Chief Judge Coughenour

CERTIFICATE OF SERVICE
I certify that a copy of the foregoing document to which this certificate is attached was served on the attorney(s) of record for defendant(s) via ~~telefax/mail~~/personal delivery on the 13th day of September, 2001.

UNITED STATES ATTORNEY
by S. North

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff,

v.

VASILIY VYACHESLAVOVICH GORSHKOV, a/k/a VASSILI GORCHKOV, a/k/a "kvakin."

Defendant

NO. CR00-550C

GOVERNMENT'S TRIAL BRIEF

Comes now the United States of America, by Francis J Diskin, United States Attorney, and Stephen C. Schroeder and Floyd G. Short, Assistant United States Attorney for the Western District of Washington, and files this Government's Trial Brief.

I. SUMMARY OF THE CASE

This defendant, VASILIY GORSHKOV, together with his coconspirator, ALEXEY IVANOV, were arrested in Seattle on November 10, 2000, and, on November 16, 2000, GORSHKOV was indicted in a one-count Indictment charging him with conspiracy. On April 5, 2001, a Superseding Indictment was returned charging him and IVANOV with conspiracy and nineteen substantive counts of violations of the Computer Fraud and Abuse Act and the wire fraud statute. Trial is set on the Superseding Indictment before the Honorable John C. Coughenour and a jury on September 17, 2001.

II. SUMMARY OF FACTS

Following an extensive, national investigation of a series of computer hacker intrusions into the computer systems of businesses in the United States emanating from Russia, ALEXEY IVANOV was identified as one of the intruders. Beginning in June of 2000, e-mail and telephone communication with IVANOV was initiated by the FBI, pursuant to an undercover lure. Early on in that communication, IVANOV identified VASILIY GORSHKOV as his "business partner." In the course of e-mail correspondence, IVANOV and GORSHKOV agreed to travel to Seattle, Washington, to meet with personnel of a computer security company named "Invita." Also as part of the events leading up to that travel, GORSHKOV and IVANOV offered to demonstrate their hacking skills on Invita's own computers. A network was set up for that purpose by Sytex, and the defendants successfully hacked into it. The results of that hack will be adduced at trial to establish the *modus operandi* of the defendants, as the same hacker tools, exploits, and other indicia were found on the tech.net.ru computers, as well as on the servers of other systems into which they intruded.

On November 10, 2000, defendant GORSHKOV[1] together with his co-defendant, IVANOV, flew into SeaTac Airport from Russia. After arriving in Seattle, IVANOV and GORSHKOV were taken to an Invita office site in Seattle, where a meeting of several hours' duration took place. Because IVANOV and GORSHKOV believed that they were meeting with personnel of Invita who were prospective partners in the business of illegally exploiting security flaws in corporate computer networks in the United States, they were asked to demonstrate their ability to hack into computer systems in the United States. Both defendants sat down at computers that belonged to Invita and were located in the office they were visiting, and they logged on to servers that they controlled in Russia. Their activities were recorded by the FBI through a computer program that generated a log of their key strokes. Among the things that GORSHKOV did with the computer during the meeting was to download a network scanning

[1] The spelling "GORSHKOV" is used throughout this memorandum. Phonetic translations of Russian names written in the Cyrillic alphabet are often written in variant ways. The spelling used is that preferred by GORSHKOV's counsel and is taken from the United States visa issued to the defendant.

program from his computer in Russia and use it to scan the entire local area network of computers located in the buildıng where the small Invıta office was located. Indeed, he informed the agents that he had conducted the scan immediately after he dıd it.

Unbeknownst to the defendants, their prospective partners in crime were really Special Agents of the FBI. After the two-hour meeting at the Invita office, the defendants were arrested pursuant to warrants issued by the United States Distnct Court for the District of Connecticut. IVANOV was arrested on an Indictment in that District, while GORSHKOV was arrested pursuant to a Matenal Wıtness Warrant. Subsequently, GORSHKOV was ındicted in this District on November 16, 2000, and was detained pending trial. On April 5, 2001, the twenty-count Superseding Indictment was returned, charging both GORSHKOV and IVANOV with conspıracy, computer intrusions, and fraud.

III. DETAILED FACTS

The Internet is a computer network that is global in scale and knows no international borders. Indıviduals can, utilizing the Internet, communicate by using, among other things, electronıc maıl ("e-mail") or chat rooms; transfer files or documents from one computer to another on the Internet utilizing the File Transfer Protocol ("FTP"), and can access and remotely take control of another computer from their computer through the Internet using vanous hackıng tools. Likewıse, a user located in one country can remotely access a computer located in another country in order to store, retneve or alter files.

