S. Department of Justice

Criminal Division

RPD:KKP:ECW
F. #2007R01826

Computer Crime & Intellectual Property Section
1301 New York Ave., Suite 600
Washington, D.C. 20530
PHONE: (202) 514-1026
FAX: (202) 514-6113

July 24, 2009

BY ECF & FEDERAL EXPRESS

The Honorable Sandra J. Feuerstein
United States District Court Judge
Eastern District of New York
Long Island Federal Courthouse
Central Islip, New York 11722

Re: United States v. Albert Gonzalez
Criminal Docket No. 08-160(S-1)(SJF)

Dear Judge Feuerstein:

The government respectfully submits this letter brief in support of a motion in limine for the admission at trial of certain foreign computer evidence. The government intends to offer into evidence: (i) a computer server from Riga, Latvia on which the defendant Albert Gonzalez stored computer hacking programs and stolen credit card data (the "Latvian Server"); and (ii) files copied from a laptop computer seized upon the July 2007 arrest of co-defendant Maksym Yastremskiy in Antalya, Turkey (collectively, the "Foreign Computer Evidence").

The government submits that the Foreign Computer Evidence possesses "distinctive characteristics, taken in conjunction with circumstances," which authenticate it. Fed. R. Evid. 901(b)(4). The government therefore seeks an in limine finding by the Court that sufficient proof exists that the Foreign Computer Evidence is authentic for its admission at trial.¹ See Fed. R. Evid. 901(a).

¹ The Foreign Computer Evidence was obtained with the assistance of the Latvian State Police and Turkish National Police, respectively. The government has submitted Mutual Legal Assistance Treaty requests to both Latvia and Turkey for testimony from the foreign nationals who assisted the United States government in obtaining the Foreign Computer Evidence. The government, however, has no power to compel foreign citizens to testify in United States court proceedings. It is uncertain

BACKGROUND

I. The Offenses

The 27-count indictment charges the defendant and co-defendants Maksym Yastremskiy ("Yastremskiy") and Aleksandr Suvorov ("Suvorov") with a scheme to steal customer credit card numbers from Dave & Buster's, a national restaurant chain with a store in Islandia, New York. An extradition request is pending with the Turkish government for Yastremskiy, who was convicted in Turkey last year of computer crimes and sentenced on January 8, 2009 to 30 years imprisonment there. Suvorov pled guilty on May 20, 2009 before Magistrate Judge A. Kathleen Tomlinson and is currently awaiting sentencing.

The government alleges that these three men conspired and acted in concert to penetrate the Dave & Buster's computer network with a "packet sniffer," a malicious computer program designed to capture customer credit card data. In brief, the defendant provided the packet sniffer to Yastremskiy, who in turn provided it to Suvorov, who had it installed on the Dave & Buster's network.

II. The Role of the Foreign Computer Evidence

Files from the Latvian Server link the defendant to the packet sniffer used in the Dave & Buster's intrusion. The Latvian Server contains two crypts, or cyber-containers. Prior to his arrest, the defendant had complete access, from anywhere in the world, to the Latvian Server crypts, which he opened and accessed with a lengthy password. A modified version of the packet sniffer was found in one of the crypts, which also contained millions of stolen credit card numbers.

Files copied from the laptop computer seized pursuant to Yastremskiy's arrest link the defendant and Yastremskiy to the packet sniffer. The files include a series of "chat logs," or recorded Internet conversations, between the defendant and Yastremskiy. In those chat logs, the defendant takes credit for supplying the packet sniffer used for the Dave & Buster's intrusion. The computer files also include an exact copy of the packet sniffer.

at this time whether these individuals will agree to travel to the United States for trial in this case, or even to be deposed, here or in their home nations. In any case, the government submits that their testimony is not required for admission of the Foreign Computer Evidence.

III. Acquisition of the Foreign Computer Evidence

A. The Latvian Server

1. Identification of the Server

On May 7, 2008, United States Secret Service ("USSS") agents arrested an accomplice of the defendant who is now cooperating with the government and is expected to be a witness at the defendant's trial ("CW 1"). USSS agents, when they arrested CW 1, found a laptop computer which was logged in to the internet protocol ("IP") address 195.3.144.9.