The individual or organization having authonzed access to an ISP or computer on the Internet will be gıven a password and user name that authorizes their use of the ISP's services and access to the Internet. Passwords that enable a system administrator to access and control a computer system or server using Unix or comparable operating software are known as "root" passwords. Passwords that enable a system administrator to access control of a computer system or server using Windows NT or comparable operating software are known as administrator passwords. Root or admınıstrator access enables a user to read, write and execute any file on the system.

Beginning in the fall of 1999, a number of Internet-related businesses in the United States suffered computer intrusions or "hacks" that originated from Russia. The hackers gained control of the victims' computers, copied and stole private data that included credit card information, and threatened to publish or use the stolen credit cards or inflict damage on the compromised computers unless the victim paid money or gave the hacker a job.

Attack on Speakeasy Network

One of these victims was an Internet Service Provider ("ISP") named Speakeasy Network, located in Seattle, Washington. Speakeasy's computer network was attacked from Russian Internet Protocol ("IP") addresses at the end of November 1999. The hacker was able to compromise the system administrator's account – the account known as "root" or the "superuser" – on several Speakeasy computers. The hacker then issued a message to everyone who was logged into that computer that he wanted to "chat" about Speakeasy's computer network security using a program called Internet Relay Chat ("IRC"), which allows real-time written communication via the Internet. The hacker identified himself with the computer "nick" or nickname, "_subb_".

On November 30, 1999, a Speakeasy employee named Max Chandler engaged in an IRC chat session with "_subb_", who identified himself as ALEXEY IVANOV (the charged co-defendant of defendant VASILIY GORSHKOV), a/k/a "subbsta". During the chat session, IVANOV transmitted to the Speakeasy employee, via IRC, an electronic copy of his resume and graphics files containing photographs of himself. Also during the chat session, IVANOV stated that he had found holes in Speakeasy's network security, that he wanted a job and $1,000 - $1,500 per month, and that he would not tell Speakeasy about the security holes until he got a job. IVANOV acknowledged that he lived in Chelyabinsk, Russia, and bragged that Speakeasy could never put him in jail for his activity. IVANOV stated that he had 2000 user passwords from Speakeasy, as well as credit cards. The Speakeasy employee told IVANOV that they would not pay him, but tried not to anger him, for fear that he would cause damage to their systems.

After a brief hiatus, IVANOV again contacted Speakeasy, just before Christmas Eve of 1999. He again demanded a job and money, stating that it would be better for Speakeasy to give him a job than for Speakeasy to get hacked, have all of its files deleted, and have its customers' credit cards used. He demonstrated that he had credit card information by posting it on a web site that Speakeasy hosted. Speakeasy still refused to pay any money to IVANOV or give him a job. IVANOV and/or his coconspirators then deleted files on one of Speakeasy's main computers and on one of its customer's computers. In addition, a few months later, a customer of Speakeasy named BP Radio learned that credit card information from its customers had been posted on a Russian web site. Speakeasy lost BP radio's business as a result.

Attacks on Additional Victims

Also in the fall of 1999, several other ISPs – including Verio, which is headquartered in Englewood, Colorado; Lightrealm (now known as Hostpro) in Kirkland, Washington; and CTS, in San Diego, California – had their computers hacked from Russia by the conspirators. Some of the ISPs, including Lightrealm and CTS, gave IVANOV an account on their systems and even made payments to him by transferring funds to Russia. One of Lightrealm's clients, then named Supplement Outlet, discovered that credit card information of its customers had been taken from Lightrealm and posted on the Internet. A similar computer attack was made on an online credit card processing company named OIB, located in Vernon, Connecticut. IVANOV, as he did in the case of Speakeasy, identified himself to OIB as the hacker of its computers and demanded money.

In the year 2000, attacks from Russia on computer systems in the United States continued to occur. In April, Nara Bank, a Korean bank located in Los Angeles, suffered an attack, including an extortion e-mail, although bank personnel were not aware of the full extent of the attack at the time. In August, a bank in Waco, Texas, named Central National Bank (CNB) - Waco, suffered a similar attack, but did not become aware of it until much later. The conspirators also compromised the computer network of the St. Clair County Intermediate School District in Michigan, using it for several nefarious purposes.

The Invita Undercover Operation

The FBI, through its field offices in Seattle and Hartford, established an undercover operation to lure IVANOV to the United States for prosecution. Having identified IVANOV through his resume, the FBI sent him an e-mail soliciting him for employment with "Invita," a computer network security start-up company located in Seattle. On July 1, 2000, IVANOV responded that he and his business partner, defendant VASILIY GORSHKOV, were interested in a consulting business or partnership. He suggested that further e-mails be sent to him at ctsavi@cts.com (his account at CTS) or to GORSHKOV at kvakin@tech.net.ru.

In the course of e-mail correspondence with Invita, IVANOV and GORSHKOV agreed to travel to Seattle and meet with Invita personnel in Seattle. The FBI placed two undercover phone calls to Russia, speaking to GORSHKOV in the first one and IVANOV in the second one. Also as part of the events leading up to their travel to Seattle, the conspirators GORSHKOV and IVANOV offered to demonstrate their hacking skills on Invita's own computers. A network was set up for that purpose for the FBI by a company called Sytex, and they successfully hacked into it.

On November 10, 2000, the FBI's undercover operation culminated with the arrival of GORSHKOV and IVANOV at SeaTac Airport. They were escorted to an Invita office site in Seattle, where a meeting of several hours' duration took place. In the office, both defendants sat down at computers that belonged to Invita and their computer activity was recorded by the FBI through a computer program that logged their keystrokes. IVANOV also had his own Toshiba laptop computer, which he connected to the local network at the office and used.

During the undercover meeting, which was recorded on video and audio tape, GORSHKOV used the Invita computer to log into his account ("kvakin") on the Russian computer named "tech.net ru" and then into his account (again, "kvakin") on the networked computer named "freebsd.tech.net.ru". From his account, GORSHKOV obtained a scanner program called "lomscan", transferred it over the Internet, and then used it to scan the entire local area network of computers located in the building where the small Invita office was located. Indeed, he ınformed the agents that he had conducted the scan immediately after he dıd it.

During the Invıta office meeting, GORSHKOV described Tech.Net.Ru as having about 15-20 employees, of whom about four were hackers. He descrıbed how they wrote hacking tools. He spoke extensively about hacking computers and trying to obtain money from the companies whose computers they hacked, with occasional success. He specifically described a hack into Webcom.com, which ıs now a Verıo company, and he mentioned that they had taken control of some banks. He also admıtted that the CTS account was obtaıned with a stolen credit card, "for hacking purposes."

GORSHKOV also made a number of statements about how they could break or hack into systems from Russia, where they are "invisible" and do not worry about the FBI. Similarly, when the undercover Special Agent asked about whether they were getting access to credıt cards, GORSHKOV said, "we'll never, when we're here, we'll never say that we got access to credıt card numbers," and laughed. He added, "The fact is that, that this kind of questıon ıs better dıscussed in Russia," and laughed again.

After the two-hour meeting at the Invita office, IVANOV and GORSHKOV were arrested. GORSHKOV was ınterviewed on that evening, and again the next day, after being advısed of his rights ın Englısh and Russian. Among other things, he admitted that he ıs "kvakin" on the Internet, that he is the manager of tech.net.ru, that there are five computers in the business, and that he has about five programmers or hackers working for him. He said that IVANOV or "subbsta" was his business partner and that he had first met IVANOV about a year or 18 months earlıer. He refused to name his other partners because he did not want them to get into trouble. With respect to hıs computer programmıng skills, GORSHKOV said that he was able to change or modify any computer program, in almost any language, but could not write complete programs himself. He admitted that he had analyzed the computer systems of Invita for security holes, but claimed that he had never trıed to hack into any U.S. computers. In the November 11 interview, he also stated that almost everything he said at the Invita meeting was a lie.

Evidence from the Russian computers tech.net.ru and freebsd.tech.net.ru

From November 14 through November 20, 2000, Special Agents of the FBI, with the assistance of a computer security professional from the University of Washington, connected to the two Russian computers named "tech.net.ru" and "freebsd.tech.net.ru". They successfully logged on to the computers by using the user name of "kvakin" and the password that GORSHKOV had used during the Invita undercover meeting, as that information was recorded by the keystroking software. With GORSHKOV's user name and password, the agents were able to access a large amount of data on the computers, including the home account of kvakin on both computers. The agents also accessed the account of subbsta (IVANOV) on tech.net.ru by using the password that IVANOV provided to them during his post-arrest interview, but they were not able to access his account on freebsd.tech.net.ru.