CW 1 explained that he and the defendant, along with others, used the computer server with this IP address to mask their criminal activities, which included hacking into commercial computer networks to steal financial data, especially credit card numbers. CW 1 said that he and the defendant, along with others, used the server as a platform to hack into other computers, and as a storage space for stolen financial data. CW 1 said that he had configured this computer server for the defendant, and that only he and the defendant had "root,"² or complete, access to the server. CW 1 said that the server contained encrypted containers, and provided USSS agents with the pass phrase for the containers.

USSS agents, using a publicly available registry maintained by the RIPE National Coordination Centre,³ determined that the IP address 195.3.144.9 was allocated to an Internet Service Provider ("ISP") in Riga, Latvia called Cronos IT.

2. Imaging, Disassembling and Transfer of the Latvian Server

The USSS, which has agents stationed in Latvia, initially asked the Latvian State Police ("LSP") to obtain a

² On many computer operating systems, the "root" is a special user account used for system administration. That user, or root, has all rights and permissions to all files and programs.

³ RIPE is one of five Regional Internet Registries worldwide, and the one responsible for the allocation and assignment of IP address space in Western Europe, the Middle East and Central Asia.

computer image of the Latvian Server. The LSP contacted Cronos IT, where an employee, Ivar Tenters, made an image of the Latvian Server (the "Latvian Image") and gave it to the LSP. On May 14, 2008, the LSP gave the Latvian Image to a USSS agent who personally brought it back to the United States. On June 10, 2008, that same USSS agent made an exact copy of the Latvian Image, using Forensic Toolkit⁴ software, and provided it for analysis to forensic examiners with the Computer Emergency Response Team ("CERT") at Carnegie Mellon University.

Meanwhile, on June 6, 2008, the government submitted a Mutual Legal Assistance Treaty ("MLAT") request for the Latvian Server itself. Tenters, in response to the MLAT request, disassembled the Latvian Server. On September 25, 2008, the Prosecutor General's Office of Latvia provided it to U.S. prosecutors.

Ultimately, the Latvian Server was provided to CERT for comparison with the Latvian Image. The purpose was to determine whether the server had been altered between May 2008, when the Latvian Image was made (and just days after the arrest of the defendant and his associates), and September 2008, when the server was disassembled for provision to the United States government pursuant to its MLAT request.

3. Distinctive Characteristics of the Latvian Server

Inspection and analysis of the Latvian Server and the Latvian Image by CERT forensic examiners has revealed the following:

- the Latvian Server and the Latvian Image are substantially identical - (i) the two crypts, which contain all of the actual files which the government intends to use at trial, are identical on the Latvian Server and the Latvian Image; and (ii) even the partitioned disk space (which contains all of the filesystem volumes) is identical on the Latvian Server and the Latvian Image;⁵ this indicates the Latvian Server was not

⁴ Forensic Toolkit, or FTK, is a commercial software program used by law enforcement agencies and others for the duplication and analysis of computer data.

⁵ The only variation which CERT examiners found on the Latvian Image was the presence of some text strings in spare disk space outside the crypts and the partitioned disk space. These

modified between May and September 2008, when it was provided to the United States government;

- data on the Latvian Server⁶ confirms that it in fact hosted IP address 195.3.144.9, the address provided by CW 1 to USSS agents, and the address specified in the government's MLAT request;
- none of the content in the computer files on the Latvian Server was altered after May 6, 2008, one day before the arrest of CW 1, and two days before the arrest of the defendant, the only two individuals with root access to the Latvian Server;
- CERT examiners successfully opened the two crypts on the Latvian Server using the password provided by CW 1; according to the examiners, the encryption software on the Latvian Server, "BestCrypt," is extremely effective, and, especially in light of the length and complexity of the password, there is no real possibility that they accidentally or fortuitously unlocked the crypts.

B. Yastremskiy's Laptop Computer

1. Seizure and Imaging of the Computer

The Turkish National Police (the "TNP") arrested Yastremskiy on July 26, 2007 pursuant to a provisional arrest warrant issued in the Southern District of California charging him with the distribution of stolen credit card numbers.⁷ USSS

strings were the sort associated with a signature or metadata created by the manufacturer or by a disk controller. CERT examiners say that this could occur if there was preexisting data on the disk used for the Latvian Image, but it does not alter their opinion that the Latvian Server and the Latvian Image are otherwise identical.

⁶ The remaining distinctive characteristics are present, in identical form, on both the Latvian Server and the Latvian Image. Consequently, the government will refer solely to the Latvian Server.

⁷ The Turkish government ultimately lodged its own charges against Yastremskiy. He was tried and convicted in Turkey, and

agents accompanied the TNP to the arrest site, a hotel near Antalya, Turkey. On July 25, prior to the arrest, while Yastremskiy was out, the TNP seized a Lamborghini laptop computer with a Cyrillic/English keyboard from Yastremskiy's hotel room (the "Yastremskiy Laptop"). USSS agents, who were waiting across the hall, took photographs of the Yastremskiy Laptop, including one of the logon screen which displayed the name "Mars."

On July 30, 2007, the TNP provided USSS agents with a computer image, or copy, of the data in the Yastremskiy Laptop. According to the TNP, a trained forensic examiner, Deputy Inspector Baris Hizir of their Ankara office, made the image (hereinafter the "Yastremskiy Image").

2. Distinctive Characteristics of the Yastremskiy Image

Inspection and analysis of the Yastremskiy Image by USSS forensic examiners has revealed the following:

- the image was created on July 30, 2007;
- none of the content⁸ in the computer files was altered between July 25 and July 30, 2007;
- the image bears the same logon screen, displaying the name "Mars," as the Yastremskiy Laptop had on July 25;

In addition, the Yastremskiy Image contains thousands of chat logs, including the following:

- conversations between Yastremskiy and the defendant; identical chat logs were found on a laptop computer seized from the defendant when a search warrant was executed at his residence in Florida on May 7, 2008;
- conversations between Yastremskiy and an undercover USSS agent; copies of these chat logs

on January 8, 2009, was sentenced to 30 years imprisonment there. An extradition request is pending with the Turkish government in connection with both this indictment and the case in the Southern District of California.

⁸ The dates on some files had changed, indicating that the files were opened for viewing, but not altered.

on the agent's computer are identical to those found on the Yastremskiy Image;

Finally, the Yastremskiy Image is substantially similar to a computer image which USSS agents made of the Yastremskiy Laptop on June 14, 2006 in Dubai, United American Emirates ("UAE"), as part of a sneak-and-peek search conducted with UAE authorities (the "Dubai Image"):

- the chat logs on the Yastremskiy Image dated June 14, 2006 and earlier are identical to those on the Dubai Image;
- the Yastremskiy Image and the Dubai Image both contain a PGP⁹ encrypted container with the file name "New PGP Disk1.pgd"; the same seventeen-character pass phrase opens both containers, which share much of the same content;
- the Dubai Image also has the "Mars" logon screen.

ARGUMENT

I. Legal Standards

A. General Standards for Authentication

Rule 901(a) of the Federal Rules of Evidence states that "[t]he requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." This standard "is satisfied 'if sufficient proof has been introduced so that a reasonable juror could find in favor of authenticity or identification.'" United States v. Dhinsa, 243 F.3d 635, 658 (2d Cir. 2001) (quoting United States v. Ruggiero, 928 F.2d 1289, 1303 (2d Cir. 1991)). Thus, while "[a] trial court has broad discretion to determine whether a piece of evidence has been properly authenticated," United States v. Tropeano, 252 F.3d 653, 661 (2d Cir. 2001), it should not exclude evidence on authentication grounds unless it finds that "no rational juror could have concluded" that the evidence is what its proponent claims. Ricketts v. City of Hartford, 74 F.3d 1397, 1411 (2d Cir. 1996).

⁹ PGP, which stands for "Pretty Good Privacy," is a type of computer encryption. A PGP encrypted container is a user-created file that can only be opened with a pass phrase. Otherwise, its contents are completely encrypted.

The Second Circuit has observed that “[t]he bar for authentication of evidence is not particularly high.” United States v. Gagliardi, 506 F.3d 140, 151 (2d Cir. 2007). The proponent of the evidence is not required “to rule out all possibilities inconsistent with authenticity, or to prove beyond any doubt that the evidence is what it purports to be” United States v. Holmquist, 36 F.3d 154, 168 (1st Cir. 1994). The proponent must merely provide “a rational basis from which the jury may conclude” that the evidence is what its proponent claims. United States v. Natale, 526 F.2d 1160, 1173 (2d Cir. 1975). “[T]he standard for authentication, and hence for admissibility, is one of reasonable likelihood.” Holmquist, 36 F.3d at 168. Put another way, authenticity may be proved by a preponderance of the evidence. United States v. Gelzer, 50 F.3d 1133, 1140-41 (2d Cir. 1995).