The agents copied a portion of the enormous amount of data that was located on the Russian computers and downloaded the copied data to a computer located at the Seattle FBI office, planning to seek and obtain a search warrant before searching the contents of the download. The downloaded data was not viewed until after the search warrant was obtained on December 1, 2000. It was examined with the help of experts, including Mr. Philip Attfield.

The quantity of data obtained by the FBI is immense. In their personal accounts on the computers, GORSHKOV and IVANOV had numerous computer hacking tools, *i.e.*, programs or "scripts" and computer code that are used to compromise or gain control of computers and computer networks in a variety of ways. Among other things, the tools will scan computers and networks for vulnerabilities, exploit those vulnerabilities to obtain users' passwords and to gain complete control of the computers, decipher or crack encrypted or encoded passwords, and convert the compromised systems into relays or "proxies" that allow the hacker to mask his identity on the Internet. Many of these tools also were found on IVANOV's Toshiba laptop computer.

The Paypal Fraud

An additional number of other computer programs or "scripts" located in kvakin's home accounts implemented a fraud scheme against the online auction company E-Bay and the online credit card payment company PayPal. E-Bay has a website on which users can auction items off to other users. Payment can be accomplished by credit card through online accounts at PayPal that are opened with an e-mail address and a credit card. GORSHKOV's scripts generated thousands of false e-mail addresses, at web sites offering free e-mail accounts, opened corresponding accounts at PayPal with stolen credit cards, generated fraudulent or "virtual" auctions at E-Bay, and initiated payments from one PayPal account to another using the stolen credit cards.

In fact, in July 2000, John Kothanek, Senior Security Investigator for PayPal, learned that an unknown individual was sending e-mail messages to Paypal.com customers stating that they had received a bonus from Paypal.com and requesting that they log onto the site listed in the email in order to receive the bonus. When customers logged onto the specific website, they were asked to input their user names and passwords. Once the information was entered, the website informed them that there had been a computer problem and asked them to please enter the information again.

The website customers were asked to log onto what seems to be a fake or mirrored Paypal.com site, named paypai.com, used to capture the required information from the customer. When customers were asked to re-enter their information, the first website redirected the customer to the proper Paypal.com website. The customers were unaware that their log on names and passwords had been stolen and could be used to purchase items from the Internet.

Mr. Kothanek identified two IP addresses connected to the fake or mirrored paypal.com website, 216.122.89.110 and 212.57.129.2. The first resolved to www.lightrealm.com, and the second resolved to www.surnet.ru, located in Moscow, Russia. Using those IP addresses as search criteria, PayPal then queried its customer database and identified hundreds of connections to PayPal from those addresses. In addition, by searching on user names and patterns, Mr. Kothanek determined that there had been hundreds of accounts opened at PayPal from several other IP addresses, principally 133.78.216.28, registered to Musashi Technical Institute in Japan; 140.239.225.222, registered to popstick at Harvardnet; 63.70.149.190, registered to the St. Clair County, Michigan, Intermediate School; 202.155.*.*, IP addresses registered to an Internet

Service Provider located in Jakarta, Indonesia; and others. Because most Internet users connect to the Internet via dynamically assigned IP addresses that generally change every time they connect, it was highly unusual to see multiple account openings coming from the same IP address. Additionally, the accounts were opened minutes apart by what seemed to be an automated process. Many of the fraudulent accounts used variants of the names "Greg Stivenson" and "Murat Nasirov."

The Government, after examining the data downloaded from tech.net.ru and freebsd.tech.net.ru, found approximately 56,000 credit card accounts that had been stolen from various online merchants in the United States. Credit card numbers were furnished to PayPal for the purpose of searching the customer database. As a result of that query, PayPal learned that thousands of those stolen credit cards had been used at PayPal by the person or persons who had opened the accounts discussed above. While PayPal managed to block many of the transactions, it has suffered a minimum loss due to the conspirators' activities of approximately $800,000.00 in chargebacks from the card issuing banks.

As noted, the government's technical expert will testify that he found in the tech.net.ru and freebsd.tech.net.ru data, scripts written in PERL (Practical Extraction Report Language) that were designed to automatically open the e-mail accounts (including the Greg Stivenson accounts), and create PayPal accounts with those e-mail addresses and stolen credit card information. In addition, personnel from several of the systems that were identified with the transactions at PayPal – including Lightrealm and the St. Clair County Intermediate School District – will testify that their computers were hacked from IP address 195.128.157.66, registered to tech.net.ru. The intruders took over their systems and used them as proxies to make other connections to the Internet. As to other compromised systems, the government's expert will testify about evidence found on the tech net computers that demonstrates that the other IP addresses registered to the Musashi Technical Institute and others also belonged to systems that the defendants had compromised.