Moreover, the Court, in ruling on admissibility, may consider evidence which would not be admissible at trial, such as hearsay. See Fed. R. Evid. 104(a). Similarly, the Court may consider as evidence of authenticity the fact that materials were provided in response to a formal MLAT request. See United States v. Rommy, 506 F.3d 108, 138 (2d Cir. 2007) (admitting wiretap transcript provided pursuant to MLAT request, even though transcriber had no specific recollection of preparing it).

Of course, meeting the standard for authentication merely makes evidence admissible (assuming all other conditions precedent are met); the question of the reliability of the evidence, and thus the weight that should be given to it, is left for the jury. See Tropeano, 252 F.3d at 661.

B. Authentication by Distinctive Characteristics

The Federal Rules of Evidence provide a non-exhaustive list of methods by which a piece of evidence can be properly authenticated. These include a demonstration that the exhibit’s “[a]pppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances,” indicate that the exhibit is what it is claimed to be. Fed. R. Evid. 901(b)(4).

Authentication by distinctive characteristics is a well-established method. See United States v. Maldonado-Rivera, 922 F.2d 934, 957-58 (2d Cir. 1990) (admitting gang communique which bore gang’s logo and included non-public details of robbery known only to co-conspirators); United States v. Bagaric, 706 F.2d 42, 67 (2d Cir. 1983), abrogated on other grounds by National Organization for Women, Inc. v. Scheidler, 510 U.S. 249, 259-60 (1994) (admitting letter mailed from Defendant A’s

residence to Defendant B which referenced mutual acquaintances and discussed circumstances of Defendant A in the first person because this provided "ample demonstration" that it was a letter from Defendant A to Defendant B); United States v. Mangan, 575 F.2d 32, 41-42 (2d Cir. 1978) (admitting as handwriting exemplars tax returns which bore signatures similar to those of defendant on file with Internal Revenue Service and were filled out with block capitals similar to those on forms in his personnel files); United States v. Campbell, 1996 U.S. App. LEXIS 12141, **14-15 (9th Cir. May 9, 1996) (admitting recording based on clarity of defendant's voice, content of the recording, and substantial evidence that tape was not altered, despite break in chain-of-custody); United States v. Bello-Perez, 977 F.2d 664, 671-72 (1st Cir. 1992) (admitting handwritten letter because (i) sender's name was similar to defendant's, (ii) letter came from prison where defendant was incarcerated, (iii) letter contained statements about defendant's circumstances, and (iv) sender identified himself as Hispanic and defendant was only Hispanic prison inmate known to addressee - despite the fact the letter was not in defendant's handwriting); United States v. Newton, 891 F.2d 944, 947 (1st Cir. 1989) (admitting letter based on internal references to defendant, including (i) request that in event of the writer's death his assets be split with defendant's wife, (ii) statement that "my lawyer knows me as [alias used by defendant]," and (iii) bank account numbers written next to known aliases of the defendant).

II. Distinctive Characteristics, in Conjunction with Circumstances, Prove that the Latvian Server is the Server Identified by CW 1 and Used by the Defendant

First, the Latvian Server is identical to the Latvian Image in all important respects. This is significant because the Latvian Image was made just days after the defendant and his accomplices were arrested. This distinctive characteristic indicates that the Latvian Server was not modified after the Latvian Image was made.

Second, data on the Latvian Server reflects the same IP address which CW 1 provided to USSS agents and which was later included in the government's MLAT request. This distinctive and absolutely unique characteristic - an IP address can be associated with only one computer at a time - confirms that the Latvian Server is in fact the same server which CW 1 will testify he configured for, and to which he shared root access with, the defendant.

Third, none of the files on the Latvian Server were altered after May 6, 2008, a date prior to the arrests of both

the defendant and CW 1, and prior to USSS agents' request for production of the Latvian Image. This distinctive characteristic proves that no one at Cronos IT or with the LSP modified the files before the Latvian Server was provided to the United States government.

Fourth, the password provided by CW 1 opens the crypts on the Latvian Server which contain both a modified copy of the sniffer used in the Dave & Buster's intrusion and millions of stolen credit card numbers. This distinctive characteristic is further proof that the Latvian Server is what it purports to be - the server which CW 1 will testify he set up for the defendant. This also indicates that no one but CW 1, or someone else with the password - not even the employees of Cronos IT - could have opened or altered the contents of the crypts, which contain all of the specific files relating to the defendant and the sniffer.

Fifth, the LSP told the USSS that Ivar Tenters, a Cronos IT employee, made the Latvian Image and ultimately disassembled the Latvian Server before providing it to the LSP in response to the MLAT request. While this is hearsay, the government submits that the Court may and should consider it in ruling on the admissibility of the Latvian Server. The Court also may and should consider the fact that the server was ultimately provided by the Latvian government pursuant to an MLAT request, which is itself evidence of authenticity.

In sum, the government submits that the distinctive characteristics described above, in conjunction with circumstances, provide ample evidence that the Latvian Server is what it purports to be - a computer server which CW 1 will testify that he and the defendant used as a hacking platform and a storage facility for hacking programs and stolen credit card data. The government therefore urges the Court to issue an in limine ruling admitting the Latvian Server into evidence at trial.

III. Distinctive Characteristics, in Conjunction with Circumstances, Prove that the Yastremskiy Image is an Exact Copy of the Yastremskiy Laptop

First, USSS agents were present when Yastremskiy was arrested and the Yastremskiy Laptop seized; they saw the computer. TNP officers immediately brought the Yastremskiy Laptop to the hotel room where USSS agents were waiting. USSS agents photographed the Yastremskiy Laptop logon screen, which displayed the name "Mars." The Yastremskiy Image has an identical logon screen.

Second, forensic examination of the Yastremskiy Image shows that none of its files were altered between seizure of the Yastremskiy Laptop on July 25, 2007 and provision of the Yastremskiy Image to USSS agents on July 30. Moreover, the Yastremskiy Image was made on July 30, the same day it was turned over to the USSS. These distinctive characteristics indicate that the TNP did not modify the hard drive of the Yastremskiy Laptop before making the Yastremskiy Image, or attempt to modify the image itself after making it.

Third, the Yastremskiy Image is substantially similar to the Dubai Image, an image which USSS agents themselves made of the Yastremskiy Laptop. The same pass phrase, seventeen characters long, unlocks the PGP encrypted containers, both named "New PGP Disk1.pgd" and with very similar content, found on the Yastremskiy and the Dubai Images. The chat logs on the Yastremskiy Image from prior to June 14, 2006, when the Dubai Image was made, are identical to those on the Dubai Image. Finally, the Dubai Image has a logon screen - displaying the name "Mars" - which is identical to the Yastremskiy Image and the Yastremskiy Laptop. These distinctive characteristics provide further evidence that the Yastremskiy Image is an exact copy of the Yastremskiy Laptop.

Fourth, the Yastremskiy Image contains chat logs which are identical to those on the defendant's own laptop computer, seized on May 7, 2008, and the laptop of an undercover Secret Service agent who was corresponding with Yastremskiy prior to his arrest. These distinctive characteristics indicate not only that the Yastremskiy Laptop was used by Yastremskiy, but that the Yastremskiy Image is a duplicate of the Yastremskiy Laptop.

Finally, the TNP has described for the government how the Yastremskiy Image was made. The TNP has provided the name of the individual, Inspector Baris Hizir, who made it, and has indicated that he is a trained forensic examiner. While this is hearsay, the Court may and should consider this in ruling on the admissibility of the Yastremskiy Image.

In sum, the government submits that the distinctive characteristics described above, in conjunction with circumstances, provide ample evidence that the Yastremskiy Image is what it purports to be - an exact copy of a laptop computer used by Yastremskiy. The government therefore urges the Court to issue an in limine ruling admitting the Yastremskiy Image into evidence at trial.

CONCLUSION

Wherefore, the government moves the Court to find that distinctive characteristics, in conjunction with circumstances, provide sufficient evidence of authentication to admit the Latvian Server and the Yastremskiy Image into evidence at trial.

Respectfully submitted,

/S/ Kimberly Kiefer Peretti
Kimberly Kiefer Peretti
Trial Attorney
United States Department of Justice
(202) 353-4249

William P. Campos
Assistant United States Attorney
Eastern District of New York
(631) 715-7837

Evan C. Williams
Trial Attorney
United States Department of Justice
(202) 307-0135

cc: René Palomino, Jr., Esq.