During October 2000, Mr. Kothanek engaged in a series of e-mail communications with "Greg Stivenson" concerning the fraudulent activity at PayPal. In these e-mails, "Stivenson" made a number of statements consistent with the admissions of the defendants during the Invita undercover meeting that they attempted to get the systems administrators at companies that they had hacked into to pay them to reveal their techniques and to refrain from doing further damage. "Stivenson" also admitted to creating the paypai spoofed site and hacking into Nara Bank, and he talked about how he was able to defeat PayPal's security measures.

In the e-mails to Mr. Kothanek, there were several explicit references to PayPal paying "Stivenson." In one message Stivenson asked: "My question is: what do you want from me? I can stop my activities with paypal. I can sell this complete system to third parties. I can help to stop such activities as mine. Best regards." In a message sent to PayPal's CTO (written in Russian), he stated: "Now with regard to questions of security, I can help, but all security questions will be decided not by a mere "thank you," because a "thank you" doesn't put food in your mouth."

These e-mail messages will be offered as conspirator statements made in furtherance of one of the objects of the conspiracy, namely to extort payments from the proprietors of systems that they had hacked.

Further evidence found on the Russian computers demonstrated that the conspirators had solicited sellers of computer parts and other goods, convincing some of these merchants to sell the parts and ship them to Kazakhstan, which is not far from Chelyabinsk. Payment was made to the merchants' PayPal accounts with stolen credit cards.

Other Private Information, Bank Records, and Credit Cards on the Russian Computers

In addition to the hacking tools and the programs and scripts for the PayPal fraud, the tech.net.ru and freebsd.tech.net.ru computers contained a vast amount of private information that had been stolen from victims' computers – including computer users' names and passwords, credit card numbers and associated information, computer network configurations, and bank records. More than 50,000 credit cards were found in the data downloaded from the two Russian computers. The credit card information came from Speakeasy, Lightrealm, CTS, Verio, and many other victims.

Bank account information and other financial records also were found on the two Russian computers. Customers' bank account records had been stolen from CNB-Waco and from Nara Bank. Nara Bank officials discovered that the conspirators accomplished, at least temporarily, actual transfers of funds from some of its customer accounts to PayPal accounts.

Computer data obtained from various victims – including Nara Bank, CNB-Waco, and CTS – confirmed the hacks and matched data downloaded from the two Russian computers. Indeed, IVANOV's account at CTS was itself a huge repository of hackers' tools, scripts, and programs, as well as tens of thousands of stolen credit cards. GORSHKOV had access to that account via scripts that allowed him to log into the account and run the hackers' tools. Hacking tools that were used by IVANOV and GORSHKOV in the test hack of Invita's computers also matched tools on the Russian computers.

In short, the data on tech.net.ru and freebsd.tech.net.ru and elsewhere demonstrates that GORSHKOV (a/k/a kvakin), IVANOV (a/k/a subbsta), and their co-conspirators engaged in numerous computer intrusions, stole credit card information and other sensitive information, and used computer code to conduct a massive fraud involving PayPal.

POTENTIAL LEGAL AND EVIDENTIARY ISSUES

A. Computer-Generated Logs and Other Data.

The Government will offer numerous log files that reflect the output of computer operating systems and other programs. Because those logs are generated by the computer without the intervention of a human agent, they neither contain nor constitute a "statement." Fed. R. Evd. 801(a) provides that "A statement is (1) an oral or written assertion or (2) nonverbal conduct *of a person*, if it is intended *by the person* as an assertion" (emphasis added). Likewise, Fed. R. Evd. 801(b) provides that "A declarant is a *person* who makes a statement." (Emphasis added). Consequently, logs and data that are generated by the computer operating system and other processes without the intervention of a human agent, cannot contain hearsay. Indeed, such data cannot be considered hearsay because the computer that generates is cannot be put on the witness stand to testify and undergo cross-examination. Assuming for purposes of this discussion that they are relevant, the admissibility of computer-generated logs depends only upon proper authentication under Fed. R. Evd. 901:

> (a) General provision. The 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.
>
> (b) Illustrations. By way of illustration only, and not by way of limitation, the following are examples of authentication or identification conforming with the requirements of this rule:
>
> (1) Testimony of witness with knowledge. Testimony that a matter is what it is claimed to be.
>
> * * * *
>
> (4) Distinctive characteristics and the like. Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances.
>
> * * * *
>
> (9) Process or system. Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.

In United States v. Whitaker, 127 F.3d 595, 601 (7th Cir. 1997), the Court held that the government properly laid the foundation for computer records and established their authentication through the testimony of the FBI agent who had retrieved the records from a co-defendant's computer during the execution of a federal search warrant of the co-defendant's home in February 1994. The agent testified that the records were retrieved from the computer using the Microsoft Money program, and that he was present when that program was installed on the computer and when the records were retrieved.

The authenticating witness need not have special qualifications. The witness does not need to have programmed the computer himself, or even need to understand the maintenance and technical operation of the computer. *See, e.g.,* United States v. Whitaker, 127 F.3d 595, 601 (7th Cir. 1997); United States v. Miller, 771 F.2d 1219, 1237 (9th Cir. 1985) (It is not necessary that the computer programmer testify in order to authenticate computer-generated records.); United States v. Moore, 923 F.2d 910, 915 (1st Cir. 1991), and cases cited.

Bald assertions that computerized records are susceptible to alteration or tampering, in the absence of actual evidence that tampering occurred, are not sufficient to prevent the admissibility of those records. In United States v. Whitaker, 127 F.3d 595, 602 (7th Cir. 1997), the Court declined to disturb the trial judge's ruling that computer records were admissible because the defendant's allegation of tampering was speculative and without evidence to support it. *Also see,* United States v. Bonallo, 858 F.2d 1427, 1436 (9th Cir. 1988) ("The fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness.") Such allegations go to the weight, but not the admissibility, of computer records. Id. at 1436.

Nice distinctions between "originals," copies or duplicates are relatively meaningless when it comes to computerized data. Recognizing this fact, Fed. R. Evid. 1001 provides the following applicable definition for computer data:

> "(3) Original. . . . If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'"

Finally, some of the computerized data that will be offered by the government will contain both non-hearsay computer-generated data, and statements of a declarant. For example, E-mail messages contain information in the headers that is computer-generated information, such as the date and time, as well as the E-mail addresses used. The body of the messages, however, contain statements of a person. In many instances, the E-mails contain statements of ALEXEY IVANOV made in furtherance of the objects of the conspiracy, and, thus, are not hearsay. Other such statements will be offered under one of the well-established exceptions to the hearsay rule, such as the business records exception.

B. Courtroom Demonstration. The government's expert, Phil Attfield, will conduct a demonstration in the courtroom in which, utilizing hacker tools found on the defendant's computers in Russia ("fuckIIS" and "msadc"), he will hack into and gain control of one computer from another. He will also demonstrate the program "l0phtcrack," also found on the defendant's computer in Russia, by using it to decrypt an encrypted password that was found in a file on the defendant's computer. The output will be shown to be identical to the output file found on the defendant's computers. Accordmg to the Court's technıcal consultant, ıt may be necessary for Mr. Attfield to leave the witness stand (with the Court's permission) in order to run the demonstration.

C. IP addresses and domain name registratıon. Through the agencies of the Amerıcan Registry of Internet Numbers (ARIN) for North America, South America, the Caribbean, and sub_Saharan Africa; RIPE NCC for Europe, Mıddle East, and parts of Africa; and APNIC for the Asian Pacific region, publically accessible databases are maintained that provide IP registratıon for the world. These databases contaın globally unique numeric identifiers that computers use to identify hosts and networks connected to the Internet, as well as contact informatıon for the system admınıstrator, and other information. IP (Internet Protocol) addresses consıst of four numbers, each smaller than 256, separated by a "." known as a "dot." The registratıon of domain names and IP addresses are maintained in databases that are accessible to the public and are relied upon by the public, as well as computer network professionals, to identıfy the owners of systems. The Government wıll ıntroduce such records pursuant to Fed. R. Evd. 803(17), as "dırectories, or other publıshed compilations, generally used and relied upon by the public or by persons ın particular occupations."

DATED this 13th day of September, 2001.

Respectfully submitted,

FRANCIS J. DISKIN
Unıted States Attorney

STEPHEN C. SCHROEDER
Assistant United States Attorney

FLOYD G. SHORT
Assıstant United States Attorney